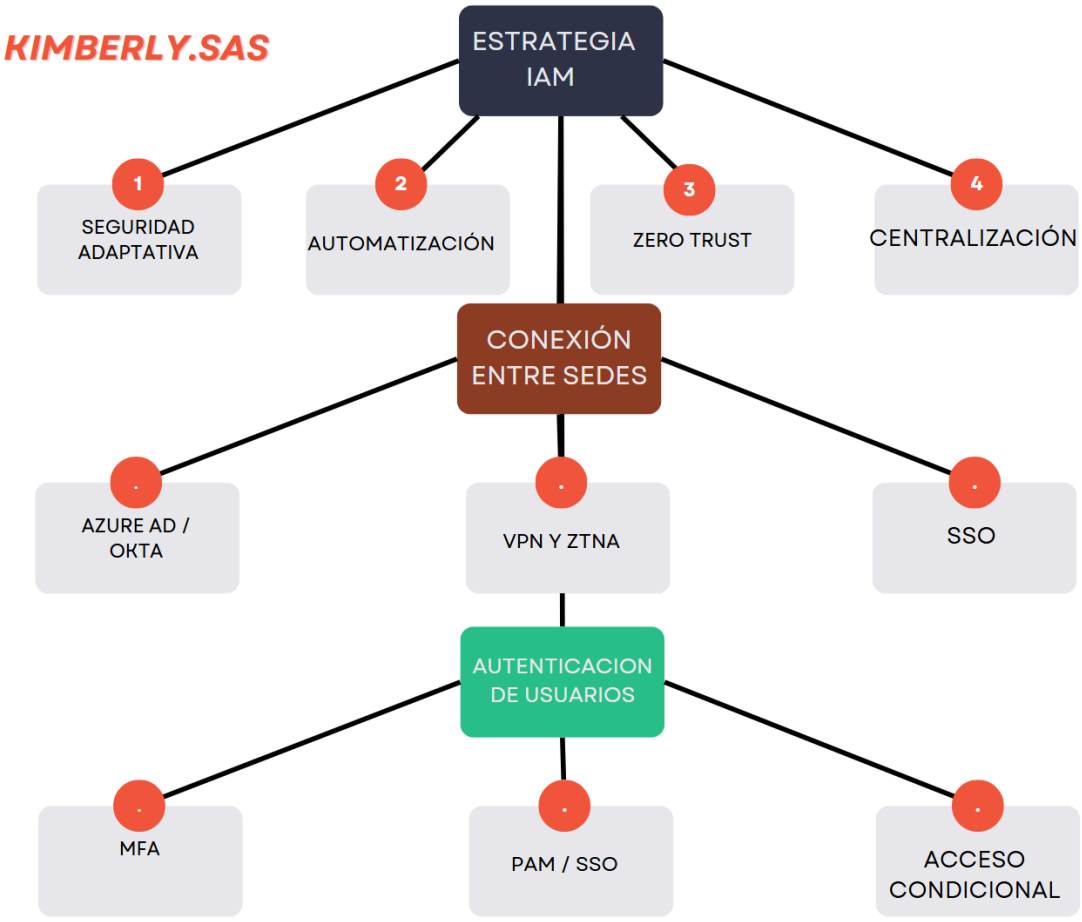
Challenge IAM GOV



Este diagrama de flujo sistematiza los pilares fundamentales para implementar una arquitectura segura en entornos de producción, garantizando robustez, escalabilidad y protección integral principalmente utilizando ZTNA.

1. Estrategia General de IAM

KIMBERLY.sas necesita una estrategia de gestión de identidades y accesos (IAM) bien definida para asegurar que los usuarios accedan solo a lo necesario, minimizando riesgos y cumpliendo con normativas de seguridad. Para lograrlo, se aplicarán los siguientes principios:

- **Centralización**: Todo el control de identidades estará en una única plataforma para facilitar la administración y seguridad. **Esto lo podemos lograr con Azure AD si la compañia define su ecosistema con Microsoft, Google Workspace para el caso de Google o Okta ya que es ideal para entornos multi numbe o SaaS**

- **Zero Trust**: No se confiará en ningún acceso hasta que se haya verificado correctamente. **Esto lo logramos con MFA en el caso de que la centralización se realice con Azure AD es mas sencillo desarrollar políticas de acceso condicional por consiguiente tendría en cuenta Okta ya que ofrece soluciones de MFA, gestión de identidad y acceso, y autenticación adaptativa adicionalmente Cloudflare Access ya que permite definir políticas de acceso granulares y autenticación para aplicaciones basadas en la web, existen muchas msa herramientas y funcionalidades que necesitamos para garantizar el entorno ZTNA sin embargo hago énfasis en los primordiales.**

- **Automatización**: Se reducirán las tareas manuales mediante flujos de trabajo automatizados **desarrollados internamente, o con playbooks y webhooks**.

- **Seguridad Adaptativa**: Los accesos se ajustarán dinámicamente según el contexto y el nivel de riesgo. Para esto es necesario contar con un plan de revisión mensual o semestral para garantizar siempre el principio de menor privilegio.

1.1. Conexión entre sedes

Para garantizar una gestión unificada entre todas las oficinas y sucursales:

- **Azure AD o Okta**: Se usará una federación de directorios para sincronizar usuarios y accesos.

- **VPN y Zero Trust Network Access (ZTNA)**:

    - Se puede implementar **GlobalProtect de Palo Alto** o **Cloudflare Warp** para validar identidades antes de otorgar acceso a la red.

    - Como alternativa, **Fortinet FortiClient VPN** permite acceso seguro y segmentación de red a un bajo costo siempre y cuando se cuente con Firewalls de fortinet y se configuren las ACL correctamente.

- **Single Sign-On (SSO)**: Se configurará en todas las sedes para simplificar la autenticación en aplicaciones empresariales y mantener los audit logs de cada uno de los usuarios y aplicaciones.

- **Firewall Fortinet**: Se establecerán reglas de acceso por ACL para segmentar la red dentro de la LAN y evitar accesos indebidos.

1.2. Autenticación de Usuarios

- **Autenticación Multifactor (MFA)**: Se exigirá en todas las aplicaciones, utilizando **Azure AD MFA**.

- **Single Sign-On (SSO) con OpenID Connect o SAML 2.0** para minimizar múltiples credenciales.

- **Acceso condicional basado en riesgos**: Se aplicarán restricciones con **Azure AD Conditional Access**.

1.3. Autorización de Usuarios

- **Modelo basado en roles (RBAC) y atributos (ABAC)** para definir accesos según funciones organizacionales y contexto.

- **Just-In-Time (JIT) Access con Azure PAM o Admin on Demand** para accesos temporales controlados. **Esto aplica tanto para usuarios como dispositivos**

- **Monitoreo de accesos con XDR de Trend Micro**, generando alertas automáticas en caso de actividades sospechosas y playbooks para la toma de acciones y aislamientos en caso de validar riesgos con criticidad alta.

1.4. Seguridad de Dispositivos

- **Administración con MDM**:
    - **Microsoft Intune** para equipos Windows.
    - **Google Device Mobile** para dispositivos Android.
    - **Mosyle o Jamf** para gestionar dispositivos Apple.

- **Cumplimiento de seguridad antes del acceso**: Se verificará estado de parcheo, antivirus y cifrado con Base Line de condicional access de los MDM y HIP de los agentes de seguridad encargados de validar comportamiento y accesos como **Trend Micro XDR, DLP, Sase, VPN, entre otros**.

- **Autenticación basada en certificados** para dispositivos corporativos con **Azure AD Certificate-Based Authentication** o el licenciamiento de Microsoft cloud defender para habilitar los features de acceso condicional basado en certificado CA en la autenticacion del usuario por SSO.

1.5. Seguridad de Usuarios Administradores

- **Privileged Access Management (PAM) con Azure PIM** para accesos controlados y revisiones periódicas, o como alternativa generar Scripts controlados por los MDM que restrinjan los cambios a los directorios criticos del sistema como el archivo sudoers para sistemas basados en Unix o registros de Windows como HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- **Separación de cuentas administrativas y operativas**. Para esto se crean los usuarios administradores custodiados por ciberseguridad y para uso exclusivo de procesos de configuraciones avanzadas, implementaciones de reglas o forense solicitada, por consiguiente las cuentas operativas las cuales son limitadas en permisos de escritura.

- **Auditoría y monitoreo con XDR de Trend Micro y Qradar, Wazuh, Apex One, entre otras**.

2. Integración de P@yroll

2.1. Componentes Necesarios

- **Federación con IAM central (Azure AD, Okta, etc.)** mediante SAML u OpenID Connect.
- **Single Sign-On (SSO) para P@yroll**.
- **Sincronización de usuarios y roles con Azure AD Provisioning**.
- **Auditoría y logging con XDR de Apex One**.

2.2. Controles de Seguridad en P@yroll

- **RBAC restringido** para limitar accesos a usuarios autorizados.
- **Restricción de accesos según ubicación y dispositivo** con **Azure AD Conditional Access**.
- **Monitoreo de accesos y transacciones con Trend Micro y XDR**.
- **Revisión periódica de accesos automatizados con Azure AD Access Reviews** y azure functions

3. Implementación con Infraestructura como Código

Para agilizar la implementación de esta estrategia y asegurar consistencia en entornos de prueba y producción, se sugiere el uso de **Terraform** para automatizar configuraciones en:

- **Azure AD**: Creación de grupos de seguridad, políticas de acceso condicional y configuraciones de MFA.
- **Firewall Fortinet**: Implementación de reglas ACL para segmentación de red y accesos.
- **VPN con FortiClient**: Despliegue automatizado de túneles VPN seguros.
- **Configuración de SIEM (Qradar, Fortinet FortiSIEM o XDR de Apex One)** para monitoreo centralizado.

Conclusión

Esta estrategia IAM, soportada con herramientas como **Azure AD, Palo Alto GlobalProtect, Fortinet FortiClient, Cloudflare Warp, Trend Micro XDR, y Microsoft Intune y/o Mosyle**, permitirá a KIMBERLY.sas mejorar su seguridad y administración de accesos de manera efectiva y escalable. La automatización con **Terraform** ayudará a mantener un entorno seguro y eficiente con menos intervención manual.