BANCO DE COMERCIO EXTERIOR DE COLOMBIA-BANCÓLDEX S.A.

TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN DE UNA SOLUCIÓN INTEGRAL DE SEGURIDAD INFORMÁTICA PARA PROTECCIÓN DE PORTALES WEB Y BASES DE DATOS.

PARTE II

BOGOTÁ D.C.

21 de abril de 2017.

INDICE

1. SOLUCIÓN TÉCNICA

1.1 REQUERIMIENTOS TÉCNICOS PARA WAF

El proponente deberá cumplir con los siguientes requerimientos de orden técnico para WAF:

a) La Solución requerida (Web Application Firewall -WAF) debe ser de tipo 'Appliance Virtual y debe estar certificada para ejecutarse sobre plataformas VMware versión 6.1 o posterior.

b) Throughput mínimo requerido es de 100 Mbps.

c) La Solución requerida debe contar con un esquema de alta disponibilidad con el fin de soportar cualquier tipo de falla relacionada con el software o hardware, proporcionando mecanismos de habilitación automática para el servicio y manteniendo el mismo nivel de seguridad, calidad y disponibilidad del servicio.

d) La Solución requerida debe incluir todos los componentes tecnológicos necesarios para soportar un esquema de contingencia, el cual debe operar en la modalidad 'Activo/Pasivo', soportando el mismo nivel de seguridad y calidad que proporcionado por el sistema principal. El esquema de contingencia estará ubicado en un datacenter externo, hacia el cual se tiene comunicación permanente a través de un canal Metro Ethernet.

e) La Solución requerida debe incluir consolas de gestión que faciliten la ejecución de las tareas administrativas tales como monitoreo, ajuste de parámetros, establecimiento de políticas, extracción de reportes, entre otras funciones. Se deben ofrecer dos (2) consolas de administración: Una consola para soportar el esquema de alta disponibilidad y otra para soportar el ambiente de contingencia. Las consolas de administración podrán ser comunes para las soluciones WAF y DBF.

f) La Solución debe permitir a los administradores del sistema visualizar, analizar y correlacionar los eventos sucedidos sobre los portales Web de manera eficiente y sencilla, con el fin de identificar las tendencias que suponen riesgos de seguridad, así como accesos no autorizados.

g) La Solución WAF debe proteger a las aplicaciones Web y a la infraestructura subyacente, mediante la detección de ataques a las aplicaciones a los servicios Web, a los servidores y a las redes a través de firmas precargadas que deben ser actualizadas de forma continua.

h) La Solución deberá permitir los modelos de seguridad positivo y negativo.

i) Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.

j) La Solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web y generar reportes que permitan realizar análisis de entorno.

k) La Solución deberá contar con un modo aprendizaje para rastrear cambios continuos en las aplicaciones web, además de reconocer cambios en la aplicación y simultáneamente protegerlas. De igual forma La Solución deberá contar con las siguientes características:
    - Deberá aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
    - Los valores aprendidos podrán ser utilizados, como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
    - El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación (directorios, url´s, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de sólo lectura o editable por el usuario) y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.
    - La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo.

l) La Solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo.

m) La Solución deberá contar con el modo de instalación proxy transparente.

n) La Solución deberá mitigar todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.

o) La Solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
    - La Solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
    - La Solución deberá desencriptar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
    - La Solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje.

p) La Solución deberá contar con funcionalidades que permitan:
    - Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
    - Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
    - Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
    - Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).

- Bloquear solicitudes de acceso basado en el país de origen de la conexión.
- Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque."

q) La Solución debe tener la capacidad de configurar alarmas automáticas para eventos que se repitan en un tiempo determinado, como por ejemplo los expuestos en el numeral r

r) La Solución deberá contar con protección para las siguientes amenazas.

- SQL injection
- Cross-site scripting (XSS)
- Parameter tampering
- Hidden field manipulation
- Session manipulation
- Cookie poisoning
- Stealth commanding
- Backdoor and debug options
- Application buffer overflow attacks
- Brute force attacks
- Data encoding
- Unauthorized navigation
- Gateway circumvention
- Web server reconnaissance
- SOAP and Web services manipulation

s) La Solución debe tener por lo menos la capacidad de configuración en modo Activo - Activo o Activo – Pasivo.

t) Validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.

u) El sistema debe soportar filtros Anti-Scraping.

v) El sistema deberá contar con una herramienta de análisis de vulnerabilidades, de Software.

w) El sistema deberá contar con protección para ataques de día cero.

x) El sistema deberá contar con actualizaciones automáticas.

y) Con el propósito de facilitar la gestión y correlación de eventos de seguridad, tanto de la solución WAF como para DBF, el Banco prefiere unificar en una única consola de gestión ambas herramientas. No obstante lo anterior, el Proponente podrá presentar tanto la solución WAF como para DBF en consolas de gestión distintas, debiendo especificar su arquitectura y modelo de gestión.

z) La solución deberá poder ser monitoreada a través de snmp y particularmente integrarse con el sistema de Monitoreo del Banco SolarWinds

Todos los elementos o componentes necesarios para dar cumplimiento a lo dispuesto en los presentes Términos de Referencia, se hayan requerido o no expresamente deberán ser brindados por el Proponente como parte integral de su propuesta y entregados en su oportunidad.

El Proponente deberá definir los términos y aclarar los conceptos que son particulares en su propuesta técnica, con el fin de tener un mejor entendimiento por parte del Banco y permitir la evaluación de la propuesta.

1.2 REQUERIMIENTOS TÉCNICOS PARA EL FIREWALL DE BASE DE DATOS (DBF)

Se anexa cuadro resumen de las Bases de Datos:

AMBIENTE	WEB SERVER	LICENCIAMIENTO BASE DE DATOS	TIPO DE PROCESADOR	SISTEMA OPERATIVO	# CORES
Producción	JBoss (Nodo 1)	N/A	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Red Hat Enterprise Linux Server release 6.5	
Producción	JBoss (Nodo 2)	N/A	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Red Hat Enterprise Linux Server release 6.5	
Contingencia	Jboss	N/A	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Red Hat Enterprise Linux Server release 6.5	

AMBIENTE	SERVIDOR BASE DE DATOS	LICENCIAMIENTO BASE DE DATOS	TIPO DE PROCESADOR	SISTEMA OPERATIVO	# CORES
Producción	ORACLE (Nodo 1)	Oracle Database Enterprise Edition por procesador	POWER7	IBM AIX 6.1	1
Producción	ORACLE (Nodo 2)	Oracle Database Enterprise Edition por procesador	POWER7	IBM AIX 6.1	1
Producción	SQLSERVER (Nodo 1) Activo	SQL SERVER ENTERPRISE	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Windows 2012 R2	4
Producción	SQLSERVER (Nodo2) Pasivo	SQL SERVER ENTERPRISE	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Windows 2012 R2	4
Contingencia	ORACLE	25 Usuarios nombrados Oracle Database Enterprise Edition	POWER7	IBM AIX 6.1	1
Contingencia	SQLSERVER	SQL SERVER ENTERPRISE	System PureFlex INTEL(R) XEON(R) CPU E5-2609 0 @ 2.40GHZ	Windows 2012 R2	4

El proponente deberá cumplir con los siguientes requerimientos de orden técnico para el FIREWALL de Base de Datos (DBF):

a) La Solución requerida (Database Firewall - DBF) debe ser de tipo 'Appliance Virtual y debe estar certificada para ejecutarse sobre plataformas VMware versión 6.1 o posterior.

b) La Solución requerida debe contar con un esquema de alta disponibilidad con el fin de soportar cualquier tipo de falla relacionada con el software o hardware, proporcionando mecanismos de habilitación automática para el servicio y manteniendo el mismo nivel de seguridad, calidad y disponibilidad del servicio de Firewall para las Bases de Datos.

c) La Solución requerida debe incluir todos los componentes tecnológicos necesarios para soportar un esquema de contingencia, el cual debe operar en la modalidad

'Activo/Pasivo', soportando el mismo nivel de seguridad y calidad que el que proporcione el sistema principal. El esquema de contingencia estará ubicado en un datacenter externo, hacia el cual se tiene comunicación permanente a través de un canal Metro Ethernet.

d) La solución debe contar con tecnología de auto-aprendizaje y requerir mínima intervención humana. El proceso de auto-aprendizaje debe partir del conocimiento de las estructura de las bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario, con el fin que se establezcan líneas base para el monitoreo y la seguridad. El modo de auto-aprendizaje se debe poder activar y/o desactivar de manera manual.

e) El Firewall de Base de Datos de propósito específico debe garantizar la protección de los datos sensibles de propiedad del Banco ante un ataque de hacking, vulnerabilidades, fuga y extracción de información, utilizando auditoria, monitoreo y bloqueo en tiempo real.

f) La Solución debe soportar como mínimo 2,000 transacciones por segundo y un throughput equivalente a 500 Mbps.

g) En cada base de datos a soportar mediante la Solución DBF se deben habilitar como mínimo tres (3) políticas de bloqueo.

h) La Solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software manejador de base de datos, a través de un único agente liviano instalado en cada servidor, sin importar el sistema operativo sobre el que se encuentren instalados.

i) La Solución deberá proveer un servicio de protección del software manejador de base de datos mediante la aplicación de parches virtuales que permita cubrir las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.

j) La Solución deberá apoyar los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/desempeño de las bases de datos y control de cambios. El módulo de administración del ciclo de vida de las vulnerabilidades debe permitir el acceso desde la misma consola de administración del sistema, no se deben requerir productos ni consolas adicionales para este fin.

k) La Solución requerida debe incluir consolas de gestión que faciliten la ejecución de las tareas administrativas tales como monitoreo, ajuste de parámetros, establecimiento de políticas, extracción de reportes, entre otras funciones. Se deben ofrecer dos (2) consolas de administración: Una consola para soportar el esquema de alta disponibilidad y otra para soportar el ambiente de contingencia. Las consolas de administración podrán ser comunes para las soluciones WAF y DBF.

l) La Solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:

- Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.

- Deberá contar con un sistema de correlación basado en la dirección de los ataques, determinando si los ataques provienen desde el interior o desde el exterior de la organización.

- Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.

- Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas y determinadas actividades en bases de datos específicas sin necesidad de alterar las aplicaciones o instalar componentes.

- Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL ó en el momento de iniciar sesión sobre las bases de datos.

m) La Solución debe contar con un módulo de administración de las vulnerabilidades de los sistemas y no deberá requerir la instalación de un segundo agente en los servidores de bases de datos para esta funcionalidad.

n) La Solución debe dar cumplimiento a todas las regulaciones que rigen a las instituciones financieras y a los estándares exigidos por la industria de forma rápida y efectiva.

o) La Solución debe alertar y bloquear en tiempo real todos los ataques y actividades no autorizadas que se estén realizando o puedan realizarse sobre las bases de datos.

p) La Solución debe automatizar los procesos de auditoría sobre las bases de datos, identificando de manera inmediata cualquier tipo de ataque, actividad malintencionada o fraudulenta.

q) La Solución debe identificar y reportar a los administradores del sistema sobre los privilegios excesivos que poseen los usuarios de bases de datos.

r) La Solución debe monitorear de forma continua y en tiempo real todas las operaciones que se realicen sobre las bases de datos, proporcionando los detalles de 'quién, qué, cuándo, dónde y cómo' se realizaron las transacciones.

s) La Solución debe realizar auditoría sobre los usuarios privilegiados que tienen acceso directo a los servidores de bases de datos y sobre los usuarios sin privilegios que tienen acceso a las bases de datos a través de las aplicaciones.

t) La Solución debe monitorear las respuestas dadas por las bases de datos con el fin de alertar y evitar la fuga de la información restringida.

u) La Solución debe permitir a los administradores del sistema visualizar, analizar y correlacionar los eventos sucedidos sobre las bases de datos de manera eficiente y sencilla, con el fin de identificar las tendencias que suponen riesgos de seguridad.

v) La Solución debe establecer líneas base de todas las actividades realizadas por los usuarios, incluyendo DML, DDL, DCL, actividades de sólo lectura (SELECTs) y el uso de procedimientos almacenados.

w) La Solución debe detectar variaciones cuando los usuarios ejecutan consultas no esperadas, alertar y bloquear a los usuarios que violen las directivas de acceso y poner en cuarentena a los usuarios que ejecuten solicitudes SQL no autorizadas, hasta que sus derechos de usuario hayan sido analizados y aprobados por el Banco.

x) El repositorio en el que se almacenaran todas las actividades capturadas por la solución de Firewall de Base de Datos no debe permitir el acceso a través de ningún mecanismo diferente al autorizado para la consola de administración que proporciona el fabricante de los appliances.

y) La solución de Firewall para Bases de Datos debe operar de forma independiente sin requerir la instalación de agentes de software sobre los servidores de base de datos que se requieren monitorear, lo cual debe ser opcional y no mandatorio.

z) La solución debe operar de manera independiente sin requerir la activación de la auditoría nativa sobre cada una de las base de datos a monitorear.

aa) La solución debe ser transparente para las bases de datos y/o aplicaciones que accedan a ellas, por lo cual, no se realizaran ni se aceptaran requerimientos de cambio en la programación, configuración u operación (triggers, stored procedures, etc.) en ninguna de ellas.

bb) La solución debe tener la capacidad de analizar y clasificar los tipos de datos almacenados en las Bases de Datos de acuerdo a las políticas del negocio. Las definiciones de tipo de datos deben poder crearse de manera flexible y granular.

cc) La solución debe monitorear toda la actividad de las bases de datos y debe almacenar los comandos SQL de acuerdo como fueron escritos o constituidos por el usuario o aplicación, incluyendo los comandos DDL, DML y DCL.

dd) La solución debe monitorear y capturar el detalle de todas las actividades realizadas sobre las bases de datos sin importar el punto de entrada, ya sean a través de conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, DB-Links, stored procedures u otros mecanismos.

ee) La solución debe realizar análisis y auditoría en tiempo real sobre todo el tráfico de red asignado, sin importar el volumen del tráfico y sin requerir la creación previa de un archivo o log para su análisis.

ff) La solución debe tener capacidad de monitorear el tráfico encriptado que gestionan las Bases de Datos.

gg) La solución debe proveer el detalle de todas las alertas ya sean falsos positivos o negativos y debe ofrecer la facilidad de cambiar las políticas a partir de las alertas.

hh) La solución debe identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, ésta actividad no debe implicar la modificación de la aplicación y/o de la base de datos.

ii) La solución debe manejar reglas y políticas de seguridad para las bases de datos y deben poder ser construidas automáticamente o manualmente, permitiendo su actualización de forma manual o automática.

jj) Las políticas específicas de control de acceso o generación de alertas deben contar con los siguientes criterios para permitir la validación de la actividad en las Bases de Datos. Los criterios deben poder usarse en cualquier número y cualquier combinación:

- Número de registros a regresar por la consulta (SQL Query).
- Número de registros afectados.
- Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada).
- Acceso a datos marcados como sensibles.
- Base de Datos, esquemas, instancia, tabla y columna accedida.
- Estado de autenticación de la sesión.
- Usuario y/o grupo de usuarios de Base de Datos conectado.
- Usuario conectado en la capa aplicación, a diferencia del usuario conectado a la Base de datos.

- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización a través de expresiones regulares).
- Logins, Logouts, Queries.
- IPs de origen y destino.
- Nombre de Host origen, Usuario firmado en el Host origen.
- Aplicación usada para la conexión a la base de datos.
- Tiempo de respuesta/procesamiento del query.
- Errores en el manejador de base de datos.
- Número de ocurrencias en intervalos de tiempo definidos.
- Por operaciones básicas (Select, Insert, Update, Delete).
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export).
- Por procedimiento almacenado o función utilizada.
- Si existe ticket asignado para los cambios.
- Hora del Día.

kk) La solución debe permitir el análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de ejecutar un proceso batch previo.

ll) La solución debe asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.

mm) La solución debe proteger contra ataques de tipo SQL y no-SQL (como buffer overflow).

nn) La solución debe gestionar alertas de emergencia para potenciales violaciones de acceso a la información a través de mensajes no bloqueantes para las consultas relacionadas con los siguientes eventos:

- Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación (física) desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

oo) La solución debe tener la capacidad de exportar datos y eventos, tales como alertas, eventos del sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio del protocolo SNMP.

pp) La solución debe contar con Políticas, Reportes, Alertas, Objetos y Transacciones pre configuradas para trabajar con bases de datos ORACLE y SQL SERVER sin importar su versión.

qq) La solución debe realizar periódicamente la evaluación exhaustiva de los riesgos relacionados con la infraestructura de base de datos, gestionando diferentes niveles o capas de la infraestructura e incluyendo los siguientes aspectos:

- Gestión de la configuración de las bases de datos tal como nivel de actualización (releáse y paquetes de seguridad),
- Configuración de las cuentas de usuario, evaluación de complejidad de las contraseñas, vigencia de contraseñas.
- Gestión de la configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

rr) La solución debe generar reportes y tendencias en tiempo real, así como permitir la fácil construcción de nuevos reportes.

1.3 CONTINUIDAD DEL NEGOCIO

El Proponente debe adjuntar su plan de continuidad del negocio que permita al Banco identificar estrategias en los casos de reemplazo del personal asignado al proyecto garantizando la transferencia de conocimiento y continuidad en la prestación del servicio contratado.

1.4 PLAN DE TRABAJO

El Proponente deberá incluir en su propuesta el plan de trabajo para la implementación de la solución, teniendo en cuenta que el tiempo requerido para la puesta en funcionamiento de la solución no podrá ser mayor a tres (3) meses, describiendo la metodología de desarrollo del proyecto, en el que indiquen los procesos/actividades requeridos para la instalación e implementación. Este cronograma debe detallar el número de días de cada actividad, los profesionales y su dedicación asociados a cada actividad.

El cronograma debe cumplir con las siguientes condiciones:

a. Explicar la relación entre las distintas actividades, e identificar rutas críticas si las hay.

b. Indicar los productos específicos a ser presentados y la fecha de entrega (por ejemplo: informes, reportes, manuales, etc.).

c. Para cada actividad relacionar el personal empleado y su dedicación.

Si la propuesta llegara a ser seleccionada, la empresa deberá entregar a Bancóldex el cronograma actualizado teniendo en cuenta la fecha de inicio del proyecto.

Bancóldex a través del Supervisor del contrato verificará el desarrollo del cronograma presentado, la dedicación del personal ofrecido, los resultados esperados y en general el cumplimiento de los compromisos adquiridos.

El proponente deberá como mínimo incluir las siguientes actividades en su plan de trabajo:

1. **Planificación del proyecto:** Etapa en la que el Proponente y el Banco acordarán el desarrollo del plan de la gestión del proyecto. En ésta etapa el Proponente deberá entregar: cronograma de trabajo, plan de alcance, plan de gestión de riesgos y demás documentos que se acuerden con el Banco.

2. **Implementación de la solución:** En esta etapa el Proponente debe describir todas las actividades requeridas para efectuar la implementación de la Solución tanto de WAF como DBF, incluyendo el esquema de alta disponibilidad y contingencia.

3. **Realización de pruebas técnicas:** El proponente deberá garantizar el planteamiento de un plan de pruebas que corroboren la funcionalidad de la solución adquirida.

4. **Integración:** En esta etapa el Proponente describirá todas las actividades requeridas para realizar la integración con los portales web y las bases de datos.

5. **Documentación:** En ésta etapa el Proponente entregará al Banco la documentación final del proyecto como manuales técnicos, manuales de instalación y configuración, manuales

de administración, diagramas de arquitectura y demás documentos que se acuerden con el Banco.

6. **Capacitación:** El Proponente debe incluir por lo menos una capacitación técnica certificada para cada producto que soporta la solución WAF y DBF. Cada capacitación deberá tener una duración mínima de 40 horas y estar planeada para que al menos cinco (5) funcionarios del Banco la reciban. Durante las capacitaciones se debe cubrir la totalidad del contenido oficial correspondiente y emitir un certificado de asistencia y cumplimiento. El Proponente debe indicar al Banco la disponibilidad de los horarios para realizar las capacitaciones en dos grupos.

   El Proponente deberá entregar en relación con la capacitación: plan de capacitación para usuarios técnicos, documentación con el contenido temático de cada una de las capacitaciones a realizar ya sea funcionales o técnicas, registros de asistencia a las sesiones de capacitación y demás documentos que se acuerden con el Banco.

Se tendrá en cuenta en la calificación al Proponente que optimice los tiempos propuestos para la implementación.

1.5 DIAGRAMA DE ARQUITECTURA TECNOLÓGICA

El proponente deberá presentar un diagrama donde se muestre claramente la arquitectura de la Solución WAF y DBF. En ésta se deberá hacer una descripción de todos los componentes requeridos en las diferentes capas de red.

1.6 PLATAFORMA TECNOLOGICA QUE SOPORTARÁ LA SOLUCIÓN

La Solución a implementarse debe correr sobre plataformas VMware versión 6.1. o posterior. El proponente deberá describir todos los requerimientos técnicos necesarios para su implementación en dicha plataforma.

1.7 SOPORTE A LA SOLUCIÓN OFRECIDA

El Proponente debe entregar la propuesta de servicios de soporte técnico para las soluciones WAF y DBF, por un periodo de tres (3) años. Se debe detallar el esquema de atención, los costos y los acuerdos de servicio que el Proponente tenga establecidos. En esta propuesta se deberán especificar como mínimo los siguientes puntos:

- Esquema detallado para las diferentes líneas de soporte (telefónico, mail, online, presencial, entre otros).
- Alcance de los servicios.
- Acuerdos de servicio (SLA).

- Valores para los servicios de soporte técnico y entrega de actualizaciones, tanto para WAF como para DBF.
- Horarios de soporte.

El proponente debe describir detalladamente cómo prestará los servicios de soporte técnico sobre la solución a implementar. Este soporte debe tener una disponibilidad durante los siete días de la semana y por las veinticuatro horas del día y estar a cargo de profesionales certificados. El tiempo máximo de atención para una solicitud crítica no deberá exceder las dos (2) horas y la solución definitiva no deberá exceder las 24 horas.

El proponente debe indicar los ajustes según incremento anual para los servicios de soporte técnico. En todo caso, éste no podrá superar el IPC vigente para el año en curso.

2. GLOSARIO

BASE DE DATOS: Conjunto de archivos de datos recopilados, definidos, estructurados y organizados sistemáticamente con el fin de suministrar información específica y adecuada a los usuarios de los sistemas transaccionales y de información.

FIREWALL: Sistema diseñado especialmente para bloquear el acceso no autorizado de usuarios o comunicaciones y permitir al mismo tiempo los usuarios o comunicaciones autorizadas.

WAF: Un Web Application Firewall es un dispositivo de hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques que pueden provenir desde Internet o desde el interior de la red

DBF: Un Database Firewall es un dispositivo de hardware o software diseñado especialmente para proteger las bases de datos contra los ataques de seguridad específicos.

THROUGHPUT: Velocidad real de transporte de datos a través de una red telemática, el cual normalmente se mide en Mbit/s y siempre será inferior al ancho de banda o bandwidth.

PROXIES ANÓNIMOS: Un proxy anónimo, también conocido como servidor de proxy anónimo, permite a un usuario acceder a un archivo, página Web, o cualquier otro recurso a través de un servidor que entrega los servicios requeridos del usuario por medio de otro servidor remoto.

MALWARE: Del inglés “malicious software”, también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

DIRECCIÓN IP: Es el identificador único de un usuario o dispositivo dentro de una red.

DIRECCIONES IP MALICIOSAS: Grupo de dispositivos o sitios web destinados a proliferar aplicaciones pirata, malware, software antivirus deshonesto y otras actividades maliciosas.

BOTNETS: Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

PHISHING: Es un término informático que significa suplantación de identidad y denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando llamadas telefónicas.

ANTI-SCRAPING: Software diseñado para evitar la ejecución de programas o software que extraen información desde sitios web.

ATAQUE DÍA CERO: Un ataque de día-cero (en inglés zero-day attack o 0-day attack) es un ataque contra una aplicación o sistema de información que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades, que por lo general, son desconocidas para la gente y el fabricante del producto.

AGENTE LIVIANO: Software que actúa para un usuario u otro programa en una relación de entidad, la cual deriva del Latin agere (hacer): un acuerdo para actuar en nombre propio.

SQL: (Structured Query Language) es un lenguaje de programación estándar utilizada para obtener información desde una base de datos y para actualizarla. Aunque SQL es a la vez un ANSI y una norma ISO, muchos productos de bases de datos soportan SQL con extensiones propietarias al lenguaje estándar.

SENTENCIA SQL: Instrucciones SQL utilizadas para construir, actualizar e introducir la información sobre una base de datos.

DML: Lenguaje de Manipulación de Datos (Data Manipulation Language) es un lenguaje proporcionado por los sistemas gestores de bases de datos que permite a los usuarios de la misma llevar a cabo las tareas de consulta o modificación de los datos contenidos en las Bases de Datos.

DDL: Lenguaje de definición de datos (Data Definition Language) utilizado para describir todas las estructuras de información y los programas que se usan para construir, actualizar e introducir la información que contiene una base de datos.

DCL: (Data Control Language) es un lenguaje proporcionado por el Sistema de Gestión de Base de Datos que incluye una serie de comandos SQL que permiten al administrador controlar el acceso a los datos contenidos en la Base de Datos.

AUDITORÍA NATIVA: Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en una base de datos.

QUERY: Término informático que se utiliza para hacer referencia a una interacción con una base de datos.

PROCESO BATCH: Se conoce como sistema por lotes, en inglés batch processing, o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo).

SNMP: El Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.