Identity and Access Management

30, 60, 90 días

AZURE IDENTITY MANAGEMENT

KS - Consulting Services

Una infraestructura de identidad bien planificada e implementada prepara el camino para un acceso seguro a sus recursos de trabajo y datos de productividad solo para usuarios y dispositivos conocidos y de confianza.

Puede parecer todo un reto implementar un esquema completo de Azure Active Directory (Azure AD) para su organización, en términos de Identidad, Accesos y mantenerlo Seguro. Nuestra propuesta identifica las tareas comunes que los clientes encuentran útiles para implementar en fases, en el transcurso de **30, 60, 90 días, o más**, para robustecer su estrategia de seguridad. Incluso las organizaciones que ya han implementado Azure AD pueden recurrir a éste ofertamiento para asegurarse de que están sacando el máximo provecho de su inversión.

KS Consulting realiza las siguientes tareas como parte de éste ofertamiento:

Casos de Uso

El alcance final a ejecutar depende de los casos de uso de definir con el cliente, considerando las siguientes capacidades de Identity and Access Management.

1. Aprovisionamiento desde aplicaciones HR y hacia plataformas en lal Nube.
2. Tratar la identidad como el perímetro de seguridad principal.
3. Centralizar la gestión de identidades.
4. Administrar invitados (guest) conectados.
5. Single-Sign On.
6. Acceso Condicional.
7. Mejoras de Seguridad rutinarias.
8. Administración de Contraseñas.
9. Forzar MFA para usuarios.
10. Control de acceso basado en roles (RBAC).
11. Menor exposición de Cuentas Privilegiadas.
12. Administrar Ubicaciones Recursos.

Estrategia de Implementación:

Las mejores prácticas sugieren tomar una estrategia de Administración de Identidades y Accesos, considerando el siguiente Roadmap Funcional:

1. Construcción de una Base de Seguridad.
    a. Privileged Identity Management para seguimiento al rol de Administrador.

   b. Self-Service Password Reset.
   c. Azure AD Password Protection.
   d. Smart Lockout de Azure Active Directory.
   e. Smart Lockout de extranet para AD FS.
   f. Azure AD Multi-Factor Authentication con Directivas de Acceso Condicional.
   g. Azure AD Identity Protection.
   h. Detecciones de riesgo para activar la MFA y Cambios de Contraseña
   i. Registro Combinado para SSPR y Azure AD MFA.
2. Importación de Usuarios, Habilitación de la Sincronización, y Administración de Dispositivos.
   a. Azure AD Connect.
   b. Password Hash Sync.
   c. Password Writeback.
   d. Azure AD Connect Health.
   e. Asignacion de licencias a Usuarios por Membresía de Grupo en AAD.
   f. Planear Acceso a Usuarios tipo Guest.
   g. Decidir una estrategia Device Management.
   h. Windows Hello for Business.
   i. Métodos Passwordless Authentication para usuarios.
3. Administración de Aplicaciones.
   a. Identificar tus Aplicaciones.
   b. Integrar aplicaciones SAAS soportadas.
   c. UtilizarApplication Proxy para Integrar Aplicaciones on-premises.
4. Auditoría de las Identidades Privilegiadas, Configuracion de Revisión de Accesos, y Administración del Ciclo de Vida del Usuario.
   a. Forzar el Uso de Privileged Identity Management.
   b. Completar Access Review para AAD Directory Roles en PIM.
   c. Implementar políticas de Membresía Dinámica de Grupos.
   d. Implementar Aprovisionamiento de Aplicaciones Basadas en Grupo.
   e. Automatizar User Provisioning y Deprovisioning.

La implementación final se realizará de acuerdo a la Definición del Alcance, considerando los Casos de Uso a Implementar.

Timeline Operativo

Con base al Alcance Definido, se tomará la Estrategia de Implementación adecuada, y se ejecutará en fases, de acuerdo al siguiente modelo operativo:

- Fase 1: Workshop, Análisis y Diseño.
- Fase 2: Habilitación de Plataformas.
- Fase 3: Configuración de Herramientas.
- Fase 4: Pruebas y Control de Calidad.
- Fase 5: Transferencia de Conocimientos.
- Fase 6: Go-Live.

El tiempo final de implementación se encuentra sujeto a Alcance:

- Básico: 30 días hábiles.
- Intermedio: 60 días hábiles.
- Avanzado: 90 días hábiles, o más.

Herramientas Tecnológicas

- Identity and Access Management.
- Single Sign-On.
- Reverse proxy.
- Multi-Factor Authentication.
- Azure RBAC.
- Supervisión de seguridad, alertas e informes basados en aprendizaje automático.
- Gestión de Identidad y Accesos para Consumidor (B2C).
- Registro de Dispositivos.
- Privileged Identity Management.
- Identity protection.
- Hybrid identity management/Azure AD connect.
- Revisiones de acceso a Azure AD.
- Identidad Segura.
- Aplicativos y Datos Seguros.

Mayor Información:

CONTENIDO

Identity and Access Management

La administración de identidades es el proceso de autenticación y autorización de entidades de seguridad. También implica controlar la información sobre esas entidades principales (identidades). Las entidades de seguridad (identidades) pueden incluir servicios, aplicaciones, usuarios, grupos, etc. Las soluciones de administración de acceso e identidad de Microsoft ayudan a TI a proteger el acceso a aplicaciones y recursos en el centro de datos corporativo y en la nube. Esta protección permite niveles adicionales de validación, como directivas multifactor de autenticación y acceso condicional. La supervisión de actividades sospechosas a través de informes de seguridad avanzados, auditorías y alertas ayuda a mitigar posibles problemas de seguridad. Azure Active Directory Premium proporciona inicio de sesión único (SSO) a miles de aplicaciones de software como servicio (SaaS) en la nube y acceso a las aplicaciones web que se ejecutan localmente.

Al aprovechar las ventajas de seguridad de Azure Active Directory (Azure AD), puede:

- Crear y administrar una única identidad para cada usuario en su empresa híbrida, manteniendo sincronizados los usuarios, grupos y dispositivos.
- Proporcionar acceso único (SSO) a sus aplicaciones, incluidas miles de aplicaciones SaaS preintegradas.
- Habilitar la seguridad de acceso a aplicaciones aplicando Multi-Factor Authentication basada en reglas para aplicaciones locales y en la nube.
- Aprovisionar acceso remoto seguro a aplicaciones web locales a través del Azure AD Application Proxy.

A continuación, se muestran las capacidades principales de **Azure Identity Management**:

1. Single Sign-On.
2. Reverse proxy.
3. Multi-Factor Authentication.
4. Azure role-based access control (Azure RBAC).
5. Supervisión de seguridad, alertas e informes basados en aprendizaje automático.
6. Gestión de Identidad y Accesos para Consumidor.
7. Registro de dispositivos.
8. Privileged Identity Management.
9. Identity protection.
10. Hybrid identity management/Azure AD connect.
11. Revisiones de Acceso a Azure AD.

Single Sign-On

SSO significa poder acceder a todas las aplicaciones y recursos que necesita para hacer negocios, iniciando sesión una sola vez con una sola cuenta de usuario. Una vez que haya iniciado sesión, puede acceder a todas las aplicaciones que necesita sin necesidad de autenticarse (por ejemplo, escriba una contraseña) una segunda vez.

Los usuarios no solo no tienen que administrar varios conjuntos de nombres de usuario y contraseñas, sino que también pueden aprovisionar o des-aprovisionar el acceso a las aplicaciones automáticamente, en función de sus grupos organizativos y su estado de empleado. Azure AD presenta controles de seguridad y de gobierno de acceso con los que puede administrar de forma centralizada el acceso de los usuarios en todas las aplicaciones SaaS.

Reverse proxy

Azure AD Application Proxy le permite publicar aplicaciones locales, como sitios de SharePoint, Outlook Web App y aplicaciones basadas en IIS dentro de la red privada y proporciona acceso seguro a los usuarios fuera de la red. Proxy de aplicación proporciona acceso remoto y SSO para muchos tipos de aplicaciones web locales con las miles de aplicaciones SaaS que admite Azure AD. Los empleados pueden iniciar sesión en sus aplicaciones desde casa en sus propios dispositivos y autenticarse a través de este proxy basado en la nube.

Multi-Factor Authentication

Azure Multi-Factor Authentication es un método de autenticación que requiere el uso de más de un método de verificación y agrega una segunda capa crítica de seguridad a los inicios de sesión y transacciones de los usuarios. Multi-Factor Authentication ayuda a proteger el acceso a datos y aplicaciones mientras satisface la demanda de los usuarios de un proceso de inicio de sesión sencillo. Ofrece una autenticación segura a través de una amplia gama de opciones de verificación: llamadas telefónicas, mensajes de texto o notificaciones de aplicaciones móviles o códigos de verificación y tokens OAuth de terceros.

Azure RBAC

Azure RBAC es un sistema de autorización creado en Azure Resource Manager que proporciona una administración de acceso detallada de los recursos de Azure. RBAC de Azure le permite controlar de forma granular el nivel de acceso que tienen los usuarios. Por ejemplo, puede limitar a un usuario a administrar solo redes virtuales y a otro usuario para administrar todos los recursos de un grupo de recursos. Azure incluye varios roles integrados que puede usar. A continuación, se enumeran cuatro roles integrados fundamentales. Los tres primeros se aplican a todos los tipos de recursos.

1. **Propietario**: tiene acceso completo a todos los recursos, incluido el derecho a delegar el acceso a otros.
2. **Colaborador**: puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
3. **Lector**: puede ver los recursos de Azure existentes.
4. **Administrador de acceso de usuario**: permite administrar el acceso de los usuarios a los recursos de Azure.

Supervisión de seguridad, alertas e informes basados en aprendizaje automático

La supervisión de seguridad, las alertas y los informes basados en aprendizaje automático que identifican patrones de acceso incoherentes pueden ayudarle a proteger su negocio. Puede usar los informes de acceso y uso de Azure AD para obtener visibilidad de la integridad y la seguridad del directorio de su organización.

Con esta información, un administrador de directorios puede determinar mejor dónde podrían estar los posibles riesgos de seguridad para que puedan planificar adecuadamente esos riesgos.

En Azure Portal, los informes se clasifican en las siguientes categorías:

- **Informes de anomalías**: contienen eventos de inicio de sesión que hemos encontrado anómalos. Nuestro objetivo es hacerle consciente de dicha actividad y permitirle determinar si un evento es sospechoso.
- **Informes de aplicaciones integradas**: proporcione información sobre cómo se usan las aplicaciones en la nube en su organización. Azure AD ofrece integración con miles de aplicaciones en la nube.
- **Informes de errores**: indique los errores que pueden producirse al aprovisionar cuentas en aplicaciones externas.
- **Informes específicos del usuario**: muestra los datos de actividad de inicio de sesión del dispositivo para un usuario específico.
- **Registros de actividad**: contienen un registro de todos los eventos auditados en las últimas 24 horas, los últimos 7 días o los últimos 30 días, y los cambios de actividad de grupo y la actividad de restablecimiento y registro de contraseñas.

Gestión de Identidad y Accesos para Consumidor

Azure AD B2C es un servicio de administración de identidades global de alta disponibilidad para aplicaciones orientadas al consumidor que se escala a cientos de millones de identidades. Se puede integrar a través de plataformas móviles y web. Los consumidores pueden iniciar sesión en todas sus aplicaciones a través de experiencias personalizables mediante el uso de sus cuentas sociales existentes o mediante la creación de nuevas credenciales.

En el pasado, los desarrolladores de aplicaciones que querían registrar clientes e iniciar sesión en sus aplicaciones habrían escrito su propio código. Y habrían utilizado bases de datos o sistemas locales para almacenar nombres de usuario y contraseñas. Azure AD B2C ofrece a su organización una mejor manera de integrar la administración de identidades de consumidor en las aplicaciones con la ayuda de una plataforma segura basada en estándares y un gran conjunto de directivas extensibles.

Cuando utiliza Azure AD B2C, los consumidores pueden registrarse en sus aplicaciones mediante sus cuentas sociales existentes (Facebook, Google, Amazon, LinkedIn) o mediante la creación de nuevas credenciales (dirección de correo electrónico y contraseña, o nombre de usuario y contraseña).

Registro de Dispositivos

El registro de dispositivos de Azure AD es la base para escenarios de acceso condicional basados en dispositivos. Cuando se registra un dispositivo, el registro de dispositivos de Azure AD proporciona al dispositivo una identidad que usa para autenticar el dispositivo cuando un usuario inicia sesión. El dispositivo autenticado y los atributos del dispositivo se pueden usar para aplicar directivas de acceso condicional para las aplicaciones hospedadas en la nube y local.

Cuando se combina con una solución de administración de dispositivos móviles como Intune, los atributos de dispositivo de Azure AD se actualizan con información adicional sobre el dispositivo. A continuación,

puede crear reglas de acceso condicional que apliquen el acceso desde los dispositivos para cumplir con sus estándares de seguridad y cumplimiento.

Privileged Identity Management

Con Azure AD Privileged Identity Management, puede administrar, controlar y supervisar sus identidades con privilegios y el acceso a los recursos de Azure AD, así como a otros servicios en línea de Microsoft, como Microsoft 365 y Microsoft Intune.

Los usuarios a veces necesitan realizar operaciones con privilegios en recursos de Azure o Microsoft 365, o en otras aplicaciones SaaS. Esta necesidad a menudo significa que las organizaciones tienen que proporcionar a los usuarios acceso con privilegios permanentes en Azure AD. Este tipo de acceso es un riesgo de seguridad creciente para los recursos hospedados en la nube, ya que las organizaciones no pueden supervisar suficientemente lo que los usuarios están haciendo con sus privilegios de administrador. Además, si una cuenta de usuario con acceso con privilegios se ve comprometida, esa infracción podría afectar a la seguridad general de la nube de la organización. Azure AD Privileged Identity Management ayuda a mitigar este riesgo.

Con Azure AD Privileged Identity Management, puede:

1. Ver qué usuarios son administradores de Azure AD.
2. Habilitar el acceso administrativo a petición y Just-In-Time (JIT) a servicios de Microsoft como Microsoft 365 e Intune.
3. Obtener informes sobre el historial de acceso de administrador y los cambios en las asignaciones de administrador.
4. Recibir alertas sobre el acceso a un rol con privilegios.

Identity protection

Azure AD Identity Protection es un servicio de seguridad que proporciona una vista consolidada de las detecciones de riesgos y las posibles vulnerabilidades que afectan a las identidades de la organización. Identity Protection aprovecha las funcionalidades existentes de detección de anomalías de Azure AD, que están disponibles a través de los informes de actividad anómala de Azure AD. Identity Protection también introduce nuevos tipos de detección de riesgos que pueden detectar anomalías en tiempo real.

Hybrid identity management/Azure AD connect

Las soluciones de identidad de Microsoft abarcan capacidades locales y basadas en la nube, lo que crea una identidad de usuario única para la autenticación y autorización en todos los recursos, independientemente de la ubicación. A esto lo llamamos identidad híbrida. Azure AD Connect es la herramienta de Microsoft diseñada para cumplir y lograr sus objetivos de identidad híbrida. Esto le permite proporcionar una

identidad común para los usuarios para las aplicaciones de Microsoft 365, Azure y SaaS integradas con Azure AD. Proporciona las siguientes características:

- Sincronización.
- AD FS e integración de federación.
- Pasar a través de la autenticación.
- Vigilancia de la salud.

Revisiones de acceso a Azure AD

Las revisiones de acceso de Azure Active Directory (Azure AD) permiten a las organizaciones administrar de forma eficaz las pertenencias a grupos, el acceso a aplicaciones empresariales y las asignaciones de roles con privilegios.

Identidad Segura

Microsoft utiliza múltiples prácticas y tecnologías de seguridad en sus productos y servicios para administrar la identidad y el acceso.

- **Multi-Factor Authentication** requiere que los usuarios usen varios métodos para el acceso, local y en la nube. Proporciona una autenticación sólida con una gama de opciones de verificación fáciles, al tiempo que acomoda a los usuarios con un proceso de inicio de sesión simple.
- **Microsoft Authenticator** proporciona una experiencia de autenticación multifactor fácil de usar que funciona con cuentas de Microsoft Azure Active Directory y Microsoft, e incluye compatibilidad con dispositivos portátiles y aprobaciones basadas en huellas dactilares.
- **Password policy enforcement** aumenta la seguridad de las contraseñas tradicionales mediante la imposición de requisitos de longitud y complejidad, rotación periódica forzada y bloqueo de cuenta después de intentos fallidos de autenticación.
- **Token-based authentication** habilita la autenticación a través de Azure Active Directory.
- **Azure role-based access control (Azure RBAC)** le permite conceder acceso en función del rol asignado por el usuario, lo que facilita proporcionar a los usuarios solo la cantidad de acceso que necesitan para realizar sus tareas de trabajo. Puede personalizar RBAC según el modelo de negocio y la tolerancia al riesgo de su organización.
- **Integrated identity management (hybrid identity)** le permite mantener el control del acceso de los usuarios a través de centros de datos internos y plataformas en la nube, creando una identidad de usuario único para la autenticación y autorización a todos los recursos.

Aplicativos y Datos Seguros

Azure Active Directory, una solución integral en la nube de administración de identidades y acceso, ayuda a proteger el acceso a los datos en las aplicaciones en el sitio y en la nube, y simplifica la administración de usuarios y grupos. Combina los servicios de directorio principales, la gobernanza avanzada de identidades,

la seguridad y la administración del acceso a aplicaciones, y facilita a los desarrolladores la creación de administración de identidades basada en directivas en sus aplicaciones. Para mejorar Azure Active Directory, puede agregar funcionalidades de pago mediante las ediciones Basic, Premium P1 y Premium P2 de Azure Active Directory.

- **Cloud App Discovery** es una característica premium de Azure Active Directory que le permite identificar las aplicaciones en la nube que usan los empleados de su organización.
- **Azure Active Directory Identity Protection** es un servicio de seguridad que usa las capacidades de detección de anomalías de Azure Active Directory para proporcionar una vista consolidada de las detecciones de riesgos y vulnerabilidades potenciales que podrían afectar a las identidades de su organización.
- **Azure Active Directory Domain Services** le permite unir máquinas virtuales de Azure a un dominio sin necesidad de implementar controladores de dominio. Los usuarios inician sesión en estas máquinas virtuales con sus credenciales corporativas de Active Directory y pueden acceder sin problemas a los recursos.
- **Azure Active Directory B2C** es un servicio de gestión de identidades global de alta disponibilidad para aplicaciones orientadas al consumidor que puede escalar a cientos de millones de identidades e integrarse en plataformas móviles y web. Sus clientes pueden iniciar sesión en todas sus aplicaciones a través de experiencias personalizables que usan cuentas de redes sociales existentes, o puede crear nuevas credenciales independientes.
- **Azure Active Directory B2B Collaboration** es una solución segura de integración de socios que apoya sus relaciones entre empresas al permitir que los socios accedan a sus aplicaciones corporativas y datos de forma selectiva mediante el uso de sus identidades autogestionadas.
- **Azure Active Directory Join** le permite ampliar las capacidades de la nube a los dispositivos Windows 10 para la administración centralizada. Permite a los usuarios conectarse a la nube corporativa u organizativa a través de Azure Active Directory y simplifica el acceso a aplicaciones y recursos.
- **Azure Active Directory Application Proxy** proporciona SSO y acceso remoto seguro para aplicaciones web hospedadas en el entorno local.