ANEXO No. 1
ANEXO TÉCNICO

CARACTERÍSTICAS TÉCNICAS DEL BIEN O SERVICIO:

Los servicios para contratar se desglosan de la siguiente manera:

Ítem	Detalle
Características principales	
1	**Privileged Account and Session Management (PASM): Gestión de cuentas y sesiones privilegiadas.**
1.1	Arquitectura y rendimiento (opción de despliegue mediante appliances virtuales on-premises o IaaS)
1.1.1	La solución se utilizará como la única puerta de acceso privilegiado y deberá permitir acceso sin exposición directa de la contraseña (modelo proxy/jump), incluyendo conexión transparente mediante clientes nativos (RDP, SSH, clientes de bases de datos), sin revelar credenciales al usuario final.
1.1.2	La solución iniciará la sesión privilegiada desde la estación de trabajo hacia los sistemas gestionados, utilizando múltiples proxies de sesión a través de un único portal web HTPS (HTML5) de inicio de sesión.
1.1.3	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 se pueden administrar de forma centralizada.
1.1.4	La solución no requerirá cambios en la topología de la red para garantizar que todas las sesiones privilegiadas estén controladas por la solución.
1.1.5	La solución se basará en una arquitectura sin agente para la administración de contraseñas y sesiones.
1.1.6	La solución se entregará en hardware o dispositivo virtual asegurado con estándares reconocidos en el mercado
1.1.7	Los componentes lógicos de conectividad, conectores o pasarelas de salto (Gateways / Proxies / Session Nodes) encargados del aislamiento y la grabación de las sesiones no estarán restringidos en cantidad por el licenciamiento del fabricante del PAM SaaS. La solución propuesta deberá ofrecer la flexibilidad de permitir el despliegue e instalación de estos componentes intermediarios tanto en entornos basados en sistemas operativos Windows Server como en distribuciones Linux empresariales o contenedores virtuales, de acuerdo con la arquitectura oficial de fábrica del fabricante ofertado, garantizando la escalabilidad del entorno híbrido de la Entidad sin costos adicionales por parte del proveedor PAM.
1.1.8	La solución ofrecerá opciones de implementación de dispositivos en proveedores de nube pública, incluidos Azure y AWS.
1.1.9	La solución admitirá no menos de 100 sesiones de grabación concurrentes (RDP, Web, SQL Server, MySQL u otras) u 800 Sesiones concurrentes SSH/Telnet por cada nodo de sesión, y podrá ampliarse para admitir miles de sesiones concurrentes.
1.1.10	Los componentes de software, servidores puente locales (Gateways), conectores o mecanismos oficiales provistos por el fabricante para enlazar de manera segura la plataforma PAM SaaS con la infraestructura híbrida de la Entidad no estarán restringidos en cantidad por licenciamiento. Estos componentes deberán estar

	incluidos sin costo adicional dentro de la oferta económica dimensionada para las cincuenta (50) cuentas privilegiadas base y deberán soportar un despliegue flexible y multiplataforma (ejecutándose según la arquitectura nativa del fabricante sobre Windows Server, distribuciones Linux empresariales o contenedores Docker) para garantizar el control de las sesiones y la rotación de credenciales.
1.1.11	Los componentes de sesión o pasarelas de salto (Gateways/Proxies) de la solución propuestos para el aislamiento, inyección de credenciales, grabación y auditoría de accesos, deberán poder desplegarse en los sistemas operativos (Windows Server y/o distribuciones Linux Enterprise) soportados oficialmente por el fabricante de la solución PAM, garantizando la escalabilidad y alta disponibilidad de la arquitectura híbrida de la Entidad sin exigir una distribución única o exclusiva.
1.1.12	Los componentes de conectividad, conectores o pasarelas locales (Gateways / Proxies) provistos por el fabricante para el aislamiento y grabación de sesiones, deberán soportar esquemas de despliegue flexibles que incluyan la ejecución nativa sobre entornos de contenedores virtuales (tales como Docker, Podman o equivalentes), de acuerdo con la arquitectura oficial del fabricante de la solución PAM SaaS, asegurando la adaptabilidad con la infraestructura híbrida y los estándares de seguridad de la Entidad.
1.1.13	La solución debe utilizar una base de datos compatible con las mejores prácticas de seguridad, que estén documentadas y sean públicas. Dicha base de datos debería permitir una alta disponibilidad en clusters activo-activo, y mecanismos para la recuperación ante desastres.
1.1.14	Los componentes de conectividad local, conectores o pasarelas de salto (Gateways / Proxies / Session Nodes) requeridos para la operación híbrida de la solución PAM SaaS, deberán soportar de forma nativa su despliegue, instalación e interoperabilidad estándar y directa sobre las plataformas de infraestructura institucional de la Entidad, correspondientes a entornos de virtualización VMware (entorno On-Premise) y entornos de nube pública como Microsoft Azure, de acuerdo con las guías y especificaciones oficiales de arquitectura del fabricante, garantizando la alta disponibilidad del servicio..
1.1.15	El núcleo de la solución PAM (Bóveda central y consola de administración) se entregará bajo la modalidad de suscripción SaaS (Software as a Service) nativa en la nube, donde el fabricante asumirá la administración y soporte de toda la pila tecnológica de dicha nube central (sistema operativo, base de datos y aplicación). Para el entorno local (*On-Premise*), la Entidad aprovisionará y administrará las plataformas de infraestructura base (servidores virtuales y sistemas operativos), sobre los cuales el contratista desplegará y mantendrá actualizados los componentes de conectividad y pasarelas (*Gateways/Proxies*) del fabricante necesarios para la operación híbrida.
1.1.16	Los appliances deben ser protegidos de fábrica por políticas de endurecimiento (hardening) y el fabricante debe proveer documentación que indique todos los controles incluidos.
1.1.17	El fabricante de la solución debe proveer actualizaciones de seguridad fáciles de instalar mediante acceso a Internet o instalación manual, incluyendo nuevas funcionalidades y parches de seguridad para los appliances.
1.1.18	La solución principal provista bajo modelo SaaS debe garantizar alta disponibilidad, resiliencia y tolerancia a fallos desde la infraestructura de nube del fabricante para la bóveda central (Vault). Asimismo, para los componentes o servidores puente locales (Gateways) requeridos en el entorno híbrido de la Entidad, la solución debe soportar el despliegue en escenarios redundantes (clúster Activo-Pasivo, Activo-

	Activo o balanceo de carga) para asegurar la continuidad de las sesiones de administración.
1.1.19	La solución propuesta deberá incluir explícitamente dentro de su oferta económica y tecnológica la totalidad de los licenciamientos corporativos de terceros (tales como CALs de Microsoft, Remote Desktop Services - RDS, o equivalentes) que sean técnicamente requeridos para la correcta operación de sus componentes o servidores puente locales, según la documentación oficial de arquitectura del fabricante. El adjudicatario garantizará la entrega de dichos componentes sin que esto genere ningún tipo de costo adicional o complementario para la Entidad durante todo el término del contrato.
1.1.20	El proveedor del PAM debe entregar diagramas de despliegues que detallen escenarios de alta disponibilidad, tolerancia a fallos y redundancia adaptables a un entorno híbrido (infraestructura On-Premise y nube Azure), detallando la cantidad de componentes, mecanismos de balanceo y requerimientos de CPU y Memoria de cada elemento propuesto.
1.1	Arquitectura y rendimiento (opción de despliegue SaaS)
1.1.1	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, permitiendo implementar aislamiento de recursos ZTNA.
1.1.2	La solución iniciará la sesión privilegiada desde la estación de trabajo hacia los sistemas gestionados, utilizando múltiples proxies de sesión a través de un único portal web HTTPS (HTML5) de inicio de sesión.
1.1.3	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.
1.1.4	La solución no requerirá cambios en la topología de la red para garantizar que todas las sesiones privilegiadas estén controladas por la solución.
1.1.5	La solución se basará en una arquitectura sin agente para la administración de contraseñas y sesiones.
1.1.6	La solución se deberá entregar como un servicio SaaS, y deberá contar con certificaciones de industria ISO 27001 y SOC 2 Type 2.
1.1.7	El proveedor deberá describir la arquitectura interna del servicio SaaS propuesto donde se asegure una alta disponibilidad, así como describir los elementos necesarios, y su impacto en el TCO, para aprovechar al máximo la solución propuesta.
1.1.8	La solución debe permitir el despliegue de motores de puertas de enlace en redes internas, para permitir establecimiento de sesiones con sistemas dentro de la red.
1.1.9	La solución admitirá no menos de 100 sesiones de grabación concurrentes (RDP, Web, SQL Server, MySQL u otras) ó 800 Sesiones concurrentes SSH/Telnet por cada nodo de sesión, y podrá ampliarse para admitir miles de sesiones concurrentes.
1.1.10	Los componentes de software, servidores puente locales (Gateways), conectores o mecanismos oficiales provistos por el fabricante para enlazar de manera segura la plataforma PAM SaaS con la infraestructura híbrida de la Entidad no estarán restringidos en cantidad por licenciamiento. Estos componentes deberán estar incluidos sin costo adicional dentro de la oferta económica dimensionada para las cincuenta (50) cuentas privilegiadas base y deberán soportar un despliegue flexible y multiplataforma (ejecutándose según la arquitectura nativa del fabricante sobre

	Windows Server, distribuciones Linux empresariales o contenedores Docker) para garantizar el control de las sesiones y la rotación de credenciales.
1.1.11	Los nodos de sesión no deben ser restringidos por licenciamiento del fabricante de PAM, y deben poder ser instalados en Linux, incluyendo RHEL, Ubuntu, CentOS, Debian, Fedora, SLES (Suse Linux).
1.1.12	Los componentes de conectividad, conectores o pasarelas locales (Gateways / Proxies) provistos por el fabricante para el aislamiento y grabación de sesiones, deberán soportar esquemas de despliegue flexibles que incluyan la ejecución nativa sobre entornos de contenedores virtuales (tales como Docker, Podman o equivalentes), de acuerdo con la arquitectura oficial del fabricante de la solución PAM SaaS, asegurando la adaptabilidad con la infraestructura híbrida y los estándares de seguridad de la Entidad.
1.1.13	La solución SaaS propuesta deberá permitir la gestión de hasta 200 activos objetivo en el marco del modelo de licenciamiento ofertado para 50 cuentas privilegiadas, asegurando que la solución pueda operar dicho volumen de activos sin requerir la adquisición obligatoria de componentes adicionales no contemplados en la oferta inicial. La Entidad no restringe el modelo de licenciamiento del fabricante, siempre que se garantice la cobertura funcional del número de activos definidos.
1.1.14	Los componentes de conectividad local, conectores o pasarelas de salto (Gateways / Proxies) requeridos para la operación híbrida de la solución PAM SaaS, deberán soportar el despliegue en escenarios redundantes y de alta disponibilidad (tales como clúster Activo-Pasivo, Activo-Activo o esquemas con balanceo de carga), de acuerdo con las guías oficiales de arquitectura del fabricante, para asegurar la continuidad de las sesiones de administración sin generar puntos únicos de falla en la infraestructura de la Entidad
1.1.15	Toda la conectividad requerida entre los componentes o pasarelas de la solución propuestos por el fabricante y la plataforma SaaS central en la nube deberá ser exclusivamente saliente (Outbound) a través de protocolos seguros (HTTPS/TLS puerto 443), garantizando que el servicio opere sin requerir la apertura de puertos entrantes (Inbound) desde Internet hacia el perímetro de la Entidad. Las comunicaciones internas entre dichas pasarelas locales y los activos objetivo (servidores y bases de datos de la SFC) se realizarán a través de los puertos lógicos nativos y seguros requeridos por el fabricante para la inyección de credenciales, rotación y control de sesiones.
1.1.16	La solución no debe imponer un límite en la cantidad de motores de puertas de enlace que se puedan desplegar en las redes internas, permitiendo administrar contraseñas y establecer sesiones en diferentes redes y datacenters distribuidos geográficamente.
1.1.17	La distribución de carga y alta disponibilidad de las pasarelas locales o motores de puerta de enlace (Gateways) requeridos en el entorno híbrido de la Entidad deberá operar de forma redundante y tolerante a fallos, soportando el despliegue en escenarios distribuidos (clúster Activo-Pasivo, Activo-Activo o mediante la integración con los mecanismos de balanceo de carga de la infraestructura de la Entidad), de acuerdo con las guías oficiales de arquitectura del fabricante, garantizando la continuidad de las sesiones de administración.
1.1.18	Al ser un servicio SaaS, el fabricante de la solución debe proveer actualizaciones de seguridad automáticas, incluyendo nuevas funcionalidades y parches de seguridad para los appliances. Si estas actualizaciones requieren detener los servicios, debe existir un mecanismo de notificación y autorización.

1.1.19	Al ser un servicio SaaS, los respaldos de la solución deben ser automáticos, las grabaciones se deben almacenar en la nube del fabricante, y el servicio debe garantizar una disponibilidad del 99.9%.
1.1.20	El proveedor del PAM debe entregar diagramas de despliegues que detallen escenarios de alta disponibilidad, tolerancia a fallos y redundancia adaptables a un entorno híbrido (infraestructura On-Premise y nube Azure), detallando la cantidad de componentes, mecanismos de balanceo y requerimientos de CPU y Memoria de cada elemento propuesto.
1.2	Descubrimiento de sistemas y cuentas
1.2.1	La solución tendrá capacidad de carga masiva de sistemas administrados, cuentas privilegiadas, usuarios finales y otras configuraciones necesarias.
1.2.2	La solución tendrá la capacidad de descubrir la información de los sistemas que serán administrados, incluyendo la dirección IP, la dirección MAC, el nombre DNS, el sistema operativo y la versión, si el sistema pertenece a un dominio de Active Directory, el listado de cuentas y sus privilegios.
1.2.3	El descubrimiento de cuentas en Windows debe incluir cuentas locales en el sistema, cuentas de dominio de Active Directory que han accedido o tienen el permiso de acceder al sistema, y los privilegios de cada cuenta descubierta.
1.2.4	El descubrimiento de cuentas en Unix/Linux debe incluir cuentas locales en el sistema, y los privilegios de cada cuenta descubierta debe incluir si pertenece al grupo root (GID=0), y si la cuenta tiene permiso "sudoers".
1.2.5	La solución permitirá al administrador definir atributos personalizados tanto para los sistemas administrados como para las cuentas privilegiadas.
1.2.6	La solución tendrá la capacidad de gestionar contraseñas de todas las cuentas privilegiadas y no privilegiadas en sistemas conocidos y desconocidos, incluyendo: Windows Unix / Linux Mac OS Directorios (AD / LDAP) Bases de datos Dispositivos de red
1.2.7	La solución propuesta deberá incluir y poner a disposición de la Entidad, como parte de sus capacidades estándar de fábrica y sin costo adicional, las herramientas y documentación técnica (tales como Kits de Desarrollo de Software - SDK, APIs REST completas o ejemplos de código) que permitan la expansión de las plataformas soportadas nativamente para los escaneos de descubrimiento. El proponente deberá garantizar que cualquier configuración, uso de estas herramientas o soporte requerido para el ecosistema de la Entidad durante la vigencia del contrato esté plenamente cubierto dentro de su oferta económica global, garantizando un TCO (Costo Total de Propiedad) cerrado.
1.2.8	La solución debe permitir el descubrimiento y gestión de cuentas y secretos en las plataformas cloud, IaaS/PaaS, gestores de identidad y de secretos efectivamente utilizados por la Entidad Dicha capacidad podrá ser provista a través de conectores nativos oficiales de fábrica o mediante integraciones basadas en las APIs del fabricante, garantizando que el alcance técnico, el despliegue y el soporte directo estén completamente incluidos dentro de la oferta económica dimensionada para las cincuenta (50) cuentas privilegiadas base, asegurando un TCO cerrado y cero costos adicionales por servicios profesionales de desarrollo.

1.2.9	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.
1.2.10	La solución tendrá la capacidad de descubrir los Servicios y las Tareas Programadas de sistemas Windows para que las credenciales privilegiadas que utilizan puedan administrarse automáticamente.
1.2.11	La solución tendrá la capacidad de descubrir cuentas de dominio de Active Directory y vincular automáticamente las cuentas descubiertas a servidores miembros específicos, para así controlar quiénes pueden acceder a estos servidores miembros.
1.2.12	La solución PAM debe contar con capacidades automatizadas de descubrimiento (Discovery) que permitan identificar de manera periódica los activos objetivos de la infraestructura (servidores y bases de datos), detectando los servicios de administración expuestos (tales como RDP o SSH) y las cuentas de usuario locales, administrativas o de servicio asociadas a dichos sistemas para su posterior enrolamiento y gestión dentro de la plataforma.
1.2.13	La solución tendrá la capacidad de agrupar sistemas de destino basados en atributos de sistema, sean estos atributos definidos manualmente o descubiertos por la solución.
1.2.14	La solución tendrá la capacidad de agrupar sistemas y cuentas en función del resultado de consultas AD / LDAP.
1.2.15	La solución ofrecerá auto-onboarding automático de sistemas Windows unidos a un dominio Active Directory, simplemente con conocer la OU (Organizational Unit) al que estos pertenecen.
1.2.16	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.
1.2.17	La solución tendrá la capacidad de programar tareas que le permitan descubrir nuevas cuentas privilegiadas y de incorporarlas automáticamente para la gestión de contraseñas.
1.2.18	La solución podrá descubrir cuentas locales en bases de datos SQL Server y Oracle, para tener visibilidad sobre las mismas y para aplicar la auto-gestión de estas cuentas.
1.2.19	La solución debe ser capaz de descubrir instancias de máquinas virtuales alojadas en VMware, Azure u Oracle.
1.3	Administración de cuentas privilegiadas y secretos (cambios automáticos de contraseñas y control de acceso a las mismas)
1.3.1	La solución propuesta deberá incluir y garantizar la capacidad técnica de realizar cambios y rotaciones automáticas de contraseñas, secretos o llaves de acceso sobre los componentes del ecosistema tecnológico de la Entidad (incluyendo sistemas operativos empresariales Windows/Linux, bases de datos corporativas, directorios de identidad y componentes de infraestructura híbrida y nube detallados en el anexo técnico). Dicha capacidad podrá ser provista a través de conectores nativos de fábrica o mediante la implementación de integraciones oficiales basadas en las APIs del fabricante, asegurando que el alcance de la configuración y el soporte directo estén completamente incluidos dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base, garantizando un TCO cerrado.
1.3.2	Además de las plataformas compatibles de fábrica, la solución tendrá la flexibilidad y la interfaz fácil de usar para configurar una plataforma personalizada para administrar la contraseña de la cuenta. La función de plataforma personalizada debe

	ser fácil de usar y permitir al usuario (el cliente) realizar la configuración sin la participación del proveedor del producto.
1.3.3	La solución propuesta deberá incluir y garantizar la capacidad técnica de realizar cambios y rotaciones automáticas de contraseñas, tokens, llaves de API y secretos sobre las plataformas y componentes del ecosistema cloud de la Entidad detallados en el anexo técnico (incluyendo componentes multi-cloud, identidades de servicios, credenciales de automatización y orquestadores). Dicha capacidad podrá ser provista a través de conectores nativos oficiales de fábrica o mediante la implementación de integraciones basadas en las capacidades de extensibilidad y APIs del fabricante, asegurando que el alcance de la configuración y el soporte directo estén completamente incluidos dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base, garantizando un TCO cerrado.
1.3.4	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.
1.3.5	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, mediante una cuenta de reconciliación.
1.3.6	La solución tendrá la flexibilidad de restablecer y aleatorizar las contraseñas de las cuentas al finalizar el tiempo solicitado por el usuario final, para eliminar el riesgo de que las contraseñas se vean comprometidas.
1.3.7	La solución admitirá la recuperación de la contraseña basada en el tiempo mediante la cual la contraseña solicitada se restablece automáticamente al vencimiento del plazo otorgado.
1.3.8	La solución tendrá la capacidad de desbloquear la cuenta al cambiar su contraseña.
1.3.9	La solución tendrá la capacidad de establecer la frecuencia de cambio de contraseña en función de la fecha y la hora.
1.3.10	La solución debe tener la capacidad de cambiar la contraseña bajo demanda, para sistemas individuales, grupales y administrados en función de criterios específicos.
1.3.11	La solución tendrá la capacidad de hacer cumplir la integridad de la contraseña, verificando que las contraseñas almacenadas en la solución sean las mismas contraseñas de los diferentes sistemas y restableciendo automáticamente las contraseñas de las cuentas cuya verificación sea fallida, además debe permitir notificación por correo de estas discrepancias.
1.3.12	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.
1.3.13	La solución tendrá la capacidad de sincronizar la misma contraseña para diferentes cuentas seleccionadas que residen en múltiples sistemas con diferentes tipos de plataforma.
1.3.14	La solución mantendrá el historial de contraseñas para cuentas privilegiadas administradas y proporcionará una manera fácil de ver las contraseñas antiguas a través de la interfaz web de la solución.
1.3.15	La solución admitirá la gestión de llaves SSH a través del almacenamiento automatizado de llaves SSH y la rotación de llaves SSH de acuerdo con un cronograma definido.

1.3.16	La solución admitirá la generación de llaves SSH con tipos de clave DSA y RSA y tamaño de clave configurable.
1.3.17	La solución tendrá la capacidad de cambiar la clave SSH bajo demanda para sistemas individuales, grupales y administrados en función de criterios específicos.
1.3.18	La solución propuesta deberá permitir que, inmediatamente después de ejecutarse la rotación automática de una contraseña, se realicen de forma segura las acciones de propagación, sincronización y actualización de la nueva credencial en los sistemas dependientes (tales como reinicio de servicios Windows, actualización de tareas programadas, modificación segura de archivos de configuración o actualización de secretos en repositorios externos). Estas acciones podrán ejecutarse mediante capacidades nativas, conectores certificados, APIs oficiales o plugins documentados y soportados directamente por el fabricante del PAM.
1.3.19	Todas las capacidades, APIs, conectores y componentes de integración necesarios para ejecutar las acciones de propagación y sincronización de credenciales descritas en el numeral anterior deberán estar completamente incluidos dentro del licenciamiento y alcance general de la solución SaaS ofertada, garantizando su funcionamiento estándar desde el despliegue inicial sin incurrir en cobros de licencias adicionales ni requerir la contratación de servicios profesionales complementarios del fabricante.
1.3.20	La solución PAM SaaS deberá incluir una capacidad de Bóveda de Secretos (Secrets Vault) técnicos para la organización de las credenciales y llaves operativas de los equipos de trabajo de TI encargados de la administración de la plataforma.
1.3.21	La bóveda de secretos del PAM debe poder ser accedida desde un portal o consola web para humanos, y desde una API REST para entidades no humanas o scripts automatizados.
1.3.22	La bóveda de secretos del PAM debe permitir almacenar credenciales (usuario/contraseña), almacenar archivos para cubrir la custodia de certificados digitales o llaves privadas, y almacenar líneas de texto para cubrir cadenas de conexión (Connection Strings).
1.3.23	Las capacidades de gestión, almacenamiento e integración de secretos técnicos descritas en este bloque no deberán requerir licenciamiento adicional y estarán incluidas en la suscripción general de las cincuenta (50) cuentas del proyecto.
1.3.24	El componente de secretos deberá permitir que el personal técnico de TI almacene y comparta credenciales operativas de forma segura entre equipos de trabajo mediante estructuras de carpetas, contenedores lógicos o cajas fuertes (Safes) controladas.
1.3.25	La bóveda de secretos del PAM debe poder ser accedida utilizando autenticación fuerte, protocolos basados en estándares modernos como FIDO2 y Single Sign-On (SSO) con cualquier proveedor de identidades corporativo bajo protocolo SAML.
1.3.26	Para facilitar la inyección segura de credenciales y la agilidad operativa del personal técnico, la solución deberá contar con interfaces oficiales de integración, consolas web unificadas o extensiones de software del fabricante compatibles con los principales navegadores web corporativos del mercado (tales como Chrome, Edge o Firefox).
1.3.27	La bóveda de secretos del PAM debe poder ser accedida de forma completa y directa desde cualquier navegador web estándar del mercado a través de su consola nativa, sin requerir la instalación obligatoria de una extensión de navegador para su funcionamiento central.
1.3.28	Se elimina

1.3.29	La bóveda de secretos del PAM debe permitir la importación masiva de secretos técnicos mediante el procesamiento de archivos estructurados en formato estándar separado por comas (CSV).
1.4	Gestión de sesiones (solicitud de sesiones grabadas y sin VPN)
1.4.1	La solución admitirá la supervisión y el registro del acceso de sesión privilegiado a través de los protocolos estándar como RDP y SSH y HTTPS y otros. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso (inyección de contraseñas).
1.4.2	La solución debe abstraer la ubicación de los usuarios finales privilegiados, permitiendo conexiones remotas desde Internet y sin requerir clientes VPN.
1.4.3	La solución admitirá el monitoreo y la grabación de sesiones privilegiadas para el acceso de cualquier aplicación de cliente para clientes gruesos de Windows, incluidos, entre otros, vSphere Client, Microsoft SQL Management Studio, SQL Developer, SAPGui, Toad y navegadores web. El inicio de sesión automático sin exponer la contraseña de la cuenta privilegiada debe ser compatible con este tipo de acceso.
1.4.4	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.
1.4.5	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 para acceso SSH.
1.4.6	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.
1.4.7	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.
1.4.8	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.
1.4.9	La solución tendrá la opción de configuración para forzar el cierre de sesión al finalizar el tiempo solicitado.
1.4.10	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 solución debe permitir búsquedas de pulsaciones o palabras clave en el total de sesiones grabadas.
1.4.11	La solución tendrá la capacidad de enmascarar contraseñas ingresadas durante sesiones RDP y SSH, para evitar que se muestren durante revisiones de auditorías.
1.4.12	La solución tendrá la capacidad de bloquear la sesión SSH cuando se ejecute un comando en la lista negra y, opcionalmente, enviar una notificación por correo electrónico al personal designado al detectar la ejecución de esos comandos.
1.4.13	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.
1.4.14	La solución permitirá al usuario autorizado reproducir la grabación seleccionada desde la interfaz web sin la necesidad de instalar software de cliente de terceros.

1.4.15	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.
1.4.16	La capacidad de reproducción de la sesión admitirá la reproducción de avance rápido.
1.4.17	El reproductor de video nativo en la consola SaaS de la plataforma debe permitir a los auditores insertar marcas de tiempo y notas de auditoría textuales directamente sobre la línea de tiempo de la sesión grabada, facilitando el análisis forense post-incidente de forma centralizada en la nube del fabricante
1.4.18	La solución admitirá el monitoreo en vivo de sesiones desde la interfaz web sin la necesidad de instalar software de cliente de terceros.
1.4.19	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.
1.4.20	La solución debe tener la opción de configuración para desactivar la grabación para el acceso a la sesión privilegiada seleccionada, pero aún así proporcionar la función de inicio de sesión automático.
1.4.21	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.
1.4.22	La solución tendrá la capacidad de archivar sesiones grabadas en el almacenamiento al menos por 90 días.
1.4.23	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.
1.4.24	La solución tendrá la capacidad de garantizar la integridad de las sesiones grabadas para evitar la manipulación.
1.4.25	La solución admitirá la grabación de sesiones con inicio de sesión automático para el sistema Windows donde el agente de autenticación RSA se implementa para la autenticación de dos factores.
1.4.26	La solución propuesta deberá tener la capacidad técnica de soportar, aislar y auditar flujos de sesión privilegiada hacia plataformas Windows que tengan habilitada de forma obligatoria la autenticación mediante tarjetas inteligentes (*Smart Card* / Certificados PKI). La plataforma deberá permitir mecanismos de inicio de sesión automatizado o inyección segura basados en las capacidades estándar de integración del fabricante (tales como emulación de Smart Cards virtuales, certificados efímeros o integraciones nativas de Single Sign-On). El proponente deberá incluir todas las configuraciones y componentes necesarios para este despliegue dentro de su oferta económica global cerrada para las cincuenta (50) cuentas privilegiadas base, ejecutando la integración de forma conjunta con el equipo de infraestructura de la Entidad en la fase de implementación.
1.4.27	La solución admitirá sesión SSH privilegiada en entornos de acceso de shell restringido.
1.4.28	La solución permitirá establecer sesiones SQL Server lanzando el cliente correspondiente (SQL Server Management Studio o Data Studio) en la estación de trabajo del usuario solicitante, sin mostrar la contraseña a los usuarios solicitantes y grabando todos los Queryx ejecutados.
1.4.29	El proveedor debe ofrecer un componente de acceso remoto seguro (arquitectura tipo bastión o gateway de salto) que permita establecer sesiones sobre activos críticos mediante protocolos estándar (RDP, SSH, Web/HTML5), de forma agentless y sin VPN, con inyección automatizada de credenciales desde la bóveda central de la

	solución propuesta. Dicho componente podrá ser nativo del fabricante PAM o integrado oficialmente bajo su portafolio de soporte.
1.4.30	El módulo de acceso remoto de la solución PAM debe integrarse de forma nativa con protocolos de autenticación federada basados en el estándar SAML (Security Assertion Markup Language). Asimismo, debe integrarse con sistemas de gestión de mesas de servicio (Sistemas de Tickets/ITSM) mediante conectores integrados de fábrica o plugins oficiales provistos y soportados directamente por el fabricante, permitiendo la validación automatizada del identificador del ticket antes de autorizar el acceso al activo objetivo.
1.4.31	El módulo de acceso remoto del PAM debe permitir el control total, supervisión interactiva y gestión completa sobre las sesiones de los sistemas operativos de los activos objetivos (como servidores Windows/Linux y bases de datos), asegurando el control absoluto de la interfaz gráfica (RDP, Web) o de línea de comandos (SSH), permitiendo la interacción remota segura sin que el tráfico de datos o de red sea desviado fuera del perímetro controlado por el PAM.
1.4.32	El módulo de acceso remoto de la solución PAM debe operar bajo una arquitectura 100% basada en navegador web (HTML5) o pasarela de saltos segura, por lo cual no debe requerir la instalación de software, agentes o clientes pesados en los equipos de los administradores o terceros, así como tampoco debe requerir el establecimiento de túneles VPN tradicionales para el inicio y desarrollo de las sesiones autorizadas.
1.4.33	El componente de acceso remoto seguro (arquitectura bastión/gateway) podrá ser nativo del fabricante PAM o provisto por un socio tecnológico bajo acuerdo oficial, siempre que el fabricante asuma responsabilidad integral de soporte y garantía. El proceso de inyección de credenciales privilegiadas en las sesiones de los activos objetivos (RDP, SSH, Web) debe realizarse de manera automatizada y directamente cifrada en la memoria del flujo de la sesión, garantizando que el usuario o tercero no tenga visibilidad del texto plano de la credencial y eliminando la necesidad de repositorios de contraseñas secundarios o sincronizaciones externas.
1.4.34	El módulo de acceso remoto debe realizar la grabación indexada y completa (en formato de video reproducible y traza de texto de comandos/eventos) de todas las sesiones ejecutadas sobre los activos objetivos. Asimismo, la solución debe integrarse de forma nativa con plataformas SIEM (Security Information and Event Management) mediante el envío de logs estructurados bajo estándares internacionales de la industria (como Syslog, CEF o LEEF) o mediante conectores oficiales de fábrica, garantizando la transmisión en tiempo real de las alertas de auditoría y cumplimiento sin requerir desarrollos de código a medida.
1.5	Administración de la solución y flujos de trabajo
1.5.1	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.
1.5.2	La solución deberá contar al menos con los roles de solicitante, aprobador y revisor para la segregación de funciones, y estos deben poder ser asignados granularmente sobre cuentas privilegiadas, sobre dispositivos administrados, o en una combinación.
1.5.3	Para asignar los roles de Solicitante, Aprobador o Revisor, 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. usuarios apropiados para solicitud.

1.5.4	Para asignar y estructurar los roles de Solicitante, Aprobador o Revisor sobre cuentas y sistemas del dominio de Active Directory, la solución propuesta deberá garantizar la capacidad de agrupar y organizar dichos elementos basándose en atributos de directorio (tales como Organizational Unit - OU, Security Groups o SAMAccountName). Esta capacidad podrá ser provista de forma nativa en el núcleo de la herramienta o mediante capacidades de configuración, integración o componentes complementarios provistos por el fabricante, asegurando que el alcance de la implantación y todo el licenciamiento necesario estén completamente incluidos dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base, garantizando un TCO cerrado.
1.5.5	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.
1.5.6	La solución propuesto debe permitir flujos de aprobación ágiles e integrados mediante notificaciones interactivas o enlaces directos (por ejemplo, vía correo electrónico corporativo), garantizando que, al interactuar con el mecanismo de autorización, la plataforma SaaS exija de manera obligatoria la autenticación previa y segura del usuario aprobador antes de conceder cualquier acceso privilegiado, asegurando la trazabilidad, el no repudio y el registro completo de la identidad del autorizador.
1.5.7	La solución propuesta deberá garantizar la flexibilidad de especificar y parametrizar a través de su interfaz de configuración web flujos de aprobación que admitan cero, uno o múltiples aprobadores para cuentas individuales o grupales, permitiendo establecer esquemas de control dual granularmente asignados. El alcance de la consultoría para el diseño, configuración y despliegue de estos flujos de trabajo sobre el ecosistema de la Entidad deberá estar completamente incluido, sin costo adicional, dentro de la oferta económica global cerrada para las cincuenta (50) cuentas privilegiadas base.
1.5.8	La solución tendrá la capacidad de restringir la cantidad y el marco de tiempo en el que los usuarios pueden solicitar contraseñas y sesiones a los sistemas administrados.
1.5.9	La solución tendrá la capacidad de restringir la dirección IP de la computadora del usuario donde se realizan solicitudes de contraseña y sesión.
1.5.10	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.
1.5.11	La solución debe ser configurable para permitir al usuario autorizado acceso a una cuenta privilegiada seleccionada para casos de emergencia.
1.5.12	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.
1.5.13	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.
1.5.14	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.

1.5.15	La solución tendrá la capacidad de enviar notificaciones por correo electrónico al personal designado en caso de falla en el cambio de contraseña.
1.5.16	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.
1.5.17	La solución tendrá la capacidad de permitir la personalización de plantillas de correo electrónico.
1.6	Interfaz de usuario
1.6.1	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.
1.6.2	La solución deberá tener una única interfaz de autoservicio que permita al usuario solicitar cuentas y sesiones privilegiadas.
1.6.3	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.
1.6.4	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.
1.6.5	La solución permitirá al usuario ver y buscar solicitudes antiguas, existentes y pendientes.
1.6.6	Todos los módulos y componentes de la solución PAM, incluyendo el módulo de acceso remoto seguro (arquitectura tipo Bastión/Gateway), deberán estar centralizados y alojados bajo el mismo portal e interfaz web de administración y usuario, con el fin de simplificar los flujos de solicitud de accesos, el control operativo, la auditoría y la gestión unificada de la plataforma. Todo el alcance de esta visualización centralizada deberá estar incluido sin costo adicional dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base.
1.7	Auditoría y reportes
1.7.1	La solución deberá respaldar la auditoría y la rendición de cuentas donde se registra cada transacción para cada solicitud.
1.7.2	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.
1.7.3	La solución propuesta deberá proporcionar las capacidades de auditoría y reporting nativas listas para usar, sin componentes de software adicionales y sin costo adicional, que permitan extraer, visualizar y exportar la información operativa asociada a los siguientes objetivos de control: Trazabilidad de credenciales: Información sobre la antigüedad, fecha de último cambio, resultados de los cambios y próximas programaciones de modificación de contraseñas de las cuentas bajo administración. Actividad de accesos: Registro transaccional detallado de las solicitudes, aprobaciones, liberaciones de credenciales y conciliación posterior al cierre de sesiones.

	Derechos y gobernanza: Reporte detallado de asignación de accesos ("quién tiene acceso a qué cuentas") e identificación de cambios delta (cuentas agregadas o eliminadas en períodos diarios, semanales o mensuales). Inventario integral: Listado de sistemas y cuentas descubiertas en la red, indicando cuáles se encuentran bajo administración (managed) y cuáles no (unmanaged), agrupados por sistema operativo. Cuentas de servicio: Visibilidad detallada de los sistemas e infraestructura TI que utilizan cuentas de servicio privilegiadas para levantar servicios o dependencias de aplicaciones. Estas capacidades podrán ser cubiertas mediante plantillas predefinidas, tableros de control integrados (dashboards) o consultas nativas de fábrica dentro de la plataforma, garantizando que el 100% de este alcance esté incluido dentro de la oferta económica para las cincuenta (50) cuentas privilegiadas base.
1.7.4	La reportería, métricas de uso y registros de auditoría de todos los módulos de la solución, incluyendo el módulo de acceso remoto seguro (arquitectura tipo Bastión/Gateway), deberán estar centralizados y disponibles desde el mismo portal web de la plataforma, garantizando una visibilidad holística, trazabilidad unificada y cumplimiento normativo sin necesidad de correlacionar registros desde consolas externa
1.8	Autenticación, seguridad y cumplimiento
1.8.1	La solución debe acreditar evaluación independiente de seguridad mediante: (a) Common Criteria EAL2+; (b) FIPS 140-2/3 Nivel 2+ con SOC 2 Tipo II vigente; o (c) combinación de ISO 27001 + SOC 2 Tipo II + FedRAMP Moderate/High o equivalente internacional, presentando evidencia documental vigente a nombre del fabricante.
1.8.2	La solución no deberá contener credenciales codificadas que no puedan administrarse.
1.8.3	La solución tendrá la capacidad de integrarse con múltiples métodos de autenticación empresarial, incluidos Active Directory, LDAP, Smart Card, RADIUS y servicios de autenticación robusta.
1.8.4	La solución deberá permitir la autenticación integrada con SAML para el inicio de sesión único (SSO - Single Sign On).
1.8.5	La solución tendrá la capacidad de integrarse con multiples directorios AD / LDAP, simultáneamente.
1.8.6	La solución admitirá la aplicación de una autenticación fuerte con RADIUS Two Factor Authentication (2FA).
1.8.7	La solución tendrá la capacidad de revocar temporalmente a los usuarios seleccionados para evitar que accedan a la misma solución PAM. Al integrarse con AD / LDAP para la autenticación, revocar al usuario en la solución no deberá deshabilitar ni bloquear la cuenta AD / LDAP.
1.8.8	La solución PAM debe incluir mecanismos para asignar etiquetas o categorías de clasificación a los activos y cuentas administradas, permitiendo organizar el inventario de activos críticos por tipo, criticidad o grupo funcional, y facilitar la aplicación de políticas de acceso diferenciadas según la categoría asignada.
1.9	Automatización mediante API
1.9.1	La solución proporcionará la capacidad de explotar sus funcionalidades a traves de un conjunto de servicios RESTful API con características integrales listos para usar sin ningún componente adicional y sin costo adicional.

1.9.2	El API REST del PAM y la gestión de secretos no debe requerir licenciamiento adicional.
1.9.3	La solución PAM debe incluir mecanismos nativos para sincronizar credenciales y secretos entre plataformas *on-premises* y bóvedas en la nube (Cloud Vaults). Para activos o plataformas específicas que requieran conectores personalizados o configuraciones de integración, el proponente deberá suministrar e implementar dichos desarrollos como parte integral de la solución estándar. El contratista será responsable del soporte, mantenimiento y actualización de estas integraciones, las cuales deberán estar incluidas al 100% dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base, sin costos adicionales por servicios profesionales.
1.9.4	La solución PAM propuesta deberá permitir y garantizar la capacidad técnica de sincronizar, replicar o exportar secretos de manera segura hacia bóvedas externas y repositorios del ecosistema de la Entidad. Dicha capacidad podrá ser satisfecha mediante funcionalidades nativas de fábrica o a través de mecanismos de interoperabilidad oficiales basados en APIs, utilidades o scripts oficialmente soportados y respaldados por el fabricante, asegurando que el alcance completo de la configuración y puesta en marcha esté incluido dentro de la oferta económica global para las cincuenta (50) cuentas privilegiadas base, garantizando un TCO cerrado y sin requerir la contratación de servicios profesionales complementarios.
1.9.5	La solución ofrecerá un Kit de desarrollo de software (SDK) que puede abordar casos de esquina, utilizando API disponibles para prácticamente todas las plataformas para permitir el acceso programático en tiempo real a las contraseñas. El SDK permite que las aplicaciones y las personas accedan al almacén de contraseñas de forma independiente, sin usar la interfaz original del producto.
1.9.6	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.
1.9.7	La solución proporcionará documentación API y programas API de muestra en al menos alguno de los siguientes lenguajes de programación: Python, C #, Java, PowerShell, Ruby y Unix Shell Script.
1.10	Integraciones
1.10.1	Integración SIEM: la solución debe tener una integración nativa con algunas de las siguientes soluciones SIEM para reenviar eventos. 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. (Exabeam, Archsight, Qradar, LogRhythm, McAfee DXL y ESM, NetIQ, Syslog, XML, JSON)
1.10.2	Integración del sistema de tickets: la solución debe tener una integración nativa con algunos de los siguientes sistemas Mesa de Ayuda para la validación de tickets: BMC, CA Service Desk, JIRA, ServiceNow
1.10.3	Integración ITSM: la solución debe tener una integración nativa con las siguientes soluciones ITSM para exportar información de activos: BMC Remedy, ServiceNow
1.10.4	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, GoGrid, GCP, IBM SmartCloud, Microsoft HyperV, Rackspace, VMWare vCenter

1.10.5	La solución PAM debe poseer la capacidad de integrarse con tecnologías de PEDM (Privileged Elevation and Delegation Management) para el control dinámico de privilegios en servidores, y con soluciones CIEM (Cloud Infrastructure Entitlement Management) para el control dinámico de privilegios en entornos de nube, ya sea mediante módulos nativos, APIs REST de la plataforma o conectores soportados oficialmente por el fabricante.
1.10.6	El sistema debe permitir la integración con plataformas de Automatización Robótica de Procesos (RPA) o herramientas de automatización de operaciones de TI mediante APIs REST, SDKs o mecanismos oficiales de interoperabilidad provistos por el fabricante, con el fin de asegurar el consumo controlado de accesos privilegiados en sistemas críticos por parte de bots o scripts automatizados.
1.10.7	El sistema debe permitir la integración con componentes de orquestación de contenedores tales como External Secrets Operator y Secrets-Agent de Kubernetes o equivalentes, utilizando capacidades nativas de la solución o APIs seguras oficialmente respaldadas por el fabricante para la inyección y rotación de secretos en entornos contenerizados.
1.11	Licenciamiento
1.11.1	El modelo de licenciamiento propuesto para 50 cuentas privilegiadas debe garantizar que la gestión de hasta 200 activos objetivo (servidores y bases de datos) no genere costos adicionales de licencia durante la vigencia del contrato. El oferente acreditará esta condición mediante carta del fabricante o ficha técnica de licenciamiento que especifique que el precio ofertado incluye la gestión de dichos activos sin restricción por cantidad.
1.11.3	El modelo de licenciamiento comercial propuesto, dimensionado para las 50 cuentas privilegiadas base de la Entidad, no deberá imponer costos ocultos, restricciones ni licenciamientos complementarios por la cantidad de activos objetivo (endpoints/targets) registrados para su custodia o auditoría dentro de los límite
1.11.4	El licenciamiento de la solución PAM no debe limitar la cantidad de cuentas privilegiadas o secretos que podrán ser almacenadas y gestionadas por la misma. La cantidad de credenciales y secretos debe ser estrictamente ilimitada.
1.11.5	La bóveda de secretos personal debe estar incluida como funcionalidad nativa, sin requerir licenciamiento adicional.
	El contratista deberá entregar la supervisión durante el plazo de ejecución del contrato la documentación técnica y funcional completa de la solución PAM implementada, la cual deberá incluir, como mínimo, manuales de instalación y configuración, guías de administración y operación, procedimientos de gestión de cuentas privilegiadas, esquemas de control y auditoría, así como documentación de seguridad asociada. La documentación deberá entregarse en idioma español, en formato digital editable, y mantenerse actualizada conforme a la configuración final implementada en la Entidad.
	El contratista deberá definir documentar e implementar y entregar dentro del plazo de ejecución del contrato, la arquitectura técnica de la solución de Gestión de Accesos Privilegiados (PAM), describiendo de manera clara sus componentes, integraciones, flujos de acceso, mecanismos de autenticación, autorización y auditoría, así como su interacción con los sistemas, aplicaciones e infraestructuras tecnológicas de la Entidad. La arquitectura deberá alinearse con los lineamientos de seguridad de la información, los principios del SGSI y las buenas prácticas de ciberseguridad, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de los accesos privilegiados.

	El contratista deberá realizar la transferencia de conocimiento asociada a la implementación de la solución PAM, garantizando que el personal técnico de la Entidad comprenda la arquitectura, configuración, flujos de operación, controles de acceso, esquemas de autorización y mecanismos de auditoría implementados. Esta transferencia deberá permitir a la Superintendencia Financiera de Colombia contar con la capacidad técnica para administrar, mantener y operar la solución de manera autónoma, así como atender eventos operativos y de seguridad relacionados con el uso de cuentas privilegiadas. Esta deberá ser llevada a cabo durante el plazo de ejecución del contrato al momento de la implementación en un horario comprendido de 3 horas, sin costo alguno para la entidad.
1.11.6	El licenciamiento de la solución no deberá restringir ni limitar la cantidad de túneles seguros, pasarelas de salto (Gateways/Proxies locales), conectores o mecanismos de comunicación automatizada saliente (Outbound) que sean necesarios desplegar dentro de la infraestructura híbrida de la Entidad para establecer sesiones, ejecutar descubrimientos o realizar rotaciones de contraseñas.
1.12	Servicios
1.12.1	La solución podrá ser implementada por el proveedor local si el mismo cuenta con la certificación del fabricante y no deben ser obligatorios los servicios profesionales del fabricante.
1.12.2	Las actualizaciones de software deben estar documentadas para ser implementadas por la organización o automáticamente, sin requerir servicios profesionales del fabricante.
1.13	Soporte
1.13.1	La solución debe contar con soporte técnico por parte del contratista de en disponibilidad 7x24x365 Ilimitada cantidad de incidentes.
1.13.2	La solución deberá ser suministrada en su última versión
1.13.3	Instalar las actualizaciones del software licenciado por la SUPERINTENDENCIA, cada vez que se liberen nuevas versiones o correcciones (parches), proporcionando los medios de instalación y la documentación respectiva o mediante la descarga desde un sitio Web.
1.13.4	El contratista deberá BRINDAR soporte y asistencia técnica telefónica y/o presencial (en caso de requerirse) para toda la solución en producción incluyendo las nuevas funcionalidades, necesarias para la instalación de nuevas versiones y/o correcciones (patches) que se suministren, o para la atención a problemas, incidentes, consultoría o implementación de nuevas funcionalidades que puedan presentarse, durante la vigencia del licenciamiento renovado, para los componentes que hacen parte del objeto de la contratación.
1.13.5	Entregar alertas y notificaciones proactivas durante la vigencia del licenciamiento.
1.13.6	Para garantizar la continuidad operativa de la solución PAM, se solicita la entrega de una Matriz de Escalamiento Jerárquico y Funcional. Esta matriz debe detallar los puntos de contacto disponibles 7x24x365, asegurando que ante un incidente crítico existan canales de comunicación directos con niveles de supervisión y gerencia, independientemente de los tiempos de resolución finales. suministrado por el contratista
1.13.7	En eventos de indisponibilidad masiva o degradación crítica atribuibles directamente al software/solución (Bug, vulnerabilidad Zero-Day o falla de arquitectura del Fabricante), el CONTRATISTA se obliga a facilitar de manera inmediata una comunicación con la super financiero para dar aviso y dar por enterado los tiempos de alcance y posible solución y puesta en marcha de la solución

1.13.8	En caso de que el equipo de soporte del CONTRATISTA no logre diagnosticar, dar alcance o proponer una solución efectiva lo más pronto posible, el CONTRATISTA se obliga a escalar de forma inmediata el caso ante el FABRICANTE de la solución PAM. El CONTRATISTA deberá gestionar y coordinar una sesión de soporte conjunto (Contratista - Fabricante - Cliente) para la resolución del problema. El desconocimiento técnico por parte del personal del CONTRATISTA no será excusa para el incumplimiento de los tiempos de respuesta y no exime al CONTRATISTA de liderar la gestión hasta la resolución definitiva del incidente

En constancia de lo anterior se firma por,

EDGAR YESID GARAY MEDINA
Firmado digitalmente por EDGAR YESID GARAY MEDINA
Fecha: 2026.07.31 10:00:25 -05'00'

Edgar Yesid Garay Medina
Estructurador Técnico
Asesor
Dirección de Tecnologías de la Información

CARLOS ARTURO D ´OTERO BISCARDI
Firmado digitalmente por CARLOS ARTURO D´OTERO BISCARDI
Fecha: 2026.07.31 09:47:13 -05'00'

Carlos Arturo D Otero Biscardi
Estructurador Técnico
Profesional
Subdirección de Operaciones