Especificaciones Funcionales y Técnicas de la Solución Requerida

Gestión Identidades Privilegiadas (PIM)

EDEESTE	
Jerarquía	Especificaciones técnicas requeridas
1	**Plataformas/Dispositivos/Sistemas Operativos soportados**
1,1	Capacidad de administrar cuentas privilegiadas de diferentes orígenes o plataformas
1.1.1	**Sistemas Operativos**
1.1.1.1	Permite administrar cuentas de Windows Server 2012-2019 y superior
1.1.1.2	Permite administrar cuentas de Linux 6-7 (RedHat, CentOs, Oracle Linux) y superior
1.1.1.3	Permite administrar cuentas de Unix (Solaris 11 y superior)
1.1.2	**Bases de Datos**
1.1.2.1	Permite administrar cuentas privilegiadas de MS SQL Server 2014-2019 y superior
1.1.2.2	Permite administrar cuentas privilegiadas de Oracle 11g-12c Family y superior
1.1.3	**Nube**
1.1.3.1	Permite administrar cuentas privilegiadas de AZURE
1.1.3.2	Permite administrar cuentas privilegiadas de AWS
1.1.4	**Virtualización**
1.1.4.1	Permite administrar cuentas privilegiadas de VMWare
1.1.4.2	Permite administrar cuentas privilegiadas de Hyper V
1.1.4.3	Permite administrar cuentas privilegiadas de Acropolis
1.1.5	**Dispositivos**
1.1.5.1	Permite administrar cuentas privilegiadas de dispositivos de red CISCO
1.1.5.2	Permite administrar cuentas privilegiadas de dispositivos de red Brocade
1.1.5.3	Permite administrar cuentas privilegiadas de dispositivos de red Fortinet
2	**Arquitectura, Seguridad y Administración**
2.1	Arquitectura de la solución
2.1.1	**Diseño/Instalación/Implementación**
2.1.1.1	Deberá implementarse como un Appliance
2.1.1.2	Deberá tener la capacidad de no requerir que se instalen agentes en los dispositivos target
2.1.2	**Alta Disponibilidad/Redundancia**
2.1.2.1	Permite un modelo de redundancia o disponibilidad Activo-Pasivo o Activo-Activo
2.1.2.2	Debe proporcionar una tolerancia a fallas y poder cambiar desde la instancia activa a la instancia de respaldo o standbye con el repositorio de claves totalmente replicado
2.1.2.3	Deberá ser capaz de soportar el modelo Activo-Pasivo o Activo-Activo con uno de los appliances colocado en un datacenter de Disaster Recovery localizado en una localidad geográfica diferente
2.1.3	**Especificaciones Mínimas de los Appliances**

SAMG

Especificaciones Funcionales y Técnicas de la Solución Requerida

Gestión Identidades Privilegiadas (PIM)

EDEESTE

Jerarquía	Especificaciones técnicas requeridas
2.1.3.1	Cantidad de Appliances: 2 Procesadores: (2) Intel® Xeon® Silver 4309Y 2.8G, 8C/16T, 10.4GT/s, 12M Cache, Turbo, HT Memoria: (2) 16GB RDIMM, 3200MT/s, Dual Rank Almacenamiento de Arranque: No BOSS Card Disco Duro: (2) 600GB Hard Drive SAS ISE 12Gbps 15K 512n 2.5in Hot-Plug Chasis: 2.5" Chassis with up to 10 HDDs (SAS/SATA) including max of 4 Universal Drives, 3 PCIe Slots, 2 CPU Controladora de Discos: PERC H355 with rear load bracket Fuentes de Poder: Dual, Hot-plug, Power Supply Fault Tolerant Redundant (1+1), 1400W, Mixed Mode; (2) C13 to C14, PDU Style, 12 AMP, 13 Feet (4m) Power Cord, North America Administración: iDRAC9, Express 15G Red: (1) Broadcom 5720 Quad Port 1GbE BASE-T Adapter, OCP NIC 3.0; (1) QLogic 2692 Dual Port 16Gb Fibre Channel HBA, PCIe Full Height Puertos: Frontales: 1 x Dedicated iDRAC Direct micro-USB, 1 x USB 2.0, 1 x VGA; Traseros: 1 x USB 2.0, 1 x USB 3.0, 2 x RJ-45 Configuración de Tarjetas Riser: Config 3, 3/4 Length, Full Height, 2 x16 Slots, SW GPU Capable Rieles: ReadyRails Sliding Rails With Cable Management Arm Ventiladores: 4 Very High Performance Fans for 2 CPU Sistema Operativo: Windows Server 2022 Standard,16CORE,Fl,No Med,No CAL, Multi Language Licenciamiento: Windows Server 2022 Standard,16CORE,Digitally Fulfilled Recovery Image Soporte de Hardware: 3 Years ProSupport with Next Business Day Onsite Service-LA
2.1.3.2	Los Appliances deben soportar un mínimo de 5,000 cuentas privilegiadas
2.2	**Seguridad en la Arquitectura**
2.2.1	**Control de Acceso**
2.2.1.1	La solución permite crear listas blancas/negra de comandos que son o no permitidos en las secciones de acceso con cuentas privilegiadas
2.2.1.2	Registra todos los comandos ejecutados a través de las secciones privilegiadas
2.2.1.3	La solución genera eventos de auditoría de las tareas realizadas dentro del sistema en formato syslog estándar o CEF para integración con soluciones SIEM.
2.2.1.4	Permite almacenar credenciales hard coded que no pueda ser cambiadas o rotadas automáticamente
2.2.2	**Administración de Llaves SSH**
2.2.2.1	Permite detectar llaves SSH pares y llaves huérfanas
2.2.2.2	Almacena de forma segura y controla el acceso a las llaves privadas SSH
2.2.3	**Seguridad en el Repositorio**
2.2.3.1	Permite encriptar todos los datos del repositorio utilizando algoritmos AES 256 bit o superior
2.2.3.2	Permite la integración con Hardware Security Module para almacenar las llaves de encripción
2.2.4	**Autenticación**
2.2.4.1	Permite integrarse con métodos de autenticación LDAP
2.2.4.2	Permite integrarse con métodos de autenticación PKI (Certificados Digitales)
2.2.4.3	Permite integrarse con métodos empresariales de autenticación RADIUS

SAMG

Especificaciones Funcionales y Técnicas de la Solución Requerida

Gestión Identidades Privilegiadas (PIM)

EDEESTE	
Jerarquía	Especificaciones técnicas requeridas
2.2.4.4	Permite autenticación con mecanismos propios de la solución
2.3	Administración de la Solución
2.3.1	**Autodescubrimiento**
2.3.1.1	La solución propuesta debe tener la capacidad de descubrir y mapear cuentas privilegiadas y cuentas de servicios de los sistemas, dispositivos y aplicaciones soportados con una herramienta integrada o stand alone
2.3.2	**Gestión de contraseñas / Gestión de credenciales**
2.3.2.1	**Cambio de Contraseña**
2.3.2.1.1	La solución propuesta deberá tener la capacidad de cambiar o rotar los passwords automáticamente cada X días, meses o años definidos
2.3.2.1.2	La solución propuesta deberá tener la capacidad de cambiar múltiples passwords en una sola vez para un solo sistema o sistemas agrupados bajo un criterio específico
2.3.2.1.3	La solución propuesta deberá tener la capacidad de cambiar manualmente un password por un administrador de la solución en cualquier momento
2.3.3.2	**Verificación de Contraseña**
2.3.3.2.1	La solución propuesta deberá tener la capacidad de verificación automática del valor de un password en el sistema correspondiente
2.3.3.2.2	La solución propuesta permite notificar aquellos passwords que están "out of sync" con el sistema
2.3.3.3	**Sincronización de Contraseña**
2.3.3.3.1	La solución propuesta deberá tener la capacidad de automáticamente reconciliar passwords que se hayan detectado como "out of sync" o que se hayan perdido o cambiado
2.3.3.3.2	La solución propuesta permite reconciliar passwords en un sistema, en múltiples o en todos los sistemas bajo el control del producto
2.3.3	**Soporte a Flujos de Trabajo**
2.3.3.1	La solución propuesta deberá tener la capacidad de que un usuario pueda solicitar el uso de una cuenta privilegiada para una fecha u hora futura
2.3.3.2	La solución propuesta deberá tener la capacidad de permitir el uso de una cuenta privilegiada solicitada y aprobada solo en el periodo de tiempo establecido
2.3.3.3	La solución propuesta deberá tener la capacidad de soportar procesos flexibles de workflows para designar múltiples aprobadores. Por ejemplo se requieren dos o mas aprobaciones antes de que el acceso sea autorizado
2.3.4	**Monitoreo y Grabación de Actividad Privilegiada**
2.3.4.1	La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, solaris, Ruteadores y Switches, Bases de Datos Oracle y SQL, Aplicaciones , entre otros.
2.3.4.2	La solución permite configurar el tiempo de retención de las grabaciones de sesiones privilegiadas por un periodo mínimo de 1 año
2.3.4.3	La solución propuesta deberá tener la capacidad de hacerse búsquedas de comandos privilegiados dentro de las grabaciones de video
2.3.4.4	La solución propuesta deberá tener la capacidad de soporta ver las sesiones en vivo/tiempo real del monitoreo de sesiones
3	Integraciones
3.1	La solución propuesta deberá tener la capacidad de generar logs como fuente de información en formato Syslog estándar o CEF para herramientas de correlación SIEM.
3.2	La solución propuesta deberá tener la capacidad de integrarse con directorios LDAP/AD

SAMG

Especificaciones Funcionales y Técnicas de la Solución Requerida Gestión Identidades Privilegiadas (PIM)	
EDEESTE	
Jerarquía	Especificaciones técnicas requeridas
3.3	La solución propuesta tiene una herramienta de respaldo y recuperacion o permite integrarse con soluciones de respaldo y recuperación existentes
4	Licenciamiento
4.1	Licenciamiento requerido para los Appliances para cumplir con las especificaciones solicitadas
4.2	La cantidad inicial de licencias es para administrar 10 usuarios
5	Soporte y Servicios Profesionales
5.1	Soporte y Mantenimiento
5.1.1	Garantía de los equipos provistos en la solución por 1 año
5.1.2	Contratos de soporte y actualizaciones del fabricante por 1 año
5.1.3	Contrato de soporte técnico para la solución por 1 año
5.2	Servicios de Implementación
5.2.1	El servicio debe de incluir la Implementación completa de la solución licenciada
5.2.2	El oferente debe indicar la Metodología de implementación que utilizará.
5.2.3	El oferente debe entregar un cronograma de las actividades para la implementación de la solución.
5.2.4	El oferente debe indicar las condiciones y/o prerrequisitos de la implementación.
5.2.5	El oferente debe contar con los ingenieros certificados capaces de instalar y brindar soporte de la solución.
5.2.6	El oferente de la solución debe presentar evidencias de que el personal propuesto para la implementación de esta solución labora en la empresa que resulte adjudicada o con el fabricante.
5.3	Entrenamientos
5.3.1	La propuesta debe incluir entrenamientos que incluya la instalación, configuración y administración de la solución para 10 personas
5.3.2	El entrenamiento debe ser impartido por un entrenador certificado
5.4	Condiciones Especificas del Suplidor
5.4.1	El oferente deberá demostrar que posee al menos tres (3) años operando en República Dominicana.
5.4.2	El oferente deberá entregar una carta del fabricante con la certificación para implementar la solución.

Jose Manzueta
Gerente de Seguridad TI

EMPRESA DISTRIBUIDORA DE ELECTRICIDAD DEL ESTE, S.A.
edeeste
TECNOLOGÍA