ANEXO 1

ESPECIFICACIONES TECNICAS

Las especificaciones técnicas del servicio se establecen a continuación:

1. **Condiciones Generales.**

1.1. La solución Database Activity Monitoring (DAM) / DBF (Database Firewall) ofertada debe tener la capacidad de capturar todas las acciones de usuario relacionadas con las bases de datos por el periodo de 1 año. Estas acciones se deben capturar sin requerir mecanismos propios-nativos de las bases de datos. Los motores que debe soportar la solución deben ser por lo menos los siguientes:

- Amazon Aurora MySQL - Amazon Redshift
- Amazon RDS for MariaDB Server - Amazon RDS for Microsoft SQL Server
- Amazon RDS for Oracle - Amazon RDS for PostgreSQL
- Azure SQL Server - Cloudera Data Platform (CDP)
- Cloudera Hadoop (CDH) - Couchbase Server
- Datastax Cassandra - Google Cloud MySQL
- Google Cloud SQL Server - Hortonworks Hadoop (HDP)
- IBM Db2 for i - IBM Db2 for LUW
- IBM Db2 for z/OS - IBM Information Management System (IMS)
- IBM Integrated Analytics System (IIAS) - IBM PureData System for Analytics (Netezza)
- Informix - MariaDB Server
- MarkLogic - Microsoft SQL Server
- MySQL - Oracle
- Pivotal Greenplum Database - PostgreSQL
- PostgreSQL On-Prem - SAP-HANA
- Sybase ASE - Sybase IQ
- Sybase SQL Anywhere - Teradata

1.2. La solución ofertada debe contar con el correspondiente respaldo del fabricante, para los servicios de garantía de hardware (si aplica), mantenimiento software y soporte técnico.

1.3. El fabricante de la solución deberá contar con un centro de investigación que se encargue de generar mecanismos de detección de ataques hacia las BD y de cumplimiento de estándares de seguridad y auditoría de la industria; estos mecanismos podrán ser firmas, políticas, vulnerabilidades, plantillas, entre otros. Dicho contenido

deberá ser descargable de forma periódica por la solución para incrementar su capacidad de detección y mitigación de amenazas y cumplimiento.

2. Integración

2.1. La solución debe soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas de terceros.

2.2. El sistema debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM) a través de syslog.

3. Monitoreo

3.1. La solución deberá incluir agentes livianos de software para monitoreo de actividad sobre el servidor, sin depender de auditoría nativa de las bases de datos o logs propios de los motores de Base de datos. Asimismo, la solución no deberá depender únicamente de dichos agentes para poder protegerlos y/o monitorearlos.

3.2. Los agentes deberán poder desactivarse si superan determinado umbral del consumo de CPU del servidor donde se encuentra instalado. Asimismo, para mejorar el performance, el agente podrá contar con políticas que permitan excluir determinados eventos (incluyendo procesos confiables del servidor de BD y/o eventos originados a partir de una IP determinada).

3.3. Los agentes deben soportar al menos los siguientes sistemas operativos: Solaris, Microsoft Windows, Oracle_Linux, Ubuntu en sus versiones funcionales y actualizadas.

3.4. Deberá registrar todas las pistas de auditoría de manera detallada de todas las actividades referentes a las bases de datos, que permita conocer por cada transacción "quién, qué, dónde, cuándo y cómo".

3.5. La solución deberá implementar un monitoreo efectivo de usuarios privilegiados (DBA, super usuarios, desarrolladores, etc.).

3.6. La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.

3.7. La solución deberá monitorear tanto el tráfico local y el remoto de las bases de datos.

3.8. La solución deberá ofrecer la posibilidad de auditar las sesiones de base de datos. La auditoría debe incluir los siguientes datos:

- Fecha y hora de la ocurrencia del evento.
- Información de usuario de base de datos.
- Información de los objetos de bases de datos (tablas, vistas, vistas materializadas, store procedures, entre otros.) consultados/modificado y los datos consultados (resultados de la consulta).
- Instancia, esquema, base de datos, objeto y operación realizada.

- Debe mostrar las variables bind en caso de que éstas sean utilizadas por la aplicación.

3.9. La solución deberá manejar funcionalidades tan amplias o granulares como se requieran, que deberán poder ser construidas manualmente. Los criterios deberán poder usarse varios a la vez y en diferentes combinaciones de ellos:

- Tipo de datos accedido.
- Acceso a datos marcados como sensibles.
- Base de Datos, Schema, Instancia, Tabla y Columna accedido.
- Estado de autenticación de la sesión.
- Usuario y/o Grupo de Usuarios de Base de Datos conectado.
- Logins, Logouts, Queries.
- IPs de origen y destino.
- Nombre de Host origen.
- Aplicación usada para la conexión a la base de datos.
- Tiempo de respuesta/procesamiento del query.
- Número de ocurrencias en intervalos de tiempo definidos.
- Por operaciones básicas (Select, Insert, Update, Delete).
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Restore).
- Por Stored Procedure o Function utilizada.
- Hora del Día.

3.10. La solución deberá soportar la importación de certificados en formato PKCS12 y PEM.

3.11. Por cada política de auditoría se podrá especificar una cuota de espacio en disco para almacenamiento de eventos, de tal forma que las políticas consideradas críticas puedan tener mayor espacio de almacenamiento que otras políticas no críticas.

3.12. Por cada política de auditoría se podrá determinar si los logs de transacciones SQL serán respaldados en un servidor externo (FTP o SCP), indicando una frecuencia de respaldo automático.

3.13. Por cada política de auditoría se podrá definir si la solución también tendrá la capacidad de almacenar los logs de respuesta de la BD al hacer una consulta a una tabla (SELECT).

3.14. La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema, entre otras; hacia otras herramientas de administración por medio de protocolos SNMP y SYSLOG.

4. Agente

4.1. La solución, para efectos de obtener los registros de auditoría de las transacciones de BD no deberá requerir ningún cambio en la configuración o contenido de la base de datos. Esto incluye:

- Creación de usuarios en las bases de datos.
- Modificación de los permisos de los usuarios existentes.

5. Perfilamiento

5.1. La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana. El proceso deberá ser constante y deberá aprender la estructura de las bases de datos, incluyendo bases de datos, tablas, aplicaciones, IP origen, querys, así como el comportamiento de cada usuario; todo esto para el establecimiento de una línea base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.

6. Descubrimiento

6.1. La solución deberá realizar descubrimientos automatizados (escaneos) en la red para identificar servidores bases de datos ya sea a nivel de servidor o puertos habilitados.

6.2. La solución deberá tener la capacidad de descubrir y clasificar información sensible dentro de las tablas de bases de datos de acuerdo con las políticas de negocio. Las definiciones de que se considera información sensible deberán poder crearse de manera flexible y granular.

7. Análisis de vulnerabilidades

7.1. La solución deberá poder realizar escaneos a las bases de datos en diferentes niveles/capas, según lo siguiente:

- Brindar un puntaje de los riesgos e indicar cómo mitigar esos riesgos.
- Escaneo de vulnerabilidades de la base de datos y configuraciones erróneas, como contraseñas predeterminadas.
- Escaneo de cumplimiento de estándares de benchmarks o hardening como CIS y DISA-STIG.

7.2. El análisis de vulnerabilidades no debe requerir la instalación de software en el servidor de la base de datos.

7.3. La solución deberá contar con un dashboard que permita comparar una tarea de escaneo de vulnerabilidades actual con uno anterior, para verificar si las vulnerabilidades o configuraciones erróneas han sido solucionadas.

8. Control de permisos de usuarios

8.1. Deberá contar con la funcionalidad de (mediante escaneos) poder realizar informes sobre:

- Permisos efectivos de los usuarios sobre los distintos objetos de las bases de datos.
- Detección de usuarios "Dormant" o en desuso y cuáles de ellos están o no bloqueados.
- Cadenas de autorización que permiten que cierto usuario (a través de ciertos roles) tenga un permiso específico.
- Relacionar un permiso otorgado a cierto usuario con quién lo otorgó (Grantee).

9. Bloqueo

9.1. La funcionalidad de Bloqueo deberá estar activa en el mismo equipo que realiza el monitoreo de actividad de la base de datos (DAM).

9.2. De acuerdo con la detección de ataque debe permitir tomar diferentes acciones:

- Bloqueo de comando SQL.
- Bloqueo de la dirección IP correspondiente a la petición, durante una cantidad de tiempo definible.

9.3. La funcionalidad de Bloqueo no deberá depender de la funcionalidad de auditoría, es decir, se podrá implementar una política de Bloqueo para determinada transacción SQL, independientemente si dicha transacción SQL tiene una política de auditoría asociada.

10. Seguridad

10.1. La solución deberá proveer detalles sobre alertas generadas y deberá tener la facilidad de modificar las políticas asociadas desde las alertas.

10.2. Deberá poder alertar en tiempo real peticiones a la base de datos dependiendo de:

- Usuarios de bases de datos, Usuarios de Sistema operativo, IP y nombre de host de origen, binario o programa utilizado para conectarse.
- Base de datos, tabla, stored procedure, esquema.
- Tablas, esquemas, columnas.
- Operaciones realizadas (DELETE, UPDATE, GRANT, ALTER, etc.).
- Horarios de ejecución de operaciones.
- Cantidad de registros devueltos en un query y tiempo de respuesta.

10.3. La solución deberá detectar anomalías y abusos a los protocolos de red, malformaciones en los protocolos SQL y firmas de ataque conocidas destinadas a los servidores protegidos.

10.4. La solución debe detectar los siguientes eventos de seguridad:

- Acceso de usuario desconocido.
- Acceso de aplicación de base de datos desconocida.
- Acceso de cliente (origen IP) desconocido.
- Intento de ejecución de inyección de comandos SQL.
- Ejecución de un Stored Procedure desconocido.
- Acceso a una base de datos y o esquema no autorizado.
- Acceso a bases de datos, esquemas o tablas previamente definidas.
- Ejecución de comandos privilegiados (DDL).
- Ejecución de comandos SQL no autorizados.

10.5. La solución deberá examinar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son ataques complejos intentando vulnerar las aplicaciones.

11. Administración

11.1. La solución deberá ser administrada desde una sola consola (centralizada) WEB que permita la gestión de las políticas (auditoría y seguridad), informes, reportes, revisión

de auditoría, monitoreo, eventos de seguridad, gestión de los distintos componentes de la solución y el monitoreo de su estado y performance.

11.2. La solución debe incluir un servidor central de administración en el cual residan el software de administración y registro de eventos generados por los diferentes componentes de la solución.

11.3. La solución deberá permitir realizar backups periódicos en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto utilizando los protocolos SCP y FTP. El backup deberá estar cifrado. La periodicidad de los backups se debe poder establecer desde la consola de administración.

11.4. Toda la configuración, administración y monitoreo de la solución se efectuará a través de la consola de administración.

11.5. La solución de administración debe permitir asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.

11.6. Deberá permitir la definición de roles de usuarios de forma granular, de tal forma que un rol tenga acceso a determinadas vistas o menus de la solución.

11.7. Proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.

11.8. La solución deberá realizar detección y análisis sobre todo el tráfico en tiempo real, sin necesidad de crear un archivo log primero para su análisis posterior.

11.9. La solución de administración permitirá, como mínimo, lo siguiente:

- Agregar, eliminar o modificar la configuración en un entorno gráfico.
- Modificar las reglas de los diferentes equipos.
- Efectuar la configuración de los componentes de la solución.
- Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema.
- Generar reportes ajustables por el usuario.

11.10. Permitir la generación de reportes, de toda la actividad registrada en los logs, en los formatos PDF y CSV.

11.11. Permitir la elección de información a ser incluida en los reportes de forma granular, con la capacidad de elegir las columnas a mostrar en los reportes y filtrar la información a ser mostrada. Asimismo, permitir diagramas ejecutivos de barra o pie en los reportes PDF.

11.12. Capacidad de automatizar la generación de reportes y su posterior remisión por email.

12. Data Risk Analitics

12.1. La solución debe contar con un mecanismo de inteligencia artificial que detecte usuarios comprometidos cuyas credenciales son robadas o que, sin saberlo, introducen malware en la institución.

12.2. La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios malintencionados que deliberadamente roban o manipulan activos corporativos

12.3. La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios descuidados que inadvertidamente ponen en riesgo datos confidenciales.

12.4. La solución debe contar con un mecanismo de inteligencia artificial que aprenda dinámicamente los patrones normales de acceso a los datos de los usuarios y luego identifique la actividad de acceso inapropiada o abusiva para alertar de manera proactiva a los equipos de TI sobre comportamientos peligrosos.

12.5. El mecanismo de analítica debe tener la capacidad de agregar patrones de comportamiento en listas blancas, por tiempos determinados para que no se emitan alertas o se generen incidentes que coincidan por el periodo establecido.

12.6. El mecanismo de analítica debe tener la capacidad de dar visibilidad ante por lo menos los siguientes eventos:

- Modificaciones a las auditorías nativas con la intención de eliminar rastro de actividades maliciosas.
- Intento de ejecución de comandos de sistema operativo aprovechando alguna vulnerabilidad en la base de datos.
- Intento de robo de credenciales de las bases de datos consultando la metadata de las mismas.
- Exfiltración de datos.
- Modificación de la configuración o inclusión de elementos dentro de la base de datos que permitan vulnerar/atacar la información.
- Inclusión de código binario (malware) en los motores de bases de datos con el objetivo de atacar o correr código arbitrario con funciones diferentes a las autorizadas.
- Ataques que aprovechando vulnerabilidades de las bases de datos hayan logrado o hayan intentado leer archivos propios del sistema operativo.

- Un usuario malintencionado ataca la base de datos e intenta explotar una vulnerabilidad o una característica de la base de datos para obtener privilegios elevados sobre recursos y / o datos.
- Un usuario malintencionado ataca la base de datos y realiza una secuencia sospechosa que se identifica como una campaña de Ransomware.
- Se utiliza una cuenta para acceder a la base de datos en un momento atípico para un usuario y su grupo de pares.
- Un usuario interactivo (humano) está utilizando una cuenta de servicio para acceder a la base de datos.
- Una persona consulta registros en exceso de lo que normalmente consulta el, su grupo de pares y la organización.
- Un usuario no ha podido iniciar sesión satisfactoriamente más veces de lo habitual para este propietario de cuenta en particular.
- Un usuario no pudo iniciar sesión (satisfactoriamente) en la base de datos desde un servidor de aplicaciones.
- Un usuario ha intentado acceder a una cantidad anormalmente alta de bases de datos diferentes durante un corto período de tiempo.
- Un usuario inició sesión en el dispositivo corporativo de otro empleado para acceder a una base de datos.
- Un usuario interactivo (humano) accede directamente a datos comerciales a los que normalmente solo se debe acceder a través de una aplicación.
- Un usuario realizó un comando que es de naturaleza altamente sospechosa y se ejecutó de una manera anormal.
- Un usuario interactivo (humano) ha consultado una base de datos utilizando consultas SQL dinámicas de forma anormal.
- Un usuario interactivo (humano) ha escaneado tablas sensibles del sistema en varias bases de datos durante un período de tiempo relativamente corto de forma anormal.

13. Requisitos de los oferentes

13.1. El oferente debe ser una empresa consolidada en el mercado con más de 10 años experiencia en el área de ciberseguridad.

13.2. El oferente debe tener personal técnico mínimo tres (3) con certificación vigente del fabricante que garantice conocimiento para participar en cualquier etapa del ciclo de vida de la solución ofertada, debe incluirse la documentación correspondiente junto con el currículo del personal asignado de al menos tres (3) personas.

13.3. El oferente deberá debe poseer un nivel de Partner Support.

13.4. El oferente deberá demostrar poseer una alianza estratégica con una entidad internacional, que certifique exclusivamente la Seguridad de la Información, mediante un programa integral de evaluación y certificación continuo en el tiempo, demostrable a través de una carta de dicho ente internacional.

13.5. Debe poseer un centro de Operaciones de Seguridad (SOC) formalmente constituido, dónde se ejecuten todo el monitoreo, análisis de riesgo total de las soluciones bridadas u otras relacionadas. Para cumplir con este punto deberá presentar declaración jurada que así lo indique. Es importante mencionar que una mesa de ayuda o un NOC no son considerados Centro de Operaciones de Seguridad. Para cumplir con este punto deberá presentar declaración jurada que así lo indique.

13.6. La empresa que podrán aportar su conocimiento técnico para la ejecución contractual debe contar con al menos 5 años de experiencia verificable en el campo sobre el cual se presenta oferta. Para verificación de este punto debe aportar al menos tres (3) cartas firmadas digitalmente o presentar listado de referencias en formato "pdf" de clientes, a los cuales brinda servicios del mismo tipo correspondientes al objeto de esta contratación. El listado debe tener detalle del nombre del cliente información del contacto (nombre, correo, número telefónico).

13.7. El oferente debe estar considerado líder como empresa consultora de servicios de ciberseguridad por analistas de mercado como Gartner, Forrester, IDC o Frost & Sullivan.

13.8. Para garantizar las mejores prácticas de TIC, se requiere que el oferente cuente con al menos tres (3) profesionales certificados en ITIL.

13.9. Para garantizar el apropiado cumplimiento de normas internas, mejores prácticas en TI y Seguridad Informática se requiere que el oferente cuente con al menos:

- Un (1) gestor de proyecto certificado como PMP Project Management Professional) emitida por el PMI (Project Management Institute) con más de 2 años de experiencia. Para lo cual deberá presentar documento donde conste dicha condición y su vigencia.
- Dos (2) profesionales certificados como ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición.
- Dos (2) profesionales certificados en ISO/IEC 27032 Cybersecurity Manager. Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dichacondición.
- Dos (2) profesionales certificados como Certified Information Systems Security Professional(CISSP). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición.