**Challenge IAM**

Estrategia IAM KIMBERLY.sas

Teniendo en cuenta que Kimberly.sas es una empresa que cuenta con más de 100 mil usuarios, múltiples sedes y más de 500 aplicaciones , se requiere implementar una estrategia IAM que garantice la seguridad en la conexión entre sedes, la autenticación, autorización y seguridad de usuarios privilegiados. A continuación, se proponen las siguientes herramientas y procedimientos:,

En primer lugar, respecto a la conexión segura entre sedes, se recomienda la implementación de un IDP centralizado como Azure AD para garantizar el acceso a SSO entre todas las sedes.También es necesario exigir una autenticación para acceder a redes internas mediante la integración de VPN.

Por otro lado, se aconseja realizar una autenticación segura para los usuarios mediante el uso de MFA obligatorio en todas las aplicaciones críticas reduciendo así el riesgo de que credenciales comprometidas sean utilizadas de forma indebida.

También es imprescindible ejecutar una estrategia que asegure la autorización de los accesos. Para ello, se propone el uso de gestión de roles , este permite definir roles por departamento y funciones.Además, la aplicación del principio de mínimo privilegio garantiza que cada usuario reciba únicamente el acceso necesario, así también la revisión periódica de accesos implementando auditorías automatizadas y así poder detectar accesos no justificados.

Por último, respecto a la ejecución de una estrategia para la seguridad de usuarios administradores, se aconseja el uso de cuentas separadas para las tareas administrativas. También la implementación de soluciones como CyberArk para monitorear el acceso privilegiado y el uso de Splunk para auditar quienes reciben los accesos privilegiados.

**Integración de la aplicación “P@yroll”**

La aplicación P@yroll , recientemente adquirida, reveló ser una aplicación crítica para la operación de nómina, por lo que se requiere una estrategia que minimice el impacto para el usuario final y garantice la seguridad del proceso. Para ello, se propone lo siguiente:

Por un lado ,se sugiere delegar la autenticación de P@yroll al proveedor de identidad central ,por ejemplo mediante SSO , utilizando protocolos SAML o OAuth. Esto permitirá a los usuarios del departamento de contabilidad acceder a la aplicación sin necesidad de múltiples credenciales.

Por otro lado, para reforzar la seguridad, se recomienda la implementación de Autenticación Multifactor ,se exigirá MFA para los usuarios de P@yroll, garantizando que solo personal autorizado pueda acceder a la información sensible.

Si bien P@yrool gestiona sus propios usuarios y roles, se sugiere realizar una sincronización con el sistema IAM central para asegurar que las políticas de acceso y privilegios sean consistentes y cumplan con el principio de menor privilegio.

Por último, se recomienda la implementación de medidas de segmentación de red y restricciones de acceso que limiten la disponibilidad de P@yroll únicamente a dispositivos y redes autorizadas. Para esto se configurarán alertas y monitoreo continuo para detectar actividades inusuales o intentos de acceso no autorizados, complementando así la seguridad integral de la aplicación.