REQUERIMIENTOS TECNICOS MINIMOS PARA LA ADQUISICION DE UNA SOLUCION SEGURA QUE PERMITA ADMINISTRAR Y GESTIONAR LOS ACTIVOS MOVILES PARA LA CAJA MAYNAS

1. **REQUERIMIENTO**

CAJA MAYNAS requiere una solución que les permita llevar a cabo la administración y gestión segura de 300 dispositivos móviles de la Caja Maynas.

2. **OBJETO**

CAJA MAYNAS con la adquisición de esta solución, tiene el objetivo de asegurar que los equipos móviles usados por los colaboradores de la institución se puedan administrar de una manera ágil y controlada.

3. **CARACTERISTICAS DE LA SOLUCION:**

Consola de administración

- Los administradores pueden acceder a la solución desde cualquier navegador web, en cualquier parte, simplemente iniciando sesión en la consola basada en Web.
- No es necesario descargar, instalar o configurar software alguno para acceder.
- La interfaz de usuario es simple e intuitiva, lo que permite a los administradores hacer las cosas con el menor esfuerzo y tiempo.
- Los paneles interactivos, filtros avanzando, opciones de búsqueda y las preferencias de usuario personalizables permiten tomar decisiones rápidas.
- La plataforma deberá poder integrarse con un SIEM/SysLOG para monitoreo de incidentes y utilización.

Autenticación de usuarios:

- Integración con AD/LDAP para heredar las políticas de contraseña corporativas o uso de usuarios locales.
- En caso de utilizar usuarios locales propios de la solución, esta debe cumplir con lo siguiente:
  - ✓ Establecer requisitos mínimos de contraseña de administrador a través de la consola.
  - ✓ Definir longitud mínima de contraseña.
  - ✓ Limitar las repeticiones recordando el historial de contraseñas (configurar el número a recordar).
  - ✓ Establecer el periodo de vencimiento de contraseñas (días).
  - ✓ Configurar a nivel de complejidad de la contraseña (alfanumérico, caracteres especiales, etc.)
  - ✓ Definir máximo número de intentos fallidos en un tiempo específico.

Control de acceso basado en roles:

- El control de acceso basado en roles (RBAC) garantiza que solo los usuarios autorizados de la consola puedan ver y administrar los activos de la empresa.
- Utilizar roles integrados y personalizados para definir los grupos de dispositivos a los que un administrador de TI pueda acceder y administrar dentro de la consola y restringir el acceso a la información y las funciones de administración de dispositivos disponibles para cada usuario de la consola.
- Registro de toda actividad de la consola y proporcionar esta actividad en un registro detallado de los usuarios que acceden al sistema. La solución mantiene y muestra esta información a usuarios autorizados para fines de auditoría e informes.

Employee location tacking

- Rastreo de información del estado del dispositivo, incluidas las coordenadas GPS, el estado de cumplimiento, el último registro del dispositivo, la información de conexión, el estado de almacenamiento, etc.
- Ubique, bloquee o limpie los dispositivos perdidos o robados.
  - ✓ Localice dispositivos utilizando el GPS en tiempo real, y el historial de rutas.

- ✓ Identifique dispositivos potencialmente perdidos o robados que no se hayan registrado durante un período de tiempo preestablecido a través de reglas de cumplimiento.
- ✓ Activar sonido de señal para localizar dispositivos."

Servicios de acceso

- La solución debe proveer un acceso a las aplicaciones corporativas indistinto de la ubicación del usuario. Este acceso se realiza mediante un portal de aplicaciones (SaaS, Web, Virtuales, etc.).
- Integración con proveedores de identidad como: Active Directory, Azure Active Ditectory, LDAP, Okta, Ping, etc.
- Habilitar inicio de sesión único (SSO) en aplicaciones y recursos corporativos con proveedores de identidad SAML o generador de tokens.
- Integrarse con proveedores de identidad existente para permitir SSO con aplicaciones publicadas.
- Aplicar políticas de acceso condicional basado por grupo de usuarios, red o tipo de dispositivo para restringir autenticación en aplicaciones corporativas.
- La solución debe proporcionar un método seguro para que aplicaciones instaladas en los dispositivos accedan a recursos corporativo. Mediante un túnel se debe establecer una VPN por aplicación, ofreciendo una autenticación y canal cifrado para el funcionamiento de la aplicación.

Autenticación multifactorial (MFA)

- La solución debe contar con autenticación multifactorial propio, el cual que debe estar integrado mediante una aplicación móvil que muestre un token.
- La solución debe contar o integrarse con autenticación multifactorial para ofrecer una variedad de funciones móviles de MFA que incluyan notificación, código TOTPS, SMS.
- Se debe configurar políticas de autenticación doble factor en las reglas de acceso, para exigir a los usuarios que inicien sesión utilizando la autenticación y luego los números del token, para aplicaciones publicadas desde el catálogo.

Gestión de dispositivos móviles

- La solución debe permitir la administración de dispositivos móviles (Android & iOS), configurando políticas restricciones, correo, WIFI, VPN, etc., en los dispositivos. Todo mediante OTA (Over the air).
- Configuración de modo quiosco en dispositivos móviles Android, presentando aplicaciones únicas o múltiples aplicaciones.
- La solución debe contar con un motor de cumplimiento y monitoreo continuo de los dispositivos, realizando acciones para evitar el incumplimiento y bloqueo automático al acceso a los recursos corporativos, borrando perfiles o dispositivos corporativos.
- Configurar auto borrado en caso de determinado número de fallos de contraseña.
- Instalación, actualización y borrado de aplicaciones en forma remota, así como la capacidad de enviar configuraciones. Esto debe ser realizado en aplicaciones internas y públicas.
- Se debe contar con una lista de aplicaciones permitidas y no permitidas, restringiendo o permitiendo el uso de estas aplicaciones según su condición.
- Integración nativa con Microsoft Exchange, Office 365, Google Apps, brindado un control en el acceso a correo electrónico.
- La plataforma deberá contar con una interfaz segura que permita aplicar adicionar políticas de seguridad a las ya existentes en ActiveSync, como ser encripción de Adjuntos, validación de equipos, cliente de correo, etc.
- En aquellos esquemas donde participen dispositivos que sean propiedad personal de los agentes del CLIENTE (BYOD), el cumplimiento de dichas funcionalidades deberá llevarse a cabo en un ambiente tipo "contenedor" donde el acceso a la información personal debe estar explícitamente restringido.

Reportes:
La solución debe contar con reportes ya establecidos, que permita obtener información de los dispositivos, usuarios, aplicaciones, etc. Estos reportes pueden ser enviados por correo electrónico automáticamente o descargados bajo demanda. Se debe permitir crear reportes personalizados de los dispositivos inscritos en la plataforma, los cuales pueden ser mostrados en gráficos (lineales, barras, circulares, etc.). Estos gráficos deben ser modificables de acuerdo con los requerimientos.

Automatización de procesos con reglas definidas, las cuales deben realizar acciones y enviar notificaciones, de acuerdo con la programación realizada.

Aplicaciones de productividad

- ✓ Integración segura con aplicaciones móviles mediante SDK propio de la solución, permitiendo brindar seguridad, DLP, SSO, tunelización, analítica y mantener privacidad del contenido.

- ✓ Permitir la integración con repositorios locales, WEBDAV, Sharepoint, One Drive, Box y repositorios públicos.
- ✓ Sincronizar archivos de los dispositivos con el repositorio de archivos internos y mantenerlos sincronizados. Evitar DLP (Data Loss Prevention), para la filtración de documentación corporativa.

- ✓ Se debe contar con una aplicación web móvil que permita el acceso a sitios de intranet o páginas web mediante una comunicación segura y contenerizada, incluyendo la posibilidad de restringir funciones.

4. REQUISITOS DEL POSTOR

El POSTOR, deberá ser representante autorizado o partner autorizado de la plataforma ofertada, el cual deberá ser acreditado mediante carta o certificado o constancia o documento del fabricante. Dicho documento deberá ser presentado en la oferta.

Con la finalidad de garantizar la calidad del servicio y el personal idóneo necesario durante el servicio de implementación y post implementación, EL POSTOR, deberá de contar con personal clave con los siguientes perfiles mínimo:

Un (01) Especialista de Implementación:

- Profesional (Bachiller o Titulado) en Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Telecomunicaciones o Ingeniería Electrónica.
- Experiencia mínima de dos (02) años como Ingeniero Especialista en soluciones de virtualización de Aplicaciones, Escritorios y MDM
- Se debe contar con la certificación o especialización oficial del fabricante en la plataforma ofertada**,** en la plataforma a proponer específicamente en lo que respecta al MDM.

5. SOPORTE DEL POSTOR

El POSTOR deberá brindar como parte de su propuesta el soporte al software del fabricante el mismo que será de modo directo con el fabricante no pudiendo aceptar modelos de soporte de tipo colaborativo o solo del partner, con la finalidad de que CAJA MAYNAS tenga los accesos directo a abrir ticket y escalar atenciones con la marca y ser atendidos por un especialista de la marca durante todo el período de cobertura del servicio.

Soporte técnico del postor:

El POSTOR deberá brindar como parte de su propuesta de servicio de soporte a CAJA MAYNAS lo siguiente:

- Entregar un documento donde se consigne la matriz de escalamiento, incluyendo los datos de Contacto para el Soporte Técnico 24x7.
- El reporte de alerta o falla critica que implica el buen funcionamiento de la solución, se hará por medio de correo electrónico o llamada telefónica a la persona de contacto indicado para tal fin.
- La atención del servicio de soporte deberá ser 24x7x365 y por el periodo de 01 año por 60 horas.

Capacitación

El POSTOR deberá brindar como parte de su propuesta capacitación al personal de CAJA MAYNAS en lo siguiente:

- Capacitación y Transferencia de Conocimiento de la solución entregada de 08 horas para hasta 6 personas.

6. OTRAS CONDICIONES DEL SERVICIO

A. PLAZO DE ENTREGA

El plazo de entrega de todos los bienes y Servicio deberá realizarse en un plazo no mayor de 30 días calendarios, para lo cual CMAC MAYNAS brindará todas las facilidades técnicas necesarias.

B. PLAZO DE PRESTACIÓN DEL SERVICIO:

El plazo para la prestación del servicio de Soporte técnico de Fabricante y suscripción licencias será de 1 año.