ANEXO TÉCNICO
"SUSCRIPCIÓN A SISTEMA DE ADMINISTRACIÓN DE ACCESO PRIVILEGIADO PAM".

<table>
<tr><th colspan="2">ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS</th></tr>
<tr><td>1.</td><td>Unidad de Medida: Unidad</td></tr>
<tr><td>2.</td><td>Cantidad de Suscripciones: Se requiere suscripción para 100 usuarios nominales.</td></tr>
<tr><td>3.</td><td>Tiempo: La suscripción deberá contar con una vigencia mínima de treinta y cinco (35) meses.</td></tr>
<tr><td>4.</td><td>Descripción de la Suscripción: Solución de Administración de Accesos Privilegiados (PAM) bajo modalidad SaaS, orientada a la gestión centralizada de credenciales privilegiadas, control de accesos administrativos, monitoreo y grabación de sesiones privilegiadas, administración de cuentas de servicio y aplicación de controles de seguridad sobre los activos tecnológicos de la Fuerza Aeroespacial Colombiana.

La solución deberá proporcionar capacidades para la gestión de privilegios Just-In-Time (JIT), control de accesos basado en riesgo, administración y rotación automática de credenciales, auditoría de actividades privilegiadas, acceso de emergencia (Break Glass) e integración con los servicios de identidad institucionales, contribuyendo al fortalecimiento de la seguridad de la información, la trazabilidad de las actividades administrativas y la reducción de riesgos asociados al uso de privilegios elevados sobre la infraestructura tecnológica institucional.</td></tr>
<tr><td>5.</td><td>A nivel de SOPORTE TÉCNICO se deberá tener durante los 35 meses, No obstante, la vigencia definitiva corresponderá al período que resulte de la oferta económica seleccionada y de la disponibilidad presupuestal asignada al proceso, pudiendo ampliarse la cobertura de la suscripción hasta agotar el presupuesto disponible, sin superar el horizonte de necesidad definido por la FAC.

• SOPORTE TÉCNICO y cumplimiento de la garantía de fábrica por el periodo de la suscripción al sistema en un esquema 7x24 incluyendo acceso al portal de soporte, soporte a casos y recursos técnicos asociados.
• Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.
• El contratista deberá ofrecer una garantía técnica durante la vigencia de la suscripción al sistema en un esquema 7x24.
• El SERVICIO TÉCNICO debe incluir atención de incidentes sobre la suscripción al sistema ofertado.
• El SERVICIO TÉCNICO debe permitir consultas a través de llamadas telefónicas, correo electrónico.
• El SERVICIO TÉCNICO debe tener el alcance de integración y afinamiento de nuevas fuentes con que cuente la Entidad.
• El SERVICIO TÉCNICO debe permitir sesiones remotas y atención de acuerdo con lo requerido por la supervisión del contrato, en caso de requerirse, en horario hábil y no hábil. Esto, con respecto a la suscripción al sistema ofertado y objeto del presente contrato.</td></tr>
<tr><td>6.</td><td>Los siguientes son los términos de respuesta del SERVICIO TÉCNICO exigible al contratista, durante mínimo los 35 meses, No obstante, la vigencia definitiva corresponderá al período que resulte de la oferta económica seleccionada y de la disponibilidad presupuestal asignada al proceso, pudiendo ampliarse la cobertura de la suscripción hasta agotar el presupuesto disponible, sin superar el horizonte de necesidad definido por la FAC.

<table>
<tr><th>PRIORIDAD</th><th>DESCRIPCIÓN</th><th>TÉRMINO DE RESPUESTA</th></tr>
</table>
</td></tr>
</table>

	1	CRÍTICA	La producción está detenida o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.	La atención deberá iniciar Mediante los canales de soporte habilitados para la solución, tales como portal de soporte, atención telefónica, correo electrónico, chat o sesiones remotas, dentro de maximo las dos (2) horas siguientes a la apertura del caso por parte del personal autorizado de la FAC.
	2	ALTA	Experimenta pérdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.	La atención deberá iniciar Mediante los canales de soporte habilitados para la solución, tales como portal de soporte, atención telefónica, correo electrónico, chat o sesiones remotas, dentro de maximo las cuatro (4) horas siguientes a la apertura del caso por parte del personal autorizado de la FAC.
	3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.	La atención deberá iniciar Mediante los canales de soporte habilitados para la solución, tales como portal de soporte, atención telefónica, correo electrónico, chat o sesiones remotas, dentro de maximo las ocho (8) horas siguientes a la apertura del caso por parte del personal autorizado de la FAC.
	4	BAJA	No impacta la operación del programa, no se experimenta pérdida del servicio y no se impide la operación de los sistemas.	La atención deberá iniciar Mediante los canales de soporte habilitados para la solución, tales como portal de soporte, atención telefónica, correo electrónico, chat o sesiones remotas, dentro de maximo las veinticuatro (24) horas siguientes a la apertura del caso por parte del personal autorizado de la FAC.
7.	El contratista deberá garantizar que se puedan escalar casos de soporte a la casa fabricante durante toda la vigencia de la suscripción a la solución contratada.			
8.	La solución deberá entregarse bajo un modelo Software as a Service (SaaS), garantizando altos niveles de disponibilidad y continuidad del servicio. La arquitectura deberá asegurar mecanismos de redundancia y recuperación ante fallas que permitan mantener la operación de la suscripción al sistema ante			

	interrupciones en cualquier componente de la infraestructura, ya sea del proveedor o de la entidad. La solución deberá evitar la existencia de puntos únicos de falla y garantizar la continuidad del servicio mediante esquemas de alta disponibilidad, balanceo de carga y mecanismos automáticos de recuperación, según las capacidades y diseño tecnológico de la suscripción al sistema propuesto.
9.	En el documento “Plan de Implementación”, el contratista detallará las actividades a realizar para la instalación, configuración e implementación de todos los componentes que forman parte de la contratación.
10.	El contratista deberá proponer las mejores prácticas para la instalación y configuración de las características solicitadas.
11.	La instalación y configuración de todos los componentes de la solución, debe estar a cargo de los técnicos designados por el contratista en acompañamiento del líder de proyecto de la Fuerza Aeroespacial Colombiana.
12.	El contratista será responsable de ejecutar las pruebas de funcionamiento y el afinamiento de todos los componentes involucrados, asegurando que cada uno cumpla con las especificaciones técnicas establecidas y garantizando su correcta operación dentro del entorno definido.
13.	La información a la cual tendrán acceso el contratista y el fabricante, así como la documentación generada durante la prestación del servicio son de propiedad exclusiva de la Fuerza Aeroespacial Colombiana, la misma deberá ser manejada con absoluta reserva, acorde al “Acuerdo de Confidencialidad y Buen Uso de la Información” que se suscriba con el contratista.
14.	La suscripción debe tener la capacidad de integrarse con el MFA que tenga la Institución a través del protocolo SAML 2.0 o el vigente para el Login.
15.	La solución deberá estar basada en la nube bajo modalidad SaaS y cumplir con una disponibilidad mensual mínima de 99.9%.
16.	Deberá otorgarse acceso a un portal de e-learning del fabricante donde la Entidad pueda llevar cursos en línea sobre la suscripción implementada.
17.	El contratista deberá garantizar que la Entidad siempre cuenta con las últimas versiones de la suscripción ofertada.
18.	La solución se utilizará como la única puerta de enlace que conecta la estación de trabajo del usuario con los sistemas administrados para obtener acceso privilegiado.
19.	La solución deberá ser accesible desde cualquier punto geográfico, y esta deberá gestionar las conexiones hacia los sistemas administrados vía proxy o túnel IPSec.
20.	La solución debe admitir un motor distribuido para la administración de contraseñas y sesiones en diferentes segmentos de red aislados y regiones geográficas, mientras que todos los sistemas y políticas de destino aún se pueden administrar de forma centralizada.
21.	La solución no requerirá cambios en la topología de la red para garantizar que todas las sesiones privilegiadas estén controladas por la solución.
22.	La solución se basará en una arquitectura sin agente para la administración de contraseñas y sesiones.
23.	La solución deberá soportar entornos híbridos y multinube incluyendo Microsoft Azure, AWS, Google Cloud Platform y nubes privadas.
24.	La solución deberá soportar como mínimo 300 sesiones concurrentes RDP o 600 sesiones concurrentes SSH y permitir su expansión para admitir miles de sesiones concurrentes mediante los mecanismos de escalabilidad propios de la arquitectura ofertada.
25.	La solución tendrá la capacidad de almacenar en caché las credenciales seleccionadas externamente. Estas credenciales se pueden usar para conexiones de "aplicación con aplicación" para mitigar la interrupción temporal de la infraestructura PAM.
Manejo de activos y descubrimientos	

26.	La solución tendrá capacidad de carga masiva para importar sistemas administrados, cuentas privilegiadas, usuarios y otros objetos necesarios.
27.	La solución tendrá la capacidad de registrar la información del sistema para los sistemas administrados, incluidos, entre otros, la dirección IP, la dirección MAC, el nombre DNS, el propietario del sistema, el tipo de plataforma y la versión, listado de cuentas y sus estados en sistemas operativos.
28.	La solución permitirá al administrador definir atributos personalizados tanto para el sistema administrado como para la cuenta privilegiada.
29.	La solución tendrá la capacidad de descubrir, inventariar y cambiar credenciales de todas las cuentas privilegiadas y no privilegiadas en sistemas conocidos y desconocidos, incluidos, entre otros: • Windows • Unix / Linux • Mac OS • Directorios (AD / LDAP) • Bases de datos • Dispositivos de red
30.	La solución proporcionará la capacidad del motor de descubrimiento distribuido que permite descubrir activos en diferentes segmentos de red aislados y regiones geográficas e informar el resultado del descubrimiento de forma centralizada.
31.	La solución tendrá la capacidad de descubrir los Servicios de Windows y las Tareas Programadas para que las credenciales privilegiadas que utilizan puedan administrarse automáticamente.
32.	La solución tendrá la capacidad de descubrir cuentas de dominio de Active Directory y vincular automáticamente las cuentas descubiertas a servidores específicos para que el usuario solicite acceso.
33.	La solución tendrá la capacidad de descubrir el software que está instalado y los puertos están abiertos en el sistema de destino.
34.	La solución tendrá la capacidad de agrupar sistemas de destino basados en atributos de sistema definidos descubiertos y personalizados.
35.	La solución tendrá la capacidad de agrupar sistemas y cuentas en función del resultado de la consulta AD / LDAP.
36.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado al descubrir nuevos sistemas objetivo o sistemas encontrados que ya no son accesibles.
37.	La solución tendrá la capacidad de descubrir nuevas cuentas privilegiadas y de incorporarlas automáticamente para la gestión de contraseñas.
Gestión de contraseñas	
38.	La solución admitirá la administración de contraseñas para las siguientes plataformas listas para usar como mínimo en: • Sistemas operativos: AIX, AS400, Z / OS, Linux, Mac OS, Solaris, Windows Desktop, Windows Server • Bases de datos: MongoDB, MySQL, Oracle, PostgreSQL, SQL Server, Sybase, Teradata • Directorios: Active Directory, LDAP, RACF • Dispositivos: BIG-IP (F5), Checkpoint, Cisco IOS, Dell iDRAC, Fortinet, HP Comware, HP iLo, Aruba, Juniper (JunOS), Palo Alto Networks, entre otros • Aplicaciones: SAP, VMware vSphere API, VMware vSphere SSH, Amazon AWS, Office 365, Workday, Nutanix.
39.	Además de las plataformas compatibles de fábrica, la solución debe tener una interfaz fácil de usar que proporcione flexibilidad para configurar una plataforma personalizada y permita administrar la contraseña de la cuenta. Su operación debe ser sencilla y

	permitir al usuario (el cliente) realizar la configuración sin la participación del proveedor del producto.
40.	La solución admitirá la definición de múltiples políticas de contraseña y la capacidad de aplicar una política de contraseña para múltiples sistemas administrados y una política de contraseña individual para cada sistema administrado.
41.	La solución tendrá la flexibilidad de definir un cronograma para restablecer y aleatorizar las contraseñas por sistema administrado y por cuenta sin conocimiento de las contraseñas existentes.
42.	La solución tendrá la flexibilidad de restablecer y aleatorizar las contraseñas de las cuentas seleccionadas al realizar el check-in para eliminar el riesgo de que las contraseñas se vean comprometidas.
43.	La solución admitirá la recuperación de la contraseña, así como su rotación automática al vencimiento de la solicitud realizada.
44.	La solución tendrá la capacidad de desbloquear la cuenta al cambiar su contraseña.
45.	La solución tendrá la capacidad de establecer la frecuencia de cambio de contraseña en función de la fecha y la hora.
46.	La solución debe tener la capacidad de cambiar la contraseña de una vez para sistemas individuales, grupales y administrados en función de criterios específicos.
47.	La solución debe tener la flexibilidad de admitir el cambio de contraseña manual a pedido por parte de un usuario autorizado.
48.	La solución tendrá la capacidad de hacer cumplir la integridad de la contraseña restableciendo automáticamente las contraseñas de las cuentas que no verificaron o que ya no se sincronizaron con las contraseñas almacenadas en la solución.
49.	La solución tendrá la capacidad de cambiar automáticamente la contraseña de inicio de sesión de los Servicios de Windows y las Tareas programadas y, opcionalmente, reiniciar los Servicios cuando la solución cambie la contraseña de la cuenta privilegiada correspondiente.
50.	La solución tendrá la capacidad de realizar una verificación de contraseña en la cuenta administrada y notificar las contraseñas 'fuera de sincronización'.
51.	La solución tendrá la capacidad de sincronizar contraseñas para cuentas seleccionadas que residen en múltiples sistemas con diferentes tipos de plataforma.
52.	La solución mantendrá el historial y registro de auditoría de los cambios realizados sobre las contraseñas de las cuentas privilegiadas administradas, permitiendo la consulta trazable de dichos eventos mediante mecanismos controlados y auditables a través de la plataforma.
53.	La solución admitirá la gestión de claves SSH a través del almacenamiento automatizado de claves SSH y la rotación de claves SSH de acuerdo con un cronograma definido.
54.	La solución admitirá la generación de claves SSH con tipos de clave RSA y tamaño de clave configurable.
55.	La solución tendrá la capacidad de cambiar la clave SSH de una sola vez para sistemas individuales, grupales y administrados en función de criterios específicos.
56.	La solución debe tener la flexibilidad de admitir el cambio de clave SSH manual a pedido por un usuario autorizado.
Gestión de Privilegios	
57.	La solución deberá contar con capacidades nativas de privilegios Just-In-Time (JIT), eliminando la necesidad de mantener privilegios administrativos permanentes en cuentas.
58.	La solución deberá permitir elevar privilegios únicamente durante una ventana de tiempo definida.
59.	La solución deberá asignar privilegios de administrador local de forma temporal bajo demanda.

60.	La solución deberá soportar elevación temporal de privilegios para: • Windows. • Linux. • Entornos híbridos. • Recursos en nube pública.
61.	La solución deberá retirar automáticamente los privilegios otorgados una vez expire el tiempo aprobado.
62.	La solución deberá soportar políticas de aprobación multinivel para la concesión de privilegios JIT.
63.	
64.	La solución deberá integrarse con Active Directory y Microsoft Entra ID para la administración de privilegios JIT.
65.	La solución deberá soportar mecanismos de acceso de emergencia (Break Glass) auditables.
66.	La solución deberá soportar privilegios Just-In-Time sin necesidad de revelar credenciales privilegiadas al usuario.
67.	La solución deberá permitir revocación inmediata de privilegios por parte de un administrador autorizado.
68.	La solución deberá permitir la creación dinámica de cuentas administrativas efímeras (Ephemeral Accounts), generadas automáticamente al momento de aprobar una solicitud de acceso y eliminadas o deshabilitadas automáticamente al finalizar la sesión o el tiempo autorizado.
69.	La solución deberá permitir que las cuentas privilegiadas permanezcan deshabilitadas, inaccesibles o inexistentes hasta que una solicitud autorizada requiera su activación.
70.	La solución deberá eliminar o deshabilitar automáticamente cuentas privilegiadas temporales una vez concluya la actividad autorizada.
71.	La solución deberá permitir la asignación dinámica de grupos privilegiados de Active Directory o Microsoft Entra ID.
72.	La solución deberá impedir la existencia de privilegios permanentes, salvo para cuentas de emergencia debidamente justificadas y auditadas.
73.	La solución deberá soportar un modelo de Zero Standing Privilege (ZSP), garantizando que los privilegios administrativos sean asignados únicamente bajo demanda, por tiempo limitado, con trazabilidad completa y revocación automática al finalizar la actividad autorizada.
Gestión de Sesiones	
74.	La solución admitirá la supervisión y el registro del acceso de sesión privilegiado a través de los protocolos estándar RDP y SSH. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso.
75.	La solución admitirá el monitoreo y la grabación de sesiones privilegiadas para el acceso de cualquier aplicación de cliente para aplicaciones de Windows, incluidos, entre otros, vSphere Client, Microsoft SQL Management Studio, SQL Developer, SAPGui, Toad, etc. y navegadores web. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso.
76.	La solución permitirá a los administradores agregar y configurar el acceso de cualquier nueva aplicación cliente con monitoreo de sesión y capacidades de inicio de sesión automático.
77.	La función de grabación de sesión de la solución admitirá el uso de herramientas de cliente comerciales: Escritorio remoto de Windows para acceso RDP y el cliente SSH preferido del usuario, como PuTTY, SecureCRT, WinSCP, etc para acceso SSH.
78.	La solución tendrá la capacidad de limitar el número de sesiones que un usuario puede abrir para cierto conjunto de cuentas privilegiadas al mismo tiempo.

79.	La solución debe permitir la carga / descarga directa y la transferencia de archivos desde los sistemas administrados hacia y desde la estación de trabajo del usuario a través de sesiones RDP y SSH. No habrá archivos residuales en la solución después de que se transfieran los archivos.
80.	La solución tendrá la capacidad de permitir a los usuarios realizar una conexión directa al sistema administrado en la interfaz web de la solución. La grabación de la sesión, el inicio de sesión automático y sin exponer las características de contraseña de cuenta privilegiada aún se aplicarán a esta forma de acceso.
81.	La solución tendrá la capacidad de permitir a los usuarios realizar una conexión directa al sistema administrado a través de sus clientes RDP y SSH favoritos sin la necesidad de iniciar sesión en la interfaz web de la solución. La grabación de la sesión, el inicio de sesión automático y sin exponer las características de contraseña de cuenta privilegiada aún se aplicarán a esta forma de acceso.
82.	La solución deberá contar con un cliente propio para la gestión de sesiones RDP, SSH y Web que permita realizar una conexión directa a los sistemas administrados sin la necesidad de iniciar sesión en la interfaz web de la solución. La grabación de la sesión, el inicio de sesión automático y sin exponer las características de contraseña de cuenta privilegiada aún se aplicarán a esta forma de acceso.
83.	La solución tendrá la capacidad de mostrar mensajes en pantalla con temporizador de cuenta regresiva para notificar al usuario antes de que el acceso aprobado exceda el marco de tiempo solicitado.
84.	La solución tendrá la opción de configuración para finalizar automáticamente una sesión de acceso remoto solicitada si el acceso aprobado excede el período de tiempo solicitado.
85.	La solución tendrá la capacidad de registro de pulsaciones de teclas para todo tipo de acceso, incluidos los clientes de aplicaciones basadas en RDP, SSH, Web y GUI. La pulsación de tecla debe poder buscarse y ubicarse temporalmente en la grabación de la sesión.
86.	La solución tendrá la capacidad de enmascarar la contraseña para la sesión RDP y SSH, incluso si se registra la pulsación de tecla.
87.	La solución deberá permitir listas blancas y listas negras de comandos para sesiones SSH.
88.	La solución deberá permitir bloquear sesiones automáticamente ante la ejecución de comandos restringidos.
89.	La solución deberá registrar y enviar al SIEM/SOAR de la Institución los eventos asociados a la ejecución de comandos considerados de alto riesgo, permitiendo la generación de alertas y mecanismos de correlación definidos por la FAC.
90.	La solución tendrá la capacidad para que el usuario autorizado busque en todos los tipos de grabación por pulsación de tecla, fecha / hora, nombre de usuario, nombre del sistema de destino y nombre de cuenta privilegiada.
91.	La solución permitirá al usuario autorizado reproducir la grabación seleccionada desde la interfaz web sin la necesidad de instalar software de cliente de terceros.
92.	La solución tendrá la capacidad de reproducción de la sesión debe admitir la reproducción desde un punto en el tiempo en la línea de tiempo y la palabra clave buscada en lugar de reproducirse desde el comienzo de la grabación.
93.	La solución tendrá la capacidad de reproducción de la sesión admitirá la reproducción de avance rápido.
94.	La solución tendrá la capacidad de visualizar en tiempo real el desarrollo de sesiones activas por usuarios con el rol destinado para tal fin.
95.	La solución permitirá al usuario autorizado proporcionar comentarios de revisión mientras reproduce la sesión grabada e indicará que la sesión grabada ha sido revisada.

96.	La solución admitirá el monitoreo en vivo de sesiones desde la interfaz web sin la necesidad de instalar software de cliente de terceros.
97.	La solución admitirá la intervención de sesión en tiempo real que permite al usuario autorizado bloquear o finalizar una sesión de forma remota cuando se realiza una actividad sospechosa.
98.	La solución debe tener la opción de configuración para desactivar la grabación para el acceso a la sesión privilegiada seleccionada, pero aun así proporcionar la función de inicio de sesión automático.
99.	La solución tendrá la flexibilidad de permitir a los usuarios conectarse de forma segura a sistemas de destino remotos a través de la función de grabación de sesión utilizando cuentas que no son administradas por la solución.
100.	La solución tendrá la capacidad de archivar sesiones grabadas en el almacenamiento a largo plazo para satisfacer los requisitos de retención de sesiones por mínimo 90 días.
101.	La solución tendrá la capacidad de reproducir la sesión archivada utilizando la aplicación sin la intervención del administrador. La sesión archivada debe estar protegida y encriptada para que no se pueda acceder fuera de la solución.
102.	La solución tendrá la capacidad de garantizar la integridad de las sesiones grabadas para evitar la manipulación.
103.	La solución admitirá la grabación de sesiones con inicio de sesión automático para el sistema Windows donde exista un múltiple factor de autenticación lógico o físico.
104.	La solución admitirá sesión SSH privilegiada en entornos de acceso de shell restringido.
105.	La solución deberá implementar mecanismos de Acceso Basado en Riesgo (Risk-Based Access Control), considerando como mínimo: • Geolocalización. • Dispositivo. • MFA. • Horario. • Tipo de activo. • Sensibilidad del sistema.
Administración y flujos de trabajo	
106.	La solución garantizará la segregación adecuada de tareas con la capacidad de Control de acceso basado en roles (RBAC) de modo que los roles y los accesos se definan adecuadamente.
107.	La solución apoyará mínimamente los roles de solicitante, aprobador y revisor para la segregación de funciones.
108.	La solución tendrá la capacidad de agrupar dinámicamente cuentas administradas en función de criterios que incluyen, entre otros, el tipo de plataforma, la versión de la plataforma, el nombre de dominio, la dirección IP, el nombre del sistema, el nombre de la cuenta, el privilegio de la cuenta, etc.
109.	La solución admitirá el flujo de trabajo basado en políticas y permitirá una configuración sencilla a través de la interfaz web para enrutar la contraseña y la solicitud de sesión a los aprobadores apropiados.
110.	La solución tendrá la flexibilidad de especificar cero, uno o múltiples aprobadores para cuentas individuales, grupales o todas administradas para control dual. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de cuentas administradas.
111.	La solución tendrá la flexibilidad de permitir que múltiples usuarios soliciten la misma contraseña de cuenta y sesión para el mismo sistema administrado en el mismo período de tiempo.

112.	La solución tendrá la capacidad de restringir el marco de tiempo y la frecuencia con la que los usuarios pueden solicitar contraseñas y sesiones a los sistemas administrados. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de cuentas administradas.
113.	La solución tendrá la capacidad de restringir la dirección IP de la computadora del usuario donde se realizan solicitudes de contraseña y sesión. La solución tendrá la flexibilidad para permitir que esta configuración se aplique a uno o grupos de usuarios.
114.	La solución tendrá la flexibilidad de permitir que se asignen múltiples políticas de aprobación a una cuenta administrada para el mismo solicitante. Esto es para admitir los casos de uso, como una cuenta privilegiada que no requiere aprobación durante el horario de oficina, pero se requiere aprobación después del horario de oficina.
115.	La solución debe ser configurable para permitir al usuario autorizado eludir las aprobaciones de una cuenta privilegiada seleccionada para casos de emergencia.
116.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico a los solicitantes y / o aprobadores cuando se haya solicitado una contraseña o sesión.
117.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al solicitante y / o aprobadores cuando el aprobador haya aprobado o rechazado la solicitud.
118.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado para cualquier contraseña o solicitud de sesión, independientemente del requisito de aprobación.
119.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado en caso de falla en el cambio de contraseña.
120.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado en caso de que la contraseña de la solución no coincida con la del sistema administrado.
121.	La solución tendrá la capacidad de permitir la personalización de plantillas de correo electrónico.
Interfaz de usuario	
122.	La solución proporcionará una única interfaz web HTML5 para que los usuarios realicen actividades relacionadas con una cuenta privilegiada, como solicitud, aprobación, reproducción de sesión y recuperación de seguimiento de auditoría, etc., y administradores para administrar cuentas privilegiadas, perfiles de usuario, grupos, organizaciones, roles y políticas.
123.	La solución deberá tener una interfaz de autoservicio que permita al usuario ver y buscar cuentas privilegiadas para acceder.
124.	La solución tendrá una interfaz de autoservicio para que el usuario autorizado recupere las credenciales y solicite una sesión de acceso privilegiado para un acceso de tiempo limitado o único.
125.	La solución permitirá al usuario especificar la fecha / hora de inicio, la duración y la razón al solicitar una contraseña y sesión de cuenta privilegiada.
126.	La solución permitirá al usuario ver y buscar solicitudes antiguas, existentes y pendientes.
127.	La solución debe tener una bóveda de contraseñas personal para los usuarios del sistema que permita almacenar secretos de tipo credencial, archivo, notas, entre otras.
128.	La solución debe tener un complemento de navegador que permita al usuario acceder de forma rápida a su bóveda personal de contraseñas.
129.	La solución debe permitir inyectar las credenciales guardadas en la bóveda de contraseñas personal del usuario en las páginas web reconociendo el dominio accedido, en los campos destinados para el login.
Auditoría, reportería y analítica	
130.	La solución deberá respaldar la auditoría y la rendición de cuentas donde se registra cada transacción para cada solicitud.

131.	La solución capturará todos los cambios realizados por los administradores en la pista de auditoría, incluido el nombre de usuario, la marca de tiempo, la actividad realizada, la dirección IP y los valores antiguos / nuevos.
132.	La solución tendrá la capacidad de generar todos los informes por frecuencia, bajo demanda o como tareas programadas.
133.	La solución admitirá mínimamente estos formatos de informe: CSV, Excel, PDF, MHTML, Word, TIFF y XML.
134.	La solución debe proporcionar los siguientes tipos de informes listos para usar sin ningún componente adicional y sin costo adicional: • Informe de antigüedad de contraseña de cuenta que proporciona la última fecha y fecha de cambio de contraseña para cada cuenta administrada. • Informe de actividades del usuario que proporciona una vista transaccional detallada de las actividades de aprobación y solicitud de sesión y contraseña. • Informe de derechos que detalla quién tiene acceso a qué cuentas. • Informe de actividad de cambio de contraseña que detalla el motivo y el resultado del cambio de contraseña. • Informe de programación de cambio de contraseña que proporciona detalles del próximo cambio de contraseña programado. • Restablecimiento de contraseña al liberar el informe de conciliación que muestra los estados de restablecimiento de finalización de solicitud de contraseñas de cuentas administradas para proporcionar evidencia auditable de que las contraseñas se han restablecido adecuadamente después de ser liberadas. • Informe de inventario de activos que proporciona una lista de todos los sistemas administrados y no administrados, activos de TI descubiertos agrupados por sistema operativo. • Informe de inventario de cuenta que proporciona una lista de todas las cuentas administradas y no administradas. • Informe delta de cuenta que proporciona cambios delta para cuentas agregadas y eliminadas de acuerdo con períodos diarios, semanales y mensuales. • Informe de cuentas administradas vs no administradas que proporciona una lista de cuentas del sistema de destino e indica cuáles están bajo administración de contraseñas. • Informe de uso de la cuenta de servicio que proporciona una lista detallada de qué sistemas están utilizando una cuenta de servicio para iniciar uno o más servicios de Windows. Informe de cumplimiento normativo que proporciona información sobre los estándares reglamentarios (pero no se limita a): COBIT, GLBA, HIPPA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST 800, PCI y SOX.
135.	La solución tendrá la capacidad de entregar informes por correo electrónico o en una carpeta compartida de forma automática según un cronograma predefinido para que el usuario no tenga que generar o recuperar informes manualmente.
136.	La solución admitirá contenido de informes enriquecido que incluye, entre otros, texto, tabla, gráficos, gráfico, barra, etc.
137.	La solución tendrá la capacidad de permitir la creación de informes personalizados.
138.	La solución tendrá una capacidad de análisis de amenazas avanzada que identifica usuarios y sistemas específicos de alto riesgo al correlacionar datos de privilegios, solicitudes anómalas y otras amenazas
Autenticación, seguridad y cumplimiento	
139.	La solución ofertada o el fabricante deberán acreditar certificación ISO/IEC 27001 vigente o informe SOC 2 Tipo II vigente o certificación Common Criteria vigente. El

	oferente deberá aportar el documento expedido por el organismo certificador o auditor correspondiente que permita verificar su vigencia y alcance.
140.	La solución no deberá contener credenciales codificadas que no puedan administrarse.
141.	La solución deberá integrarse mediante estándares abiertos tales como SAML 2.0, OAuth 2.0, OpenID Connect (OIDC), SCIM y protocolos posteriores soportados por la industria.
142.	La solución admitirá la autenticación nativa mediante segundo factor de autenticación TOTP, sin integración con otros componentes en la red.
143.	La solución admitirá la creación de usuarios locales que puedan consumir las credenciales y los accesos administrados.
144.	La solución permitirá definir políticas de acceso condicional establecido por periodos específicos de tiempo, días de la semana y horarios específicos, orientado para personal interno, terceros, colaboradores y contratistas.
145.	La solución admitirá la autenticación integrada de Windows y SAML para el inicio de sesión único.
146.	La solución admitirá la aplicación de una autenticación fuerte con RADIUS Two Factor Authentication (2FA).
147.	La solución tendrá la capacidad de integrarse con varios dominios de directorios AD / LDAP simultáneamente.
148.	La solución tendrá la capacidad de revocar temporalmente a los usuarios seleccionados para evitar que los usuarios accedan a la solución para realizar una solicitud de acceso con privilegios. Al integrarse con AD / LDAP para la autenticación, revocar al usuario en la solución no deberá deshabilitar ni bloquear la cuenta AD / LDAP.
149.	La solución tendrá la capacidad de integrarse con el Módulo de seguridad de hardware (HSM) listo para usar utilizando el estándar PKCS # 11.
Administración del sistema y APIs	
150.	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado cuando haya una nueva versión de los paquetes de software disponibles o se hayan instalado automáticamente.
151.	La solución tendrá la capacidad de realizar copias de seguridad programadas y ad-hoc programadas en sus configuraciones de estado operativo.
152.	La solución tendrá la capacidad de restaurar sus configuraciones de estado operativo desde la copia de seguridad.
153.	La solución tendrá la capacidad de enviar información de salud del sistema basada en umbrales predefinidos a través de syslog a la solución SIEM/SOAR de la institución.
154.	La solución tendrá la capacidad de enviar información de salud del sistema en base a umbrales predefinidos por correo electrónico.
155.	La solución deberá ofrecer un Kit de Desarrollo de Software (SDK) que permita atender escenarios específicos y casos de uso avanzados mediante acceso programático en tiempo real a las funcionalidades de la plataforma. El SDK permite que las aplicaciones y las personas accedan al almacén de contraseñas de forma independiente, sin usar la interfaz original del producto.
156.	La solución ofrecerá un Kit de desarrollo de software (SDK) para permitir la administración de contraseñas de cualquier sistema.
157.	La solución proporcionará RESTful API con características integrales que permiten la administración de la solución mediante programación, que incluye, entre otros, agregar / modificar / eliminar sistemas / cuentas administradas, actualizar políticas de acceso, agregar / eliminar usuarios, recuperación de credenciales de cuenta privilegiadas, solicitud y lanzamiento privilegiado sesión, etc.
158.	La solución proporcionará documentación API y programas API de muestra en al menos los siguientes lenguajes de programación: Python, C #, Java, PowerShell y Unix Shell Script.

159.	La solución proporcionará una utilidad de línea de comandos con una capacidad similar a la API. La utilidad de línea de comandos debe ser compatible con las plataformas Windows, Linux, AIX y Solaris
160.	Integración SIEM: La solución debe tener la capacidad de integración nativa con el SIEM/SOAR de la institución para reenviar eventos o a través del protocolo Syslog. El tipo de eventos debe incluir, entre otros, umbrales predefinidos basados en el estado del sistema, cambios en la configuración del sistema, inicio / cierre de sesión del usuario, solicitud de acceso privilegiado del usuario, solicitud de aprobación / rechazo del aprobador.
161.	Integración de Vulnerability Management: la solución debe tener una integración nativa con las siguientes soluciones de Vulnerability Management como proveedor de credenciales para el análisis autenticado: Tenable.
162.	Integración en la nube: la solución debe tener una integración nativa con las siguientes plataformas de nube y virtualización para descubrir máquinas virtuales en línea / fuera de línea: AWS, GCP, Microsoft Hyper-V, Rackspace, VMware vCenter, Nutanix.
163.	La suscripción deberá integrase y configurarse para funcionar en sinergia con las tecnologías implementadas por la FAC en el momento del inicio de esta y durante la totalidad de su vigencia, tales como sistemas, plataformas, dispositivos, directorios y servicios definidos por la FAC para la administración y control de accesos privilegiados, garantizando la correcta comunicación entre la solución PAM y los activos tecnológicos objeto de administración.
164.	El contratista deberá entregar la suscripción debidamente configurada, parametrizada y operativa, garantizando el correcto funcionamiento de sus módulos, consolas de administración, mecanismos de acceso privilegiado, gestión de credenciales e integraciones requeridas por la FAC.
165.	El contratista deberá entregar junto con la suscripción el diseño, configuración y validación en conjunto con el personal técnico de la FAC de las políticas de acceso privilegiado, flujos de aprobación, mecanismos de acceso de emergencia (Break Glass), privilegios Just-In-Time (JIT), controles de acceso basados en riesgo y demás funcionalidades requeridas para la adecuada gestión de privilegios.
166.	El contratista deberá entregar junto con la suscripción la implementación y verificación de los mecanismos de monitoreo, grabación, auditoría y trazabilidad de sesiones privilegiadas, garantizando el registro adecuado de las actividades realizadas por usuarios autorizados sobre los sistemas administrados, de acuerdo con las políticas definidas por la Entidad.
167.	El contratista deberá garantizar durante la vigencia de la suscripción el acompañamiento técnico necesario para el ajuste, validación y optimización de la solución implementada, incluyendo la verificación de integraciones, políticas de acceso, rotación de credenciales, monitoreo de sesiones y demás componentes habilitados, conforme a las necesidades operativas de la FAC y a las capacidades incluidas dentro de la suscripción contratada.
168.	El oferente deberá informar la marca y modelo del producto o servicio ofertado.
169.	La suscripción de esta solución deberá iniciar el 20 de diciembre de 2026 y tener de vigencia mínima de treinta y cinco meses 35 meses. No obstante, la vigencia definitiva corresponderá al período que resulte de la oferta económica seleccionada y de la disponibilidad presupuestal asignada al proceso, pudiendo ampliarse la cobertura de la suscripción hasta agotar el presupuesto disponible, sin superar el horizonte de necesidad definido por la FAC.
170.	El contratista deberá realizar 30 horas de transferencia de conocimiento de la tecnología al personal de la FAC que designe el supervisor del contrato. Se debe certificar la entrega de esta transferencia será en el plazo de ejecución del contrato y deberá ser realizada en la ciudad de Bogotá o de forma virtual.
171.	El oferente deberá aportar certificación expedida por el fabricante de la solución, en la

	cual se acredite que es distribuidor autorizado para la comercialización de la suscripción ofertada y que cumple con las especificaciones del anexo técnico.

NOTA 1: El contratista deberá entregar a la Fuerza Aeroespacial Colombiana (FAC) y al Supervisor del contrato un documento suscrito por su representante legal, mediante el cual manifieste de manera expresa que dichas suscripciones adquiridas deberán ser activadas en los plazos que establezca la FAC, con el fin de garantizar la continuidad operativa y evitar la afectación del funcionamiento de las plataformas actualmente en uso.

NOTA 2: Durante la vigencia de la suscripción, el contratista se obliga a ejecutar y soportar ante la supervisión del contrato las siguientes actividades y entregables:

a) Cuando se generen cambios realizados en la suscripción contratada, el contratista estará en la obligación de informar a la entidad de forma detallada los cambios realizados a detalle y los horarios en que se realizó.

b) Presentar ante la supervisión al momento de realizar el acta de inicio del contrato el "Plan de Transferencia de Conocimiento" para su respectiva revisión, validación y aprobación técnica.

NOTA 3: Atendiendo la necesidad institucional de garantizar la adecuada apropiación, administración y aprovechamiento de la "SUSCRIPCIÓN A SISTEMA DE ADMINISTRACIÓN DE ACCESO PRIVILEGIADO PAM", se establece como obligación del contratista:

1. Durante la vigencia de la suscripción, el contratista deberá desarrollar actividades de transferencia de conocimientos orientadas al fortalecimiento de las habilidades necesarias para la administración autónoma de la solución ofrecida, las cuales serán impartidas por la casa matriz o el fabricante, y estarán dirigidas como mínimo a dos (2) funcionarios del componente técnico de la Dirección de Seguridad Informática y Electrónica.

2. Las actividades de transferencia de conocimientos se priorizarán para su realización en la ciudad de Bogotá D.C. En caso de que, por necesidades del servicio, se requiera desarrollar dichas actividades fuera de la guarnición de Bogotá, el contratista asumirá la totalidad de los gastos asociados al desplazamiento del personal designado, incluyendo transporte, alojamiento y alimentación.

	
T1. LUSBIN HERNANDEZ HERNANDEZ	MY. LUIS MAURICIO LEON PINZON
Comité técnico estructurador	**Gerente del Proyecto**