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	La solución admitirá la alta disponibilidad en modo Activo-Pasivo con conmutación por error automáticamente y manualmente dentro del mismo sitio Datacenter o entre datacenters sin necesidad de licencias adicionales.
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 nodos de sesión no deben ser restringidos por licenciamiento del fabricante de PAM, y deben poder ser instalados en Windows Desktop o Windows Server.

Este documento es clasificado como Información Publica

1.1.11	Los nodos de sesión deben poder ser instalados en Linux, incluyendo RHEL, Ubuntu, CentOS, Debian, Fedora, SLES (Suse Linux) y Amazon Linux.
1.1.12	Los nodos de sesión deben poder ser instalados en contenedores de Docker.
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	La solución debe entregarse en formato de appliance virtual, soportando las plataformas: VMware o Azure.
1.1.15	La solución no debe entregarse en software, ya que se requiere que el fabricante del PAM asuma el soporte de todos los componentes incluidos en la oferta económica, incluyendo el sistema operativo, la base de datos y el software de la herramienta.
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	Los appliances virtuales del PAM deben poder desplegarse en cluster Activo-Pasivo o Activo-Activo.
1.1.19	El despliegue del PAM no debe requerir licenciamiento CAL de Microsoft (Client Access License), tampoco debe requerir despliegue de Remote Desktop Services de Microsoft (RDS).
1.1.20	El proveedor del PAM debe entregar diagramas de despliegue con escenarios multi-datacenters, que incluyan clusters Activo-Pasivo y Activo-Activo, y que detalle la cantidad de componentes y requerimientos de CPU y Memoria de cada componente.
1.1.21	Para redes industriales (Operational Technology), los nodos de sesión o pivotes del PAM deben cumplir con los requerimientos del Modelo Purdue (Purdue Enterprise Reference Architecture (PERA)), en el que no se permite enviar flujos de tráfico hacia la red OT..
1.1	Arquitectura y rendimiento (opción de despliegue SaaS, sin appliances)
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.

Este documento es clasificado como Información Publica

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 nodos de sesión no deben ser restringidos por licenciamiento del fabricante de PAM, y deben poder ser instalados en Windows Desktop o Windows Server.
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 nodos de sesión no deben ser restringidos por licenciamiento del fabricante de PAM, y deben poder ser instalados en contenedores de Docker.
1.1.13	La solución en nube debe permitir hasta 200 nodos de sesión, para distribuirlos en diferentes zonas geográficas, sin requerir licencias adicionales.
1.1.14	Los nodos de sesión deben poder desplegarse en clusters Activo-Activo, sin requerir balanceador de carga.
1.1.15	Los nodos de sesión no deben requerir recibir tráfico de red por ningún puerto TCP o UDP, ya que esto representa un riesgo que la organización no está dispuesta a asumir. Toda la comunicación TCP/IP de los nodos de sesión debe ser saliente (outbound).
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	El balanceo de los motores de puerta de enlace debe ser automático y no debe requerir de balanceadores externos.
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%.

Este documento es clasificado como Información Publica

1.1.20	Para redes industriales (Operational Technology), los nodos de sesión o pivotes del PAM deben cumplir con los requerimientos del Modelo Purdue (Purdue Enterprise Reference Architecture (PERA)), en el que no se permite enviar flujos de tráfico hacia la red OT..
1.1.21	El mismo despliegue de PAM que se utilice para la red IT, debe poder ser utilizado para ofrecer accesos remotos seguros hacia las redes OT, sin requerir licenciamiento adicional
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 permitirá la expansión de las plataformas soportadas nativamente para escaneos de descubrimiento, mediante un Software Development Kit (SDK), gratuito y con ejemplos para diferentes funcionalidades.

Este documento es clasificado como Información Publica

1.2.8	La solución permitirá el descubrimiento de cuentas y secretos, listos para usar y sin necesidad de servicios profesionales, sobre las siguientes plataformas: AWS IAM AWS Secrets Manager Secrets y Assume Role + EC2 Azure Key Vault Credentials Cisco Defense Orchestrator API Tokens Cisco Umbrella API Keys Cloudflare API Tokens CrowdStrike Sensor Installation Tokens Datadog App Keys Delinea Secret Server Passwords Elastic API Keys Entra ID Service Principals Fortanix App Secrets GitHub Organization Secrets GitLab Project Access Tokens Grafana Service Account Tokens Hashicorp Vault Secrets Hitachi Ops Center Passwords Hitachi VSP Storage Passwords JIRA Server User Passwords Okta OICD Client Secrets y User Passwords PingOne App Secrets y User Passwords Rapid7 InsightVM Shared Credentials Secrets Safe Passwords SkyTap API Tokens Snowflake User Passwords Splunk Enterprise User Passwords Wix Secrets Manager Secrets
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 tendrá la capacidad de descubrir el software que está instalado y los puertos están abiertos en el sistema de destino.
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.

Este documento es clasificado como Información Publica

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 permitirá cambios automáticos de contraseñas para las siguientes plataformas listas para usar: Sistemas operativos: AIX, HP-UX, AS400, Linux, Mac OS, Solaris, Windows Bases de datos: MongoDB, MySQL, Oracle, PostgreSQL, SQL Server, Sybase, Teradata Directorios: Active Directory, LDAP,IBM RACF Dispositivos: BIG-IP (F5), Checkpoint, Cisco IOS, z/OS y z/VM, Dell iDRAC, Fortinet, HP Comware, HP iLo, Juniper (JunOS), Palo Alto Networks, entre otros Aplicaciones: SAP, VMware vSphere API, VMware vSphere SSH, Amazon AWS, Office 365, Workday, Salesforce
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.

Este documento es clasificado como Información Publica

1.3.3	La solución permitirá cambios automáticos de contraseñas y secretos, listos para usar y sin necesidad de servicios profesionales, sobre las siguientes plataformas: AWS IAM AWS Secrets Manager Secrets y Assume Role + EC2 Azure Key Vault Credentials Azure Storage Account Access Keys Cisco Defense Orchestrator API Tokens Cisco Umbrella API Keys Cloudflare API Tokens Contraseñas en archivos CrowdStrike Sensor Installation Tokens Datadog App Keys Delinea Secret Server Passwords Elastic API Keys Entra ID Service Principals Fortanix App Secrets GCP Service Accounts Access Keys GitHub Organization Secrets GitLab Project Access Tokens Grafana Service Account Tokens Hashicorp Vault Secrets Hitachi Ops Center Passwords Hitachi VSP Storage Passwords JIRA Server User Passwords Okta OICD Client Secrets y User Passwords PingOne App Secrets y User Passwords Rapid7 InsightVM Shared Credentials SailPoint Identity Security Cloud Source Secrets Service Now User Passwords Secrets Safe Passwords SkyTap API Tokens Snowflake User Passwords Splunk Enterprise User Passwords Wix Secrets Manager Secrets Workday Integration Password
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.

Este documento es clasificado como Información Publica

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	Después de rotar cada contraseña, la solución debe permitir la configuración de acciones adicionales con la nueva contraseña, para propagar la nueva clave en diferentes sistemas. Estas acciones deben incluir reiniciar servicios de Windows, escribir la nueva clave en archivos de configuración y escribir la clave en bóvedas cloud como Azure Key Vault o Hashicorp.
1.3.19	Las acciones de propagación de credenciales deben incluir como mínimo: reiniciar servicios de Windows, escribir la nueva clave en archivos de configuración y escribir la clave en bóvedas cloud como Azure Key Vault o Hashicorp, nativamente, sin requerir licenciamiento adicional y sin requerir servicios profesionales.

Este documento es clasificado como Información Publica

1.3.20	El PAM debe incluir una bóveda de secretos personal para equipos de trabajo de la organización.
1.3.21	La bóveda de secretos del PAM debe poder ser accedida desde un portal web para humanos, y desde una API REST para entidades no humanas.
1.3.22	La bóveda de secretos del PAM debe permitir almacenar credenciales (usuario/contraseña), almacenar archivos para cubrir certificados digitales, y almacenar líneas de texto para cubrir Connection Strings.
1.3.23	La bóveda de secretos del PAM no debe requerir licenciamiento adicional.
1.3.24	La bóveda de secretos del PAM debe permitir que las personas almacenen contraseñas de negocio y las compartan de manera segura entre equipos de trabajo de esta organicación. Esto permite reemplazar herramientas como Keepass y centralizar de manera controlada las credenciales que no son cuentas privilegiadas administradas por el PAM.
1.3.25	La bóveda de secretos del PAM debe poder ser accedida utilizando autenticación fuerte, FIDO2 y SSO con cualquier proveedor de identidades SAML.
1.3.26	La bóveda de secretos del PAM debe poder ser accedida desde una extensión de navegadores como Google Chrome, Microsoft Edge, Mozilla Firefox.
1.3.27	La bóveda de secretos del PAM debe poder ser accedida directamente también desde cualquier navegador web, sin requerir una extensión de navegador.
1.3.28	La bóveda de secretos del PAM debe poder ser accedida desde una aplicación para Android y iOS.
1.3.29	La bóveda de secretos del PAM debe permitir importación masiva de secretos mediante archivo separado por comas.
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.

Este documento es clasificado como Información Publica

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	La solución permitirá al usuario autorizado proporcionar comentarios de revisión mientras reproduce la sesión grabada e indicará que la sesión grabada ha sido revisada.
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.

Este documento es clasificado como Información Publica

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 admitirá sesión privilegiada con inicio de sesión automático para la plataforma Windows donde la autenticación con "smart card" esté habilitada.
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	Ya que el PAM es un componente crítico y comúnmente interviene en controles de cambio delicados, debe incluir un módulo desarrollado por el mismo fabricante para establecer sesiones de mesa de ayuda y resolver oportunamente cualquier inconveniente relacionado con el PAM.
1.4.30	El módulo de soporte remoto del PAM debe poder integrarse con método de autenticación SAML, y debe integrarse con sistemas de tickets.
1.4.31	El módulo de soporte remoto del PAM debe permitir tomar el control de las estaciones de trabajo y dispositivos móviles de los usuarios del PAM.
1.4.32	El módulo de soporte remoto del PAM no debe requerir la instalación de software en las estaciones de trabajo de los usuarios del PAM, y no debe requerir VPNs para su funcionamiento.
1.4.33	El módulo de soporte remoto del PAM se debe integrar nativamente con la bóveda del PAM, para inyectar estas credenciales en sesiones remotas si es necesario.
1.4.34	El módulo de soporte remoto del PAM debe grabar las sesiones, y debe integrarse con el SIEM para garantizar auditoría y cumplimiento.
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.

Este documento es clasificado como Información Publica

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 los roles de Solicitante, Aprobador o Revisor sobre cuentas y sistemas de dominio de Active Directory, la solución tendrá la capacidad de agrupar dinámicamente cuentas y sistemas basados en atributos de dominio como Organizational Unit (OU), Security Group, SAMAccount Name, y otros.
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	Las aprobaciones de solicitudes podrán ser con autenticación fuerte, para certificar el usuario aprobador, o mediante un link sin autenticación, para simplificar el proceso.
1.5.7	La solución tendrá la flexibilidad de especificar cero, uno o múltiples aprobadores para cuentas individuales, grupales o todas las cuentas administradas, permitiendo un control dual granularmente asignado.
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.

Este documento es clasificado como Información Publica

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 del PAM, incluyendo el módulo de soporte, deben estar alojados en el mismo portal web para simplificar la solicitud de accesos, gestión y operación del mismo.
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.

Este documento es clasificado como Información Publica

1.7.3	La solución debe proporcionar los siguientes tipos de informes listos para usar sin ningún componente adicional y sin costo adicional: -Informe de antigüedad de contraseña de cuenta que proporciona la última fecha y fecha de cambio de contraseña para cada cuenta administrada. -Informe de actividades del usuario que proporciona una vista transaccional detallada de las actividades de aprobación y solicitud de sesión y contraseña. -Informe de derechos que detalla quién tiene acceso a qué cuentas. -Informe de actividad de cambio de contraseña que detalla el motivo y el resultado del cambio de contraseña. -Informe de programación de cambio de contraseña que proporciona detalles del próximo cambio de contraseña programado. -Restablecimiento de contraseña al liberar el informe de conciliación que muestra los estados de restablecimiento de finalización de solicitud de contraseñas de cuentas administradas para proporcionar evidencia auditable de que las contraseñas se han restablecido adecuadamente después de ser liberadas. -Informe de inventario de activos que proporciona una lista de todos los sistemas administrados y no administrados, activos de TI descubiertos agrupados por sistema operativo. -Informe de inventario de cuenta que proporciona una lista de todas las cuentas administradas y no administradas. -Informe delta de cuenta que proporciona cambios delta para cuentas agregadas y eliminadas de acuerdo con períodos diarios, semanales y mensuales. -Informe de cuentas administradas vs no administradas que proporciona una lista de cuentas del sistema de destino e indica cuáles están bajo administración de contraseñas. -Informe de uso de la cuenta de servicio que proporciona una lista detallada de qué sistemas están utilizando una cuenta de servicio para iniciar uno o más servicios de Windows.
1.7.4	La reportería de todos los módulos del PAM, incluyendo el módulo de soporte, deben estar alojados en el mismo portal web para garantizar visibilidad holística de actividades privilegiadas.
1.8	Autenticación, seguridad y cumplimiento
1.8.1	La solución debe estar acreditada con el certificado Common Criteria.
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.

Este documento es clasificado como Información Publica

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
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	El PAM debe permitir sincronizar credenciales y secretos entre plataformas on-premises y bóvedas cloud, nativo sin requerir servicios profesionales y sin costo adicional.
1.9.4	Como mínimo, el PAM debe permitir sincronizar secretos hacia AWS Secrets Manager, Azure Key Vault, Google Secret Manager, archivos de texto y Hashicorp Vault, nativo, sin requerir licencias adicionales y sin requerir servicios profesionales ni desarrollo de software.
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

Este documento es clasificado como Información Publica

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 poder integrarse nativamente con otras soluciones PAM como PEDM (Privileged Elevation and Delegation Management) para control dinámico de privilegios en estaciones de trabajo y servidores, y CIEM (Cloud Infrastructure Entitlement Management) para control dinámico de privilegios en nube y otras herramientas.
1.10.6	Debe permitir integraciones nativas con Automation Anywhere y con BluePrism, para diversas automatizaciones que requieren accesos privilegiados en sistemas críticos.
1.10.7	Debe permitir integraciones con External Secrets Operator y Secrets-Agent de Kubernetes.
1.11	Licenciamiento
1.11.1	La solución PAM debe permitir 2 opciones de licenciamiento: por cantidad de usuarios (User-Based) o por dispositivo administrado (Asset-Based), lo que sea más conveniente para el proyecto, contemplando un alcance para 50 cuentas privilegiadas custodiar.
1.11.2	Si posterior a la adquisición del producto, la organización decide cambiar el modo de licenciamiento, esto debe ser factible sin ninguna penalidad. Es decir, será posible cambiar de User-Based a Asset-Based, o viceversa.
1.11.3	Para el licenciamiento User-Based, la cantidad de Assets debe ser ilimitada, y para el licenciamiento Asset-Based, la cantidad de usuarios debe ser ilimitada.
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.

Este documento es clasificado como Información Publica

	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 limitar la cantidad de componentes proxies requeridos para establecer sesiones y tomar otras acciones como escaneos de descubrimientos y cambios 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.

Este documento es clasificado como Información Publica

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: 2026.05.13 15:34:07 -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: 2026.05.13 12:00:13 -05'00'

Carlos Arturo D Otero Biscardi
Estructurador Técnico
Profesional
Subdirección de Operaciones

Este documento es clasificado como Información Publica