1. OBJETO

Contratar la renovación del servicio de soporte de fábrica y actualizaciones para la plataforma de gestión de usuarios privilegiados Cyberark. (Línea PAA 130018824)

1.1. ALCANCE DEL OBJETO

Renovar soporte de fabrica para 10 licencias de usuarios privilegiados de la plataforma tecnológica CIBERARK de la ANM. Cuya renovación nos permite mantener las actualizaciones vigentes en la plataforma y tener escalamiento ante problemas o configuraciones de nivel especializado.

2. CUADRO DE CANTIDADES

No	Descripción del Producto	Resumen Cantidades priorizadas	PLAZO	UNIDAD	CANTIDAD
1	Gestión de Usuarios Privilegiados) Para la plataforma CIBERARK (soporte de fabricante	+ Renovación Soporte fabrica para 10 licencias de usuarios.	12	MES	1 Renovación

3. CLASIFICADOR UNSPSC

CÓDIGO	SEGMENTO	FAMILIA	CLASE
43231500	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software funcional específico de la empresa
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software
81112300	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de Hardware de computador

4. CARACTERISTICAS TECNICAS.

La ANM solicita la renovación del servicio de actualizaciones y soporte con fabricante por 12 meses; Solución tecnológica Cyberark permite realizar un seguimiento de las actividades desarrolladas por los usuarios privilegiados registrados en la plataforma. Dicha plataforma contiene las siguientes características:

- La entidad es propietaria de la aplicación y de las bóvedas de almacenamiento de datos. Así como el licenciamiento de 10 usuarios.

- El alcance de la solicitud corresponde a la renovación del servicio de soporte técnico por parte del fabricante, mas no del licenciamiento.
- Administra una bóveda de claves para cuentas administradoras que salvaguarda las claves de persona.
- Esta herramienta realiza la Gestión de Identidades privilegiadas, permitiendo almacenar de manera segura las credenciales de cuentas con altos privilegios de los recursos de la infraestructura de TI de la Entidad.
- Realiza el registro de todas las actividades realizadas con las cuentas privilegiadas.
- Realiza uso de cuentas privilegiadas bajo demanda y basado en un perfil establecido soportado a través de un flujo de aprobaciones el cual sea flexible para asignar múltiples aprobadores

ESPECIFICACIONES TECNICAS GENERALES DE LA HERRAMIENTA
• Soporta y controla el acceso y capacidades de los usuarios privilegiados en los siguientes sistemas operativos: - Windows Server 2008 - Windows Server 2012 - Windows Server 2016 - Windows Server 2019 - Windows Server 2022 - Linux: Oracle Linux, Linux RedHat - Sistema de Virtualización Vmware mínimo versión 6.0 • Controla el acceso y capacidades de los usuarios privilegiados en los siguientes bases de datos: - SQL Server 2014 y 2016 - MySQL - Oracle 10g, 11g y 12c - MongoDB • Permite parametrizar el ingreso de políticas que permitan restringir acciones/configuraciones sobre el sistema operativo y/o base de datos • Cuenta con un módulo de reportes que contiene: a. Customización de look&Feel b. Configuración de Idioma español c. Auditorías de las acciones del administrador de la solución e. Registro de información relevante: usuario, terminal Id, fecha y hora (Timestamp), opción o recurso utilizado, acción y código de retorno • Cuenta con la protección de los siguientes módulos en la infraestructura de Servidores: - Control de acceso: - Control de privilegios. - Monitoreo a modo warning y a modo de fallos - Protección Proactiva de Intrusiones - Eliminar o mitigar vulnerabilidades de seguridad identificada • Permite encriptar la información sensible (credenciales de usuarios privilegiados) bajo algoritmos de encripción tales como: AES-256, RSA-2048, HSM integration, FIPS 140-2 validated cryptography • Cuenta con un módulo propietario para la grabación de las sesiones con altos privilegios que se generen hacia los diferentes recursos de infraestructura de la

organización, realizando funciones específicas como el monitoreo, control y aislamiento de las sesiones.

- La suite de gestión de identidades privilegiadas permite auditoría a nivel de keystroke en sesiones SSH
- La suite de gestión de identidades privilegiadas permite a usuarios privilegiados monitorear sesiones privilegiadas en tiempo real, visualizándolas o controlándolas acorde a configuraciones predeterminadas.

FUNCIONALIDADES EN LA GRABACIÓN DE SESIONES

- La solución realiza Gestión de identidades privilegiadas cuente con un módulo propietario para la grabación de las sesiones con altos privilegios que se generan hacia los diferentes recursos de infraestructura de la organización, realizando funciones específicas como el monitoreo, control y aislamiento de las sesiones.

- La suite de gestión de identidades privilegiadas permite auditoría a nivel de comandos SQL y grabación de sesiones en bases de datos
- La suite de gestión de identidades privilegiadas permite auditoría a nivel de keystroke en sesiones SSH
- La suite de gestión de identidades privilegiadas permite a usuarios privilegiados monitorear sesiones privilegiadas en tiempo real, visualizándolas o controlándolas acorde a configuraciones predeterminadas.
- El módulo de grabación de sesiones contiene su propio códec de seguridad

FUNCIONALIDADES DE ADMINISTRACIÓN DE CONTRASEÑAS

- La suite de gestión de identidades privilegiadas permite controlar y monitorear el acceso privilegiado a sistemas y dispositivos sensibles a través de la grabación de sesiones usando SSO privilegiado y sin divulgar las credenciales usadas para el acceso.
- La suite de gestión de identidades privilegiadas está en capacidad de gestionar cuentas privilegiadas de los siguientes sistemas:
  - ✓ Aplicaciones Web en Java
  - ✓ Acceso Remoto: o HP iLo v2.0
  - ✓ o DRAC 5 y DRAC 6
  - ✓ Base de Datos
  - ✓ o Bases de Datos Oracle V10g, 11g,12c o superior. o Microsoft SQL Server 7 y superior.
  - ✓ o Sybase Adaptive Server Enterprise 12.5.2 o MySQL version 5 y superior.
  - ✓ Dispositivos de Red.
  - ✓ Cisco,HP-Aruba,
  - ✓ 4.7.2 Sistemas Operativos
  - ✓ Cuentas de Dominio de Windows (Windows /2012/2012 R2 with Service Pack 1 Active Directory server/ 2016) Windows Server 2019 Estandar – Datacenter.

- ✓ Cuentas Locales de Windows (Windows /2012/2012R2 with Windows 2016 – Windows 2019 Estandar Datacenter / Windows 8/ Windows 10 / Windows 11)
- ✓ Sun Solaris 5.8
- ✓ HP-UX 11.x
- ✓ IBM AIX 5
- ✓ RHEL 3
- ✓ ESXi 5.0, ESX/ESXi 4.1, ESX/ESXi 4.0, ESX 3.5
- ✓ Appliance de Seguridad
- ✓ Fortinet Firewall
- ✓ o NetScreen versión 5.3.0r2.0 y superior.
- ✓ Sitios Web
- ✓ Cuentas de Servicios

- La suite de gestión de identidades privilegiadas permite sincronizar cuentas de servicios de Windows. Es decir, si el Software de Administración de Identidades Privilegiadas cambia una contraseña de una cuenta de Dominio de Windows usada para logon en un servicio, la nueva contraseña debe actualizarse de forma automática en el mismo. Soporta los siguientes servicios:
  - ✓ . Windows Services Accounts
  - ✓ · Windows Scheduled Tasks
  - ✓ · Windows IIS Application Pools Passwords
  - ✓ · Windows COM+ Applications
  - ✓ · Windows IIS Directory Security (Anonymous Access) Passwords
- La suite de gestión de identidades privilegiadas provee aprovisionamiento automático de cuentas locales de Windows y permite la integración con Directorio Activo para administrar cuentas privilegiadas del Dominio de Windows.
- La suite de gestión de identidades privilegiadas provee aprovisionamiento automático para las cuentas de host Root de VMWare ESX. El vCenter corporativo se integra a la solución para mantener la política de contraseñas en el ambiente de vCenter.

CONOCEMOS, ACEPTAMOS Y NOS COMPROMETEMOS A CUMPLIR CON TODOS LOS REQUERIMIENTOS MÍNIMOS OBLIGATORIOS ESTABLECIDOS EN ESTE DOCUMENTO, LOS CUALES SE ENTENDERÁN COMO OFERTA TÉCNICA MÍNIMA.

FIRMA DEL OFERENTE: _____
NOMBRE DEL OFERENTE: _____
NOMBRE DE LA EMPRESA OFERENTE: _____