centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1107

Procedimiento de Empleo Seguro
One Identity Manager

Febrero de 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: 083-24-095-5.
Fecha de Edición: febrero de 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
2024.03.01 11:17:44 +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. **One Identity Manager es una solución de gobierno y gestión de identidades (IAM)** que permite automatizar la gestión de los accesos de los usuarios, permitiendo que accedan a las aplicaciones y a los datos estrictamente necesarios para desempeñar su trabajo.
2. Además, One Identity Manager (IM):
    a) Ofrece una solución completa para revisiones de usuarios, aplicaciones y acceso a datos.
    b) Gestiona sistemas y aplicaciones SaaS de manera unificada.
    c) Gestiona el riesgo de los empleados basándose en reglas de pertenencia a roles, accesos a aplicaciones o datos, y cualquier otra relación del empleado dentro de los organismos.
    d) Proporciona una interfaz para poder definir políticas organizativas de obligado cumplimiento, y revisar y controlar aquellas excepciones de manera centralizada.
    e) Dispone de paneles de control de gobierno donde los empleados con responsabilidades podrán disponer de métricas reales sobre riesgos, permisos, uso, campañas de certificación, etc.
    f) Permite un modelado de roles de negocio y control de acceso.
    g) Proporciona un portal de autoservicio para el empleado final.
    h) Cuenta con flujos de aprobación para cualquier proceso interno de certificación, solicitud de permisos o accesos, excepciones, etc.
    i) Genera informes de auditoría e histórico de los objetos gestionados.
    j) Gobierno de cuentas privilegiadas, de servicio, cuentas de aplicaciones, sub-identidades, etc.
    k) Cuenta con mecanismos para el cumplimiento de las políticas organizativas.
    l) Es capaz de gobernar los datos no estructurados como sistemas de ficheros, *SharePoint, One Drive*, etc.
3. One Identity Manager está formado por cuatro componentes principales:
    a) El ***Fat Client* (Herramientas Administrativas pesadas)**. Es el componente utilizado para la configuración inicial del producto, ya que este proporciona herramientas de edición y sincronización. Además, el *Fat Client* incluye una aplicación para la parte de administración (*Manager*), pero su interacción se realiza a través del *Web Service*.
    b) El ***Job Service.*** Es el componente que realiza la sincronización y provisión de los datos entre la base de datos y cualquier sistema conectado. También se encarga de extraer los diferentes procesos que se encuentran en la cola y

ejecutarlos. Es el encargado de la realización de actividades en la base de datos.

c) ***Web UI***. Es el componente que implementa la interfaz gráfica, a través de la cual los usuarios pueden acceder a las funciones administrativas del producto, junto con el acceso a la aplicación para el cambio de contraseña (***Password Reset Portal***).

d) ***Web Service.*** Es una REST API que proporciona las mismas funcionalidades que *Web UI*, así como la interfaz que la aplicación *Manager* hace uso para la gestión administrativa y las políticas de contraseñas. Junto con *Web UI* permiten la realización de la gestión del producto, así como la adición de nuevos usuarios y roles.

4. En la siguiente imagen se muestra un esquema con los diferentes componentes del producto:

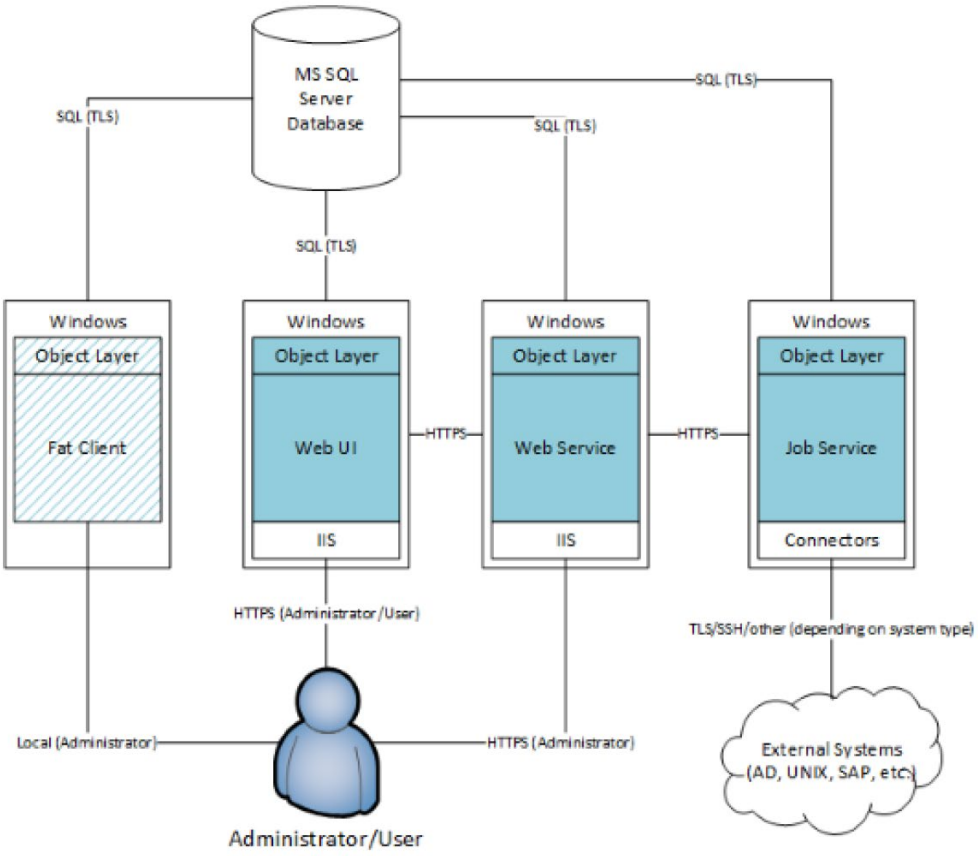

Ilustración 1 – Arquitectura y componentes de One Identity Manager

5. Además, IM proporciona los conectores y todas las plantillas requeridas para la gestión de los siguientes sistemas externos:

- *Active Directory.*
- *UNIX/Linux.*
- *Exchange 2016 y 2019.*

- *SharePoint 2016 y 2019.*
- *Azure AD.*
- *Exchange Online.*
- *SharePoint Online.*
- *Google G-Suite.*
- *LDAP (incluyendo AS/400, RACF, ACF2, Top Secret).*
- *SAP.*

6. One Identity Manager separa estos componentes en una arquitectura de tres (3) capas:
   a) Repositorio Central (Capa de Datos).
   b) *Web* y *Application Server* (Capa de Presentación).
   c) *Provisioning* (*job*) / *Application Server* (Capa de Aplicación).
7. La siguiente imagen resume el concepto y funcionalidades del producto:

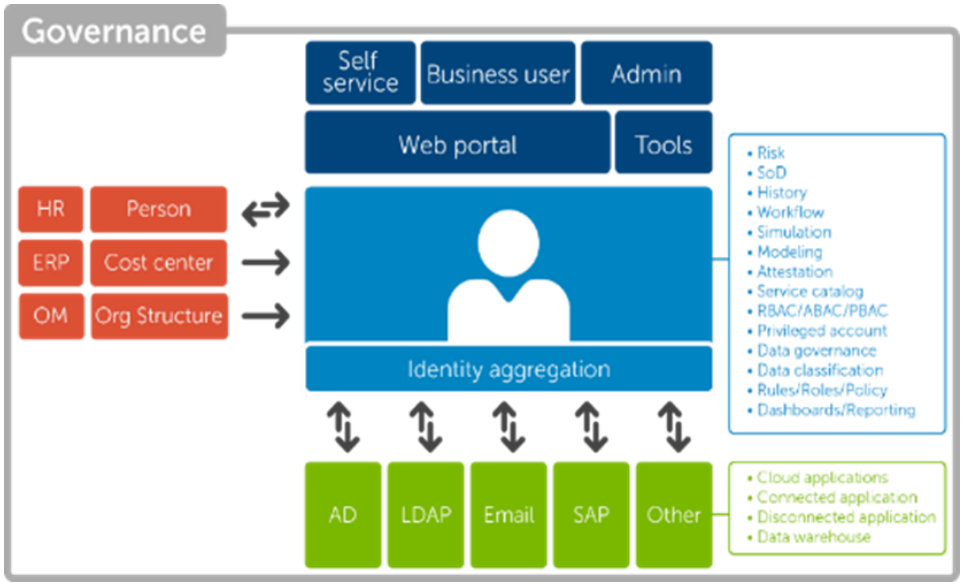

Ilustración 2 – Funcionalidades de *One Identity Manager*

8. Con respecto a la conexión de los usuarios al producto, la administración de One Identity Manager se lleva a cabo mediante consolas GUI, usando HTTPS para conectarse al servidor de aplicación. Los usuarios finales se conectan a One Identity Manager mediante una consola Web usando también HTTPS.

2. OBJETO Y ALCANCE

9. El objeto del presente documento es servir como guía de buenas prácticas de seguridad durante la configuración del producto **One Identity Manager v9.0 LTS**.

10. One Identity Manager se puede desplegar en entornos *on-premise*, cloud públicas o privadas y, además, se ofrece como servicio SaaS. El objeto de este documento es describir las configuraciones de seguridad recomendadas en instalaciones tanto *on-premise* como cloud privadas y públicas. **Se destaca que la cualificación del producto solo abarca su despliegue *on-premise*.** El servicio SaaS ha quedado fuera del alcance de la cualificación por lo que no hay evidencia de la fortaleza de sus mecanismos de seguridad.

11. El repositorio, basado en una base de datos relacional, contiene todos los datos (identidades, estructuras, derechos, recursos, roles, etc.) y configuraciones del sistema (flujos de trabajo, reglas, formularios).

12. Las aplicaciones web proporcionadas, como el portal del usuario final del empleado o las aplicaciones web administrativas, se pueden ejecutar en diferentes servidores de aplicaciones web en entornos distribuidos, como una solución de alta disponibilidad.

13. El servidor de aprovisionamiento procesa la sincronización con los sistemas de origen y destino. Todos los componentes del sistema admiten escalabilidad vertical y horizontal.

14. Los clientes *Fat Client* son utilizados para la administración y configuración de One Identity Manager. Los requisitos *software* para estos clientes de administración son:

    a) Sistema Operativo *Windows 10 (32 bits o 64bits),* versión mínima 1511.

    b) Sistema Operativo *Windows 11* (*64 bits*).

    c) *Microsoft .NET Framework 4.8 o superior*.

    d) Microsoft Edge WebView2

15. Se recuerda que el *software* necesario para la utilización de este producto debe **disponer de soporte de seguridad del fabricante y estar correctamente actualizado y bastionado.**

16. El *software* recomendado para la instalación de los componentes de One Identity Manager es el siguiente:

    a) Sistema Operativo *Windows Server 2022.*

    b) *Microsoft .NET Framework 4.8* o superior.

    c) *Microsoft Internet Information Services (IIS)* 10.0. con, al menos, los siguientes componentes instalados:

        - *Web Server > Common HTTP Features > Static Content*
        - *Web Server > Common HTTP Features > Default Document*

- *Web Server > Application Development > ASP.NET*
- *Web Server > Application Development > .NET Extensibility*
- *Web Server > Application Development > ISAPI Extensions*
- *Web Server > Application Development > ISAPI Filters*
- *Web Server > Security > Basic Authentication*
- *Web Server > Security > Windows Authentication*
- *Web Server > Performance > Static Content Compression*
- *Web Server > Performance > Dynamic Content Compression*

d) Microsoft SQL Server 2019 o superior – SQL Azure Managed Instance.

17. **Se recomienda que cada componente se instale en servidores independientes**.
18. A continuación, se indican los requerimientos mínimos del *hardware* para cada componente de One Identity Manager:

IM Component	Procesador	Memoria	Almacenamiento Disco
SQL Server	8 physical cores 2.5 GHz+	16 GB+ RAM	100 GB
Job Service	8 physical cores 2.5 GHz+	16 GB RAM	40GB
Web UI	4 physical cores 1.65 GHz+	16 GB RAM	40GB
Web Service	8 physical cores 2.5 GHz+	16 GB RAM	40GB
Cliente Pesado Administración	4 physical cores 2.5 GHz+	4 GB+ RAM	1GB

Tabla 1 – Requisitos *hardware* de los componentes de One Identity Manager

3. ORGANIZACIÓN DEL DOCUMENTO

19. El documento se compone de los siguientes apartados:

a) **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

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

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

d) **Apartado 7.** En este apartado se recoge una *checklist* con las tareas a realizar y el estado de cada una de ellas.

e) **Apartado 8.** Incluye las referencias utilizadas en el presente documento.

f) **Apartado 9.** En este apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

20. Para instalar IM es necesario descargar la versión deseada, en este caso la **9.0LTS**, que se encuentra disponible en la web de soporte de One Identity (OIM90.zip).

21. Además, en la web de descarga de IM se puede encontrar el valor del hash, el cual se puede usar para verificar la integridad del fichero descargado mediante el comando *Get-FileHash* en la consola *Powershell*:

```
$ Get-FileHash OIM90.zip | Format-List
```

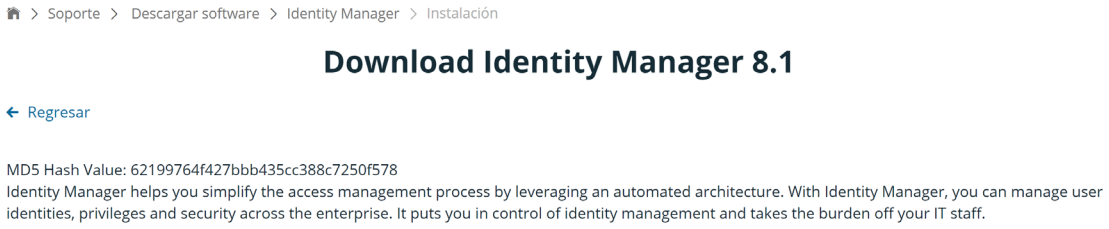

Ilustración 3 – Descarga de software de One Identity Manager

22. Otro paso adicional para verificar la autenticidad del *software* es comprobar el certificado del *autorun.exe*. Para esto, se debe visualizar las propiedades del instalador, *autorun.exe* y verificar la pestaña de firmas digitales. En dicha pestaña se debe **verificar que la empresa firmante es One Identity LLC., y comprobar la validez del certificado.**

4.2 ENTORNO DE INSTALACIÓN SEGURO

23. Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado disponga de autorización para la configuración, despliegue y mantenimiento del producto. Además, se requiere de un control de acceso físico para limitar el personal con acceso físico al producto.

4.3 REGISTRO Y LICENCIAS

24. IM no requiere la activación de licencias para su instalación o uso.

4.4 CONSIDERACIONES PREVIAS

25. IM requiere una serie de requisitos para su instalación y operación, a nivel de cuentas y permisos de usuarios, tanto en los sistemas donde van a desplegarse sus componentes como en los sistemas finales a gestionar.

26. Estos requisitos se encuentran definidos en la guía de instalación de IM [REF1], en el apartado *Installation prerequisites*.

27. **La instalación del SQL Server queda fuera del ámbito de este documento**. Sin embargo, el servidor SQL Server debe cumplir una serie de requisitos, así como contar con usuarios con determinados permisos, descritos en la guía de instalación

de IM [REF1], en el apartado *Installation prerequisites > Minimum system requirements for database server*.

28. Además, IM también requiere de un conjunto de puertos para su conectividad con otros sistemas, como se recoge en la guía de instalación de IM [REF1], en el apartado *Installation prerequisites > Communications ports and firewall configuration*.

29. También **se debe habilitar el modo de operación seguro FIPS**, el cual se encuentra explicado en el apartado 5.1.3 HABILITAR FIPS.

4.5 INSTALACIÓN

30. A continuación, se identificarán los procesos de instalación de los diferentes componentes de One Identity Manager en el siguiente orden:

    - Herramientas administrativas.
    - Base de Datos.
    - Servicio One Identity Manager.
    - Servidor de la aplicación.
    - Portal Web.

4.5.1 HERRAMIENTAS ADMINISTRATIVAS (FAT CLIENTS)

31. Siempre es recomendable comenzar la instalación de One Identity Manager instalando las herramientas y componentes de configuración del producto. Los diferentes requisitos están descritos en el apartado 2. OBJETO Y ALCANCE.

32. A continuación, se indican los pasos a seguir para la instalación de dichas herramientas:

    a) Lanzar el instalador *autorun.exe* desde el directorio raíz del archivo de instalación.

    b) Ir a la pestaña *Installation* y seleccionar la opción *Install*. Esto lanza la interfaz de instalación.

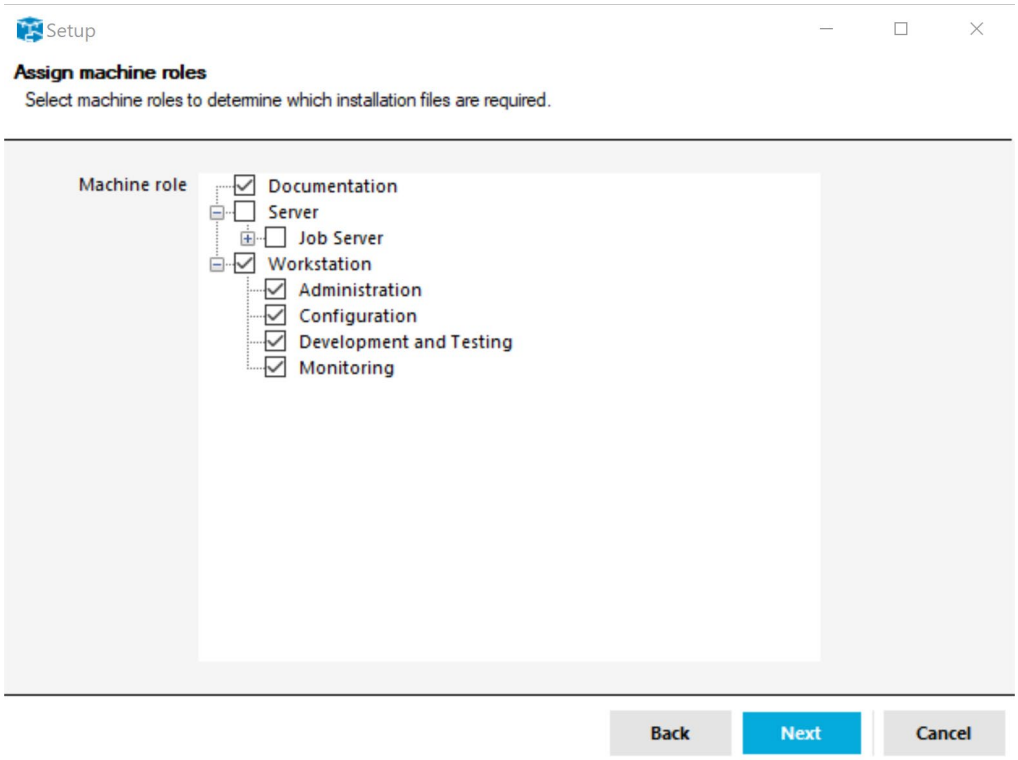

Ilustración 4 – Selección elementos de instalación Herramientas Administrativas de IM

c) Confirmar las condiciones de licencia.

d) En las siguientes páginas, se deberá añadir la información necesaria para su instalación.

33. Para mayor información sobre el proceso de instalación de componentes, se recomienda ir a la guía de instalación de IM [REF1], al apartado *Installing One Identity Manager components*.

4.5.2 BASE DE DATOS

34. Una vez instaladas las herramientas administrativas, se debe crear y configurar la base de datos de One Identity Manager. Es importante notar que la base de datos **no forma parte del producto**, es decir, pertenece al entorno operacional y es responsabilidad del usuario realizar la configuración y gestión necesaria para su correcto uso con el producto.

35. Previamente se ha de asegurar que se cumplen los diferentes requisitos descritos en el apartado 4.4 CONSIDERACIONES PREVIAS y 2. OBJETO Y ALCANCE.

36. Para proceder a la instalación, se ejecuta la herramienta de *Configuration Wizard*, la cual nos permitirá crear una base de datos, así como toda su estructura nueva, o usar una base de datos existente y actualizar su esquema. Además, se recomienda que el *Configuration Wizard* cree la base de datos, así como todos los elementos en el *SQL Server*.

37. Este procedimiento está detallado en la siguiente sección de la guía de instalación de IM [REF1], en el apartado *Installing One Identity Manager > Installing and configuring a One Identity Manager database*.

38. Por otro lado, en entornos de producción, se debe **cifrar la información contenida en la base de datos**. Para ello, se puede definir en One Identity Manager la forma de realizarlo mediante la herramienta de administración *Designer*. Se puede elegir el parámetro de configuración *Common | EncryptionScheme* para definir qué método de cifrado queremos usar:

    a) **RSA**: Cifrado RSA con AES para grandes datos (por defecto).

    b) **FIPS CompliantRSA**: Este método es usado si el cifrado debe cumplir el estándar FIPS 140-2. La política de seguridad local de "***Use FIPS compliant algorithms for encryption, hashing, and signing***" debe estar habilitada.

39. Se recomienda usar claves RSA de longitudes mayores o iguales a **3072 bits**, para proporcionar la seguridad necesaria.

40. El cifrado se lleva a cabo mediante el programa de *Crypto Configuration*. Con este programa un fichero de cifrado es creado, y los contenidos de las columnas de la base de datos que son afectados, son convertidos. Los datos cifrados son almacenados en la tabla "*DialogDatabase*".

41. **Es recomendable realizar una copia de seguridad de la base de datos antes de cifrar los datos**, por si fuese necesario volver al estado previo de la base de datos.

42. Para obtener más información sobre este proceso, se recomienda consultar la guía de instalación de IM [REF1], el apartado *Installing One Identity Manager > Installing and configuring a One Identity Manager database > Encrypting database information.*

4.5.3 SERVICIO ONE IDENTITY MANAGER

43. Una vez desplegada la base de datos, se procede a la instalación del servicio de One Identity Manager (*Job Service*). Es importante notar que se deben cumplir los requerimientos descritos en el apartado 2. OBJETO Y ALCANCE.

44. Este servicio se encarga de conectar One Identity Manager con los sistemas finales y ejecutar todas las tareas relativas a la gestión del ciclo de vida de los objetos en esos sistemas: altas, bajas, modificaciones, etc.

45. La instalación del servicio, se encuentra detallada en profundidad en la guía de instalación de IM [REF1], en el apartado *Installing One Identity Manager > Installing and Configuring the One Identity Manager Service*.

4.5.4 SERVIDOR DE APLICACIÓN

46. El *Application Server* es el componente que proporciona conexión de acceso a la base de datos. Debe de cumplir con los requisitos descritos en el apartado 2. OBJETO Y ALCANCE.

47. Para la instalación de este componente, se debe seguir los pasos descritos en la guía de instalación de IM [REF1] *Installing and updating an application server*.

48. Durante la instalación, a la hora de seleccionar diferentes configuraciones para el servidor, **se debe usar SSL/TLS mediante la opción Enforce SSL**, ya que con esta opción solo se permite el uso de sitios que estén protegidos mediante SSL. Además, con respecto a la autenticación Web, se recomienda seleccionar ***Windows Authentication (Single sign-on).***

49. En la página de configuración del ***Set Session token certificate*****,** se puede definir el certificado para la creación y chequeo de los tokens de sesión. El certificado debe tener, al menos, una longitud de clave de **3072 bits**.

4.5.5 PORTAL WEB

50. El Portal web proporciona una interfaz gráfica a través de la cual, los usuarios pueden acceder a las funciones administrativas del producto, junto con el acceso al *Password Reset Portal*, que permite realizar el cambio de contraseña.

51. El Portal Web además proporciona una interfaz web de auto servicio a los usuarios a través de la cual pueden solicitar acceso a aplicaciones, sistemas o recursos publicados en One Identity Manager.

52. Previo a su instalación, se debe verificar que se cumplen los requisitos descritos en el apartado 2. OBJETO Y ALCANCE. Por otro lado, para su instalación se recomienda seguir los pasos indicados en la guía de instalación IM [REF1], en el apartado *Installing, configuring and maintaining the Web Portal.* En este apartado también se indica cómo se realiza la configuración, actualización y desinstalación del componente.

53. Es importante tener en cuenta que se debe **seleccionar el uso de SSL con la opción *Enforce SSL***, para que solo se permitan usar sitios seguros que hagan uso de SSL para la instalación. Además, al igual que con el servidor de aplicación, se recomienda hacer uso de ***Windows Authentication (Single sign-on)*** para la autenticación Web.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

54. Es importante notar que el producto hace uso de las librerías criptográficas, junto con la implementación de TLS, del sistema operativo (*Microsoft Windows*), para el uso seguro de los protocolos y de las funcionalidades criptográficas necesarias.

55. Estas librerías son ***FIPS-Compliant***, y son las siguientes:

    a) *bcryptprimitives.dll*, con certificado FIPS: *CMVP2937*.

    b) *cng.sys* con certificado FIPS: *CMVP2936*.

56. Los cambios a realizar para el correcto uso de los protocolos y algoritmos criptográficos se han de hacer desde el registro de Windows, ya que, como se ha mencionado anteriormente, el producto hace uso de las librerías del sistema operativo. El enlace recomendado para realizar dicha acción es: https://docs.microsoft.com/es-es/windows-server/security/tls/tls-registry-settings.

57. En el enlace anterior se indica:

    a) Cómo configurar la versión de cliente y servidor TLS a usar, mediante las claves de registro. **Se deberá usar, al menos, TLS 1.2**.

    b) Las *cipher suites* soportadas por cada versión de Windows, en modo *FIPS compliant* o no, y cómo configurar el listado de *cipher suites* a negociar y el orden, mediante directivas de grupo.

    c) A partir de Windows 10 y Windows Server 2016, se añaden claves de registro para especificar:

        i. Tamaño mínimo de clave RSA del cliente TLS para *cipher suites* con RSA como *Key Exchange*. **Se deberán usar claves de, al menos, 3072 bits** de longitud.

        ii. Tamaño mínimo de clave RSA del cliente TLS en *cipher suites* con DH como *Key Exchange*. **Se deberán usar claves de, al menos, 3072 bits** de longitud.

58. Siempre que se seleccione un algoritmo, se deberá hacer uso de longitudes de claves con una **fortaleza de, al menos, 128 bits**.

5.1.1 CONFIGURAR TLS EN SQL SERVER

59. Para configurar el uso de **TLS 1.2** para la conexión de los datos almacenados en la base de datos de IM, es necesario configurar el servidor SQL para forzar las conexiones cifradas como se describe en las secciones *Install on single server*, *Install accross multiple servers* y *Configure server*, del siguiente artículo: *https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017*

5.1.2 HTTPS EN SERVICIOS WEB

60. Tanto el portal web como el portal de aplicación se recomienda que se instalen en servidores IIS que fuercen las conexiones HTTPS. Durante la instalación de estos componentes se especifica la URL del servicio usando HTTPS. No es necesaria ninguna configuración porque HTTPS está habilitado de forma predeterminada durante la instalación.

61. IM proporciona rutas de comunicación confiables mediante HTTPS para administradores remotos que acceden a la interfaz de usuario web. IM requiere que todos los usuarios inicien la comunicación a través de la ruta confiable para la autenticación inicial del usuario y la ejecución de las funciones de administración.

62. Además, el producto cuenta con las bibliotecas criptográficas de Microsoft Windows (bcryptprimitives.dll y cng.sys) para los protocolos seguros y, por lo tanto, para la conexión HTTPS (es decir, HTTP sobre TLS).

5.1.3 HABILITAR FIPS

63. No es necesario realizar ninguna configuración para usar IM con componentes nativos, o IM junto con SSH *SecureBlackbox* como parte del conector Unix, para sincronizar y aprovisionar al sistema Unix. IM, así como el componente SSH *SecureBlackbox*, utilizan la tecnología criptográfica de la configuración del sistema operativo Windows subyacente.

64. Para establecer la configuración FIPS en un sistema operativo Windows, se recomienda ir al enlace indicado en la referencia [REF22].

65. Los pasos básicos para habilitar el modo FIPS en sistemas operativos *Microsoft Windows* como se indica en los artículos referenciados son:

    a) Ejecutar *gpedit.msc*.

    b) Ir a *Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options*.

    c) Establecer el valor de ***System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing*** *a "**Enabled**".*

5.2 DEFINICIÓN DE IDENTIDAD Y CREDENCIAL

66. Los datos del usuario se almacenan principalmente dentro de la base de datos, en la tabla *Person*. La configuración de los datos del usuario empresarial se encuentra descrita en la guía de administración de identidades [REF19], en el capítulo *Employee administration.*

67. Los usuarios se pueden crear con *Manager* (consultar la sección *Entering employee master data* de la guía [REF19]) y el Portal Web (consultar el capítulo *Adding employees* de la guía de usuario del portal web [REF20]). Los datos de usuario también se pueden crear a partir de sistemas externos mediante sincronización y utilizando la asignación automática de empleados.

68. Para la asignación automática de empleados, primero se deben vincular los usuarios del sistema de destino a los empleados en One Identity Manager, como se describe en la guía de administración para la conexión con Active Directory [REF5] en el capítulo *Active Directory User accounts > Automatic Assignment of Employees to Active Directory User Accounts*.

69. El estado de las credenciales de usuario se puede ver y editar utilizando *Manager* y el portal web. Además, la contraseña del usuario se puede restablecer mediante:

    a) El *Manager*, cambiando la contraseña en los datos maestros del usuario (ver guía de administración de identidades [REF19], capítulo *Employee administration > Entering employee master data*).

    b) El *Password Reset Portal*: iniciando sesión en el *Password Reset Portal* mediante una contraseña u OTP y cambiar la contraseña (consultar la guía de usuario del Portal Web [REF20], capítulo *Change password*).

5.3 AUTENTICACIÓN

70. Para realizar cualquier función de gestión, los usuarios deben autenticarse con IM, independientemente de la interfaz de gestión que se utilice.

71. IM admite diferentes tipos de módulos de autenticación, que se describen con más detalle en la guía de autenticación y autorización de IM [REF3], en el capítulo *One Identity Manager Authentication modules*.

72. Para confiar en Active Directory solo como autenticación empresarial, se debe seleccionar uno de los siguientes métodos de autenticación en IM. Estos son los métodos de autenticación que utilizan credenciales de directorio activo para iniciar sesión en IM:

    - *Active Directory user account (role-based).*
    - *Active Directory user account (manual input/role-based).*
    - *Active Directory user account.*
    - *Active Directory user account (manual input).*
    - *User account.*
    - *User account (role-based).*

73. Las principales diferencias entre los diferentes módulos de autenticación son:

    a) Los módulos de *Active Directory* requieren que el directorio activo esté sincronizado con IM y el módulo buscará la información en este para identificar a los usuarios.

    b) El módulo *User account (role-based)* buscará en la tabla *Person* del Active Directory usado para almacenar las identidades.

    c) El módulo *User account* buscará en la tabla *DialogUser* del Active Directory que almacena las cuentas de usuarios internos.

74. One Identity Manager puede configurarse para permitir/no permitir métodos de autenticación específicos para el producto en su conjunto, o se puede configurar para permitir/no permitir diferentes métodos para interfaces de gestión de manera individual.

75. Para mayor información, se recomienda ir a los capítulos *Enabling authentication modules* y *Disabling or enabling Authentication modules for applications* de la guía de autenticación y autorización [REF3].

76. Además, de forma predeterminada, el portal web utiliza los siguientes módulos de autenticación:

    a) *Active Directory user account* (basada en roles o *role-based*): módulo de autenticación principal mediante el inicio de sesión único basado en identidad de Windows.

    b) ***Empleado*** o ***Employee*** (basado en roles): módulo de autenticación alternativo utilizado como respaldo si falla la autenticación de inicio de sesión único.

77. El método de autenticación de *Empleado* (basado en roles) **debe estar deshabilitado**. Para solo permitir el método *Active Directory*, se debe reconfigurar el módulo de autenticación para ser Active Directory user account (manual input/role-based) o *None*. El resto de métodos de autenticación deben estar desactivados. Para mayor información se deberá referir a la guía de instalación de IM [REF1], a los capítulos *Configuring the Web Portal* y *Authentication data for the web application*.

5.4 TRANSMISIÓN DE LA IDENTIDAD Y CREDENCIAL

78. One Identity Manager transmite los datos de identidad y credenciales del sujeto a otros sistemas externos conectados compatibles y autorizados. A continuación, se describe cómo realizar la transferencia con los diferentes componentes externos:

    a) **Directorio Activo**: Se debe habilitar **SSL** y configurar para sincronizar regularmente, tal y como se describe en la guía de administración de conexión con Active Directory [REF5], en el capítulo *Setting up Active Directory Synchronization > Creating a synchronization project for initial synchronization of an Active Directory domain.*

    b) ***Unix/Linux***: El conector utiliza siempre **SSH** para conectarse al host Unix. Se deberá configurar una sincronización de manera regular, tal y como se describe en la guía de administración para la conexión con sistemas Unix [REF6], en el apartado *Setting Up Synchronization with a Unix-Based Target system > Creating a synchronization project for initial synchronization of a Unix host.*

    c) ***Exchange 2016 y 2019***: Se ha de habilitar el **uso de SSL** y configurar la sincronización de manera regular, tal y como se describe en le guía de administración para la conexión con Microsoft Exchange [REF7], en el apartado *Setting up synchronization with a Microsoft Exchange*

environment > Creating a synchronization project of a Microsoft Exchange environment.

d) ***SharePoint 2016 y 2019***: Se debe configurar la conexión con *SharePoint* y su sincronización regular, tal y como se describe en la guía de administración para la conexión con SharePoint [REF8], en el apartado *Setting up Sharepoint Farm synchronization > Creating a Synchronization Project for initial Synchronization of SharePoint Farm.*

e) ***Azure Active Directory***: Se deberá configurar la conexión con el cliente de Azure Active Directory, y su sincronización de manera regular, tal y como se indica en la guía de administración para la conexión con Azure [REF9], en el capítulo *Setting up synchronization with an Azure Active Directory client > Creating a Synchronization Project for initial Synchronization of an Azure Active Directory client.*

f) ***Exchange Online***: Se ha de configurar la conexión con el entorno de Exchange Online y programar una sincronización regular, tal y como se describe en la guía de administración para la conexión con Exchange Online [REF10], en el apartado *Setting up synchronization with an Exchange Online environment > Creating a synchronization project for initial synchronization of an Exchange Online Environment*.

g) ***SharePoint Online***: Se debe configurar la conexión con la instancia de SharePoint Online y se debe programar la sincronización de manera regular, tal y como se indica en la guía de administración para la conexión con SharePoint Online [REF11], en el apartado *Synchronizing a SharePoint Online environment > Setting up the initial synchronization > Preparing a remote connection server for access to the SharePoint Online tenant.*

h) ***Google G-Suite***: Se debe configurar la conexión a G-Suite y programar la sincronización regular, tal y como se describe en la guía de administración para la conexión con Google G-Suite [REF12], en el apartado *Synchronizing a G Suite > Creating a synchronization project for initial synchronization of G Suite.*

i) ***LDAP***: Se debe **habilitar SSL/TLS** en la configuración adicional, junto con la programación de la sincronización regular, tal y como se describe en la guía de administración para la conexión con LDAP [REF13], en el apartado *Setting up LDAP Directory Synchronization > Creating a synchronization project for initial synchronization of a LDAP domain.*

j) ***Mainframe CA ACF2***: El conector accede al sistema de destino a través de LDAP. Para garantizar el uso de un canal seguro, se deberá configurar la conexión para que haga uso de **SSL**, tal y como se describe en la guía del conector LDAP [REF14], en el apartado *Initializing and configuring the LDAP connector for CA ACF2.*

El conector no viene con asignaciones predefinidas para los datos de identidades o credenciales. Por lo tanto, One Identity Manager no es responsable de los datos transmitidos. Se puede crear una asignación, tal y

como se describe en la guía [REF14], en el capítulo apartado *Initializing and configuring the LDAP connector for CA ACF2 > User mapping information*.

79. A continuación, se muestra una tabla con los diferentes protocolos usados en los canales de comunicación seguros para la transferencia de datos de identidades y credenciales entre el producto y los diferentes componentes externos.

	Attributes Transmitted		
External System / ESM product	Identity Data	Credential Data	Secure Channel
Active Directory	X	X	LDAPS (TLS)
Unix/Linux	X	X	SSH
Exchange 2010, 2013, 2016	X		HTTPS
SharePoint 2010, 2013, 2016	X		HTTPS
Azure AD	X	X	HTTPS
Exchange Online	X		HTTPS
SharePoint Online	X		HTTPS
Google G-Suite	X	X	HTTPS
Mainframe (AS/400, RACF, ACF2, Top Secret)	X	X	LDAPS (TLS)
LDAP	X	X	LDAPS (TLS)

Tabla 2 – Protocolos y Canales de Comunicación Sistemas Finales en IM

80. **Se debe seleccionar siempre la versión TLS 1.2 o superior en aquellas comunicaciones que hagan uso de TLS.**

5.5 ADMINISTRACIÓN DEL PRODUCTO

5.5.1 ADMINISTRACIÓN LOCAL Y REMOTA

81. IM puede ser administrado mediante los siguientes mecanismos:

    a) ***Application Server*** y ***Portal Web***: Estos servicios permite la administración remota del producto. Además, la instalación del servidor de aplicaciones obliga al uso de sitios web IIS habilitados para HTTPS por defecto. Como se ha mencionado anteriormente, para obtener más información, consulte la guía de instalación de IM [REF1], capítulo *Installing and updating an application server*. Además, a través del *Application Server* se pueden realizar llamadas a la **REST API** para gestionar IM, así como los objetos gestionados.

    b) **Herramientas Administrativas o *Fat Clients*** instaladas en puestos de trabajo (ver requisitos): IM tiene una serie de consolas pesadas de

administración, las cuales se conectan a los *Application Servers* mediante HTTPS. Estas Herramientas Administrativas o *Fat Clients* permiten la configuración de diferentes elementos de IM como:

i. Conectores a los sistemas finales.
ii. Procesos personalizados.
iii. Gestión de las estructuras organizativas.
iv. Gestión de las políticas de gobierno de IM.
v. Etc.

5.5.2 CONFIGURACIÓN DE ADMINISTRADORES

82. En IM, las identidades (usuarios) que realizan tareas administrativas pueden ser asignados a roles de aplicación de administrador. Un administrador puede crear y editar roles de aplicación. Para obtener más información sobre los roles de la aplicación, se recomienda consultar el capítulo *One Identity Manager Application roles > Creating and editing application roles* de la guía de autorización y autenticación [REF3].
83. Los permisos se otorgan a través de grupos de permisos. Cada rol de la aplicación se asigna a un grupo de permisos.
84. Los grupos de permisos predeterminados que otorgan permisos para administrar usuarios que pertenecen a un rol de aplicación son los siguientes:

- Grupos de permisos no basados en roles:

a) AAD_EditRights_Methods
b) VI_ADS_EditRights_Methods
c) VI_Attestation_EditRights
d) VI_Compliance_EditRights
e) CSM_EditRights
f) VI_EBS_EditRights
g) VI_Exchange_EditRights
h) VI_Notes_EditRights
i) O3S_EditRights_Methods
j) PAG_EditRights_Methods
k) VI_QERPolicy_EditRights
l) VI_ITShop_EditRights
m) UNX_EditRights_Methods

- Grupos de permisos basados en roles:

a) Para cada tipo de sistema de destino, hay un rol de aplicación de administrador del sistema de destino dedicado.

b) vi_4_ATTESTATIONADMIN_ADMIN

c) vi_4_CUSTOM_ADMIN

85. Para obtener más información sobre los grupos de permisos y las funciones de la aplicación, consulte la guía de autenticación y autorización de One Identity Manager [REF3]:

- Información general en el capítulo *Granting One Identity Manager schema permissions*.
- La creación de grupos de permisos se describe en el capítulo *Creating permissions groups*.
- La modificación de los permisos asociados con un grupo de permisos se describe en capítulo *Editing table permissions and column permissions*.
- El anidamiento de grupos de permisos jerárquicos se describe en el capítulo *Permissions group dependencies*.
- La asignación de una identidad a los grupos de permisos efectivos se describe en el capítulo *Rules for determining the valid permissions for tables and columns*.
- Las funciones de la aplicación se describen en el capítulo *Application roles overview*.
- Los roles de aplicación de administrador del sistema de destino dedicados para cada tipo de sistema de destino, se describen en el capítulo *Application roles for target systems.*

5.5.3 POLÍTICA DE CONTRASEÑAS

86. IM también actúa como punto central para la aplicación de políticas de contraseñas, al definir las políticas que las contraseñas deben cumplir. Se ha de tener en cuenta que el administrador debe asegurarse de que los sistemas externos no apliquen políticas de contraseñas más estrictas que IM o, de lo contrario, la sincronización de contraseñas puede fallar debido a políticas contradictorias.

87. Para configurar las políticas de contraseñas, desde la herramienta *Designer* > *Base Data* > *Security Settings* > *Password Policies* se pueden configurar los siguientes parámetros:

- Longitud mínima y máxima de la contraseña. Se deberá configurar una longitud mínima de **12 caracteres,** aunque se recomienda una longitud de 15.
- Máximo número de *logins* fallidos. Se deberá configurar el bloqueo de las cuentas al introducir, como mucho, **5 intentos erróneos**.
- Validez de la contraseña. El valor recomendado para la vigencia y expiración de contraseñas es de 30 días

- Histórico de contraseñas. No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas
- Complejidad. Las contraseñas deberán estar compuestas por una mezcla de mayúsculas, minúsculas, números y caracteres especiales (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”).
- Caracteres permitidos o denegados.

88. Los portales Web de One Identity Manager pueden configurarse para establecer un tiempo máximo de inactividad mediante la configuración del *web.config*, mediante el parámetro ***session timeout***. Este parámetro está por defecto a 00:05:00, es decir, 5 min.

89. Además, los *Fat Clients* pueden configurarse para crear una conexión estableciendo *timeouts* de establecimiento de la sesión. Esto se realiza tal y como se observa en la siguiente imagen:

    a) Al abrir cualquiera de las Herramientas de Administración seleccionar “*Add new connection*”.

    b) Seleccionar “*Application Server*”.

    c) Añadir la URL del Application Server.

    d) Pinchando en *Options – Advanced Options*, se pueden configurar parámetros específicos de la conexión como se muestra a continuación.

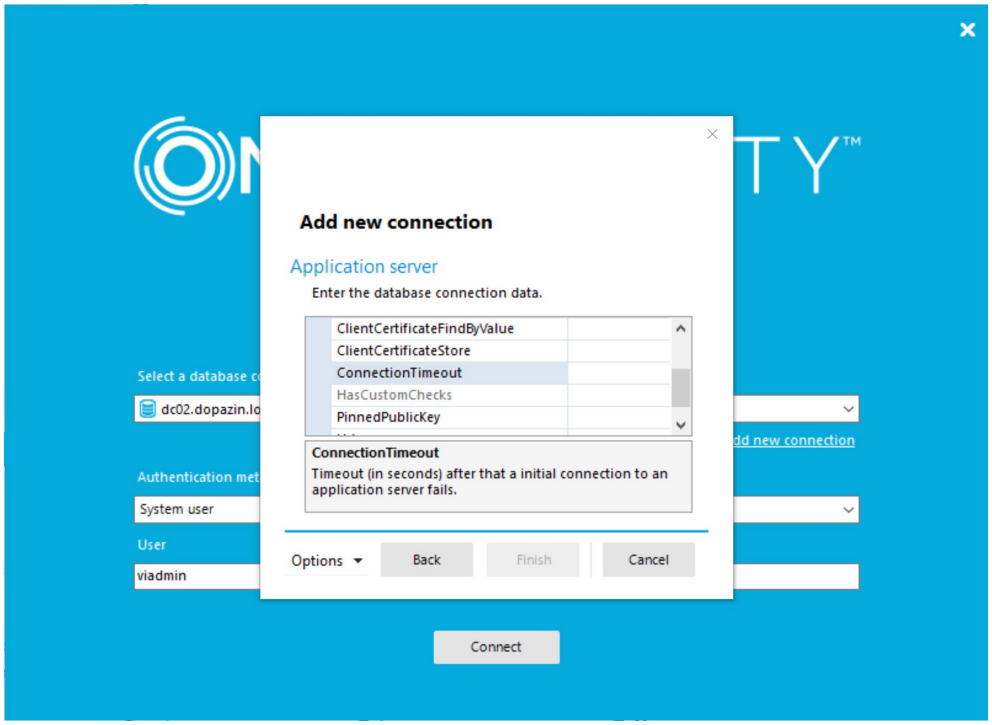

Ilustración 5 – Configuración Conexión Herramientas Administrativas de IM

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

90. IM invoca las librerías criptográficas del sistema operativo donde está instalado para las funciones criptográficas, por lo que no es necesario realizar ninguna configuración de los protocolos seguros. Estas configuraciones deben realizarse a nivel de sistema operativo. Las bibliotecas criptográficas de *Microsoft Windows* utilizadas por el producto para todas las conexiones TLS, SSH y HTTPS son: *bcryptprimitives.dll* (CMVP2937) y *cng.sys* (CMVP2936).

91. IM proporciona canales de comunicación confiables usando TLS v1.1 y TLS v1.2 para las siguientes conexiones:

    - Autenticación externa de usuarios y administradores (AD).
    - Transferencia de datos de políticas (recopilación y aprovisionamiento).
    - Transferencia de registros de auditoría (base de datos SQL).
    - Comunicaciones entre el servicio web y los componentes del servicio de trabajo (con conectores) mediante el uso de HTTPS (HTTP sobre TLS).

92. **Se deberá usar TLS 1.2 para las comunicaciones mencionadas.**

93. Los conectores de *mainframe* (*AS / 400, RACF, ACF2, Top Secret*), *LDAP* y Active Directory utilizan **LDAPS**, que establece una conexión TLS entre IM y estos tipos de sistemas externos antes de que se transfiera cualquier mensaje LDAP.

94. Además, IM proporciona canales de comunicación confiables entre él y los sistemas basados en UNIX que utilizan **SSH** para la transferencia de datos de políticas. Para esta conexión, IM hace uso de *SecureBlackbox*, el cual invoca bibliotecas criptográficas del sistema operativo para funciones criptográficas subyacentes.

5.7 GESTIÓN DE CERTIFICADOS

95. Los certificados y sus claves privadas asociadas se guardan en el almacén de certificados de Windows. Windows almacena claves privadas cifradas mediante RSA. Toda la gestión de claves es responsabilidad de los componentes criptográficos del sistema operativo en los que se basa el producto.

5.8 SERVIDORES DE AUTENTICACIÓN

96. IM soporta diferentes métodos de autenticación. El recomendado es *Active Directory*. Los componentes que usan este método de autenticación son los portales Web que usan la autenticación de Windows integrada en los IIS, por lo que no es necesario configurar nada concreto en IM, ya que la autenticación recae en el propio sistema operativo subyacente.

97. Además del módulo de autenticación de *Active Directory* se pueden instalar y configurar otros módulos de autenticación:

    a) *System Users*: Estos usuarios son usuarios de One Identity Manager almacenados en la base de datos con la contraseña. Todas las autenticaciones que hagan uso de este módulo utilizarán TLS o SSL

configurados en One Identity Manager para conectarse a la base de datos SQL o los sitios web de IIS.

b) *Employee*: Estos usuarios son usuarios de IM almacenados en la base de datos con la contraseña. Todas las autenticaciones que utilicen este módulo harán uso de TLS o SSL configurados en One Identity Manager para conectarse a la base de datos SQL o los sitios web de IIS.

c) *LDAP user account*: La cuenta de usuario debe existir en la base de datos de IM y, además, debe existir en el sistema LDAP de autenticación. La configuración de la autenticación segura se realiza desde la herramienta de administración *Designer*, en la sección: "*TargetSystem | LDAP | Authentication | Authentication*" donde se pueden configurar los siguientes parámetros de seguridad:

   i. *Secure*
   ii. *Encryption*
   iii. *SecureSocketsLayer*
   iv. *ReadonlyServer*
   v. *Signign and Sealing*
   vi. *Delegation*
   vii. *ServerBind*

   Para más información, se recomienda consultar la sección *One Identity Authentication modules > LDAP user account (role-based)* de la guía de autorización y autenticación de IM [REF3].

d) *OAuth 2.0/OpenID Connect*: IM soporta la autenticación basada en estándares OAuth 2.0. Para una completa guía de configuración de este módulo de autenticación, se recomienda consultar la siguiente sección *OAuth 2.0/OpenID Connect configuration* de la guía autorización y autenticación de IM [REF3].

5.9 ACTUALIZACIONES

98. Actualizar IM incluye las diferentes actualizaciones de las herramientas que lo componen: la base de datos, los servidores y las estaciones de trabajo.

99. Dichas actualizaciones están disponibles en la web de soporte de One Identity, y se pueden descargar y comprobar su integridad de la misma manera que se descarga el *software* para la instalación inicial. Por otro lado, también se puede realizar la actualización de manera automática mediante el archivo ejecutable *Update.exe*, que se encuentra dentro de la carpeta del instalador de IM.

100. Antes de realizar cualquier proceso de actualización, se deberá **realizar una copia de seguridad de la base de datos** de One Identity Manager.

101. Además, se deberá usar un usuario con permisos de administración en la base de datos para poder realizar la actualización correctamente.

102. Para más información acerca de las actualizaciones, los pasos exactos que se deben seguir para realizar la actualización de cada uno de los componentes de One Identity Manager, y las diferentes recomendaciones a tener en cuenta durante la actualización, se recomienda consultar la sección *Updating One Identity Manager* de la guía de instalación de IM [REF1]. En caso de querer realizar la actualización automática, se deberá consultar la sección *Automatic updating of One Identity Manager* de la guía de instalación de IM [REF1].

5.10 ALTA DISPONIBILIDAD

103. One Identity Manager se puede desplegar en alta disponibilidad, principalmente basada en el balanceo de los servicios Web, por medio de balanceadores de tráfico *hardware*, junto con las opciones de balanceo y alta disponibilidad de Microsoft SQL, tal y como se muestra en la imagen siguiente:

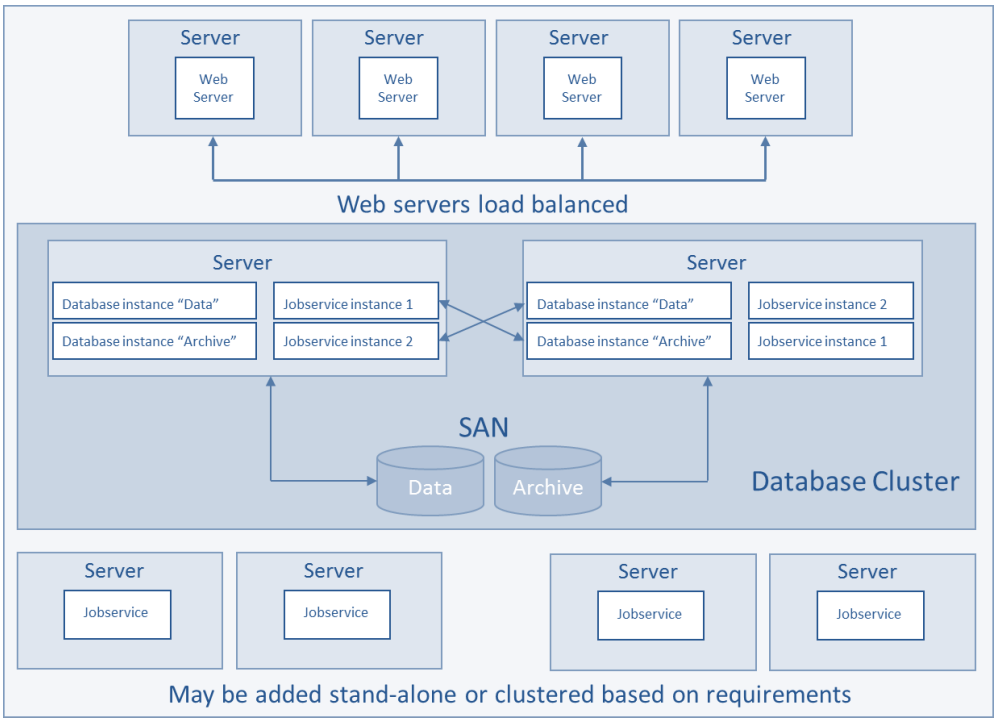

Ilustración 6 – Ejemplo de Configuración en HA de IM

104. Como se observa en la imagen anterior, cada elemento de IM se configura en alta disponibilidad (HA) en base a la tecnología de Microsoft subyacente:

a) **Base de Datos MS SQL**: IM soporta el modelo tradicional de clúster Active-Pasivo de Microsoft, además de la tecnología de SQL *Always On* para proporcionar HA para las bases de datos de IM. Esta configuración es propia de *Microsoft*.

b) **Componentes Web como Portal Web o Portal de Aplicación**: Están basados en tecnología de Microsoft IIS. La técnica de HA de estos servicios Web se basa en un escalado horizontal con un balanceo de carga, normalmente basado en *hardware*, aunque también se puede optar por un balanceo de carga basada en *software*.

c) ***Job Servers***: Componente de IM instalado en servidores Windows los cuales realizan las tareas de gestión del ciclo de vida de las cuentas. Este servicio es el único de los anteriores cuya HA es gestionada por el propio IM. Cada *Job Server* es asignado a una serie de roles o responsabilidades, y es el propio IM el encargado de repartir los trabajos a realizar mediante diferentes criterios lógicos y de rendimiento de manera automática.

105. Para el almacenamiento de los datos se deberá disponer de **replicación SAN**. Esta replicación permite obtener una redundancia de los discos en caso de desastres mediante la replicación del almacenamiento mediante tecnologías propias de las cabinas de discos.

5.11 AUDITORÍA

106. Las funcionalidades de auditoría se ejecutan siempre que IM esté siendo ejecutado. Esta funcionalidad no se puede iniciar o finalizar de manera separada a IM.

107. Ofrece varias funciones para archivar información histórica:

- Cambios en los datos.
- Información de proceso.
- Mensajes en el historial del proceso.

108. Para cambios de datos, las columnas individuales en la base de datos principal se pueden marcar para cambiar y/o eliminar registro.

109. A través de *Web UI*, se puede acceder a los diferentes registros de la base de datos. En el caso de que la base de datos no se encuentre disponible, no se generarán registros de auditoría ya que no se permitirá realizar cambios en los datos.

5.11.1 REGISTRO DE EVENTOS

110. Por defecto, no todos los eventos auditables dan lugar a la generación de registros de auditoría. Para habilitar toda la auditoría necesaria, se deben realizar los siguientes pasos:

- Registrar los inicios y cierres de sesión de One Identity Manager: En *Designer*, se deben activar las opciones *Common | Journal | LoginAudit y Common | Journal | LogoffAudit*. Para más información, se recomienda consultar la guía de supervisión y resolución de problemas [REF15], el capítulo *Configuring logging in One Identity Manager > Recording logins and logoffs in the system journal*.
- Registrar los cambios de datos: En *Designer*, se deben activar las opciones *Common | ProcessState | PropertyLog y Common | ProcessState | PropertyLog | AllDefaultPropertiesForModel.* Para mayor información, se recomienda consultar la guía de configuración [REF16], el capítulo *Tracking changes with process monitoring > Logging data changes*.
- Se debe configurar el registro del sistema de destino para generar datos de auditoría. Para obtener más información, se recomienda consultar la guía

de referencia de la sincronización del sistema de destino [REF17], el capítulo *Configuring the synchronization log*.

- Por defecto, hay una serie de atributos que están marcados para auditar sus cambios. Aun así, IM permite extender la auditoría de cualquier atributo de cualquier tabla, de manera personalizada. Para ello, se deben etiquetar/configurar las columnas adicionales requeridas para que formen parte del registro de datos de cambios, tal y como se describe en la guía de configuración de IM [REF16], en el capítulo *Tracking changes with process monitoring > Labeling columns for recording changes to data*. En dicha sección se indica cómo se ha de configurar cada columna para que se generen registros de auditoría cuando se realicen cambios en los datos.

111. Los diferentes procesos que generan registros de auditoría son:

a) El uso de mecanismos de autenticación. Estos se almacenan en la tabla *SQL DialogJournal.*

b) La creación o modificación de datos de identidades y credenciales. Se almacenan en la tabla SQL *DialogWatchOperation.*

c) La creación o modificación de atributos por parte del usuario.

d) Los intentos de transmisión de información y de sincronización de datos con sistemas de terceros. Se almacenan en las tablas *SQL DPRJournal, DPRJournalObject y DPRJournalMessage.* Además, los procesos de sincronización también se almacenan en la tabla *SQL JobHistory*.

e) Establecimiento de comunicación con el servidor de auditoría y modificación de funcionalidades de auditoría. Se almacena en la tabla *SQL DialogWatchOperation.*

f) Modificaciones de funciones de seguridad. Estos registros se almacenan en las tablas *SQL DialogWatchOperation* y *DialogWatchProperty*.

g) Uso de funcionalidades de gestión. Se almacenan en las tablas *SQL DialogWatchOperation* y *DialogWatchProperty*.

h) Uso de canales y rutas seguras.

112. Para más información con respecto a auditoría, se recomienda ir a la guía de administración Common Criteria [REF21], al apartado *Audit data generation (FAU_GEN.1)*. En este apartado se describe en profundidad los registros de auditoría generados por el producto.

5.11.2 ALMACENAMIENTO

113. IM almacena los eventos de registro en la base de datos desplegada en el Servidor MS SQL, como se ha comentado previamente, pero además ofrece la posibilidad de archivarlos en una base de datos específica para almacenar el histórico de eventos sin que esto afecte a la base de datos de One Identity de producción.

114. Esta nueva base de datos de archivado (*History Database*) se puede desplegar en el mismo servidor MS SQL o en otro diferente según los requerimientos e infraestructura de los usuarios.

115. El período de retención para estos datos se puede configurar en la base de datos principal y, al expirar, los procesos programados copian los datos en *HistoryDB* y eliminan los datos de la base de datos principal.

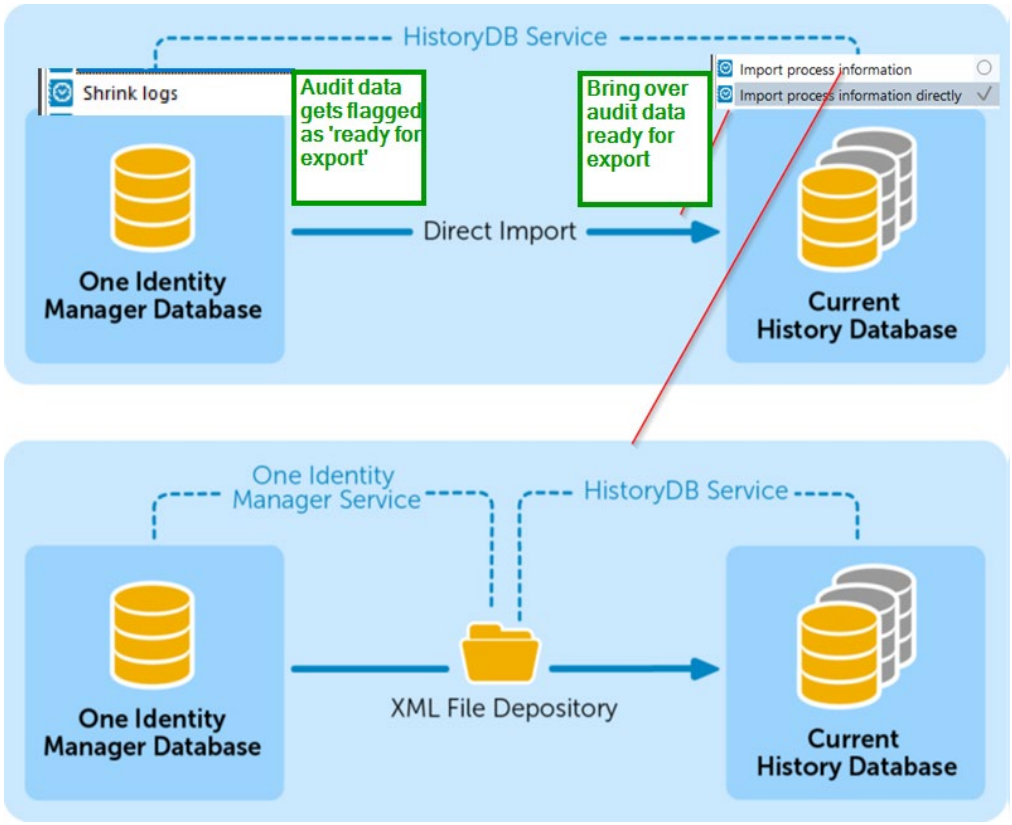

Ilustración 7 – Proceso de archivado a la base de datos History Database

116. Para configurar los periodos máximos de retención, a través de la herramienta de administración *Designer*, IM proporciona los siguientes parámetros:

    a) *Common | ProcessState | PropertyLog | LifeTime*

    Este parámetro de configuración especifica el periodo máximo de retención en la base de datos para las entradas de registro del seguimiento de cambios.

    b) *Common | ProcessState | ProgressView | LifeTime*

    Este parámetro de configuración especifica el periodo máximo de tiempo que los datos de registro de la información del proceso se pueden mantener en la base de datos.

    c) *Common | ProcessState | JobHistory | LifeTime*

    Este parámetro de configuración especifica el periodo máximo de retención en la base de datos para las entradas de registro del historial del proceso.

117. **Se debe configurar TLSv1.2 para la conexión para el envío de los registros de auditoría almacenados en la base de datos SQL de IM.** Para ello, es necesario configurar el servidor SQL para forzar el cifrado, tal y como se describe en el siguiente enlace: *https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017*

118. Para obtener más información de configuración de las capacidades de archivado de One Identity Manager, consulte la guía de archivado de datos [REF18].

5.12 *BACKUP*

119. One Identity Manager almacena todos los datos de configuración y del cliente en una base de datos de Microsoft SQL. En el caso de habilitar el archivado de registros de auditoria en una base de datos adicional, también se debería tener una base de datos de histórico (*History Database*). Es por ello que los componentes principales a realizar una copia de seguridad son las bases de datos donde los datos son almacenados en One Identity Manager. Por lo tanto, se requiere un *backup* completo de las bases de datos, siguiendo los procedimientos estándar de Microsoft SQL para realizarlos, los cuales se encuentran descritos en el enlace [REF23].

120. Los *backups* de las bases de datos de One Identity Manager deben almacenarse en un **sistema de ficheros externo a los servidores** donde se despliegan los componentes de One Identity Manager.

6. FASE DE OPERACIÓN

121. Durante la fase de operación de One Identity Manager se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

- Comprobaciones periódicas del *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado.
- Comprobaciones periódicas de los sistemas de antivirus desplegados en los servidores donde se han desplegado los componentes de One Identity Manager.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura en aquellos servidores donde se han desplegado los componentes de One Identity Manager.
- Realizar copias de seguridad, al menos diarias, de las bases de datos de One Identity Manager.
- Realizar pruebas de restauración del servicio mediante las copias de seguridad en caso de desastre.
- Mantener los registros de auditoria en la base de datos de histórico, asegurando que el personal autorizado pueda acceder a ellos.
- Configurar el archivado de eventos y borrado en base a los criterios específicos requeridos.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Configuración de componentes de administración	☐	☐	
Configuración de Base de Datos	☐	☐	
Configuración de *Job Server* y *Application Server*	☐	☐	
Configuración del Portal Web	☐	☐	
Configuración de BACKUP & ARCHIVADO periódico	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (modo FIPS)	☐	☐	
Requisitos mínimos de contraseñas	☐	☐	
Configurar timeouts de sesión	☐	☐	
Configurar el método de autenticación	☐	☐	
Configurar el logging de todo el tráfico relevante	☐	☐	
Configurar puertos y protocolos en modo seguro (TLS 1.2, ciphersuites, claves de fortaleza 128 bits, como mínimo, etc.)	☐	☐	

8. REFERENCIAS

REF1 Guía de Instalación de One Identity Manager
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/installation-guide

REF2 Guía de cifrado de las conexiones con bases de datos SQL
https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017

REF3 One Identity Manager Guía de autorización y autenticación.
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/authorization-and-authentication-guide

REF4 One Identity Manager Guía de administración del archivado.
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/data-archiving-administration-guide/3#TOPIC-1131185

REF5 One Identity Manager Guía de administración para la conexión con Active Directory.
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-active-directory

REF6 One Identity Manager Guía de administración para la conexión con sistemas Unix.
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-unix-based-target-systems

REF7 One Identity Manager Guía de administración para la conexión con sistemas Microsoft Exchange.
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-microsoft-exchange

REF8 One Identity Manager Guía de administración para la conexión con SharePoint
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-sharepoint

REF9 One Identity Manager Guía de administración para la conexión con Azure Active Directory
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-azure-active-directory

REF10 One Identity Manager Guía de administración para la conexión con Exchange Online
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-exchange-online

REF11 One Identity Manager Guía de administración para la conexión con SharePoint Online
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-sharepoint-online

REF12 One Identity Manager Guía de administración para la conexión con Google G-Suite
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-g-suite

REF13 One Identity Manager Guía de administración para la conexión con LDAP
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/administration-guide-for-connecting-to-ldap

REF14 One Identity Manager Guía del conector LDAP
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/ldap-connector-for-ca-acf2-reference-guide

REF15 One Identity Manager Guía de resolución de problemas y errores
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/process-monitoring-and-troubleshooting-guide

REF16 One Identity Manager Guía de configuración
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/configuration-guide

REF17 One Identity Manager Guía para la sincronización con un sistema externo
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/target-system-synchronization-reference-guide

REF18 One Identity Manager Guía de archivado de datos
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/data-archiving-administration-guide

REF19 One Identity Manager Guía de administración de identidades
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/identity-management-base-module-administration-guide

REF20 One Identity Manager Guía de usuario del Portal Web
https://support.oneidentity.com/es-es/technical-documents/identity-manager/9.0/web-portal-user-guide

REF21 Guía de administración para configuración Common Criteria
https://www.niap-ccevs.org/MMO/Product/st_vid11003-agd.pdf

REF22 Validación FIPS 140-2
https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation

REF23 Realizar copia de seguridad completa de base de datos SQL Server
https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server?view=sql-server-ver15

9. ABREVIATURAS

AD	*Active Directory*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad TIC, CPSTIC
ENS	Esquema Nacional de Seguridad.
FIPS	*Federal Information Processing Standards*
GUI	*Graphical User Interface*
HA	*High Availability (Alta Disponibilidad)*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Secure Hypertext Transfer Protocol*
IAM	*Identity and Access Management*
IM	*One Identity Manager*
IIS	*Internet Information Services*
LDAP	*Lightweight Directory Access Protocol*
RACF	*Resource Access Control Facility*
REST	*Representational State Transfer*
RSA	*Rivest–Shamir–Adleman*
SQL	*Structured Query Language*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*

PUBLICACIONES DE DEFENSA

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