edeeste
Empresa Distribuidora de Electricidad del Este

INFORME TÉCNICO

PROYECTO GESTIÓN DE IDENTIDADES PRIVILEGIADAS (PIM)

JUNIO 2022

DIRECCIÓN DE TECNOLOGÍA

Y.P

Para: **Comité de Compra y Contrataciones de EDEEste**

De: **Yaneyri Pérez**
Directora Tecnología de Información

Asunto: **Informe de Justificación Proyecto Gestión de Identidades Privilegiadas (PIM)**

Fecha: 14 de junio del 2022

Estimado Comité de Compra y Contrataciones de EDEEste:

Luego de un cordial saludo, tenemos a bien presentarle un informe mediante el cual solicitamos y sustentamos la justificación para el proyecto **Gestión de Identidades Privilegiadas (PIM)** que será implementado en nuestra plataforma de Tecnología de la Información (TI), incluido en el plan de compras con el número TI223CP354, Comparativa de precios.

En este sentido, procedemos a exponerle nuestras motivaciones al respecto, conforme se detalla a continuación:

I. Antecedente o Necesidad de la Compra

La empresa Distribuidora de Electricidad del Este "EDEEste" está en un proceso de mejorar su plataforma de seguridad tecnológica, ya que los hackers, malwares, empleados descontentos o deshonestos, errores de usuarios, especialmente en el caso de las cuentas de super usuario (identidades privilegiadas), comprenden los vectores de ataques más comunes a nivel global.

SAMG

Está demostrado por los distintos incidentes de Cyber-Seguridad a nivel global que las personas son el eslabón más débil en la cadena de seguridad de las infraestructuras tecnológicas, por lo tanto, si el personal asigna y administra las contraseñas de las identidades privilegiadas los riesgos inherentes a tal condición de debilidad se mantienen latentes.

Y.P.

JVA

En tal virtud EDEEste busca mitigar los riesgos en materia de seguridad, inherentes al uso inapropiado o no autorizado de las cuentas con privilegios de administración o super usuarios que pueden dar al traste con la alta disponibilidad e integridad de las Base de Datos

de las distintas plataformas tecnológicas, por lo que se hace necesario la adquisición de una solución que de manera automática permita la administración centralizada de todo el conjunto de cuentas privilegiadas que conforman la infraestructura tecnológica de la empresa.

II. Objetivo General

Gestionar el acceso de diez (10) usuarios de cuentas privilegiadas y asegurar en bóveda digital las cuentas privilegiadas de las bases de datos Oracle y SQL.

III. Alcance

El presente informe abarca la gestión del acceso a diez (10) usuarios y la implementación del resguardo de manera digital en una bóveda o repositorio para las cuentas o identidades privilegiadas de las Base de Datos (Oracle 12c-19c Family y MS SQL Server 2014-2019) de la tecnológica crítica de la empresa, de manera tal que se pueda administrar, auditar y supervisar su uso, al tiempo que se aplican las políticas de seguridad de contraseñas y controles de cambios en la infraestructura.

SAMG

IV. Situación Actual

JVA

En el presupuesto 2022 se incluyó una partida para crear una bóveda digital para el resguardo de los usuarios privilegiados, a los fines de dar cumplimiento a la necesidad de proteger de forma proactiva la infraestructura tecnológica critica, se evaluó la plataforma de seguridad TI.

Y.P.

En la auditoria anual de la base de datos SQL realizada junio 2021 se recomienda tener una Bóveda, donde se guarde cualquier procedimiento que pueda realizar un Administrador DBA en la Base de Datos SQL, coincidiendo con lo planificado por el área de Seguridad de Sistema.

En la actualidad EDEEste en su plataforma de seguridad TI cuenta con firewalls para la red interna y la red perimetral, ambos trabajando en alta disponibilidad asegurando la continuidad del servicio ante la falla de algún equipo, brindado un control y gestión del tráfico de red; de igual manera la empresa cuenta con una plataforma de Antivirus Endpoint con el cual se mitiga la propagación de virus informáticos; asimismo se incorporó un appliance analizador de datos y generador de reportes estadísticos proporcionados por los equipos de perímetros; también contamos con un Cisco Identity Services Engine (ISE) para el control de acceso a la red; asimismo se cuenta con varios Dominios Activos para la autenticación de los usuarios y la asignación de privilegios.

Dentro de los riesgos tecnológicos operacionales identificados tenemos:

- ✓ Los riesgos inherentes al uso de contraseñas privilegiadas en las funciones tecnológicas operativas; lo cual puede afectar la estabilidad de la infraestructura tecnológica si ocurriese un uso indebido y/o no autorizado de dichas contraseñas.
- ✓ El riesgo de que ante una eventual intrusión de un atacante por vía interna o externa pueda escalar privilegios al determinar una contraseña privilegiada y causar daños a la data de la empresa.
- ✓ El riesgo de depender de personas de tecnología para el control de llaves criptográficas e identidades privilegiadas de aplicaciones y servicios críticos de la empresa, en vez de procesos automáticos y herramientas para el almacenamiento seguro de las mismas.

Al no contar con una herramienta especializada no podemos reforzar el cumplimiento de una adecuada política de gestión de identidades privilegiadas alineada a la criticidad de los servicios y plataformas operativas que desde tecnología ofrecemos como ente movilizador del negocio.

SAMG

JVA

V. Situación Propuesta

Implementar una solución de Gestión de Identidades Privilegiadas que proporcione acceso privilegiado seguro a los activos críticos (Base de Datos) y cumplir con los requisitos de cumplimiento al administrar y monitorear cuentas y accesos privilegiados. Ofreciendo características que permitan la administración y almacenamiento de las credenciales y cerrar la brecha de seguridad identificada en la auditoria.

Y.P

Beneficios

Con la inversión en un proceso de Gestión de Identidades Privilegiadas a través de una solución tecnológica, logramos retornos tangibles a corto y mediano plazo con la implementación, eficientizando dicho proceso obteniendo una adecuada gestión de los riesgos entre otros beneficios, como son:

- ✓ Previene ataques a identidades privilegiadas por la complejidad de las contraseñas asignadas de forma automática
- ✓ Restringe el uso compartido de contraseñas

- ✓ Permite revisar comportamientos riesgosos en el uso de identidades privilegiadas en tiempo real
- ✓ Integración con el sistema de identidad y control de accesos.
- ✓ Forzad a cumplir los estándares de seguridad y marcos regulatorios en materia de identidades privilegiadas.
- ✓ Facilita el proceso de auditoría de cumplimiento de las políticas de control de acceso a las Base de Datos.
- ✓ Mitigación de vulnerabilidades por la renovación (rotación) de las contraseñas de cuentas privilegiadas de forma periódica y automática (sin el factor humano).
- ✓ Centraliza la administración de Cuentas Privilegiadas.
- ✓ Almacena las credenciales privilegiadas en un entorno seguro (Encriptado).
- ✓ Trazabilidad y monitoreo de acciones ejecutadas con las cuentas privilegiadas sobre los activos (Base de Datos).
- ✓ Permite el uso de contraseñas privilegiadas sin que el usuario administrador tenga conocimiento de la misma.
- ✓ Permite realizar segregación de perfiles con acceso a las identidades privilegiadas.
- ✓ Establece un procedimiento estandarizado para la solicitud, aprobación, uso y revocación de acceso a cuentas privilegiadas.

SAMG

JVA

YP

En la implementación de este proyecto se cubrirá el acceso de diez (10) usuarios de cuentas privilegiadas a las Bases de Datos de la infraestructura tecnológica, para completar la recomendación de la auditoria a la base de datos SQL.

En el presupuesto 2023 estaríamos incluyendo otra fase para incluir los usuarios privilegiados de los equipos de comunicaciones del Data Center, los servidores controladores del dominio, y equipos de seguridad perimetral como son:

Departamento	Equipos / Servicios
Infraestructura TI	Servidores, Servicios en la Nube
Comunicaciones TI	Switches, Enrutadores, Appliance
Seguridad TI	Firewall, Antivirus, Appliance

VI. Condiciones Específicas de la Compra

EDE Este requiere realizar la compra de la Solución detallado en el cuadro económico:

Concepto	Precio RD$
Licencia para 10 usuarios (Protección de credenciales, aislamiento de sesión, grabación y detección, capacidad para gestionar la administración local); Equipo Appliance 2; Garantía de los equipos por 3 años; Contratos de soporte y actualizaciones del fabricante por 3 años; Contrato de soporte técnico para la solución por parte del proveedor local por 3 años; Soporte a la implementación de la solución por 3 años; Entrenamientos para la instalación, configuración y administración de la solución para 10 participantes.	3,951,942.22

SAMG

JVA

Y.P

Nota: Estos precios son estimados.

Anexos:
Documentos Requerimientos Técnicos.

VISTOS: La Ley No. 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, su posterior modificación contenida en la Ley No. 449-06, el Reglamento de Aplicación de la citada Ley instituido mediante el Decreto No. 543-12, de fecha 6 de septiembre del 2012, los Manuales de Procedimientos, las Resoluciones del Órgano Rector, y la normativa legal aplicable al procedimiento.

Luego de lo previamente expuesto, tenemos a bien recomendar.

RECOMENDACIÓN

1) **AUTORIZAR** la adquisición e implementación de un Sistema de Gestión de Identidades Privilegiadas (PMI) por un monto de **tres millones novecientos cincuenta y un mil, novecientos cuarenta y dos pesos dominicanos con 22/100 (RD$ 3,951,942.22)**.

Agradecemos la atención, reciba un cordial saludo.

Muy atentamente,

Área Solicitante:	
Preparado por:	**Revisado por:**
Juan Vianey Arias	**Jose Manzueta**
Encargado de Monitoreo TI	Gerente de Seguridad TI
Aprobado por:	**Revisado por:**
Yaneyri Pérez	**Iván Ortiz**
Directora Tecnología de la Información	Director Corporativo TI del Consejo Unificado

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

ANEXOS

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**
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,FI,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
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
3.3	La solución propuesta tiene una herramienta de respaldo y recuperación 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 3 años
5.1.2	Contratos de soporte y actualizaciones del fabricante por 3 años
5.1.3	Contrato de soporte técnico para la solución por 3 años
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 Específicas 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.