

ANEXO DE ESPECIFICACIONES TÉCNICAS

La entidad requiere adquirir una solución de Gestión de Accesos Privilegiados (PAM) para la administración, control, monitoreo y auditoría de accesos privilegiados sobre la infraestructura tecnológica de la Secretaría Distrital de Cultura, Recreación y Deporte – SCRD

Servicio de gestión de accesos privilegiados (PAM)	Cantidad
Adquisición del licenciamiento en suscripción de la solución PAM para diez (10) administradores nominales por doce (12) meses.	10
Implementación, puesta en marcha y parametrización de la solución de PAM	1
Especialista en Seguridad	1
Gerente de Proyectos para liderar la planificación, el seguimiento y la ejecución del proyecto.	1
Bolsa de horas de soporte	50

Condición general de la solución:

La solución PAM ofertada deberá corresponder a una solución integrada de un único fabricante bajo una sola plataforma nativa. No se aceptará la utilización de software de código abierto dentro de la solución ofertada.

Especificaciones Técnicas Requeridas

1. La solución debe permitir una implementación modular de los controles a nivel de Administración de Cuentas Privilegiadas:
 - SAPM Shared Accounts Management
 - AAPM Application to Application Password Management
 - PSM: Privileged Session Management
 - SUPM: Superuser Privileged Management
2. La solución debe permitir soportar al menos los siguientes sistemas objetivos:
 - Servidores Windows
 - Servidores UNIX/LINUX
 - Servidores ORACLE

- Mainframes IBM
- Dispositivos de red
- Servicios en la nube
- Plataformas WEB de diferentes Fabricantes

Para efectos del dimensionamiento del proceso, se estima un alcance de aproximadamente ciento diez (110) servidores. El despliegue del agente se realizará principalmente sobre plataformas Windows y Linux/Unix, de acuerdo con el alcance definido por la Entidad

3. La solución debe soportar tecnologías de Bases de datos (RDBMS) o Directorios (LDAP) para su repositorio.
4. La solución debe soportar los siguientes modos y entornos de trabajo en modo seguro:
 - Modo: FIPS 140-2 o FIPS 140-3
 - Entorno: IPv4 y IPv6
5. La solución debe almacenar la información de los usuarios y contraseñas en forma encriptada en su repositorio propio de usuarios.
6. La solución debe permitir controles de acceso granulares basado en perfiles de tiempo (día/fecha/hora) a nivel de usuario o de grupo de usuarios
7. La solución SAPM debe poder ser provista en los siguientes factores de forma:
 - Virtual Appliance (VMware, OVA, KVM)
 - En la nube (Azure: Nube de Microsoft en formato VHD)

Este despliegue debe contemplar adicionalmente lo siguiente:

- Híbrido, una parte On-Premise y su replicación en nube
 - No requerir de motores de base de datos
 - No requerir de sistemas operativos
8. La solución SAPM debe permitir soportar la Administración de Cuentas Privilegiadas en los siguientes entornos de trabajo:
 - On-Premise (servidores, dispositivos de red, etc)
 - Servicios en la Nube
 - Nube privada

- Nube Privada sin acceso a internet
 - Nube pública
9. La solución SAPM debe operar utilizando módulos criptográficos validados bajo los estándares FIPS 140-2 o FIPS 140-3. La validación de dichos módulos deberá ser verificable mediante documentación o fuente oficial correspondiente.
10. Plataforma gráfica: Acceso web 7x24 a la consola de la solución PAM, que permita consultar en tiempo real e histórico la disponibilidad de sus componentes, el estado de las sesiones privilegiadas y demás indicadores relevantes del servicio.
11. La solución ofertada deberá acreditar al menos dos (2) certificaciones Common Criteria correspondientes a versiones actuales y/o anteriores de la misma solución o producto ofertado. Las certificaciones podrán corresponder a versiones distintas, siempre que permitan verificar que pertenecen a la misma línea de producto o solución tecnológica ofrecida. Su existencia y correspondencia deberán ser verificables mediante fuentes oficiales.
12. La solución debe incorporar una arquitectura de clúster activo-activo con replicación transaccional distribuida y base de datos embebida endurecida, garantizando disponibilidad continua sin requerir licenciamiento de bases de datos externas.
13. La solución debe tener la capacidad para forzar la rotación periódica y automática de credenciales administrativas en sistemas Windows, Linux, Unix y bases de datos, mediante políticas de complejidad estricta y verificación inmediata de sincronización.
14. La solución debe tener el mecanismo de liberación controlada de credenciales en contingencia (Break-Glass) con doble aprobación requerida, notificación automática, rotación obligatoria e inmediata tras la ventana de emergencia y auditoría inalterable de eventos.
15. La solución debe incluir un motor de descubrimiento continuo de infraestructura y cuentas de servicio, locales y de dominio en entornos híbridos y multi-cloud, identificando credenciales huérfanas o nuevas instancias sin control centralizado de seguridad.
16. La solución debe tener integración nativa con directorios corporativos (Active Directory, Entra ID, LDAP) para el aprovisionamiento de usuarios, mapeo de roles basado en grupos y autenticación federada multifactor mediante SAML 2.0 y OIDC.
17. La solución debe tener la capacidad para descubrir, almacenar, asociar y rotar automáticamente pares de llaves SSH (privadas y públicas) en servidores Unix/Linux, eliminando el uso de llaves estáticas no reguladas en el acceso administrativo.
18. La solución debe tener un sistema de flujo de trabajo configurable para solicitud de acceso privilegiado temporal (Just-In-Time) con justificación operativa, integración con ITSM para

validación de tickets y revocación automática al expirar el periodo.

19. La solución debe tener la capacidad para crear grupos jerárquicos de dispositivos y cuentas compartidas gobernados por políticas contextuales que evalúen ubicación IP, rango horario, método de conexión y perfil del operador para autorizar accesos.
20. La solución debe tener la provisión de una bóveda centralizada con cifrado AES-256 o superior para la custodia de credenciales, donde las llaves maestras de cifrado residan exclusivamente en un módulo HSM. Se aceptará la utilización de HSM virtuales o servicios de HSM en la nube, siempre que cumplan con las condiciones técnicas y de seguridad establecidas en el presente Anexo y con la validación FIPS exigida. La SCRД proveerá las máquinas virtuales y el almacenamiento requeridos para la implementación; el HSM deberá ser provisto por el contratista y los componentes, conectores, licencias y configuraciones propios de la solución necesarios para su operación deberán estar incluidos en la oferta, sin costos adicionales para la Entidad respecto del valor ofertado.
21. La solución debe tener la capacidad de gestionar contraseñas de cuentas de servicio en tareas programadas de Windows y servicios del sistema, actualizando automáticamente las dependencias sin requerir reinicios manuales de los servidores afectados.
22. La solución debe incluir soporte para la rotación de credenciales en plataformas de virtualización y nube (VMware vCenter, AWS IAM, Azure AD, GCP), gestionando de manera unificada el acceso a las consolas de orquestación.
23. La solución debe incluir un mecanismo de comprobación de integridad de cuentas (Check Password) que valide periódicamente si la contraseña almacenada en la bóveda coincide con la definida en el sistema destino, alertando discrepancias.
24. La solución debe incluir la generación de reportes de cumplimiento y auditoría de accesos preconfigurados (PCI-DSS, SOX, ISO 27001), exportables a formatos estándar, detallando quién accedió a qué recurso, cuándo y bajo qué autorización.
25. La solución debe incluir la capacidad para delegar la administración de políticas de acceso y rotación a nivel de unidades de negocio o subsidiarias, manteniendo una segregación estricta de datos y roles en arquitecturas multi-tenant.
26. La solución debe incluir un mecanismo de autenticación robusta para la interfaz administrativa del appliance, soportando integración con tarjetas inteligentes (Smart Cards, PIV/CAC) y tokens de hardware FIDO2 para operadores de máxima seguridad.
27. La solución debe tener disponibilidad de una API RESTful documentada y bidireccional que permita automatizar el 100% de las tareas de administración, aprovisionamiento de dispositivos y gestión de políticas desde plataformas de orquestación externas.
28. La solución debe incluir la capacidad de ocultar completamente el valor en texto claro de la contraseña al operador (Password Hiding), permitiendo el uso de la credencial únicamente a

través de la inyección en sesión.

29. La solución debe incluir un módulo de gestión masiva que permita la importación, actualización y eliminación de miles de cuentas objetivo y políticas mediante archivos estructurados o scripts, optimizando el despliegue inicial y mantenimiento.
30. La solución debe contar con control de acceso concurrente (Check-out/Check-in exclusivo), bloqueando temporalmente el acceso de otros administradores a una misma cuenta compartida mientras esté siendo utilizada, evitando colisiones en cambios de configuración.
31. La solución debe tener la capacidad de personalizar scripts de rotación y verificación de contraseñas mediante lenguajes estándar o comandos de terminal para soportar sistemas legados, aplicaciones desarrolladas a la medida y appliances de red.
32. La solución SAPM debe poder gestionar las sesiones hacia los diferentes motores de bases de datos que tiene la entidad, independientemente de donde se encuentre el usuario que requiera la sesión hacia el motor de base de datos sin la necesidad de requerir licenciamiento de Windows Remote Services.
33. La solución debe incluir la provisión de conectores, librerías y daemons para reemplazar contraseñas estáticas incrustadas (Hardcoded Secrets) en scripts y archivos de configuración por llamadas dinámicas y seguras a la bóveda centralizada.
34. La solución debe tener un mecanismo de validación estricta de la aplicación solicitante mediante verificación combinada de firma digital, hash binario del ejecutable, ruta de ejecución autorizada y usuario del SO para evitar suplantaciones.
35. La solución debe tener soporte para entornos de orquestación modernos (Kubernetes, Docker), permitiendo que contenedores obtengan secretos de corta duración en tiempo de ejecución sin persistencia en imágenes ni repositorios de código.
36. La solución debe incluir un módulo cliente para aplicaciones críticas capaz de almacenar en memoria cifrada las credenciales consumidas, asegurando operatividad continua y cero impactos en los sistemas de negocio ante eventuales interrupciones de red.
37. La solución debe tener disponibilidad de SDKs y APIs nativas para lenguajes empresariales comunes (Java, .NET, Python, Go, C/C++) que faciliten la integración transparente sin necesidad de reescribir la lógica base de aplicaciones.
38. La solución debe contar con control activo para impedir que credenciales temporales o secretos invocados por llamadas a aplicaciones queden expuestos en archivos de log de depuración o volcados de memoria, forzando la sanitización inmediata.
39. La solución debe tener la capacidad para rotar contraseñas de cuentas de servicio en bases de datos y reconfigurar automáticamente grupos de conexiones (connection pools) en servidores de aplicaciones sin generar desconexiones a usuarios finales.

40. La solución debe contar con integración nativa y certificada con pipelines de integración y despliegue continuo (Jenkins, GitLab CI, Azure DevOps) para inyectar credenciales temporales de forma automatizada durante las fases de construcción y despliegue.
41. La solución debe tener capacidad de gestionar alias de aplicaciones y mapeos lógicos, permitiendo que múltiples instancias de una misma aplicación soliciten credenciales bajo una identidad consolidada para simplificar la gestión de permisos.
42. La solución debe contar con autenticación mutua mediante certificados TLS (mTLS) en todas las comunicaciones entre el agente para aplicaciones, los contenedores orquestados y el appliance central de bóveda para garantizar la confidencialidad de tránsito.
43. La solución debe incluir un mecanismo de protección contra ataques de fuerza bruta o denegación de servicio a nivel de API, implementando límites de peticiones (rate limiting) y suspensión temporal de aplicaciones infractoras.
44. La solución debe realizar la generación de trazabilidad específica para transacciones de aplicación a aplicación, registrando la IP de origen, proceso invocador, secreto solicitado y estado de la autorización para auditoría forense detallada.
45. La solución debe contar con la capacidad de crear scripts de rotación post-cambio (Post-Change Scripts) que se ejecuten automáticamente en los servidores de aplicaciones para reiniciar servicios específicos tras la rotación de la credencial en bóveda.
46. La solución debe de contar con una arquitectura escalable de alta concurrencia para el módulo de aplicaciones, capaz de procesar miles de solicitudes de credenciales por segundo para satisfacer las demandas de clústeres de microservicios empresariales.
47. La solución debe realizar la provisión de un proxy REST/SOAP intermedio que intercepte y autentique automáticamente las llamadas entre aplicaciones, inyectando los tokens de seguridad requeridos sin modificar el código del sistema cliente.
48. La solución debe incluir el soporte para la gestión del ciclo de vida de llaves de API (API Keys) y tokens OAuth de servicios de terceros, custodiándolos y entregándolos dinámicamente a las aplicaciones internas.
49. La solución debe realizar la validación de la segmentación de red en peticiones a aplicaciones, rechazando de forma proactiva solicitudes de credenciales que provengan de subredes no declaradas en la política de confianza de la aplicación.
50. La solución debe contar con una herramienta CLI centralizada que permita a los administradores de sistemas y automatizadores extraer credenciales de forma segura dentro de scripts bash o PowerShell sin exponer la lógica de autenticación.
51. La solución debe realizar la sincronización automática de políticas de acceso a secretos en nodos distribuidos geográficamente, reduciendo la latencia de respuesta para las aplicaciones

alojadas en diferentes regiones de nube o centros de datos.

- 52.** La solución debe contar con integración con plataformas de gestión de configuración de infraestructura como código (Ansible, Terraform, Chef) para recuperar parámetros secretos durante el aprovisionamiento automatizado de nuevos entornos.
- 53.** La solución AAPM debe permitir reemplazar las varias instancias de una contraseña embebida en un 'script', con una única instancia residente en la solución AAPM. Permitiendo cambiar contraseñas de servidores o de cuentas de servicio en forma automática dependiendo de las necesidades y periodicidad de la entidad.
- 54.** La solución debe incluir acceso proxy transparente a consolas y servidores (RDP, SSH, HTTPS, VNC) sin requerir software cliente en la estación del administrador ni agentes en los destinos, reduciendo superficie de ataque.
- 55.** La solución debe incluir la conexión a sesiones administrativas con auto-login donde la plataforma inyecta la contraseña o llave directamente en el canal seguro, impidiendo que el operador conozca o capture la credencial en texto claro.
- 56.** La solución debe incluir registro en video inalterable de todas las acciones gráficas (RDP/HTTPS/VNC) y transcripción completa de flujos de comandos, almacenados con cifrado y firma digital para garantizar la cadena de custodia forense.
- 57.** La solución debe contar con la capacidad de indexación por reconocimiento óptico de caracteres (OCR) sobre sesiones gráficas, permitiendo a los auditores realizar búsquedas inmediatas de palabras clave y saltar al momento exacto del video.
- 58.** La solución debe contar con prevención de exfiltración de portapapeles: Inspección de cadenas y patrones estructurados durante la sesión gráfica/terminal, bloqueando o enmascarando datos confidenciales al intentar copiarlos hacia el portapapeles del endpoint local.
- 59.** La solución debe realizar la inspección y bloqueo de transferencia de archivos: Capacidad para analizar contenido de archivos transferidos por SFTP/RDP en sesión, aplicando bloqueo inmediato ante detección de información clasificada o extensiones restringidas.
- 60.** La solución debe contar con un motor de filtrado de comandos en tiempo real para sesiones SSH y Telnet capaz de alertar, enmascarar o interrumpir la ejecución de comandos peligrosos o listas negras, desconectando la sesión instantáneamente.
- 61.** La solución debe incluir un módulo de supervisión que permite a los oficiales de seguridad observar en tiempo real sesiones en curso, unirse en modo cuatro ojos (Four-Eyes Principle) e interactuar, o forzar cierre inmediato.
- 62.** La solución debe interceptar y bloquear la carga de datos confidenciales, extraídos de sesiones privilegiadas, hacia servicios de almacenamiento web o aplicaciones en la nube personales, aplicando políticas centralizadas.

63. La solución debe realizar el aislamiento de sesiones web para consolas de nube (AWS, Azure, Portales SaaS) en un navegador virtualizado y efímero, inyectando credenciales y restringiendo la descarga de artefactos o visibilidad de secretos.
64. La solución debe contar con el soporte para proxies RDP y SSH nativos, permitiendo a los administradores utilizar sus herramientas de conexión preferidas (MSTSC, PuTTY, SecureCRT) mientras la plataforma intermedia y graba la sesión transparentemente.
65. La solución debe contar con un mecanismo de tolerancia a fallos para grabaciones de sesión, asegurando que, si la conexión con el almacenamiento central se pierde, la grabación se mantenga en un búfer local temporalmente.
66. La solución debe realizar la optimización avanzada de ancho de banda y latencia para sesiones gráficas remotas, permitiendo una experiencia de administración fluida incluso en conexiones WAN de bajo rendimiento o alta dispersión geográfica.
67. La solución debe contar con políticas de terminación automática de sesiones por inactividad o expiración del tiempo concedido en el flujo Just-In-Time, forzando la desconexión del usuario y alertando sobre intentos de reconexión.
68. La solución debe contar con la capacidad para lanzar applets de conexión integrados directamente desde el portal web del usuario, utilizando tecnologías modernas sin dependencia de plugins obsoletos como Java, Flash o controles ActiveX.
69. La solución debe contar con una herramienta dedicada para la reproducción de sesiones que permite avanzar, retroceder, acelerar la velocidad de reproducción y exportar fragmentos específicos de incidentes de seguridad para su análisis externo.
70. La solución debe contar con una integración con el portapapeles de la sesión para permitir la inyección manual de macros de comandos preaprobados o textos largos, sin necesidad de habilitar el copiado irrestricto desde la máquina local.
71. La solución debe realizar el bloqueo a nivel de protocolo de canales virtuales RDP innecesarios (redirección de impresoras, redirección de unidades locales, audio) para reducir los vectores de exfiltración o infección de malware.
72. La solución debe tener soporte para conexiones a bases de datos relacionales a través de proxies especializados, registrando y filtrando consultas SQL ejecutadas por DBAs y bloqueando sentencias DDL/DML destructivas no autorizadas.
73. La solución debe realizar el mapeo dinámico de puertos locales para aplicaciones cliente-servidor especializadas (thick clients), estableciendo túneles seguros y auditados a través del gateway PAM hacia los sistemas críticos de la organización.
74. La solución debe contar con una interfaz unificada de acceso (Workspace) que consolide en un solo panel todos los accesos aprobados del usuario, clasificados por entorno, criticidad y tipo

de conexión para una navegación eficiente.

75. La solución debe tener la capacidad para establecer límites de conexiones concurrentes globales o por usuario hacia un mismo activo crítico, previniendo la saturación de recursos en los equipos de destino.
76. La solución debe contar con mecanismos de autenticación y autorización reforzada para sesiones privilegiadas de mayor riesgo, permitiendo la implementación de controles tales como Segundo Factor de Autenticación (MFA), re-autenticación/Step-up Authentication, aplicación de políticas contextuales, flujos de aprobación jerárquica u otros mecanismos equivalentes oficialmente soportados por el fabricante que aseguren la legitimidad del acceso.
77. La solución debe realizar la redirección de la consola de administración fuera de banda (iLO, iDRAC, ALOM) a través del portal de sesiones seguras, grabando el acceso a nivel de BIOS y recuperación de desastres.
78. La solución debe contar con la capacidad para auditar e intermediar sesiones X11 para servidores Unix, capturando de manera gráfica la interacción del administrador con aplicaciones que requieren interfaz de ventanas nativa.
79. La solución debe contar con la capacidad de aplicar controles de acceso obligatorios basados en módulos de kernel en servidores Linux/Unix/Windows, interceptando llamadas al sistema para gobernar qué procesos, archivos y puertos puede manipular un administrador.
80. La solución debe realizar la neutralización de escalación de privilegios delegando tareas a usuarios estándar sin compartir la contraseña de root ni conceder permisos sudo irrestrictos, confinando la ejecución a binarios validados criptográficamente.
81. La solución debe realizar la restricción de exfiltración a medios extraíbles (Kernel-level): Bloqueo de escritura hacia dispositivos USB o montajes de red secundarios o portapapeles, interceptando llamadas al sistema en el host para proteger información clasificada.
82. La solución debe realizar la protección de integridad de archivos (FIM) con detección y bloqueo en tiempo real de modificaciones no autorizadas sobre binarios, bibliotecas compartidas y configuraciones, impidiendo alteraciones incluso por usuarios con privilegios máximos.
83. La solución debe realizar un blindaje contra evasión de auditoría (Tamper Protection) que impide a administradores locales detener los demonios de seguridad, modificar registros de auditoría o eliminar políticas de acceso desde la consola nativa.
84. La solución debe realizar la asignación dinámica de privilegios por contexto, elevando temporalmente permisos de usuarios locales únicamente durante ventanas de mantenimiento aprobadas y restaurando las restricciones de forma automática al finalizar el evento.
85. La solución debe realizar la trazabilidad inequívoca de usuarios compartidos en el host, correlacionando de forma vinculante las acciones ejecutadas por cuentas genéricas

(root/administrator) con la identidad nominativa real del usuario que inició sesión.

86. La solución debe realizar la microsegmentación basada en host que restrinja las comunicaciones de red entrantes y salientes a nivel de proceso o usuario específico, bloqueando el tráfico lateral no autorizado de cuentas comprometidas.
87. La solución debe realizar la sustitución empresarial centralizada para comandos nativos de delegación (sudo/su), unificando las políticas de escalación a través de múltiples distribuciones Unix y Linux desde una consola de gestión única.
88. La solución debe realizar la gestión proactiva del Control de Cuentas de Usuario (UAC) en entornos Windows, permitiendo a los empleados ejecutar aplicaciones corporativas requeridas sin necesidad de otorgarles privilegios de Administrador Local permanentes.
89. La solución debe contar con reglas de confinamiento (Sandboxing) para aplicaciones vulnerables expuestas a internet, limitando estrictamente el alcance de los procesos comprometidos y evitando que afecten el sistema operativo subyacente.
90. La solución debe tener la capacidad de operar y aplicar políticas de seguridad en modo desconectado, garantizando que los controles a nivel de sistema operativo permanezcan activos, aunque el agente pierda comunicación con el servidor central.
91. La solución debe contar con políticas de control de ejecución de scripts y binarios (Application Whitelisting) evaluando hashes SHA-256, firmas digitales y rutas autorizadas antes de permitir que un proceso sea invocado por el usuario.
92. La solución debe contar con un motor de control de argumentos y parámetros, permitiendo que un administrador ejecute un comando de servicio, pero bloqueando sintaxis o flags específicos (ej. permitir 'service httpd restart', bloquear 'service httpd stop').
93. La solución debe tener un módulo centralizado de distribución automatizada de políticas de kernel y agentes, permitiendo actualizar miles de servidores simultáneamente asegurando consistencia regulatoria en centros de datos distribuidos.
94. La solución debe realizar el despliegue compatible y cooperativo con herramientas nativas de seguridad de sistemas operativos modernos, como SELinux o AppArmor, agregando capas de control de usuario sin generar conflictos de kernel.
95. La solución debe realizar la interceptación de manipulaciones directas sobre el registro de Windows (Registry Keys), protegiendo claves críticas de inicio, configuración de red y políticas locales contra alteraciones maliciosas o ransomware.
96. La solución debe realizar la generación y resguardo de registros locales firmados digitalmente y enviados en tiempo real a repositorios syslog o SIEM remotos, garantizando que no haya pérdida de datos de auditoría durante ataques.
97. La solución debe tener la capacidad de aplicar políticas de aislamiento lógico de tenants y

aplicaciones dentro de un mismo sistema operativo, evitando que procesos de una unidad de negocio accedan a la memoria de otra.

- 98.** La solución debe contar con control granular de acceso a servicios y demonios del sistema, restringiendo qué cuentas de usuario pueden iniciar, detener o reconfigurar servicios críticos de bases de datos o middleware web.
- 99.** La solución debe contar con un motor de analítica basada en Machine Learning que construye perfiles de comportamiento basal por administrador y detecta patrones anómalos, tales como horarios inusuales, secuencias atípicas o acceso a recursos no habituales.
- 100.** La solución debe contar con la generación de una puntuación de riesgo contextual y dinámica en tiempo real durante la sesión interactiva, evaluando heurística de comandos, destino de conexión e interacción con configuraciones críticas.
- 101.** La solución debe tener la capacidad de accionar respuestas defensivas automáticas al superarse los umbrales de riesgo predefinidos, incluyendo notificación crítica al SOC, aumento del nivel de grabación, y terminación forzada e inmediata de la sesión.
- 102.** La solución debe contar con la integración bidireccional estructurada de eventos enriquecidos, logs firmados y alertas de comportamiento anómalo en formatos estándar (CEF, Syslog RFC 5424) hacia plataformas SIEM, XDR y herramientas de orquestación (SOAR).
- 103.** La solución debe contar con la detección de anomalías de ubicación geográfica e inconsistencias temporales (viajes imposibles), alertando si una misma credencial es utilizada desde ubicaciones físicas incompatibles con la ventana de tiempo transcurrida.
- 104.** La solución debe realizar la identificación de anomalías basadas en análisis de grupos de pares (Peer Group Analysis), detectando si un usuario accede a sistemas privilegiados que típicamente son administrados por otros equipos de TI.
- 105.** La solución debe tener visualización interactiva del riesgo de identidades (Dashboard de Amenazas), mostrando un ranking de los usuarios, cuentas de servicio y activos con mayor puntuación de riesgo para facilitar la priorización del SOC.
- 106.** La solución debe realizar la monitorización y correlación de múltiples fallos de autenticación seguidos por intentos de bóveda de contraseñas, detectando e interrumpiendo tempranamente ataques de fuerza bruta o escalamiento lateral de adversarios.
- 107.** La solución debe contar con una interfaz de Threat Hunting especializada que permita a los analistas de seguridad realizar consultas complejas sobre metadatos de sesiones, eventos de acceso y patrones de riesgo histórico para investigaciones forenses.
- 108.** La solución debe contar con algoritmos de aprendizaje continuo (Self-Learning Baselines) que ajustan automáticamente las políticas de normalidad a medida que evolucionan los roles y responsabilidades de los administradores en la organización.

- 109.**La solución debe realizar el análisis de desviación de comandos en sesiones de terminal, ponderando el riesgo de cada instrucción ejecutada contra el historial del usuario y emitiendo alertas sobre comandos exploratorios sospechosos.
- 110.**La solución debe realizar la suspensión preventiva y automatizada de cuentas de usuario en el directorio corporativo o en la bóveda tras la confirmación repetida de comportamientos anómalos graves o sospecha de compromiso de credencial.
- 111.**La solución debe tener una integración transparente con ecosistemas EDR/XDR de agentes de endpoint para correlacionar la postura de riesgo del dispositivo de origen del administrador antes de autorizar la inyección de la credencial privilegiada.
- 112.**La solución debe contar con la capacidad de generar informes consolidados de riesgo cibernético a nivel ejecutivo, cuantificando la reducción de la superficie de ataque y evaluando la madurez de la adopción del modelo Zero Trust de privilegios.
- 113.**La solución debe generar el alertamiento de evasión de políticas, detectando cuando cuentas huérfanas o sistemas no gestionados intentan eludir el portal proxy PAM conectándose directamente a los servidores destino a través de la red.
- 114.**El contratista deberá entregar los manuales y la documentación técnica correspondiente a la solución, necesarios para su implementación y operación. Durante las actividades de implementación y puesta en marcha deberá realizar el acompañamiento técnico necesario para que los administradores designados por la SCRD conozcan las funcionalidades y operación de la solución. No se establece una obligación independiente de capacitación ni una intensidad horaria específica.

Perfiles Requeridos

1. Gerente de Proyectos

1.1 Rol y Función Principal:

- Se requiere un (1) Gerente de Proyectos para liderar la planificación, el seguimiento y la ejecución del proyecto.

1.2 Formación Académica:

- Título profesional en Ingeniería de Sistemas, Ingeniería de Computación, Ingeniería de Telecomunicaciones o carreras afines (reconocidas conforme al SNIES).
- Especialización y/o maestría en Gerencia de Proyectos, Dirección o Gestión de Proyectos, Ingeniería de Software, Sistemas, Tecnologías de la Información, Seguridad de la Información o áreas afines relacionadas con la gestión de proyectos tecnológicos.

1.3 Experiencia Exigida:

- Acreditar un mínimo de cuatro (4) años de experiencia específica, o
- Acreditar la participación en mínimo tres (3) proyectos en gestión de proyectos de soluciones de software.

1.4 Certificaciones Requeridas:

- PMP (Vigente).
- Scrum Master Professional, PSM (Professional Scrum Master) o CSM (Certified Scrum Master).
- ITIL v4 o ITIL 4 Foundation.

2. Especialista en Seguridad

2.1 Rol y Función Principal:

- Se requiere un (1) Especialista en Seguridad encargado de realizar la implementación de requerimientos y el soporte de la solución de seguridad contratada.

2.2 Formación Académica:

- Título profesional en Ingeniería de Sistemas, Ingeniería de Computación, Ingeniería de Telecomunicaciones o carreras afines (reconocidas conforme al SNIES).

2.3 Experiencia Exigida:

Acreditar un mínimo de tres (3) años de experiencia específica, o acreditar la participación en mínimo dos (2) proyectos en soluciones de gestión de usuarios privilegiados (PAM).

El Gerente de Proyectos y el Especialista en Seguridad deberán corresponder a personas distintas. La dedicación exclusiva del cien por ciento (100 %) aplicará durante la implementación y hasta la entrega a satisfacción de la solución PAM.

Certificaciones Requeridas

1. Certificación oficial del Fabricante o mayorista en la solución de gestión de accesos y seguridad implementada.
2. Certificación acreditada en soluciones PAM expedida por el fabricante o mayorista de la solución.
3. Certificación en soporte técnico en soluciones PAM expedida por un fabricante o mayorista.

Para el presente proceso es necesario realizar la acreditación de la experiencia la cual se realizará con base en la información registrada en el Registro Único de Proponentes (RUP). El proponente deberá acreditar un mínimo de dos (2) contrato y un máximo de cinco (5) contratos terminados y/o liquidados, registrados bajo alguno de los siguientes códigos de clasificación de bienes y servicios UNSPSC:

Código UNSPSC
43231500
43233200

- Objeto y alcance de los contratos
- Los contratos aportados para acreditar la experiencia deberán contemplar actividades relacionadas, como mínimo, con la administración y/o adquisición y/o renovación y/o personalización y/o actualización y/o soporte de soluciones tecnológicas de gestión de identidades y/o usuarios privilegiados.
- Las actividades anteriormente descritas podrán ser acreditadas de manera parcial o total mediante uno o varios de los contratos presentados, siempre que las respectivas certificaciones cumplan con las demás condiciones y requisitos establecidos en el presente documento.
- Condiciones para la acreditación de la experiencia
- Fecha de inicio: Se deberá indicar la fecha de inicio de cada uno de los contratos presentados.
- Fecha de terminación: Todos los contratos aportados deberán encontrarse terminados a la fecha de cierre del proceso de Selección Abreviada con Subasta Inversa Electrónica.
- Antigüedad de la experiencia: Los contratos acreditados deberán haber sido iniciados, ejecutados y finalizados dentro de los cinco (5) años anteriores, contados a partir de la fecha de cierre del presente proceso. Este requisito busca garantizar experiencia reciente en tecnologías de gestión de identidades, considerando la evolución tecnológica de estas soluciones y la necesidad de contar con tecnologías que no se encuentren en condición de obsolescencia.
- Valor de los contratos: La sumatoria de los valores de los contratos aportados deberá ser igual o superior al presupuesto oficial del presente proceso, correspondiente a **DOSCIENTOS VEINTICUATRO MILLONES TRESCIENTOS TREINTA Y NUEVE MIL DOSCIENTOS CATORCE PESOS M/CTE (\$224.339.214).**
- Porcentaje de participación: Cuando el contrato haya sido ejecutado mediante consorcio o unión temporal, se deberá indicar claramente el porcentaje de participación del proponente.