ANEXO B1

I. Solución de protección de Base de Datos (DBF)

A. Características Generales

1. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe estar compuesta por agentes y hardware appliance. Al ser un appliance físico debe contar con el sistema operativo endurecido.
3. El requerimiento para el equipo de Protección es para una nueva implementación. Los equipos con los que cuenta el MEF para ser protegidos tendrán las siguientes características:

Servidor Físico	Sistema Operativo	DBMS	Cantidad Total de Cores/vCPU	Tipo	Ambiente	Ubicación (Nombre Datacenter)	Estado en el Cluster (Activo/Pasivo/Standalone)
Intel Xeon 6248 2.5Ghz cores: 2proc x 20 cores c/u Total: 80 vCPU	RHEL	MySQL	12	Máquina Virtual	Producción	DC1	Activo
	RHEL	MySQL	16	Máquina Virtual	Producción	DC1	Activo
	RHEL	MySQL	16	Máquina Virtual	Producción	DC1	Activo
	RHEL	MySQL	4	Máquina Virtual	Producción	DC1	Activo
Intel Xeon 6248 2.5Ghz cores: 2proc x 20 cores c/u Total: 80 vCPU	RHEL	MariaDB	4	Máquina Virtual	Producción	DC1	Activo
	RHEL	MariaDB	6	Máquina Virtual	Producción	DC1	Activo
	RHEL	MariaDB	4	Máquina Virtual	Producción	DC1	Activo
	RHEL	MariaDB	4	Máquina Virtual	Producción	DC1	Activo
	RHEL	MariaDB	4	Máquina Virtual	Producción	DC1	Activo
Intel Xeon 6248 2.5Ghz cores: 2proc x 20 cores c/u Total: 80 vCPU	Windows Server	SQL Server	4	Máquina Virtual	Producción	DC1	Activo
	Windows Server	SQL Server	4	Máquina Virtual	Producción	DC1	Activo
	Windows Server	SQL Server	16	Máquina Virtual	Producción	DC1	Activo
Intel Xeon 6248 2.5Ghz cores: 2proc x 20 cores c/u Total: 80 vCPU	Windows Server	SQL Server	16	Máquina Virtual	Producción	DC1	Activo
	Windows Server	SQL Server	8	Máquina Virtual	Producción	DC1	Activo
	Windows Server	SQL Server	4	Máquina Virtual	Producción	DC1	Activo
Principal Power System 9080-M9S Cores: 64	AIX	Oracle	15	LPAR	Producción	DC1	Activo
	AIX	Oracle	2	LPAR	Producción	DC1	Activo
	AIX	Oracle	2	LPAR	Producción	DC1	Activo
	AIX	Oracle	10	LPAR	Producción	DC1	Activo
	AIX	Oracle	2	LPAR	Producción	DC1	Activo
	AIX	Oracle	1	LPAR	Producción	DC1	Activo
	AIX	Oracle	1	LPAR	Producción	DC1	Activo
	AIX	Oracle	1	LPAR	Producción	DC1	Activo
	AIX	Oracle	0.5	LPAR	Producción	DC1	Activo
	AIX	Oracle	0	LPAR	Producción	DC1	Activo
	AIX	Oracle	0	LPAR	Producción	DC1	Activo
Intel Xeon 6248 2.5Ghz cores: 2proc x 20 cores c/u Total: 80 vCPU	RHEL	Oracle	48	LPAR	Producción	DC1	Activo
	RHEL	Oracle	8	LPAR	Producción	DC1	Activo
Contingencia Power System E950 9040-	AIX	Oracle	15	LPAR	Producción	DC2	Activo
	AIX	Oracle	2	LPAR	Producción	DC2	Activo
	AIX	Oracle	2	LPAR	Producción	DC2	Activo

MR9 Cores: 40	AIX	Oracle	10	LPAR	Producción	DC2	Activo
	AIX	Oracle	2	LPAR	Producción	DC2	Activo
	AIX	Oracle	1	LPAR	Producción	DC2	Activo
	AIX	Oracle	1	LPAR	Producción	DC2	Activo
	AIX	Oracle	1	LPAR	Producción	DC2	Activo
	AIX	Oracle	0.5	LPAR	Producción	DC2	Activo
	AIX	Oracle	0	LPAR	Producción	DC2	Activo
	AIX	Oracle	0	LPAR	Producción	DC2	Activo

B. Características de detección

1. Toda la gestión de los componentes y funciones administrativas deberán ser hechas a través de una interfaz web, accesible por el navegador, sin la necesidad de instalación de aplicaciones adicionales.
2. Debe permitir el monitoreo de las transacciones realizadas en las Bases de Datos en tiempo real, y sin impacto relevante en el procesamiento del servidor de Bases de Datos.
3. Debe poder sincronizar hora a través del protocolo NTP con un servidor de la organización o externo.
4. La solución no debe depender de los logs nativos (audits) de las Bases de Datos y no debe requerir ninguna modificación a la base de datos ni a los sistemas que se utilicen.
5. Debe permitir el monitoreo de tráfico por puertas SPAN, redes TAP y agentes ejecutados en el servidor de Base de Datos, cubriendo la mejor combinación en ese ambiente.
6. Debe permitir el control sin sobrecargar los recursos de base de datos, evitando la función de uso de bases de datos residentes, lo que afecta el rendimiento o la estabilidad del Database Manager, tales como triggers, trace, log de transacción de nivel completo de auditorías nativas.
7. Debe permitir la monitorización en tiempo real de cualquier manipulación al esquema de base, tales como la inserción o remoción de tablas o columnas y el fortalecimiento del control de cambios en la política.
8. Debe estar basada en políticas de seguridad para efectuar acciones automáticas que los clientes pueden utilizar para abordar adecuadamente las violaciones de política, incluyendo las acciones de alerta y personalización en tiempo real.
9. Debe permitir que la información de controles de seguridad y de control utilizados por la solución que se integra (fácilmente exportado) a otros sistemas de gestión de la seguridad (por ejemplo, soluciones. SIEM). Se conoce a SIEM como = Seguridad de la Información y Gestión de Eventos. Esta integración debe ocurrir a través de mensajes de registro del sistema, SNMP Traps (Simple Network Management Protocol) y / o el intercambio de archivos de texto , lo que garantiza la integración con el entorno existente.
10. Debe permitir que todos los datos recogidos sean almacenados en un repositorio centralizado que no puede ser modificado por cualquier usuario o administrador de la solución, proporcionando una fuente de información 100 % (cien por ciento) confiable para la auditoría y análisis forense.
11. Además de permitir el monitoreo de tráfico por la red, también se proporciona un control con un de agente de software que controla todos los accesos a la base de datos, incluso cuando se lleva a cabo por

usuarios con privilegios de forma local en el servidor de base de datos (acceso a través de memoria compartida)

12. Debe permitir que la solución a utilizar y configurar los usuarios puede no corresponderse con los administradores de bases, lo que le permite ser utilizado por ejemplo por los auditores o área de cumplimiento del equipo. Ofreciendo la posibilidad de permiso y puntos de vista basado en roles y grupos definidos.
13. Debe permitir la separación de funciones, lo que permite funciones independientes de los auditores y el personal de seguridad.
14. Debe permitir el almacenamiento de la información auditada en un entorno distinto al de los servidores de producción, proporcionando un formato seguro para proteger la información almacenada.
15. Debe tener una consola central para la gestión de todas sus características, los informes y los recursos disponibles.
16. Debe permitir alta disponibilidad para que todos los componentes (colector y agregador de información) tengan un miembro de backup en caso de fallo en el servidor principal.
17. Debe tener la capacidad de balanceo de carga automático basada en los agentes.
18. Debe tener la capacidad de proteger los datos sensibles y privados almacenados en bases de datos a través de un acceso no deseado con parámetros de bloqueo.
19. Permitir la creación de un log para la auditoría de todas las actividades en la base de datos. La inclusión de información tal como: quién, qué, cuándo, dónde y cómo de cada transacción realizada.
20. Debe permitir el monitoreo, registro y control de acceso para comandos DDL, DML y DCL realizados en la base de datos, manteniendo un registro granular y centralizado. (DDL = Data definition language (Create, drop, alter table, etc); DML = Data Manipulation Language (select, insert, delete, update); DCL = Data Control Language (grant, revoke).
21. Debe permitir filtros y análisis en tiempo real para proveer información requerida en auditorias.
22. Debe permitir el monitoreo en tiempo real de cualquier manipulación al esquema de base de datos, tales como la inserción o remoción de tablas y columnas, y el fortalecimiento del control sobre la politica de cambios.
23. Debe permitir la monitorización en tiempo real de todos los comandos SQL realizados.
24. Debe permitir el monitoreo en tiempo real de todas las excepciones reportadas por la base de datos, tales como errores de acceso, permisos de acceso denegados y errores SQL.
25. Debe basada en políticas de seguridad para efectuar acciones automáticas que los clientes pueden utilizar para abordar adecuadamente las violaciones de política, incluyendo las acciones de alerta y personalización en tiempo real.
26. Debe permitir que la información detallada sobre el origen de las transacciones de bases de datos, a fin de obtener la trazabilidad completa de las transacciones para un análisis posterior.
27. Debe permitir la identificación de los usuarios / acceso a través de numerosas informaciones incluyendo nombre-usuario, el sistema operativo de nombre de usuario (login de dominio), dirección MAC, nombre de host y la dirección IP.
28. Debe tener la capacidad de supervisar y aplicar políticas al usuario privilegiado (por ejemplo, el DBA).
29. Debe proporcionar un componente que permita la localización y clasificación de la información sensible en las bases de datos.

30. Debe tener la capacidad de enmascarar o deformar la vista de los datos solicitados a la base de datos, ya sea por aplicación o consulta directamente en la base, de acuerdo al perfil de cada usuario. Se aceptará integrar una herramienta de terceros para cumplir con la capacidad de enmascaramiento dinámico de ser necesario, en caso de que la herramienta antes mencionada sea de tipo virtual, la entidad brindará el entorno virtual incluyendo la licencia de virtualización, así como también la licencia del sistema operativo (Windows o Linux), todo licenciamiento adicional necesario para la implementación de la herramienta como base de datos (no se aceptarán bases de datos tipo express) u otros necesarios, deberá ser proporcionado como parte de la solución. También se aceptará soluciones que realicen esta función sobre data estática, conocido en el mercado como Enmascaramiento Estático.
31. Debe permitir la generación de alertas cuando ocurran múltiples intentos de login fallidos.
32. Debe capturar y reportar cuales son los usuarios de la base de datos y cuáles son sus permisos.
33. Debe permitir proteger datos sensibles y privados almacenados en filesystems, a través del bloqueo parametrizable de los accesos indeseados, como mínimo en los siguientes sistemas de archivos: EXT3, EXT4, XFS, JFF y JFS2 (opcional).
34. Debe permitir la creación de un log para la auditoría de todas las actividades en los filesystems. La inclusión de información tal como: quién, qué, cuándo, dónde y cómo de cada transacción realizada. (opicional)
35. Debe permitir filtros y análisis en tiempo real a la información que permita proveer información necesaria para la auditoría. (opcional)
36. Debe permitir el monitoreo en tiempo real de todas las acciones tomadas en archivos de tipo .DOC .(opcional)
37. Debe permitir el monitoreo en tiempo real de todas las acciones tomadas en archivos de tipo .XLS . (opcional)
38. Debe permitir el monitoreo en tiempo real de todas las acciones tomadas en archivos de tipo .PDF . (opcional)
39. Debe permitir la identificación de los usuarios / acceso a través de diversos parámetros incluyendo el nombre-usuario en el OS, nombre de usuario del OS, dirección MAC, nombre de host y la dirección IP.
40. Debe poseer la capacidad de monitorear y aplicar políticas para usuarios privilegiados (Ejemplo: ROOT).
41. Debe contar con reportes pre-configurados para auditoría y cumplimiento, que incluya templates para regulaciones de seguridad.
42. Debe permitir la personalización de los reportes existentes en forma simple, a través del proceso de "drag and drop" combinando columnas y diferentes filtros de búsqueda.
43. Para los reportes y alertas la solución debe soportar interfaces estándar, incluyendo, pero no limitado a: SNMP, SMTP y exportación de archivos en formato CSV.
44. Debe tener disponibilidad de reporte preconfigurado para auditoría y compliance.
45. Debe tener disponibilidad de reporte preconfigurado para auditoría y compliance.
46. Debe permitir la representación de los reportes en forma de gráfico.
47. Debe permitir el monitoreo/protección en ambientes AIX
48. Debe permitir el monitoreo/protección en ambientes Red Hat Enterprise Linux.

49. Debe permitir el monitoreo/protección en ambientes Windows Server
50. Debe permitir el monitoreo/protección en ambientes Oracle (Incluyendo ASO/SSL)
51. Debe permitir el monitoreo/protección en ambientes Microsoft SQL Server
52. Debe poseer un componente de red especializado para ataques de base de datos.
53. Debe contar con mecanismos de protección cuando esté operando en forma de port mirror.
54. Debe permitir la exportación de logs mediante protocolo SYSLOG, en forma segura, u otro método de exportación de logs segura.
55. Debe detectar y alertar ante cualquier cambio en el estado de los servicios en los servidores que contienen las bases de datos

C. Servidor de consola de Administración.

1. La consola de gestión deberá ser un appliance físico y permitir la administración de toda la solución, el contratista podrá ofertar virtual appliance en un servidor físico hardenizado para este punto, debiendo proporcionar todos los componentes necesarios para la implementación. Asimismo, deberá tener una capacidad de 14TB utilizable, con discos en RAID1 o superior. Para el caso de la consola de tipo apliance físico debe tener la posibilidad de ser migrada a un entorno virtual de requerirse.
2. Debe permitir la adquisición de Software Appliance, pudiendo también ser instalada en ambientes virtuales.
3. Debe ser competitiva y homologada para ser ejecutada en máquinas virtuales VMWare.
4. La administración de los equipos debe centralizarse a través de un servidor dedicado a dicho propósito.
5. Debe permitir realizar la configuración de toda la solución.
6. Debe contar con una interface gráfica de usuario (GUI) la cual se podrá elegir al menos entre los idiomas inglés y/o español.
7. Debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.
8. Debe poseer una Interface basada en línea de comando (CLI) para administración de la solución, el cual debe permitir una comunicación cifrada. Se aceptarán también soluciones que no posean una interfaz basada en línea de comando (CLI) siempre y cuando se garantice que todas las capacidades de administración se encontrarán disponibles en la interfaz gráfica GUI.
9. La solución debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales.
10. La solución cuenta con la capacidad de asignar un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar (RBAC).
11. La solución debe permitir filtros de acceso a los administradores al conectarse desde ciertas direcciones IP. Dicha funcionalidad podrá ser atendida mediante el sistema operativo de virtualización o el sistema operativo donde se instalará dicha solución.
12. La solución debe contar con soporte de SNMP versión 3.
13. La solución debe permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica, esta funcionalidad podrá ser atendida mediante la asignación de roles realizada por el administrador.

14. El sistema de gestión debe proveer estadísticas en tiempo real del estado de salud de la solución en el dashboard, considerando parámetros como utilización de CPU y número total de sesiones concurrentes.
15. Debe permitir generar reportes de forma manual o automática en formatos PDF, HTML y formato CSV.
16. Debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+(opcional).
17. Debe permitir la configuración de NTP.
18. Debe permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.