bSide
LET'S GROW TOGETHER

Microsoft
Solutions Partner

AZURE SECURE IAM

LA SEGURIDAD COMO VENTAJA ESTRATÉGICA

LA IDENTIDAD ES EL NUEVO PERÍMETRO

Durante años, protegimos nuestras empresas con firewalls y perímetros físicos. Pero en la era del trabajo remoto y la nube, ese muro ha desaparecido. **Hoy, lo que define si una organización es segura o no, es la gestión de identidades.**

+80%

De los ataques exitosos involucraron **credenciales comprometidas.**

No fue a causa del ~~Firewall~~

No fue a causa del ~~Antivirus~~

Hoy la pregunta ya no es si tenemos firewall o antivirus, la pregunta es: **¿sabemos con certeza quién tiene acceso a qué, dentro de nuestra organización?**

Secure IAM nace precisamente para recuperar el control del acceso digital del negocio.

99.9%

De los ataques basados en contraseñas se pueden prevenir con MFA correctamente implementado.

¿QUÉ PASA SIN UN MODELO IAM ROBUSTO?

En la mayoría de las organizaciones encontramos el mismo patrón no importa si tienen 200 o 200,000 usuarios.

Cuentas Huérfanas

Ex-empleados con acceso activo semanas o meses después de su salida.

Privilegios Excesivos

Usuarios con más permisos de los necesarios, ampliando la superficie de ataque.

Provisión Manual

Procesos lentos, inconsistentes y sin trazabilidad. El equipo de TI es el cuello de botella.

Visibilidad Nula

Sin logs centralizados ni alertas. Los incidentes se detectan semanas después.

Sin MFA en Accesos Críticos

Credenciales como único factor. Un phishing basta para comprometer la organización.

Cumplimiento en Riesgo

Auditorías de ISO 27001, SOX, NIST se convierten en proyectos de emergencia.

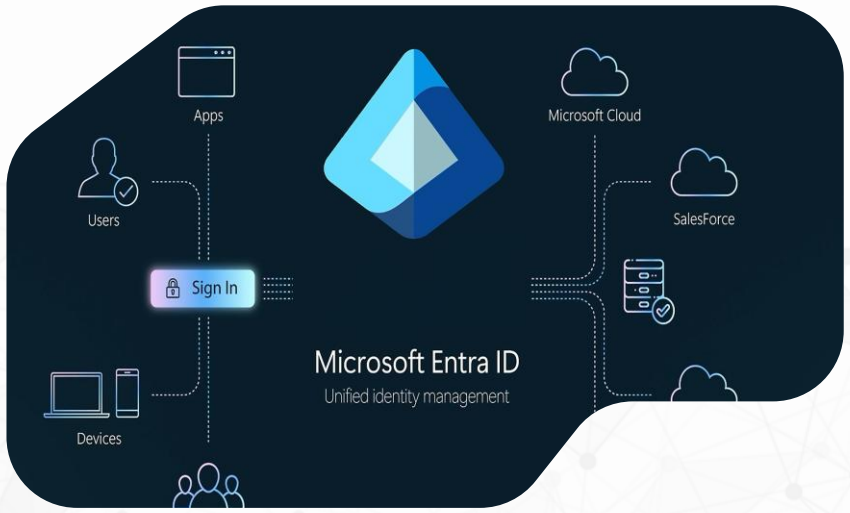
El problema es que cada acceso innecesario es una puerta abierta. Y muchas veces el riesgo es invisible... hasta que ocurre el incidente.

Pero este no es un problema técnico, es un problema de gobierno y tiene solución.

SECURE IAM, NUESTRO FRAMEWORK DE TRABAJO

El framework de las 4 A’s de la identidad está diseñado para operar, escalar y gobernar identidades de forma segura en entornos híbridos y en la nube.

Nuestro modelo proporciona una estructura clara y operativa para transformar la gestión de identidades en una capacidad estratégica automatizada y auditable; construida sobre **Microsoft Entra ID y alienada con la arquitectura Zero Trust.**



Las 4 As de la identidad:

ADMINISTRACIÓN

Automatizamos el ciclo de vida completo de cada identidad, desde el alta hasta la baja, sin intervención manual.

AUTENTICACIÓN

Verificamos que quien accede es realmente quien dice ser, con MFA, biometría y acceso adaptativo.

AUTORIZACIÓN

Aplicamos el principio de mínimo privilegio, con accesos temporales, just-in-time y completamente trazables.

AUDITORÍA

Todo queda registrado, correlacionado y disponible como evidencia.

SERVICIOS AZURE SECURE IAM

ADMINISTRACIÓN

Garantiza que cada identidad exista durante el tiempo necesario, con los atributos correctos y accesos alineados a su función.

Beneficio al negocio:

Reduce cuentas huérfanas, errores manuales y riesgos de acceso indebido.

Servicios:

- Aprovisionamiento automatizado de identidades
- Decomiso inmediato (Joiner-Mover-Leaver)
- Gestión dinámica de grupos
- Recertificación periódica de accesos

AUTENTICACIÓN

Verifica que la identidad que solicita el acceso es legitima aplicando autenticación resistente a ataques y ajustados al nivel de riesgo.

Beneficio al negocio:

Reducción del 99.9% en compromisos de cuentas por phishing.

Servicios:

- Autenticación multifactor centralizada
- Autenticación sin contraseñas
- Autenticación adaptativa basada en riesgos
- Detección de identidades comprometidas y anomalías

AUTORIZACIÓN

Asegura que cada identidad, humana o no humana, cuente únicamente con los permisos necesarios para su función.

Beneficio al negocio:

Reducción del 70%-80% en privilegios excesivos y eliminación de accesos innecesarios.

Servicios:

- Control de accesos basado en roles (RBAC)
- Control de accesos basado en atributos (ABAC)
- Gestión de privilegios con enfoque Just-in-Time (PIM)
- Segregación de funciones (SoD)

AUDITORÍA

Mantiene un registro de las identidades y accesos para detección de amenazas y demostración de cumplimiento.

Beneficio al negocio:

Reducción del 80% en tiempos de respuesta ante incidentes y aprobación expedita de auditrías.

Servicios:

- Loggin centralizado de eventos de identidad
- Retención extendida y análisis retrospectivo
- Alertas de seguridad en tiempo real
- Dashboards y reportes de cumplimiento

MICROSOFT ZERO TRUST ARCHITECTURE

SERVICIOS AZURE SECURE IAM

ADMINISTRACIÓN

Tecnología por capacidad crítica

- **Entra ID Lifecycle + Graph API**
  Aprovisionamiento automatizado
- **Entra Connect**
  Decomiso inmediato (Joiner-Mover-Leaver)
- **Entra ID Acess Reviews**
  Recertificación periódica de accesos

Licencia adquirida:
Entra ID P1, P2

AUTENTICACIÓN

Tecnología por capacidad crítica

- **Entra ID MFA**
  Autenticación multifactor centralizada
- **Conditional Access**
  Autenticación sin contraseñas
- **Entra ID Protection**
  Autenticación adaptativa basada en riesgos
- **Defender for Identity**
  Detección de identidades comprometidas y anomalías

Licencia adquirida:
Entra ID P1, P2, Microsoft 365 E5

AUTORIZACIÓN

Tecnología por capacidad crítica

- **Azure RBAC**
  Control de accesos basado en roles (RBAC) y en atributos (ABAC)
- **Entra PIM**
  Gestión de privilegios con enfoque Just-in-Time (PIM)
- **Microsoft Defender for Cloud Apps**
  Segregación de funciones (SoD)

Licencia adquirida:
Entra ID P1, P2, Microsoft 365 E5

AUDITORÍA

Tecnología por capacidad crítica

- **Entra ID Audit Logs**
  Loggin centralizado de eventos de identidad
- **Azure Monitor Log Analytics**
  Retención extendida y análisis retrospectivo
- **Microsoft Sentinel**
  Alertas de seguridad en tiempo real
- **Purview Advanced Audit**
  Dashboards y reportes de cumplimiento

Licencia adquirida:
Entra ID P1, Azure Subscription, Microsoft 365 E5

MICROSOFT ZERO TRUST ARCHITECTURE

PAQUETES SECURE IAM, EVOLUCIÓN SEGÚN MADUREZ

Cada etapa construye sobre la anterior

IMPACTO AL NEGOCIO

IAM Esencial (Entra ID P1)
Base sólida de control de accesos a la nube

Actividades:
- Diseño y modelo IAM
- Configuración del tenant
- Usuarios, grupos dinámicos
- SSO (SAML, OIDC, Oauth)
- Políticas básicas de Conditional Access
- MFA para roles críticos
- Delegación y documentación operativa

IAM Gobernado (Entra ID P2)
Reduce riesgos de privilegios y accesos

Actividades:
- IAM Esencial
- PIM para roles Entra ID y Azure RBAC
- Just-In-Time con aprobación y duración
- Access Reviews (grupos, apps, roles)
- Conditional Access basado en riesgo
- Reportes y evidencia de auditoría
- Playbooks operativos

IAM Avanzado (Entra ID P2)
Gobernanza completa del ciclo de vida con entornos complejos

Actividades:
- IAM Gobernado
- Entitlement Management completo
- Catálogos y Access Packages
- Gobierno de usuarios externos (B2B)
- Modelo Joiner–Mover–Leaver integrado
- Integración con sistemas RRHH
- KPIs + acompañamiento en auditorías

MADUREZ

Célula Recomendada: Senior Security Architecture + Azure Security Specialist

OFERTA DE VALOR

Una pregunta frecuente es: ¿necesito comprar herramientas nuevas? La respuesta es no. todo lo que implementamos está dentro del ecosistema Microsoft que probablemente ya tienen o están adoptando.

No añadimos complejidad, reducimos la que ya existe. Y al operar sobre plataformas Microsoft nativas, **garantizamos la máxima compatibilidad, el mejor soporte y el menor costo total de propiedad posible.**

Somos:

Especialistas en el stack de Microsoft.

Integramos de manera nativa sin herramientas de terceros.

Implementamos arquitecturas escalables y preparadas para el futuro.

La gestión de identidades ya no es una opción técnica, es una decisión estratégica para la continuidad de su negocio. No esperen a ser parte de la estadística del 80%. Hagamos de la identidad su mayor fortaleza.

bSide
LET'S GROW TOGETHER

Microsoft
Solutions Partner

AZURE SECURE IAM

LA SEGURIDAD COMO VENTAJA ESTRATÉGICA