ANEXO A1

I. Solución de Firewall de Aplicaciones (WAF)

A. Características Generales

1. Debe estar licenciada para 25 subdominios para 4 dominios por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe estar dimensionada para soportar como mínimo un tráfico de 400 Mbps basado en HTTP/HTTPS.
3. Debe estar configurado en alta disponibilidad activo-pasivo, y la alta disponibilidad debe darse entre los equipos de la misma sede y entre las diferentes sedes de los centros de datos. La solución también deberá poder realizar el despliegue de modo activo-activo.
4. Debe admitir una comunicación segura entre todos sus componentes.
5. La solución firewall de aplicaciones y su consola deben ser provistas como servidor Appliance de tipo específico. También se podrá ofertar para la consola un servidor físico hardenizado.
6. La solución debe integrarse a un servidor HSM de forma nativa o por medio de un balanceador. Las integraciones podrán ser mediante PKCS#11 y/o Java (JCA/JCE)(opcional) y/o Microsoft CAPI (opcional) y/o CNG y/o OpenSSL.
7. Debe permitir realizar la configuración de toda la solución on-premise y para los componentes en nube como mínimo las configuraciones de seguridad. Se aceptarán soluciones que permitan realizar configuraciones separaras para componentes on-premise y componentes nube, la propuesta del postor deberá incluir lo necesario para proteger y administrar la plataforma on-premise y en nube sin incurrir en gastos adicionales a MEF.

B. Características de Firewall de Aplicación

1. Debe estar dimensionada para soportar una protección de aplicaciones de por lo menos 400 Mbps basado en HTTP/HTTPS. Deberá poder tener capacidad de crecimiento.
2. El dispositivo debe tener una latencia menor a 5 milisegundo.
3. Se requiere como mínimo cuatro (04) interfaces de cobre de 1Gbps y mínimo cuatro (04) interfaces de fibra de 10G SFP+.
4. Debe poder ser desplegado bajo al menos tres de los siguientes modos:
    a. Bridge.
    b. Fullproxy
    c. Reverse Proxy transparente.
    d. Reverse Proxy no transparente.
    e. Cluster (tráfico en esquema activo-standby o activo-activo).
5. Debe soportar acciones de política en modo bloqueo (activa) y reporte (pasiva).
6. Debe tener cobertura total de las vulnerabilidades clasificadas en "OWASP Top 10 2021 Project"
7. Debe proteger contra al menos los siguientes ataques de inyección:
    a. SQL.
    b. NoSQL.
    c. OS.
    d. LDAP injection.
8. Debe proteger contra ataques "Buffer Overflow".

9. Debe proteger contra amenazas producto del uso mal intencionado del protocolo Piggyback y/o explotación de protocolos malintencionados.
10. Debe proteger contra ataques de "Cross-Site-Scriptting (XSS)"
11. Debe proteger contra ataques de fuerza bruta (Brute Force Attacks).
12. Debe proteger contra inyecciones de comando al sistema operativo (OS).
13. Debe proteger contra ataques de "Cross Site Request Forgery (CSRF)"
14. Debe proteger contra amenazas del tipo "Hot Link".
15. Debe proteger contra el robo de información en base a patrones personalizados y/o campos que el administrador defina como información sensible.
16. Debe proteger contra ataques que busquen acceder al sistema de archivo del servidor haciendo uso de ataques como "Path (directory) Traversal".
17. Debe proteger contra ataques "Directory Listing".
18. Debe proteger contra ataques "Parameter Pollution (HPP).
19. Debe proteger contra el envío de entradas falsas a aplicaciones que utilizan parámetros artificiales y valores de parámetros que evaden mecanismos de seguridad simples.
20. Debe proteger contra amenazas que buscan la modificación de cookies establecidas por la aplicación.
21. Debe proteger contra la suplantación de sesiones TCP legítimas que estén en progreso, como cookies de la capa de sesión.
22. Debe proteger contra la explotación de vulnerabilidades inherentes a los formatos de "web service", estructura y operaciones. Así como manipulaciones de diccionario y codificación.
23. Debe proteger contra la explotación de vulnerabilidades que puedan quedar expuestas en el código interno desarrollado.
24. Debe proteger contra el uso de privilegios o accesos ocultos que las aplicaciones puedan exponer de manera inintencionada.
25. Debe ser capaz de proteger contra al menos los siguientes ataques y garantizar al menos 400 Mbps de tráfico limpio:
    - ✓ Proteger puertos de los siguientes ataques DoS:
        a. Ataques enviados a múltiples destinos de broadcast ICMP con direcciones IP de origen suplantadas.
        b. Paquetes con dirección IP de origen igual a la dirección IP de destino.
        c. Ataques enviados a múltiples destinos de broadcast UDP con direcciones de origen suplantadas.
        d. Paquetes con puerto de origen igual al puerto de destino.
        e. Paquetes TCP con todos los bits de control establecidos en 1
        f. Paquetes TCP con número de secuencia igual a 0 y/o bits FIN, URG y PSH establecidos.
        g. Paquetes TCP o UDP con puerto de origen o destino igual a 0.
    - ✓ Debe permitir repeler ataques del tipo DoS SYN
    - ✓ Proteger contra los siguientes ataques DDoS de aplicación:
        a. Múltiples peticiones con respuestas largas.
        b. Conexiones de bajo throughput (Low and Slow)
        c. Múltiples peticiones a páginas que consumen mayores recursos de servidor.

La funcionalidad deberá ser hibrida (OnPremise y Cloud), para lo cual debe cumplir con los requerimientos Técnicos solicitados en las Especificaciones Técnicas, además los componentes de tipo cloud deberán ser propios del mismo fabricante de la solución y no tercerizadas con otras empresas y deberán contar con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 y FedRAMP(Opcional).

26. Debe proteger contra ataques conocidos que estén catalogados en una base de datos del fabricante y que se actualicen periódicamente.
27. Debe poder generar eventos y bloquear "Application Paths" permitiendo al administrador realizar estos ajustes de forma manual o a través de la auto generación de políticas de forma dinámica, comparando al menos los siguientes elementos de la petición:
    a. Método.
    b. Path.
    c. Extensión.

    Como, por ejemplo:

    GET /trashfire.mpeg HTTP/1.1
    GET /images/image01.gif HTTP/1.1
    GET /images/webhelp/15267.jpeg HTTP/1.1
    PUT /PostDestination/MyFile.txt HTTP/1.1
28. Debe poder mitigar ataques de fuerza bruta, impidiendo la ejecución de herramientas automatizadas que intentan adivinar usuarios y/o contraseñas. Así mismo el dispositivo debe ser capaz de reconocer de forma automática aquellas direcciones IP compartidas, como por ejemplo las de un proxy AOL, con el fin de evitar mitigar usuarios autorizados que se encuentran detrás de un PROXY.
29. Para la protección de ataques contra bases de datos de tipo inyección, el dispositivo debe contar con un motor que implementa al menos ANSI SQL y diccionarios líderes como ser MSSQL y ORACLE. La solución WAF debe proteger contra ataques de SQL Inyection dentro del OWASP Top Ten. Está protección podrá ser provista con un motor propio de la solución o agregando firmas de bloqueo actualizables por el fabricante, además de la posibilidad de customizar meta metacaracteres en valores de parámetros específicos definidos por la entidad.
30. Debe ser capaz de mitigar ataques, que incluso puedan encontrarse codificados, dentro de ciertos parámetros HTTP.
31. Debe poder monitorear el comportamiento de los archivos que son cargados a las aplicaciones WEB según los principios mencionados por OWASP para la carga de archivos, generando eventos de seguridad (reporte o bloqueo) bajo condiciones que determine el administrador. Estas condiciones deben basarse en al menos lo siguiente:
    a. Application Path.
    b. Extensión.
    c. Método HTTP.
    d. Permisos de recuperación de archivo (opcional).
32. Debe contar con filtros de seguridad que validen al menos los siguientes parámetros de manera global:
    a. URL.
    b. Path.
    c. XML.
    d. Webservices.
    e. Cookie Parameters.

33. Debe permitir al administrador seleccionar de forma manual o en base a la auto generación de políticas, los métodos HTTP permitidos o denegados en diferentes Path de la aplicación.
34. Debe permitir generar logs que guarden información de la cabecera (header) y cuerpo (body) de diferentes peticiones y respuestas. Estos logs deben ser almacenados en el dispositivo.
35. Debe prevenir la fuga de información sensible a través del análisis de patrones en el cuerpo (body) de las respuestas HTTP y el bloqueo o reemplazo de los mismos por caracteres falsos. Estos patrones podrían ser, por ejemplo, números de tarjetas de crédito o cualquier patrón que sea configurable por expresiones regulares por el administrador.
36. Debe detectar y contrarrestar al menos los siguientes tipos de ataque en peticiones de operación SOAP:
    a. Diccionario.
    b. Encoding.
    c. Manipulación de la estructura.
37. Debe poder permitir o denegar una petición XML haciendo uso de filtros que verifiquen los parámetros o valores de esta petición.
38. Debe poder prevenir la modificación de cookies realizando la comparación entré las cookies establecidas por el servidor y aquellas que responden usuarios remotos.
39. Debe poder detectar bots y ataques del tipo "scrapping" que operen en un entorno de IP dinámico y generen actividad detrás de un sNAT (source NAT) como por ejemplo un proxy o una red Enterprise. Permitiendo, de esta manera, realizar el rastreo y bloqueo de estos bots agnóstico a la IP.
40. Debe mitigar solicitudes fingerprint que expongan el contenido o estructura de la aplicación.
41. Debe poder generar políticas y refinamientos de forma automática.
42. Debe brindar protección haciendo uso de modelos de seguridad positivo y negativo.
43. Debe mostrar ataques históricos o en tiempo real, en un determinado periodo de tiempo, mostrando al menos la siguiente información:
    a. Top Attack Category.
    b. Top Sources.
    c. Top Attacked Hosts.
    d. Attacks by action.
    e. Attack Severity.
    f. Geolocation
44. Debe ofrecer protección para impedir la ejecución automatizada de web scraping o clone site.
45. Debe permitir la exportación de logs mediante protocolo SYSLOG, en forma segura, u otro método de exportación de logs segura.
46. Debe permitir establecer protección para el control de acceso por geolocalización.

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. La administración de los equipos debe centralizarse a través de un servidor dedicado a dicho propósito.
3. Debe permitir realizar la configuración de toda la solución.
4. Debe contar con una interface gráfica de usuario (GUI) la cual se podrá elegir al menos entre los idiomas inglés y/o español.
5. Debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.
6. 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.
7. La solución debe permitir al administrador del sistema autenticarse vía usuario/contraseña o vía certificados digitales.
8. 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).
9. 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.
10. La solución debe contar con soporte de SNMP versión 3.
11. 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. Dichas funcionalidades podrán estar deshabilitadas aun cuando son mostradas en la interfaz gráfica.
12. 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.
13. Debe permitir generar reportes de forma manual o automática en formatos PDF, HTML y formato CSV.
14. Debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+(opcional).
15. Debe permitir la configuración de NTP.
16. Debe permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.
17. Deberá permitir crear reglas personalizadas para la protección de anomalías en aplicaciones.
18. Debe permitir la protección por doble factor de autenticación.
19. Debe contar con reportes para auditoría y cumplimiento, los mismos que si no están pre configurados, deberán ser configurados en la implementación por el postor ganador, deberá incluir templates para regulaciones de seguridad.