Guía de Seguridad de las TIC
CCN-STIC 1116

Procedimiento de Empleo Seguro
Microsoft Entra ID

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:23:53 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. Microsoft Entra ID es una solución de gestión de identidades y accesos basada en la nube, que conecta a empleados, clientes y socios a sus aplicaciones, dispositivos y datos.
2. La solución proporciona un acceso adaptable seguro, una forma de proteger el acceso a los recursos y datos mediante una autenticación sólida y políticas de acceso adaptables basadas en el riesgo sin comprometer la experiencia del usuario.
3. Proporciona una experiencia de inicio de sesión rápida y sencilla en todo su entorno multicloud para mantener a sus usuarios productivos, reducir el tiempo de gestión de contraseñas y aumentar la productividad, proporcionando una gestión unificada de identidades, para gestionar todas las identidades y el acceso a todas las aplicaciones en una ubicación central, tanto si están en la nube como on-premises, para mejorar la visibilidad y el control.
4. Para más información sobre la funcionalidad de Microsoft Entra ID se puede consultar la siguiente guía ofrecida por el fabricante, **¿Qué es Microsoft Entra ID? [**REF1]**.**

2 OBJETO Y ALCANCE

5. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft EntraID.

3 ORGANIZACIÓN DEL DOCUMENTO

6. Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
7. Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
8. 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.
9. 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

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

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

4.3 REGISTRO Y LICENCIAS

16. Se requiere la obtención de una licencia de Microsoft 365.
17. Para más información sobre las licencias se puede consultar la guía **Licencias de Microsoft Entra** [REF3].

4.4 CONSIDERACIONES PREVIAS

18. 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

19. El producto consta de los siguientes componentes principales:
    a) Microsoft Entra ID: servicio de gestión de identidades y accesos en la nube que permite administrar usuarios, identidades, credenciales, atributos, autenticación y acceso a recursos protegidos.
    b) Azure Portal: portal de gestión utilizado por los administradores autorizados para acceder a las funciones de administración del producto.
    c) API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
20. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    a) Azure Portal: acceso al portal de gestión.
    b) Azure Gateway: equilibrador de carga de tráfico web.
    c) Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.

d) Azure Monitor Activity Log: registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción.
e) Azure Storage: solución de almacenamiento en la nube.

5 FASE DE INSTALACIÓN

21. En este apartado se describe la implementación del producto. Consta de los siguientes pasos:

    a) Alta del servicio en Microsoft Azure.
    b) Activación de Microsoft Entra ID.

5.1 ALTA DEL SERVICIO EN LA NUBE

22. Al tratarse de un servicio en la nube, se requiere el alta en la plataforma de Microsoft Entra ID mediante la adquisición de la suscripción correspondiente y la asignación de un usuario autorizado para el acceso inicial al servicio.

23. Una vez dado de alta el servicio, los usuarios autorizados podrán acceder al portal y proceder a la activación y configuración de Microsoft Entra ID conforme a los permisos asignados.

5.2 ACTIVACIÓN MICROSOFT ENTRA ID

24. El proveedor proporciona documentación acerca de los primeros pasos con Microsoft Entra ID en la guía **Inicio rápido: Creación de un nuevo inquilino en Microsoft Entra ID** [REF14].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

25. 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 guía **¿Qué es el centro de Administración de Microsoft Entra ID?** [REF4]**.**
26. 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 Microsoft Entra ID antes de cualquier interacción con el producto.
27. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft 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

28. Los mecanismos de autenticación de Microsoft Entra ID incluyen autenticación basada en contraseñas, autenticación multifactor (MFA) y métodos de autenticación sin contraseña, como Windows Hello for Business y claves de seguridad FIDO2. Mas detalles en la guía **¿Qué métodos de autenticación y comprobación están disponibles en Microsoft Entra ID?** [REF15].
29. Las políticas de acceso condicional de Microsoft Entra ID se utilizan para aplicar reglas en la asociación inicial de los atributos de seguridad de los usuarios, garantizando que solo se asocien tras una autenticación exitosa bajo condiciones predefinidas.
30. El control de acceso basado en roles (RBAC) gestiona los permisos, asegurando que solo los sujetos autorizados actúen en nombre de los usuarios. Las políticas de RBAC definen los roles y permisos asociados con cada usuario, garantizando que solo los usuarios autenticados puedan tener sus atributos de seguridad asociados a sujetos que actúan en su nombre.
31. Microsoft Entra ID permite definir y gestionar atributos de seguridad personalizados, que pueden asociarse con los usuarios tras una autenticación exitosa, permitiendo un control de acceso más detallado y asegurando que solo los usuarios autenticados tengan sus atributos de seguridad asociados a los sujetos que actúan en su nombre.
32. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF5].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

33. 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.

34. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

35. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

36. El producto utiliza RBAC (Control de Acceso Basado en Roles) para acceder a los recursos. A continuación, se enumeran cuatro roles fundamentales integrados. A continuación, se enumeran los roles integrados utilizados para controlar el acceso a los recursos de Azure relacionados con el producto:

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

37. Estos roles permiten controlar quién tiene permiso para realizar acciones específicas sobre los recursos de Azure relacionados con el producto. Para la asignación de roles se deberá aplicar el principio de mínimo privilegio, concediendo únicamente los permisos necesarios para la función a realizar. Para ampliar la información sobre los roles, se puede consultar la guía **Roles integrados de Microsoft Entra ID [REF7]**.

38. Las sesiones expiran después de un período establecido por el administrador en Microsoft Entra ID. Los valores predeterminados son:

    a) Duración máxima de la sesión: 1440 minutos.
    b) Duración mínima de la sesión: 5.

39. El producto utiliza diferentes mecanismos de seguridad como 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:

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

40. 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 [REF6].**

41. El producto es capaz de administrar las directivas de contraseñas. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Microsoft Entra ID. Los siguientes requisitos de directiva de contraseñas de Microsoft Entra ID se aplican a todas las contraseñas que se crean, cambian o restablecen en Microsoft 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	Un mínimo de 12 caracteres y un máximo de 256.
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

42. Para ampliar la información sobre las políticas de contraseñas, se puede consultar la información proporcionada por el fabricante en el enlace **Directiva de contraseñas combinada y comprobación de si hay contraseñas no seguras en id. de Microsoft Entra** [REF16]**.**

43. Para ampliar la información sobre los roles, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID** [REF7].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

44. La conexión al producto, al tratarse de un servicio en la nube, se realiza mediante HTTPS con TLS1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

45. 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.

46. 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-884** [REF5]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

47. El producto se asegura 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

48. 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

49. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el producto es parte de la infraestructura de Azure.

50. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

51. 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

52. 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

53. El producto genera registros de auditoría clasificados por actividades que son auditadas en la infraestructura Azure, para más información se puede consultar la guía **¿Qué son los registros de auditoría de Microsoft Entra ID?** [REF8]. Puede buscar estos eventos buscando en el registro de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:

a) Inicio y fin de funciones de auditoría. Estas funciones no se aplican ya que se trata de un servicio en la nube y la funcionalidad está siempre activada, y ni el inicio ni el fin se pueden gestionar.

b) Operaciones de gestión de roles como crear/ver/borrar asignaciones de roles y crear/ver/borrar definiciones de roles personalizados.
c) Cambios en la configuración del sistema. Cuando se produce un cambio o modificación en la configuración, se guarda el evento.
d) Proceso de login de personal autorizado: debido a la arquitectura y modo de funcionamiento de la infraestructura Azure, la plataforma utiliza sesiones y no se dispone de un evento específico de cierre de sesión. Las sesiones pueden finalizar por expiración, cierre manual o revocación, quedando registrados los eventos de inicio de sesión y auditoría asociados. Los inicios de sesión (*sign-ins*) se registran con los siguientes estados:
    i. Éxito: Inicio de sesión exitoso.
    ii. Fallo: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.
    iii. Interrumpido: La contraseña del usuario está caducada, y por lo tanto su login o sesión ha finalizado. Cuando se usuario se le pregunta si desea mantenerse con la sesión iniciada en el navegador, para hacer futuros inicios de sesión más sencillos.

54. Eventos relacionados con la funcionalidad del producto:

a) Cambios a usuarios.
b) Cambios a grupos
c) Cambios a aplicaciones
d) Cambios a actividades de seguridad personalizadas

55. El Audit Log se muestra en la página de búsqueda de registros de auditoría.

a) Los resultados de una búsqueda en el Audit Log se muestran con la siguiente información:
b) Fecha: La fecha y hora en que ocurrió el evento.
c) Dirección IP: La dirección IP del dispositivo utilizado durante la actividad registrada. La dirección IP se muestra en formato IPv4 o IPv6.
d) Usuario: El usuario (o cuenta de servicio) que realizó la acción que desencadenó el evento.
e) Actividad: La actividad realizada por el usuario. Este valor corresponde a las actividades que seleccionaste en la lista desplegable de Actividades. Para un evento del Audit Log de Exchange admin, el valor en esta columna es un cmdlet de Exchange.
f) Elemento: El objeto creado o modificado como resultado de la actividad correspondiente. No todas las actividades tienen un valor en esta columna.
g) Detalle: Información adicional sobre una actividad. De nuevo, no todas las actividades tienen un valor.

6.11.2 ALMACENAMIENTO LOCAL

56. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. Se puede acceder a los registros de auditoria mediante el portal de Microsoft Entra ID en la funcionalidad Audit Logs.

6.11.3 ALMACENAMIENTO REMOTO

57. La opción de enviar eventos a un servidor local no está disponible de forma directa. No obstante, el producto permite transmitir la información de auditoría a Azure Log Analytics workspace, Azure Storage y Azure Event Hub mediante TLS 1.2 o TLS 1.3. Para más información, consultar la guía **Configuración de diagnóstico de Microsoft Entra ID** [REF17].

6.11.4 BACKUP

58. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft 365.

7 FASE DE OPERACIÓN

59. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta tanto por el proveedor del servicio, como por la organización cliente.

60. En particular, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:

    a) Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
    b) Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.
    c) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
    d) Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

61. Microsoft Entra ID 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 IMPLEMENTACIÓN DE PROTOCOLOS RADIUS CON EAP-TLS

63. El producto ha implementado los protocolos RADIUS (RFC 2865, RFC 2869) con EAP-TLS (RFC 5216) para manejar las solicitudes de autenticación provenientes de otro componente del entorno, como el Network Access Server (NAS, servidor de acceso a la red).

64. La implementación de estos protocolos permite verificar la corrección e integridad de los paquetes que contienen solicitudes de autenticación de usuarios finales o entidades, asegurando que solo las solicitudes válidas sean procesadas.

65. Este enfoque proporciona una autenticación segura, utilizando el protocolo EAP-TLS para garantizar la validez y protección de los datos transmitidos durante el proceso de autenticación.

66. Para obtener más información sobre la implementación de RADIUS y EAP-TLS, consultar la guía **Autenticación RADIUS** [REF9]**.**

7.2 POLÍTICA DE CONTRASEÑAS Y MFA

67. El producto implementa una política por defecto para evitar contraseñas débiles. Además, está preparado para usar autenticación multifactor (MFA) y acceso condicional.

68. Los siguientes requisitos de política de contraseñas se aplican a todas las contraseñas que se creen, cambien o restablezcan en el producto:

    a) Caracteres permitidos:

i. Caracteres mayúsculas (A - Z)
ii. Caracteres minúsculas (a - z)
iii. Números (0 - 9)
iv. Símbolos: -@#$%^&*-_!+=[]{}|:',.?/`~" ();<>
v. Espacios en blanco

b) Caracteres no permitidos:
i. Caracteres Unicode

c) Longitud de la contraseña:
i. Se requiere un mínimo de doce caracteres
ii. Se permite un máximo de 256 caracteres

d) Complejidad de la contraseña (mínimo tres requisitos):
i. Caracteres mayúsculas
ii. Caracteres minúsculas
iii. Números
iv. Símbolos

e) Contraseñas no recientes:

69. Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser igual a la contraseña actual o a las contraseñas utilizadas recientemente.

70. Además, el producto permite combinar una credencial basada en contraseña con una credencial no basada en contraseña, utilizando Microsoft Authenticator para establecer una autenticación multifactor (MFA). Para entornos ENS ALTA, se recomienda exigir MFA a todos los usuarios, especialmente a administradores y cuentas privilegiadas, mediante las capacidades de MFA y acceso condicional del producto.

71. Para obtener más información sobre las políticas de contraseñas y autenticación multifactor, consultar las guías Autenticación basada en contraseña [REF10], Habilitar autenticación multifactor [REF11].

7.3 MECANISMOS DE SINCRONIZACIÓN DE IDENTIDAD Y CREDENCIALES

72. El producto admite dos mecanismos de trabajo para sincronizar la identidad y las credenciales transmitidas con otros productos:

a) **Microsoft Entra ID Connect Sync**: La provisión se realiza en el servidor de sincronización local, y la configuración se almacena en dicho servidor local.
b) **Microsoft Entra ID Cloud Sync**: La configuración de provisión se almacena en la nube y se ejecuta en la nube como parte del servicio de provisión de Microsoft Entra ID.

73. Para obtener más información sobre los mecanismos de sincronización de identidad y credenciales, consultar la guía **Documentación de identidad híbrida** [REF12].

7.4 ASOCIACIÓN DE ATRIBUTOS DE SEGURIDAD DE USUARIOS

74. El producto hace cumplir las siguientes reglas en la asociación inicial de los atributos de seguridad de los usuarios con los sujetos que actúan en su nombre:

a) Los atributos de seguridad del usuario se asocian solo tras una identificación y autenticación exitosa.
b) Se validan las políticas de acceso condicional.

c) Se validan las listas de control de acceso basadas en roles (RBAC).
d) Se validan los atributos de seguridad personalizados.

75. Estas validaciones aseguran que solo los usuarios autenticados con permisos adecuados puedan tener sus atributos de seguridad asociados a sujetos que actúan en su nombre.

76. Para obtener más información sobre la gestión de atributos de seguridad y el control de acceso, consultar la guía **¿Qué es RBAC de Microsoft Entra ID?** [REF13].

8 REFERENCIAS

77. Indicar documentación que se haya referenciado a lo largo de la guía.

[REF1] ¿Qué es Microsoft Entra ID?
https://learn.microsoft.com/es-es/entra/fundamentals/whatis

[REF2] Microsoft Entra ID
https://entra.microsoft.com/

[REF3] Licencias de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/fundamentals/licensing

[REF4] ¿Qué es el centro de administración de Microsoft Entra ID?
https://learn.microsoft.com/es-es/entra/fundamentals/entra-admin-center

[REF5] 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

[REF6] Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/authentication/howto-password-smart-lockout

[REF7] Roles Integrados de Microsoft Entra ID
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

[REF8] ¿Qué son los registros de auditoría de Microsoft Entra ID?
https://learn.microsoft.com/es-es/entra/identity/monitoring-health/concept-audit-logs

[REF9] Autenticación RADIUS
https://learn.microsoft.com/es-es/entra/architecture/auth-radius

[REF10] Autenticación basada en contraseña
https://learn.microsoft.com/es-es/entra/architecture/auth-password-based-sso

[REF11] Habilitar autenticación multifactor de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/authentication/tutorial-enable-azure-mfa

[REF12] Documentación de identidad híbrida
https://learn.microsoft.com/es-es/entra/identity/hybrid/

[REF13] ¿Qué es RBAC de Microsoft Entra ID?
https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/custom-overview

[REF14] Inicio rápido: Creación de un nuevo inquilino en Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/fundamentals/create-new-tenant

[REF15] ¿Qué métodos de autenticación y comprobación están disponibles en Microsoft Entra ID?
https://learn.microsoft.com/es-es/entra/identity/authentication/concept-authentication-methods

[REF16] Directiva de contraseñas combinada y comprobación de si hay contraseñas no seguras en id. de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/authentication/concept-password-ban-bad-combined-policy

[REF17] Configuración de diagnóstico de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/monitoring-health/howto-configure-diagnostic-settings

9 ABREVIATURAS

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
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ENS	Esquema Nacional de Seguridad.
FIDO2	Fast Identity Online 2
HTTPS	Secure Hyper Text Transfer Protocol.
ID	Identity
IM	Identity Management
MFA	Autenticación Multifactor.
NAS	Network Access Server
NTP	Network Time Protocol.
RADIUS	Remote Authentication Dial-In User Service
RBAC	Control de Acceso Basado en Roles.
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security.
WAF	Firewall de Aplicación Web