SOLICITUD DE INFORMACIÓN PARA LA ELABORACION DEL ESTUDIO DE MERCADO

El Servicio Nacional de Aprendizaje SENA, de conformidad con los principios de transparencia para la contratación, convoca públicamente a todos los interesados en proporcionar información para consolidar el estudio de mercado del proceso con las siguientes condiciones.

OBJETO	Contratar el soporte técnico especializado, mantenimiento, y actualización del licenciamiento de la solución de gestión de accesos privilegiados (Privileged Access Manager – PAM) del SENA, incluyendo las actividades necesarias para garantizar su operación, estabilidad, seguridad y correcta administración dentro de la infraestructura tecnológica de la entidad.
VALIDEZ DE COTIZACIÓN	La cotización debe tener validez de 90 días calendario, contados a partir de la fecha de presentación de la misma.
FECHA LÍMITE DE RECEPCION DE COTIZACIONES	La cotización debe ser entregada y/o radicada a más tardar el 13 de noviembre de 2026 a las 05:00 p.m.
LUGAR PARA PRESENTAR LA COTIZACIÓN	La cotización debe ser entregada mediante la plataforma SECOP II
TIEMPO DE EJECUCIÒN DEL CONTRATO	Hasta el 31 de diciembre de 2026.
PLAZO DE ACTUALIZACIONES, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO	Un (1) año contado a partir de la activación del licenciamiento.

1. GENERALIDADES.

1.1 OBJETO.

Contratar el soporte técnico especializado, mantenimiento, y actualización del licenciamiento de la solución de gestión de accesos privilegiados (Privileged Access Manager – PAM) del SENA, incluyendo las actividades necesarias para garantizar su operación, estabilidad, seguridad y correcta administración dentro de la infraestructura tecnológica de la entidad.

1.2 OBJETIVO.

El Servicio Nacional de Aprendizaje – SENA es un establecimiento público del orden nacional, dotado de personería jurídica, patrimonio propio e independiente y autonomía administrativa, adscrito al Ministerio del Trabajo, cuya misión consiste en materializar la función estatal de invertir en el desarrollo social y técnico de los trabajadores colombianos. En cumplimiento de dicho mandato constitucional y legal, la Entidad ofrece y ejecuta formación profesional integral orientada a la incorporación y cualificación del talento humano en actividades productivas que contribuyan al desarrollo social, económico y tecnológico del país.

Para la adecuada ejecución de su objeto misional, el artículo 8 del Decreto 249 de 2004 establece las funciones de la Oficina de Sistemas, dentro de las cuales se destacan: (i) asesorar a la Dirección General y a las demás dependencias en la implementación de sistemas, normas y procedimientos de informática; (ii) investigar y evaluar la incorporación de avances tecnológicos; (iii) conceptuar, definir y evaluar necesidades relacionadas con la adquisición, adaptación, desarrollo, custodia, mantenimiento y actualización de bienes y plataformas informáticas; (iv) efectuar seguimiento al desarrollo informático institucional y coordinar los sistemas de información, la sistematización y digitalización de procesos; (v) definir y actualizar plataformas tecnológicas y emitir conceptos técnicos en la adquisición de software y hardware; y (vi) coordinar la definición y aplicación de indicadores de gestión y responder por las metas previstas en los planes y proyectos de la dependencia.

En coherencia con dichas funciones, la estrategia institucional en materia de Tecnologías de la Información y las Comunicaciones (TIC) se orienta a:

- Alinear las TIC con la estrategia organizacional.
- Integrar y robustecer los sistemas de información.
- Fortalecer los servicios de infraestructura tecnológica.
- Promover la apropiación institucional de las TIC.
- Consolidar la función de TI como eje transversal de gobernanza digital.
- Optimizar la eficiencia económica en la gestión tecnológica.

En este contexto, la implementación de una solución de Gestión de Accesos Privilegiados (Privileged Access Management – PAM) constituye un componente crítico del modelo de seguridad digital y gobierno de TI de la Entidad. Un sistema PAM es una tecnología especializada en la administración, control, supervisión y auditoría de cuentas con privilegios elevados (cuentas administrativas o *"superusuarios"*), las cuales poseen la capacidad de modificar configuraciones críticas, acceder a información sensible, instalar o desinstalar componentes, administrar bases de datos y alterar la operación de servidores físicos y virtuales, sistemas operativos y aplicaciones corporativas.

Desde una perspectiva técnica y de gestión del riesgo, la Gestión de Accesos Privilegiados cumple funciones esenciales tales como:

- Custodia segura de credenciales: Almacenamiento cifrado de contraseñas administrativas en bóvedas digitales, evitando su divulgación o uso indebido.
- Control de acceso basado en políticas: Otorgamiento de privilegios bajo el principio de mínimo privilegio y necesidad de conocimiento.
- Trazabilidad integral: Registro detallado de todas las acciones ejecutadas con cuentas privilegiadas.
- Grabación y monitoreo de sesiones: Captura completa, de inicio a fin, de las sesiones administrativas, facilitando auditorías internas y externas.
- Rotación automática de contraseñas: Mitigación del riesgo de accesos no autorizados posteriores a la finalización de contratos o cambios de personal.
- Soporte a procesos de auditoría y cumplimiento normativo: Generación de evidencia verificable frente a estándares de control interno, seguridad de la información y responsabilidad administrativa.

Dada la magnitud de la infraestructura tecnológica del SENA y la participación del personal SENA en actividades que requieren accesos administrativos, la adopción de una solución como Gestión de Accesos Privilegiados (PAM) resulta estratégica para mitigar riesgos de fraude, sabotaje, fuga de información, alteración de datos o indisponibilidad de servicios. Asimismo, fortalece el sistema de control interno, la gestión de incidentes de seguridad y la responsabilidad funcional en el manejo de activos críticos de información.

En el año 2019, el Servicio Nacional de Aprendizaje – SENA, mediante el Contrato No. CO1.PCCNTR.1070203, adquirió una solución tecnológica de seguridad informática, junto con el correspondiente licenciamiento a perpetuidad.

Desde su implementación, dicha solución ha presentado un desempeño satisfactorio, contribuyendo de manera significativa a la implementación y fortalecimiento de controles de seguridad efectivos y eficaces, orientados a la protección de los activos de información de la entidad. En este sentido, la herramienta ha permitido robustecer las capacidades institucionales en materia de gestión de riesgos de seguridad de la información, así como consolidar el Modelo de Seguridad y Privacidad de la Información adoptado por el SENA.

Durante la ejecución del Contrato CO1.PCCNTR.4946663 de 2023, la solución Privileged Access Manager (PAM) se llevó a cabo de manera continua actividades técnicas, operativas y de acompañamiento. Estas acciones se desarrollaron en cumplimiento de las obligaciones contractuales y se ajustaron a los cambios estructurales presentados en la infraestructura tecnológica de la entidad.

La solución PAM constituye un control crítico de seguridad sobre:

- Accesos privilegiados a servidores
- Consolas administrativas
- Portales web críticos
- Cuentas con privilegios elevados sobre infraestructura tecnológica

Suspender o cambiar la solución implicaría:

- Pérdida de trazabilidad histórica de sesiones.
- Desconfiguración de políticas ya definidas.
- Riesgo de exposición de cuentas privilegiadas.
- Necesidad de reentrenamiento del personal técnico.
- Reimplementación completa del modelo de seguridad.

Posteriormente, la migración de infraestructura hacia Oracle Cloud Infrastructure (OCI), derivada de la finalización del servicio con Telefónica, generó impactos operativos que afectaron temporalmente la adopción plena de la herramienta, sin que ello implicara incumplimiento contractual por parte del proveedor. Sin embargo, PAM opera únicamente en ambiente OCI, sin esquema de Disaster Recovery (DR), lo cual representa un riesgo operativo que debe ser mitigado.

Dado que la herramienta ya se encuentra desplegada en OCI, con políticas configuradas y activos sincronizados, se requiere dar continuidad al soporte especializado y acompañamiento técnico certificado para restablecer el esquema del DR y con el fin de fomentar su uso como una herramienta estratégica de ciberseguridad, la opción técnicamente más eficiente y segura es la continuidad con los servicios de soporte, mantenimiento y actualizaciones sobre el licenciamiento con el que cuenta actualmente la entidad, para evitar reprocesos, costos de transición y riesgos de seguridad.

En razón de lo anterior, la Entidad requiere contar con información veraz, técnica y financieramente sustentada que refleje las condiciones actuales del mercado frente a los requerimientos descritos, con el propósito de estructurar una estimación presupuestal objetiva, transparente y ajustada a la realidad económica del servicio.

Lo anterior se enmarca en el cumplimiento del régimen de contratación estatal previsto en la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1510 de 2013 y el Decreto 1082 de 2015, así como de los principios de transparencia, economía, responsabilidad, planeación y selección objetiva. En consecuencia, el presente documento tiene carácter preliminar y estimativo; el alcance definitivo de la prestación de los servicios será definido en los estudios previos, sus anexos y en el respectivo proceso de selección contractual.

1.3 ALCANCE.

La prestación de servicios mencionadas en la sección *"1.1 Objeto"*, incluye todos los aspectos consignados en este documento y se describen a continuación:

DESCRIPCION	CANTIDAD
Renovación del soporte de Licencias de CA PAM - PRIVILEGED ACCESS MANAGER por un (1) año. (Stand alone) Que incluya: 1. Analítica de la gestión de las cuentas privilegiadas. 2. Control, grabación, bóveda de contraseñas y flujos de aprobación.	1190
Renovación del soporte de Licencias para protección de sistemas operativos. Por un (1) año.	197
El servicio de soporte incluye: 1. Servicio de mantenimiento en sitio 7x24 durante un (1) año, prestado por personal especializado del proveedor, para la atención de incidentes críticos, requerimientos operativos y actividades que requieran intervención presencial, garantizando la continuidad y disponibilidad de la plataforma. 2. Gestión y resolución de incidentes. Atención especializada de incidentes funcionales y técnicos reportados por la entidad, incluyendo análisis, diagnóstico, escalamiento y seguimiento hasta su cierre. 3. Gestión, descarga, validación e instalación de actualizaciones, parches de seguridad y nuevas versiones liberadas por el fabricante durante el período de vigencia del licenciamiento, garantizando la estabilidad, seguridad y correcto funcionamiento de la solución. 4. Ejecución de mantenimientos preventivos y correctivos trimestrales para la revisión integral de la plataforma, incluyendo la validación de servicios, configuraciones, rendimiento, integraciones y componentes críticos, con el fin de asegurar su óptima operación y estabilización. 5. Realización de evaluaciones (Assesment) semestrales con una duración mínima de una (1) semana cada una, orientadas a identificar oportunidades de mejora, optimización de procesos, fortalecimiento de controles de seguridad y maximización del aprovechamiento de la solución. Como resultado se entregará un informe ejecutivo y técnico con hallazgos, recomendaciones y plan de acción propuesto. 6. Prestación de servicios de acompañamiento técnico para la implementación de mejores prácticas de administración, operación y gobierno de accesos privilegiados, alineadas con las recomendaciones del fabricante y los requerimientos de la entidad. 7. Realización de jornadas de transferencia de conocimiento presenciales cada cuatro (4) meses, dirigidas al personal designado por la entidad, con	1

una intensidad mínima de dieciséis (16) horas cada una. Adicionalmente, se realizarán sesiones extraordinarias de capacitación cuando se implementen actualizaciones o cambios relevantes que puedan impactar la operación o administración de la plataforma. 8. Cuatro (4) boucher para certificación de producto, con acompañamiento de la experiencia del proponente.	

1.4 LUGAR Y FECHA PARA PRESENTAR LA COTIZACIÓN.

La cotización debe ser entregada y/o radicada a más tardar el día 13 de noviembre de 2026 mediante la plataforma secop II.

1.5 VALIDEZ DE LA COTIZACIÓN.

La cotización debe tener validez de 90 días calendario, contados a partir de la fecha de presentación de la cotización.

1.6 LENGUAJE DE PRESENTACIÓN DE LA INFORMACIÓN.

La cotización debe ser presentada en idioma español, los documentos que son de fabricantes pueden ser presentados en idioma inglés, siendo estos últimos aquellos los publicados oficialmente.

2 REQUERIMIENTOS TÉCNICOS

2.1 GENERALIDADES TÉCNICAS

Las especificaciones técnicas de los servicios requeridos se describen a continuación y serán prestadas por un período de un (1) año, contado a partir de la activación de las licencias en la entidad.

DESCRIPCION	CANTIDAD
Renovación del soporte de Licencias de CA PAM - PRIVILEGED ACCESS MANAGER por un (1) año. (Stand alone) Que incluya: 1. Analítica de la gestión de las cuentas privilegiadas. 2. Control, grabación, bóveda de contraseñas y flujos de aprobación.	1190
Renovación del soporte de Licencias para protección de sistemas operativos. Por un (1) año.	197

El servicio de soporte incluye: 1. Servicio de mantenimiento en sitio 7x24 durante un (1) año, prestado por personal especializado del proveedor, para la atención de incidentes críticos, requerimientos operativos y actividades que requieran intervención presencial, garantizando la continuidad y disponibilidad de la plataforma. 2. Gestión y resolución de incidentes. Atención especializada de incidentes funcionales y técnicos reportados por la entidad, incluyendo análisis, diagnóstico, escalamiento y seguimiento hasta su cierre. 3. Gestión, descarga, validación e instalación de actualizaciones, parches de seguridad y nuevas versiones liberadas por el fabricante durante el período de vigencia del licenciamiento, garantizando la estabilidad, seguridad y correcto funcionamiento de la solución. 4. Ejecución de mantenimientos preventivos y correctivos trimestrales para la revisión integral de la plataforma, incluyendo la validación de servicios, configuraciones, rendimiento, integraciones y componentes críticos, con el fin de asegurar su óptima operación y estabilización. 5. Realización de evaluaciones (Assesment) semestrales con una duración mínima de una (1) semana cada una, orientadas a identificar oportunidades de mejora, optimización de procesos, fortalecimiento de controles de seguridad y maximización del aprovechamiento de la solución. Como resultado se entregará un informe ejecutivo y técnico con hallazgos, recomendaciones y plan de acción propuesto. 6. Prestación de servicios de acompañamiento técnico para la implementación de mejores prácticas de administración, operación y gobierno de accesos privilegiados, alineadas con las recomendaciones del fabricante y los requerimientos de la entidad. 7. Realización de jornadas de transferencia de conocimiento presenciales cada cuatro (4) meses, dirigidas al personal designado por la entidad, con una intensidad mínima de dieciséis (16) horas cada una. Adicionalmente, se realizarán sesiones extraordinarias de capacitación cuando se implementen actualizaciones o cambios relevantes que puedan impactar la operación o administración de la plataforma. 8. Cuatro (4) boucher para certificación de producto, con acompañamiento de la experiencia del proponente.	1

SOPORTE, GARANTÍA Y MANTENIMIENTO

Dada la criticidad de una solución de Gestión de Accesos Privilegiados (PAM) dentro del modelo de seguridad de la información institucional, el esquema de soporte, garantía y mantenimiento deberá asegurar la continuidad operativa, la integridad de las credenciales privilegiadas y la trazabilidad permanente de las sesiones administrativas.

1. Soporte técnico
El servicio deberá contemplar:

- Soporte 7x24 directamente por el fabricante, con acceso a mesa de ayuda especializada, escalamiento a niveles avanzados (L2/L3) y tiempos de respuesta acordes con la criticidad del incidente.
- Soporte en sitio por parte del proveedor, prestado por personal técnico certificado en la solución ofertada y con experiencia comprobable en:

  ✓ Administración de bóvedas de credenciales.
  ✓ Gestión de sesiones privilegiadas (PSM).
  ✓ Integración con servicios de directorio (AD/LDAP).
  ✓ Configuración de políticas de acceso basado en roles (RBAC).
  ✓ Implementación de autenticación multifactor (MFA).
  ✓ Integración con SIEM y herramientas de monitoreo.

El soporte deberá cubrir la totalidad de las configuraciones, personalizaciones e integraciones implementadas en la plataforma.

2. Actualizaciones, parches y nuevas versiones
Durante la vigencia del contrato de suscripción y soporte, se deberá garantizar:

- Derecho a nuevas versiones, actualizaciones mayores y menores, parches de seguridad y hotfixes liberados por el fabricante.
- Instalación y despliegue controlado de dichas actualizaciones en ambientes productivos y, cuando aplique, en ambientes de prueba.
- Validación posterior a la actualización (post-upgrade validation) para asegurar la correcta operación de:

  ✓ Bóveda de contraseñas.
  ✓ Grabación de sesiones privilegiadas.
  ✓ Rotación automática de credenciales.
  ✓ Integraciones con sistemas corporativos.

El mantenimiento deberá cubrir integralmente la solución durante toda la vigencia contractual.

3. Mantenimientos preventivos y revisiones periódicas
Con el fin de garantizar la estabilidad, rendimiento y cumplimiento de buenas prácticas de seguridad:

- Cada cuatro (4) meses se deberá realizar una revisión técnica integral de la plataforma, que incluya:

- ✓ Validación del estado de los componentes (virtual appliance, servidores, bases de datos).
- ✓ Verificación de políticas de acceso y segregación de funciones.
- ✓ Revisión de logs, capacidad y desempeño.
- ✓ Evaluación de respaldos y mecanismos de recuperación.
- ✓ Aplicación de mantenimientos preventivos requeridos.

- Cada seis (6) meses se deberá realizar un assesment técnico de mínimo una (1) semana, que incluya:
  - ✓ Evaluación de madurez del modelo PAM implementado.
  - ✓ Análisis de cobertura de cuentas privilegiadas.
  - ✓ Revisión del cumplimiento del principio de mínimo privilegio.
  - ✓ Identificación de brechas frente a estándares de seguridad.

Como resultado, se deberá entregar un informe técnico detallado, acompañado de un plan de trabajo con acciones correctivas y de mejora, el cual deberá ser ejecutado por el proveedor previa validación de la Entidad.

4. Transferencia de conocimiento
Se deberán realizar jornadas presenciales de transferencia de conocimiento cada cuatro (4) meses, con una intensidad mínima de dieciséis (16) horas por sesión, dirigidas hasta un máximo de diez (10) funcionarios designados por la Entidad.

Las capacitaciones deberán cubrir, como mínimo:
- Administración avanzada de la plataforma.
- Gestión de incidentes relacionados con accesos privilegiados.
- Configuración de políticas y flujos de aprobación.
- Análisis de grabaciones y generación de evidencias para auditoría.
- Buenas prácticas en gobierno de accesos privilegiados.

Cuatro (4) boucher para certificación de producto, con acompañamiento de la experiencia del proponente.

5. Autenticación multifactor (MFA) – Segundo Factor
El oferente deberá suministrar una herramienta tipo aplicación móvil (APP) que funcione como mecanismo de doble factor de autenticación (MFA), integrada de manera nativa o certificada con la solución PAM ofertada.

El segundo factor deberá basarse en el estándar Time-based One-Time Password (TOTP), algoritmo ampliamente adoptado que genera contraseñas dinámicas de un solo uso a partir de una clave secreta compartida y del tiempo actual, conforme a estándares internacionales (por ejemplo, RFC 6238).

La solución de MFA deberá:

- Ser compatible con todo el licenciamiento ofertado.
- Permitir la aplicación obligatoria de segundo factor para accesos administrativos y de alto riesgo.
- Soportar políticas adaptativas según criticidad del recurso.
- Garantizar altos niveles de disponibilidad y seguridad criptográfica.

En conjunto, este esquema de soporte, mantenimiento y fortalecimiento continuo deberá asegurar la resiliencia, disponibilidad, seguridad y evolución controlada de la plataforma PAM implementada, en concordancia con los lineamientos de gobierno de TI y gestión de riesgos de la Entidad.

SERVICIOS DE CONFIGURACIÓN E IMPLEMENTACIÓN

El oferente debe garantizar que la solución cumpla con los siguientes requerimientos funcionales los cuales deben quedar implementados:

- Capacidad de administración centralizada y segura que permita automatizar la gestión de las contraseñas de las cuentas de administración de sistemas, servicios y aplicaciones, así como poder aplicar políticas de contraseñas fuertes para el acceso a los dispositivos.
- Controlar el acceso a las cuentas privilegiadas
- Administrar y monitorear sesiones de cuentas privilegiadas, así como los comandos y acciones llevadas a cabo en tiempo real permitiendo la grabación de la sesión y su posterior revisión por auditoría.
- Control de comandos y filtrado de acciones que una cuenta privilegiada y/o el administrador puede ejecutar
- Visión global del uso de cuentas privilegiadas a través de reportes y tableros de control que permitan el cumplimiento de regulaciones
- Bóveda para la protección de los usuarios/contraseñas de los usuarios privilegiados.

Los servicios de implementación deben contemplar las siguientes actividades:

- Implementación de licencias, de los equipos implementados, según licenciamiento.
- Gestión y control de dispositivos y todas sus cuentas privilegiadas, de los equipos implementados, según licenciamiento.
- Descubrimiento de todas las cuentas de los equipos implementados, según licenciamiento.
- Identificación de cuentas huérfanas de los equipos implementados, según licenciamiento.
- Implementar por lo menos la grabación de hasta 1200 sesiones concurrentes.
- Configurar la solución sin agentes para la toma de las sesiones y gestión de las cuentas privilegiadas
- Reconciliación entre la solución y las cuentas que se gestionaran por la solución.

- Implementación de analítica de las cuentas privilegiadas para los equipos implementados, según licenciamiento.
- Protección sistemas operativos (entre Windows y Linux), de los equipos implementados, según licenciamiento.
- Configuración de 5 flujos para cuentas privilegiadas.
- Servicios de instalación y configuración de la adquisición de acuerdo con el tipo de licenciamiento ofertado.
- Transferencias de conocimiento
- Acompañamiento Post- producción
- Ejecución en conjunto con el SENA del proceso de entregas y despliegues a fin de entregar la solución a la operación generando la documentación correspondiente
- El proyecto debe incluir los ambientes Producción y DR (Disaster Recovery) en línea, es decir que el ambiente de DR NO debe ser pasivo.
- La solución debe grabar las sesiones sin la necesidad de incurrir en licenciamientos adicionales tanto de la solución como de sistemas operativos.

SOPORTE PROVEEDOR
Servicio 7X24 por proveedor, (en caso de desborde de requerimientos, se debe contar con máximo 3 especialistas y mínimo 1, según las necesidades de los servicios, la cantidad de requerimientos serán acordadas con el SENA)

Soporte remoto 7X24 por el fabricante para el licenciamiento del SENA

CARACTERISTICAS DEL PROPONENTE
1. Certificaciones: Certificación emitida por el fabricante donde se evidencie que es canal autorizado en COLOMBIA para el suministro de licencias y servicio de soporte de las soluciones ofertadas.
2. El oferente debe ser Partner certificado por el fabricante.

Lo anterior se fundamenta en la necesidad de garantizar la continuidad, estabilidad y correcta operación de la solución de Gestión de Accesos Privilegiados (PAM), la cual ya se encuentra implementada en la Entidad bajo un esquema de licenciamiento perpetuo.

En este sentido, la presente contratación no corresponde a una adquisición inicial de la solución, sino a la renovación de servicios de soporte, mantenimiento y actualización sobre una plataforma existente, lo que implica la necesidad de asegurar:

- Compatibilidad técnica con la arquitectura ya desplegada en la Entidad.
- Continuidad en la administración de licencias existentes sin interrupción del servicio.
- Acceso a soporte especializado del fabricante sobre una solución ya productiva.
- Mitigación de riesgos asociados a la pérdida de soporte o desactualización tecnológica.

OBLIGACIÓN RELACIONADA CON LA RETENCIÓN Y ALMACENAMIENTO DE GRABACIONES DE SESIONES PAM:

El contratista deberá garantizar la correcta operación de los mecanismos de grabación de sesiones de la solución de gestión de accesos privilegiados (Privileged Access Management – PAM), asegurando la captura, conservación, disponibilidad, integridad, confidencialidad y consulta de la totalidad de las sesiones privilegiadas ejecutadas sobre los activos tecnológicos administrados por la Entidad.

Para tal efecto, el contratista será responsable de dimensionar, configurar y mantener la capacidad de almacenamiento requerida para soportar la retención de las grabaciones generadas por la solución PAM, de conformidad con las políticas, lineamientos y tiempos de conservación definidos por el SENA. Lo anterior deberá contemplar el crecimiento proyectado de la operación, la concurrencia de sesiones, la duración promedio de las conexiones, mecanismos de compresión, redundancia, respaldo, recuperación y demás condiciones técnicas necesarias para garantizar la continuidad y disponibilidad del servicio.

Asimismo, el contratista deberá implementar mecanismos de protección de la información almacenada, incluyendo controles de acceso, trazabilidad, cifrado y medidas de seguridad que preserven la autenticidad e integridad de las grabaciones, permitiendo su consulta para fines de auditoría, monitoreo, análisis forense, investigación de incidentes de seguridad y cumplimiento normativo.

La definición de los tiempos de retención, criterios de conservación y disposición final de las grabaciones corresponderá al SENA, mientras que la implementación técnica, sostenibilidad operativa y soporte serán responsabilidad del contratista durante la ejecución del contrato.

EQUIPO DE TRABAJO

PERFIL	FORMACIÓN	EXPERIENCIA	CERTIFICACIONES
Profesional de Soporte y Operación de la Solución PAM	Título Profesional en: • Ingeniería de Sistemas o • Ingeniería de Computación o • Ingeniería de Software o • Ingeniería Electrónica o • Ingeniería de Telecomunicaciones o • Ingeniería Telemática o • Ingeniería Industrial o • Administración Informática o afines.	Mínimo tres (3) años en licencias PAM.	Certificación del fabricante en: 1. Proven Professional, Privileged Access Manager Support. 2. Proven Professional, Privileged Access Manager Implementation.

NOTA: El Profesional de Soporte y Operación de la Solución PAM debe estar vinculado directamente mínimo 6 meses antes de la firma del contrato, se debe adjuntar certificación.

NOTA 2: El oferente no puede subcontratar estos servicios.

PERFIL	FORMACIÓN	EXPERIENCIA	CERTIFICACIONES
Gerente de Proyecto	Título Profesional en: • Ingeniería de Sistemas o • Ingeniería de Computación o • Ingeniería de Software o • Ingeniería Electrónica o • Ingeniería de Telecomunicaciones o • Ingeniería Telemática o • Ingeniería Industrial o • Administración Informática o afines. Título de posgrado en: • Especialización y/o Maestría en Gerencia de Proyectos. • Certificado PMP vigente. • Certificado Scrum Master Profesional • ITIL v4	Experiencia profesional de mínimo cuatro (4) años, la cual será contada a partir de la obtención de la matricula y/o tarjeta profesional. **Experiencia especifica:** Participación en mínimo 3 proyectos en gerencia de proyectos de soluciones de software.	Certificación del fabricante en: 1. Proven Professional, Privileged Access Manager Support. 2. Proven Professional, Privileged Access Manager Implementation.

NOTA: El implementador debe estar vinculado directamente mínimo 6 meses antes de la firma del contrato, se debe adjuntar certificación.

NOTA 2: El oferente no puede subcontratar estos servicios.

ACUERDOS DE NIVEL DE SERVICIOS

Alcance del impacto	TIEMPO DE ATENCIÓN		TIEMPO DE SOLUCION	
	Telefónico/Remoto	En sitio	Telefónico/Remoto	En sitio
Crítico o Impacto Tipo 1	Inmediato	2 horas	2 horas	4 horas
Medio o Impacto Tipo 2	1 hora	4 horas	3 horas	6 horas
Bajo o Impacto Tipo 3	2 horas	8 horas	4 horas	8 horas

CRÍTICO / ALTO (Impacto 1): Son aquellos que suponen una caída importante de producción con un grave impacto en el servicio a usuarios. Son los problemas que cumplen con las siguientes condiciones:

- Errores que impiden el acceso a una parte importante de la funcionalidad de la aplicación y, por ende, la operatividad de la misma.
- Errores que dan lugar a la caída de la aplicación o del sistema.
- Errores que en términos de necesidades del negocio y/ o de número de usuarios afectados tienen un peso significativo.
- Errores que impiden la instalación de la aplicación

MEDIO (Impacto 2): Problemas o defectos que afectan un área específica de la plataforma o software instalado, estando parcialmente fuera de servicio, pero sin pérdida de eficiencia, ni causando degradación del rendimiento ni impacto para el cliente. Son aquellos problemas que denotan errores en la funcionalidad (bloqueo de parte de ella).

BAJO (Impacto 3): Son aquellos problemas que denotan errores de formato (colores, solapamiento de elementos en la pantalla, faltas de ortografía), información adicional inexistente o inadecuada (mensajes de error, información de ayuda, etc.), consultas generales y problemas secundarios sobre funcionalidades activas, fallos en la documentación, imperfecciones de proyecto y consultas operacionales asociadas a fallas menores. Para los casos de bajo impacto, el horario de atención se limita a horario de oficina.

CONSECUENCIAS POR INCUMPLIMIENTO

Se establecen los siguientes mecanismos para garantizar el cumplimiento de los ANS:

1. **Compensaciones en servicio:** El contratista deberá otorgar extensiones del servicio de soporte y mantenimiento sin costo adicional, de acuerdo con el impacto del incumplimiento:
   - Impacto Tipo 1: tres (3) días calendario de extensión
   - Impacto Tipo 2: dos (2) días calendario de extensión
   - Impacto Tipo 3: un (1) día calendario de extensión

Estas compensaciones no excluyen la aplicación de sanciones contractuales.

2. **Multas por incumplimiento de ANS:** Sin perjuicio de la cláusula penal, la Entidad podrá imponer multas por cada evento de incumplimiento, así:
   • Impacto Tipo 1: 0,5% del valor total del contrato
   • Impacto Tipo 2: 0,3% del valor total del contrato
   • Impacto Tipo 3: 0,1% del valor total del contrato

Las multas serán acumulables y podrán hacerse efectivas con cargo a la garantía de cumplimiento.

1. **Cláusula penal pecuniaria:** En caso de incumplimiento grave o reiterado, la Entidad podrá hacer efectiva la cláusula penal hasta por el diez por ciento (10%) del valor del contrato, sin perjuicio de la declaratoria de incumplimiento.

2. **Incumplimientos reiterados:** Cuando se presenten más de tres (3) incumplimientos en un mismo mes o más de cinco (5) acumulados durante la ejecución, la Entidad podrá:

   - Hacer efectiva la garantía de cumplimiento, en los términos establecidos en el contrato
   - Declarar el incumplimiento del contrato
   - Iniciar el procedimiento de caducidad, si a ello hubiere lugar

3. **Verificación del cumplimiento:** El supervisor del contrato verificará los ANS con base en registros de la mesa de servicios, reportes del proveedor y demás evidencias técnicas.

4. **Regla de incumplimiento:** Se configurará incumplimiento cuando los tiempos de atención o solución superen los umbrales definidos, contados desde el registro del incidente.

3. FORMATO COTIZACIÓN.

La oferta económica (cotización) deberá incluir todos costos directos de acuerdo con los requerimientos descritos en el presente documento.

- ✓ La validez de la oferta debe ser de 90 días.
- ✓ En la cotización debe constar el NIT, Dirección, Teléfono, Fax y Correo Electrónico

NOTA 1: El valor deberá ser suministrado en pesos colombianos. Se deberán incluir todos los factores estimados que puedan afectar el precio, incluyendo la TRM aplicada a la oferta.

NOTA 2: La cotización deberá incluir todos costos directos e indirectos, impuestos, tasas y demás contribuciones que haya lugar.

NOTA 3: Sólo se recibirán cotizaciones que incluyan la totalidad de los ítems a adquirir, con las especificaciones sugeridas, cualquier ítem adicional que considere el proveedor deberá tener en cuenta la respectiva justificación y explicación de este.

NOTA 4: La información remitida servirá de base para la elaboración de un estudio de mercado y, por tanto, no constituye en sí misma una oferta y consecuentemente NO obliga a las partes a la celebración de ningún tipo de contrato ni de inicio de un proceso de contratación.

NOTA 5: El SENA, podrá realizar ajustes en los productos a adquirir de acuerdo con sus necesidades teniendo en cuenta el estudio de mercado respectivo.

NOTA 6: La información que reporte cada cotizante se considerará veraz y ajustada a los parámetros del mercado y por tanto la misma será fundamental para determinar los valores del mercado para adelantar el proceso de contratación, por lo que cada cotizante se hace responsable de la información que reporta en el formato de cotización.

NOTA 7: El alcance de la adquisición se precisará en los estudios previos y sus anexos y en el proceso de contratación. La información contenida en este documento y sus anexos es una estimación general y global.

Esperamos con este documento encontrar y recibir la información real y precisa, que refleje la realidad de los precios actuales conforme a los requisitos que se exponen y garantizar con ello un proceso objetivo, transparente y eficaz.

Diligenciar el Formato Propuesta Económica Estudio de Mercado.

EDGAR MARTÍN CUBIDES ROJAS
Jefe Oficina de Sistemas
Dirección General – SENA

Proyectó: Claudia Ferro García – Contratista Oficina de Sistemas

Revisó: Juan Francisco González Vidal – Coordinador Grupo Integrado de Gestión Operativa de Servicios Tecnológicos