centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1115

Procedimiento de Empleo Seguro
Azure Identity Access Management (IAM)

Octubre 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-119-X

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 09:37:13 +02'00'

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. Azure Identity Access Management (IAM) es una solución de identidad que ofrece servicios en la nube para asegurar que las personas adecuadas, dispositivos y componentes de software accedan a los recursos correctos en el momento preciso.
2. Esta solución de identidad administra el acceso a aplicaciones y datos de una organización. Usuarios, dispositivos y aplicaciones poseen identidades. Los componentes de IAM respaldan la autenticación y autorización de estas y otras identidades. El proceso de autenticación regula quién o qué utiliza una cuenta, mientras que la autorización define lo que un usuario puede hacer dentro de las aplicaciones.
3. El control de acceso basado en roles de Azure (Azure RBAC) se utiliza para otorgar el acceso a recursos.
4. Azure RBAC es el sistema de autorización utilizado para administrar el acceso a los recursos de Azure. Para conceder el acceso, se asignan roles a usuarios, grupos, principios de servicio o identidades administradas en un ámbito específico.
5. Azure RBAC dispone de varios roles integrados en Azure que pueden asignarse a usuarios, grupos, principios de servicio e identidades administradas. Las asignaciones de roles son la manera de controlar el acceso a los recursos de Azure.
6. Para más información sobre el control de acceso basado en roles, consultar la guía ¿Qué es el control de acceso basado en rol de Azure (RBAC)? [REF1].

2 OBJETO Y ALCANCE

7. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Azure Identity Access Management (IAM).
8. Esta solución se sitúa dentro de la familia Gestión de Identidades (IM) del catálogo CPSTIC y está cualificada para categoría ENS ALTA.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Azure Portal** [REF2] y se enviarán de forma segura los accesos pertinentes a la plataforma.
10. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
11. Una vez dado el alta en la plataforma se podrán activar las licencias por cada usuario dentro de la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
13. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.
14. Sólo los usuarios autorizados y con la licencia activa podrá acceder al producto.

4.3 REGISTRO Y LICENCIAS

15. Los servicios prestados son mediante contratación y no es necesario la instalación. Las licencias se activan por cada usuario dentro de la suscripción contratada.

4.4 CONSIDERACIONES PREVIAS

16. Al tratarse de un servicio alojado en la nube, la principal consideración previa es tener conexión a Internet y estar dado de alta en la plataforma para hacer uso del producto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El producto consta de los siguientes componentes principales:
    - Servicio en la nube: Espacio del usuario en la nube accesible mediante el uso de Microsoft Azure portal.
    - API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
18. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    - Azure Portal: acceso al portal de gestión.
    - Entra ID: autenticación de usuarios, acceso condicional, políticas.
    - Azure Gateway: equilibrador de carga de tráfico web.
    - Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.
    - Azure Monitor Activity Log: registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción.
    - Azure Storage: solución de almacenamiento en la nube.

5 FASE DE INSTALACIÓN

19. En este apartado se describe la implementación del producto.

5.1 ALTA DEL SERVICIO EN LA NUBE

20. Al tratarse de un servicio en la nube, se requiere el alta en el portal de Microsoft Azure Portal adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del servicio.
21. Una vez que se encuentre dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

22. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. Para más información sobre el producto se debe consultar la **Documentación completa de RBAC** [REF3]**.**
23. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por Azure Entra ID antes de cualquier interacción con el producto.
24. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

25. El producto usa la infraestructura de Azure vinculado a Microsoft Entra ID, para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.
26. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
27. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.
28. Más información en la guía **CCN-STIC-884A Guía de configuración segura para Azure** [REF4]**.**

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

29. Al ser un producto en la nube que forma parte de la infraestructura de Microsoft Azure, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLS 1.2 o superior para el establecimiento de las comunicaciones seguras.
30. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

31. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del producto se realiza de forma remota.
32. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure Entra ID. Sólo los usuarios con el rol de

administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

33. El producto utiliza Azure RBAC (Control de Acceso Basado en Roles) para acceder a los recursos. A continuación, se enumeran cuatro roles fundamentales integrados. Los primeros tres se aplican a todos los tipos de recursos:

    - Propietario (Owner): Tiene acceso completo a todos los recursos, incluyendo el derecho para delegar el acceso a otros.
    - Colaborador (Contributor): Puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
    - Lector (Reader): Puede ver los recursos existentes de Azure.
    - Administrador de Acceso de Usuario (User Access Administrator): Le permite gestionar el acceso de los usuarios a los recursos de Azure.

34. Estos roles son esenciales para controlar quién tiene permiso para realizar acciones específicas en los recursos de Azure, asegurando una gestión segura y eficiente del acceso.

35. El producto utiliza Azure Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad haciendo uso de la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:

    - Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 10
    - Duración del bloqueo: 60 segundos

36. Para más información sobre los diferentes mecanismos de seguridad de la tecnología Smart Lockout y cómo modificar los valores establecidos, se puede consultar la siguiente guía, **Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra** [REF5].

37. El producto utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Azure Entra ID. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Azure Entra ID. Los siguientes requisitos de directiva de contraseñas de Azure Entra ID se aplican a todas las contraseñas que se crean, cambian o restablecen en Azure Entra ID:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > Espacio en blanco
Caracteres no permitidos	Caracteres unicode

Longitud de la contraseña	Aunque el producto establezca un mínimo de 8 caracteres y un máximo de 256, se deben establecer contraseñas de 12 a 256 caracteres.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos
Contraseña no utilizada recientemente	Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser la misma que las contraseñas actuales o usadas recientemente.

Tabla 1. Política de contraseñas

38. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID** [REF6].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

39. Todo acceso al producto se realiza mediante el uso de HTTPS con TLS1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

40. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure los certificados usan RSA con longitud de clave de 2048 bits. Este cifrado es suficientemente robusto y, aunque se considera seguro para las comunicaciones en el momento de creación de este documento, se recomienda la utilización de RSA con longitud de clave de 3072 bits.
41. Para la gestión y configuración de la longitud de clave ver la subsección “Creación de claves” de la sección “3.1.2.2 Protección de claves criptográficas” de la guía **CCN-STIC-884A** [REF4]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

42. El producto usa Microsoft Entra ID para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.

6.7 SINCRONIZACIÓN

43. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

44. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el servicio es parte de la infraestructura de Azure.
45. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

46. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas del producto de manera automatizada.

6.10 ALTA DISPONIBILIDAD

47. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

48. Debido a que el producto es parte de la infraestructura de Azure, hace uso de Azure Activity Monitor Log para auditar todos los eventos que se generan por parte del producto y otros servicios de Azure, que el producto utiliza para funcionar correctamente. Para más información, se puede consultar la guía oficial de **Uso del registro de actividad de Azure Monitor y la información del registro de actividad** [REF7]**.**
49. El servicio genera registros de auditoría clasificados por actividades que se auditan en la infraestructura de Azure, para más información se puede consultar la guía **Esquema de eventos del registro de actividad de Azure** REF8**.** Se pueden buscar estos eventos buscando el Activity Log en el portal de seguridad y cumplimiento, seleccionando las siguientes categorías:

    - Proceso de inicio de sesión del personal autorizado (estos eventos proceden de la integración con Entra ID). Debido a la arquitectura y modo de operación de la infraestructura Azure, la plataforma utiliza la capacidad de sesiones y no hay eventos de cierre de sesión. Los inicios de sesión (sing-ins) se registran con los siguientes estados descritos:
        - Éxito: inicio de sesión exitoso.
        - Fallo: Error al validar las credenciales debido a que el nombre de usuario o la contraseña no son válidos.

    - Interrumpido: La contraseña del usuario ha caducado, por lo que su login o sesión ha sido finalizado. Cuando se pregunta al usuario si desea seguir conectado a este navegador para facilitar el inicio de sesión en el futuro.
  - Cambio en las credenciales del usuario (estos eventos provienen de la integración con Entra ID)
  - Cambios en la configuración del producto seleccionando la categoría apropiada:
    - Crear/Borrar asignación de roles.
    - Crear/actualizar/borrar definición de rol personalizado.
  - Eventos relacionados con la funcionalidad del producto buscando la categoría apropiada en las actividades (actividades de respuesta):
    - Actualizar Política de Métodos de Autenticación.

50. El Activity Log se muestra en la página de búsqueda de registros de auditoría.
51. Los resultados de una búsqueda en el Activity Log se muestran con la siguiente información:
    - El tipo de evento identificado corresponde a "Autorización:acción" y "Autorización:ámbito": La acción realizada por el usuario (crear asignación de funciones, eliminar asignación de funciones, crear o actualizar definición de rol...) y el ámbito de la acción.
    - El usuario que produce el evento corresponde a la propiedad "Caller": Quién inició la acción.
    - Fecha y hora del evento corresponde a la propiedad "EventTimestamp": Hora en que ocurrió la acción.
    - Resultado del evento corresponde a la propiedad "Status:value": Estado de la acción.
52. El producto sobrescribe los registros siguiendo los criterios más antiguos. Cada tipo de datos se almacena durante un período diferente:
    - "Métricas" tienen una retención de 93 días,
    - "Logs" son configurables hasta 12 años a través de Azure Portal y API, y 7 años a través de PowerShell.
53. IAM registra eventos de seguridad y auditoría en el Activity Log de la suscripción. Este registro proporciona información sobre cambios en los recursos, configuración de alertas y actividades relacionadas con el producto realizadas por un administrador.

6.11.2 ALMACENAMIENTO LOCAL

54. Al tratare de un servidor en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada.

6.11.3 ALMACENAMIENTO REMOTO

55. La opción de enviar eventos de registros a un servidor no está disponible. Únicamente se pueden enviar los registros a los siguientes recursos de Azure: Azure Storage, Azure Event Hubs y Azure Log Analytics workspace.
56. Para más información sobre cómo realizar el envío de registros a los recursos de Azure mencionados, se puede consultar la siguiente guía, **Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage** [REF9].REF9

6.12 BACKUP

57. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

7 FASE DE OPERACIÓN

58. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.
59. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:
60. Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
    - Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.
    - Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
    - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.
61. Microsoft Identity Access Management (IAM) ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.
62. En las siguientes subsecciones de la fase de operación, se analizarán dichas funcionalidades en detalle, haciendo referencia, cuando corresponda, a la documentación oficial proporcionada por el proveedor para garantizar su uso de manera segura, eficiente y conforme a las directrices establecidas.

7.1 COMPROBACIÓN DE ACCESO DE UN USUARIO

63. Para poder comprobar si un usuario tiene acceso a un recurso concreto de Azure, se deben enumerar sus asignaciones. Una forma rápida de comprobar el acceso de un usuario es utilizar la característica “Comprobar acceso” de la página “Control de acceso (IAM)”.
64. Para más información se debe consultar la guía **Inicio rápido: Comprobación del acceso de un usuario a un único recurso de Azure** [REF10]**.**

7.2 ENUMERACIÓN DE ASIGNACIONES DE ROLES

65. El **control de acceso basado en rol (RBAC)** [REF1] de Azure es el sistema de autorización que puede utilizar para administrar el acceso a los recursos de Azure.
66. Para determinar a qué recursos tienen acceso los usuarios, grupos, entidades de servicio o identidades administradas, se deben mostrar sus asignaciones de roles.
67. Para más información se debe consultar la guía **Enumeración de asignaciones de roles de Azure mediante Azure Portal** [REF10]**.**

7.3 ASIGANCIÓN DE ROLES A OTROS USUARIOS

68. El **control de acceso basado en rol (RBAC)** [REF1] tiene varios roles integrados de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas.

69. Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure.
70. Para información sobre cómo asignar roles, consulte **Pasos para asignar un rol de Azure** [REF12][REF11]**.**

7.4 CREACIÓN O ACTUALIZACIÓN DE ROLES PERSONALIZADOS

71. Si los roles integrados de Azure no cumplen las necesidades específicas de su organización se pueden crear roles personalizados.
72. Para crear un rol personalizado se debe seguir la guía de **Roles personalizados en recursos de Azure** [REF13].

7.5 USO DEL CONTROL DE ACCESO BASADO EN ATRIBUTOS DE AZURE (AZURE ABAC)

73. El control de acceso basado en atributos (ABAC) es un sistema de autorización que define el acceso en función de los atributos asociados a las entidades de seguridad, los recursos y el entorno de una solicitud de acceso.
74. Con ABAC, puede conceder a una entidad de seguridad acceso a un recurso en función de los atributos. Azure ABAC hace referencia a la implementación del control de acceso basado en atributos para Azure.
75. Para más información sobre ABAC y como implementarlo se debe consultar la guía **¿Qué es el control de acceso basado en atributos de Azure (Azure ABAC)?** [REF14].

8 REFERENCIAS

[REF1] ¿Qué es el control de acceso basado en rol de Azure (RBAC)? https://learn.microsoft.com/es-es/azure/role-based-access-control/overview

[REF2] Microsoft Azure Portal
https://portal.azure.com

[REF3] Documentación completa de RBAC
https://learn.microsoft.com/es-es/azure/role-based-access-control/

[REF4] CCN-STIC-884A Guía de configuración segura para Azure
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/4253-ccn-stic-884a-guia-de-configuracion-segura-para-azure/file.html

[REF5] Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/authentication/howto-password-smart-lockout

[REF6] Roles Integrados de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/permissions-reference

[REF7] Uso del registro de actividad de Azure Monitor y la información del registro de actividad
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-insights

[REF8] Esquema de eventos del registro de actividad de Azure
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-schema

[REF9] Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/resource-logs

[REF10] Inicio rápido: Comprobación del acceso de un usuario a un único recurso de Azure
https://learn.microsoft.com/es-es/azure/role-based-access-control/check-access

[REF11] Enumeración de asignaciones de roles de Azure mediante Azure Portal
https://learn.microsoft.com/es-es/azure/role-based-access-control/role-assignments-list-portal

[REF12] Pasos para asignar un rol de Azure
https://learn.microsoft.com/es-es/azure/role-based-access-control/role-assignments-steps

[REF13] Roles personalizados en los recursos de Azure
https://learn.microsoft.com/es-es/azure/role-based-access-control/custom-roles

[REF14] ¿Qué es el control de acceso basado en atributos de Azure (Azure ABAC)?
https://learn.microsoft.com/es-es/azure/role-based-access-control/conditions-overview

9 ABREVIATURAS

ABAC	Attribute-Based Access Control.
API	Interfaz de Programación de Aplicaciones.
CCN	Centro Criptográfico Nacional.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSP	Cloud Service Provider.
ENS	Esquema Nacional de Seguridad.
HTTPS	Secure Hyper Text Transfer Protocol.
IAM	Identity Access Management.
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado).
TLS	Transport Layer Security.
WAF	Firewall de Aplicación Web.

PUBLICACIONES DE DEFENSA

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