TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN DE UNA SOLUCIÓN DE GESTIÓN DE ACCESOS PRIVILEGIADOS (PAM)"

1. OBJETIVO

El presente proceso tiene por objetivo la adquisición de una solución de gestión de accesos privilegiados (PAM), que permita controlar, asegurar y monitorear todas las cuentas y actividades que tienen permisos elevados.

2. PLAZO

- **Plazo de implementación**: será de treinta (35) días calendario, computados a partir del día siguiente de la firma del contrato.
- **Plazo de licencia de uso**: Mínimo un año o perpetuo.

3. ALCANCES GENERAL DEL SERVICIO

El servicio debe contar con lo siguiente:

- El modo de licenciamiento deberá ser por usuarios que administren la solución PAM ofertada, permitiendo al menos 10 usuarios administradores y sin límite de equipos a ser gestionados con la solución PAM.
- Debe permitir al menos 25 llaves SSH.
- La plataforma debe ser instalada en modalidad On-premise.
- El proveedor debe encargarse de la Implementación del software, configuración, puesta en marcha y pase a producción.
- Deberá contar además con funcionalidades de integración con Active Directory.

4. CAPACIDADES DE LA SOLUCIÓN:

- La solución debe contar con la posibilidad de crear roles específicos según las necesidades de la organización, dichos role deben permitir configurar la visibilidad, la edición, la gestión, y el uso de las contraseñas de la organización.
- Debe contar con la posibilidad de importar usuarios que administraran la solución PAM desde el directorio activo por medio del protocolo LDAP, asimismo, debe contar con la opción para autenticare en la herramienta por medio del servidor de RADIUS o con la opción para autenticare en la herramienta por medio de SmartCard/PKI/Certificado.
- La herramienta debe permitir realizar el doble factor de autenticación por medio de otras aplicaciones como Google Authenticator, Microsoft Authenticator, RADIUS, seguridad DUo, entre otras.
- La herramienta debe contar con la opción de la creación de un Super-Admin, con acceso a toda la gestión de las contraseñas, recursos, llaves y certificados de la organización.
- La herramienta debe contar con la capacidad de auditar todos los intentos de logon fallidos a la herramienta.
- La herramienta debe contar con la posibilidad de implementar la metodología de Zero Trust (Confianza Cero) para los usuarios y recursos de la herramienta.
- La herramienta debe contar con la posibilidad de realizar el descubrimiento de activos de TI y cuentas privilegiadas.

- La herramienta debe soportar conexiones de tipo RDP, SSH, Telnet, HTTP,HTTPS ,SQL y VNC.
- La solución debe funcionar en entorno basado en web.
- La solución debe contar con la posibilidad de brindar acceso a los recursos (permitir el uso de una contraseña) por un tiempo limitado.
- La solución debe contar con controles propios para implementar la elevación de privilegios para las cuentas locales de Windows y de dominio.
- La solución debe contar con opciones para iniciar sesiones remotas con un solo click, sin la necesidad de revelar las credenciales de acceso en texto plano.
- La solución debe contar con la capacidad de implementar el control de comandos SSH para dispositivos que se conecten por ese medio.
- Se debe tener la opción de grabar todas las conexiones a los recursos gestionados por medio de las sesiones de RDP, SSH, VNC, SQL y HTTPS.
- La solución debe contar con la posibilidad de auditar en tiempo real la sesión de un usuario.
- La solución debe contar con la posibilidad de terminar la sesión de un usuario en caso de detectar actividad sospechosa en su comportamiento o por inactividad.
- La solución debe tener la capacidad de realizar una conexión directa a todos los dispositivos y sitios web gestionados.
- Todas las conexiones realizadas por medio de la herramienta deben ser completamente seguras ante ataques como XSS o Man In the Middle.
- La solución debe contar con la posibilidad de ser un repositorio seguro y centralizado de todas las contraseñas privilegiadas de la organización.
- La solución debe contar con la posibilidad de definir un propietario de la contraseña, encriptar la propia contraseña y con opciones para compartir la contraseña con otros usuarios o grupos de usuarios de la organización.
- La solución debe contar con controles para la aprobación del uso de una contraseña por parte de un usuario.
- La solución debe contar con la posibilidad de acceder a los registros de acceso a todas las contraseñas, es necesario conocer quién, que y cuando se accede a una contraseña o llave SSH.
- La herramienta debe contar con la capacidad de programar reportes de manera periódica y enviadas por correo.
- Debe contar con la posibilidad de exportar reportes en formato PDF, Excel o impreso y reportes de acuerdo a las necesidades.
- La solución debe permitir la gestión de acceso mediante múltiples factores humano, permitiendo que ninguna persona tenga control total sobre una función critica o un activo altamente sensible.

5. SOPORTE

Solución debe incluir el soporte técnico ante incidentes o problemas con la solución:

- Contar con una mesa de ayuda propia para brindar el soporte 24x7, por lo menos un (01) año.

- El postor deberá entregar documento consignando la matriz de escalamiento, incluyendo los datos de Contacto para el soporte técnico.

- El reporte de alerta o falla critica que afecte el buen funcionamiento de la solución, se hará por medio de correo electrónico y de forma inmediata al personal responsable del uso de la herramienta (Administrador de Infraestructura)

- Deberá entregar documento donde evidencie el correcto funcionamiento de la herramienta

- Ante cambios de personal durante el tiempo de soporte debe ser notificado al correo

  incidente_seguridad_operativo@cajamaynas.pe
  infraestructura@cajamamayna.pe

6. CAPACITACIÓN

Se debe ofrecer una capacitación de al menos 8 horas para 11 personas en el uso de la plataforma a nivel usuario para el equipo de TI de la entidad.

7. ENTREGABLES:

- El proveedor deberá entregar un informe final de implementación del servicio, conteniendo lo siguiente: el comprobante o documento que acredite la activación de la licencia de uso y el detalle de las actividades realizadas.
- Manuales en formato digital del uso de la solución.
-

8. FORMA DE PAGO

Es un pago único que se realizará luego que el proveedor culmine con la implementación de la solución, previa conformidad de la Gerencia de Tecnología de la Información.

9. PENALIDADES

En caso el contratista no cumpla con la ejecución de la implementación objeto del contrato dentro del plazo establecido, la Entidad aplicará una penalidad por mora por cada día de atraso. La penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde F tiene los siguientes valores:

- Para los plazos menores o iguales a sesenta (60) días, para bienes, servicios en general y consultorías: F=0.40.

- Para plazos mayores a sesenta (60), para bienes, servicios en general y consultorías: F=0.25.

El monto máximo de la penalidad aplicable no puede exceder el monto máximo del diez por ciento (10%) del monto total contratado. La Entidad tiene el derecho a exigir, además de la penalidad, el cumplimiento de la obligación.

10. CONFIDENCIALIDAD

El proveedor guardará reserva respecto de las actividades y acciones encomendadas, así como de la información privilegiada que le concierne en el ejercicio de su actividad, no revelando en forma oral o escrita, hechos, datos, procedimientos y documentación no autorizada o confidencial de acuerdo a Ley.

11. ACCESO A LA INFORMACIÓN

El proveedor debe facilitar la entrega de cualquier información requerida por la UAI, OCI, SAE, CGR, SBS o cualquier ente de control, relacionado con el ejercicio del presente servicio.