ANEXO B4

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

MARCA	
MODELO	
NUMERO DE PARTE DEL FABRICANTE	
CANTIDAD	

Característica	**Fuente (**Folletos, brochures, certificados, enlaces web, catálogos, instructivos, hojas de datos y/o manuales técnicos, o carta del fabricante.**)**	**Pág.**	**Ítem, numeral, capítulo de la pagina**	**Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.**
I. Solución de protección de Base de Datos (DBF)				
B. Características de detección				
1. Debe poder sincronizar hora a través del protocolo NTP con un servidor de la organización o externo.				
2. 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 utilizen.				
3. 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.				
4. 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.				

5. 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.				
6. 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.				
7. 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.				
8. 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.				
9. Además de permitir de 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)				
10. 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.				
11. 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.				
12. 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.				
13. 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).				
14. 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.				
15. Debe permitir la monitorización en tiempo real de todos los comandos SQL realizados.				