ANEXO N°1 - ESPECIFICACIONES TÉCNICAS

1. WAF Web

El contratista deberá suministrar una suscripción WAF Web destinada a la protección de las aplicaciones institucionales públicas expuestas a Internet que se encuentren, o que sean definidas por la Entidad, para operar desde el centro de datos alterno.

La solución deberá cumplir, como mínimo, con las siguientes características:

- Proteger aplicaciones web y servicios publicados mediante los protocolos HTTP y HTTPS.
- Permitir la incorporación, modificación y retiro controlado de aplicaciones, dominios, URL, direcciones IP, certificados y demás elementos necesarios para la publicación segura de los servicios institucionales.
- Contar con mecanismos de detección, alerta y bloqueo frente a ataques comunes contra aplicaciones web, incluidos, como mínimo, inyección SQL, *cross-site scripting* —XSS—, inclusión local o remota de archivos, ejecución de comandos, divulgación de información sensible, explotación de vulnerabilidades conocidas, cargas maliciosas y ataques automatizados.
- Permitir la configuración de políticas de seguridad por aplicación, URL, método HTTP, dirección IP, encabezado, parámetro, cookie u otros atributos pertinentes.
- Permitir el uso de políticas en modo de detección, alerta, bloqueo o mitigación, de acuerdo con la criticidad de la aplicación y previa validación de la Entidad.
- Permitir la creación y administración de reglas, excepciones, listas de permitidos, listas de bloqueo y firmas o patrones personalizados, cuando las condiciones de seguridad de las aplicaciones lo requieran.
- Contar con mecanismos de protección contra automatización maliciosa, bots, exploración de vulnerabilidades, intentos reiterados de autenticación y otros comportamientos anómalos, en la medida en que estos hagan parte de la suscripción ofrecida.
- Generar registros de tráfico, eventos, alertas, ataques detectados, bloqueos, cambios de configuración, accesos administrativos, errores y eventos de disponibilidad.
- Permitir el envío de registros al SOC o a la plataforma de monitoreo definida por la Entidad, utilizando los mecanismos y formatos compatibles con su arquitectura de seguridad.
- Incluir la suscripción y el soporte del servicio WAF en nube, con vigencia desde la suscripción del acta de recibo a satisfacción y hasta el 6 de julio de 2028, garantizando durante ese periodo la totalidad de las funcionalidades contratadas, y permitir la implementación de controles de seguridad basados en políticas internas hacia los servidores web de la Entidad.
- Proteger aplicaciones web sin importar su ubicación (on-premise o en nubes públicas).
- Integrarse con nubes públicas y privadas (por ejemplo, AWS, Azure y GCP).
- Detección de bots basada en inteligencia artificial mediante modelos de aprendizaje automático (machine learning), complementados con reglas por firmas y umbrales, y con técnicas de engaño mediante señuelos.
- Ser compatible con IPv6.

- Acreditar, en una evaluación independiente de eficacia de firewall de aplicaciones web (WAF/WAAP) con vigencia no mayor a dos (2) años, una tasa de bloqueo igual o superior al noventa por ciento (90%) sobre el conjunto de ataques evaluado y una tasa de falsos positivos igual o inferior al dos por ciento (2%). Se acredita con el informe completo del laboratorio, no con el resumen.
- Integrarse con soluciones de entorno virtual aislado (sandbox) sin requerir desarrollos adicionales por parte de la Entidad.
- Contar con soporte técnico del fabricante en esquema 7×24×365 durante toda la vigencia del contrato, con actualizaciones, acceso al portal de soporte y recursos técnicos. La solución en nube debe integrarse con el WAF FortiWeb 1000E existente y con las demás soluciones de ciberseguridad de la Entidad, conformando una plataforma unificada de protección de aplicaciones web (gestión y correlación centralizadas, políticas homogéneas y un único punto de escalamiento para el conjunto) para la centralización y el análisis de eventos.
- Estar dimensionada y licenciada, desde el inicio del servicio, para soportar como mínimo un ancho de banda de 50 Mbps y hasta veinte (20) sitios o aplicaciones web. La implementación inicial comprende las diez (10) aplicaciones críticas identificadas por la Entidad; las restantes se incorporarán, dentro de ese límite y sin costo adicional por aplicación, a medida que la dependencia usuaria las valide durante la vigencia de la suscripción. El contratista no podrá solicitar costos adicionales por insuficiencia del dimensionamiento, de los componentes o del licenciamiento de su solución, ni por ampliaciones de licenciamiento, capacidad o infraestructura, lo anterior debe estar incluido en la oferta.
- Proteger los subdominios frente a: Cross-Site Scripting (XSS), inyección SQL, RFI, LFI, ejecución de comandos de sistema, malware, exploits, fuga de información del servidor, fuerza bruta, ClickJacking, botnets, repetición de cookies, robo de datos de tarjetas, CSRF, desbordamiento de encabezados HTTP, bots maliciosos, ataques de intermediario (MITM), XML malformado, validación de parámetros HTTP conforme al RFC, man-in-the-browser, rastreadores y scrapers, con protección de API y JSON y revisión de tokens JWT; y frente a las amenazas del OWASP Top 10 (edición 2025) y del OWASP API Security Top 10 (edición 2023).
- La protección de interfaces de programación se construirá con inteligencia artificial en dos modelos: protección de esquema (aprendizaje de la estructura REST del tráfico) y protección de riesgo (aprendizaje de los valores de los parámetros), con capacidades de API Gateway, validación de esquema, límites JSON/XML y entidades XML.
- Aprender el patrón de interacción de los usuarios con las aplicaciones mediante aprendizaje automático y detección de anomalías, y aplicar ese aprendizaje al ajuste de las reglas de protección.
- Soportar interoperabilidad con OpenAPI 3.0.
- Disponer de detección de bots basada en biometría de comportamiento —movimiento del apuntador, uso del teclado, pantalla táctil y desplazamiento— y de un mecanismo de ajuste de reglas que permita reducir los falsos positivos sin desactivar la firma que los origina.
- Contar con un módulo de escaneo antimalware para los archivos cargados a las aplicaciones, con detección y bloqueo de malware conocido, e integrar funcionalidad de entorno virtual aislado (sandbox) sin costo adicional para amenazas de día cero.

- Validar y reportar que las credenciales usadas para acceder a las aplicaciones de los subdominios protegidos no hayan estado comprometidas.
- Detectar y eliminar información sensible del servidor en los encabezados HTTP y en las páginas de respuesta.
- Permitir la configuración de versiones seguras de TLS para mejorar la seguridad hacia el usuario final.
- Permitir importar los certificados digitales SSL propios del dominio, para garantizar la conexión segura entre el cliente y el servidor.
- Disponer de caché configurable por tipo de contenido y de red de distribución de contenido, administrables desde la consola de la Entidad.
- Permitir el envío de alertas por correo electrónico.
- Permitir la integración con soluciones SIEM vía syslog y el envío de todos los registros de acceso a un servidor syslog externo para análisis y almacenamiento a largo plazo, incluyendo AWS S3 y Azure Blob.
- Mostrar, en un tablero de control, los ataques detectados y bloqueados y el score de amenazas de la aplicación durante un rango de tiempo.
- Permitir modificar los encabezados HTTP relacionados con las políticas de Content Security Policy (CSP) en las aplicaciones.
- Disponer de mecanismos de gestión de identidad y acceso (usuarios, roles y permisos) para el acceso administrativo a la plataforma.
- Disponer de medidas propias de continuidad y de recuperación ante desastres sobre la plataforma del proveedor, con redundancia entre puntos de presencia, de modo que la indisponibilidad de uno de ellos no interrumpa la inspección del tráfico protegido.
- Suministrar, configurar y mantener, con su licenciamiento, el mecanismo de direccionamiento del tráfico, por balanceo global (GSLB) o redirección DNS, hacia la infraestructura dispuesta por la UBPD en el Sitio de Recuperación ante Desastres - DRP, conforme a la arquitectura y los procedimientos de continuidad de la Entidad.
- Incluir, sin costo adicional, el servicio de Content Delivery Network (CDN), de modo que se acceda a las aplicaciones desde el punto de presencia más cercano.
- Operar con cifrado de extremo a extremo en los canales de comunicación entre la infraestructura de la Entidad y la plataforma del proveedor de servicios en nube, y en el tráfico administrativo hacia la consola de gestión. El servidor de origen no será alcanzable desde internet por fuera de la plataforma del servicio contratado, mediante restricción por rangos de origen o mecanismo equivalente que el contratista configurará y acreditará en las pruebas de aceptación. Esta restricción no deberá afectar la operación del FortiWeb 1000E sobre el tráfico que le corresponde.
- El traslado de las políticas de protección y la configuración del direccionamiento.
- Garantizar una disponibilidad mensual del servicio igual o superior al 99,99 %, verificable con el reporte de disponibilidad de la plataforma del proveedor, conforme al Acuerdo de Nivel de Servicio del numeral de soporte técnico.
- Operar de manera simultánea y sincronizada con el WAF FortiWeb 1000E de la Entidad, en esquema activo-activo, de modo que cada componente reconozca el tráfico que el otro está filtrando y un mismo ataque no se registre por duplicado ni deje de registrarse. La sincronización

comprende las políticas de protección, las listas de bloqueo y la escala de severidad de los eventos.
- Quedar en capacidad de asumir las funciones de filtrado y de monitoreo del WAF FortiWeb 1000E cuando este deje de estar disponible, sin intervención manual sobre las políticas de protección y conservando el registro de los eventos. Esta condición se acredita en las pruebas de aceptación mediante un ejercicio de conmutación.

2. FortiWeb 1000E físico

El contratista deberá garantizar la continuidad del soporte y licenciamiento del equipo físico FortiWeb 1000E, instalado en el centro de datos principal, hasta el seis (6) de julio de 2028. Como mínimo, el servicio deberá incluir:

- Licenciamiento y suscripciones requeridas para el funcionamiento de las funcionalidades de seguridad contratadas y habilitadas en el equipo.
- Acceso a actualizaciones de firmas de seguridad, reputación, patrones de ataque, vulnerabilidades conocidas y demás contenidos de seguridad suministrados por el fabricante.
- Acceso a actualizaciones de firmware y parches de seguridad disponibles y recomendados por el fabricante, previa validación técnica, planeación de la ventana de mantenimiento y autorización de la Entidad.
- Soporte técnico especializado del fabricante o de un canal autorizado, para la atención de incidentes, fallas, errores de configuración, análisis de comportamiento, escalamiento de casos y recomendaciones de remediación.
- Garantizar, durante toda la vigencia del soporte contratado, el acceso a las actualizaciones de software y de firmware y el reemplazo de partes de hardware, conforme a las condiciones del fabricante.
- Reposición de partes o reemplazo de hardware por falla, conforme al nivel de servicio ofrecido por el fabricante y adquirido por la Entidad.
- Verificación periódica del estado de licenciamiento, conectividad con los servicios de actualización, capacidad disponible, salud de hardware, versiones de firmware, vigencia de certificados y funcionamiento de las políticas de seguridad.
- Elaboración de recomendaciones de actualización, ajuste, endurecimiento o mejora de la configuración, identificando el riesgo atendido, impacto potencial, plan de implementación y mecanismo de reversión.

3. Administración técnica especializada

El contratista deberá prestar la administración técnica especializada de ambas soluciones WAF en coordinación permanente con el personal designado por la Entidad. Esta actividad no sustituye la participación técnica institucional, sino que la complementa mediante conocimiento especializado de la plataforma, buenas prácticas de seguridad y acompañamiento en la operación.

ANEXO N°1 - ESPECIFICACIONES TÉCNICAS

La administración incluirá, como mínimo:

- Levantamiento inicial del inventario de aplicaciones, servicios, políticas, perfiles, reglas, certificados, integraciones, cuentas administrativas y configuraciones vigentes. La Entidad entregará al contratista el detalle de las direcciones, la ubicación y la asociación de cada aplicación con los componentes de seguridad, por mecanismos controlados y con obligaciones de confidencialidad una vez suscrito el contrato.
- Elaboración y entrega de una línea base de configuración para cada solución, incluyendo la identificación de diferencias entre el WAF Web y el FortiWeb 1000E.
- Diseño, ajuste, implementación, validación y documentación de políticas de protección para las aplicaciones institucionales.
- Mantenimiento de la concordancia, homogeneidad y paridad funcional de las políticas, reglas, perfiles, firmas personalizadas, listas de permitidos, listas de bloqueo y parámetros de seguridad que deban operar en ambas soluciones.
- Replicación controlada de las políticas entre el WAF Web y el equipo físico, cuando técnicamente proceda y previa validación de compatibilidad, evitando configuraciones divergentes entre el centro de datos principal y el alterno.
- Aplicación de actualizaciones de firmas y contenidos de seguridad, así como la evaluación de su impacto antes de su paso a producción.
- Análisis y ajuste de falsos positivos, falsos negativos, eventos recurrentes, excepciones y comportamientos propios de las aplicaciones protegidas.
- Gestión de cambios conforme a los procedimientos de la Entidad, incluyendo solicitud, análisis de impacto, respaldo de configuración, aprobación, implementación, validación posterior y plan de reversión.
- Administración de usuarios, perfiles, privilegios y mecanismos de acceso administrativo y manteniendo trazabilidad de las actividades realizadas.
- Entrega de respaldos de configuración antes y después de cambios relevantes, en el medio o repositorio autorizado por la Entidad.
- Transferencia de conocimiento al equipo técnico de la UBPD sobre la operación, consulta de eventos, administración de políticas y procedimientos de contingencia.
- Informar de manera inmediata a la Entidad sobre vulnerabilidades, fallas de seguridad, eventos críticos, expiración próxima de certificados, agotamiento de capacidad, indisponibilidades, inconsistencias de licenciamiento, riesgos de configuración o cualquier situación que pueda afectar la disponibilidad, integridad, confidencialidad o continuidad de las aplicaciones protegidas.
- Permitir y facilitar las actividades de seguimiento, verificación y supervisión que realice la Entidad, suministrando la información, evidencia documental, registros, informes y accesos de consulta que sean requeridos para verificar el cumplimiento contractual.
- No divulgar, copiar, transferir, almacenar en repositorios no autorizados, usar para fines distintos a la ejecución contractual ni permitir el acceso de terceros a la información o activos tecnológicos de la Entidad.
- No efectuar cambios en producción sin la autorización previa de la Entidad, salvo que se trate de una actuación urgente para contener un incidente crítico, caso en el cual deberá informar inmediatamente a la Entidad, documentar la intervención y presentar el respectivo informe.

- Documentar las diferencias que, por razones de arquitectura, funcionalidad, versión, licenciamiento o condiciones propias de las aplicaciones, impidan la réplica exacta de una política entre ambas soluciones, indicando el riesgo, la medida compensatoria y la recomendación técnica correspondiente.

4. Integración con el SOC

Las dos soluciones deberán alinearse con los procesos, procedimientos, casos de uso y capacidades de monitoreo del SOC de la Entidad, cuya suscripción se encuentra vigente hasta 2027. El SIEM del SOC está dimensionado para la correlación de eventos de al menos 300 dispositivos o 4.050 eventos por segundo (EPS) críticos. Si durante la vigencia del contrato el SOC o el SIEM de la Entidad cambia, el contratista reconfigurará el envío de registros, alertas y eventos hacia el nuevo destino, sin costo adicional para la UBPD.

El contratista deberá:

- Configurar y mantener el envío de registros, alertas y eventos del WAF Web y del FortiWeb 1000E hacia la herramienta, colector, SIEM o mecanismos de ingesta definidos por la Entidad. La solución deberá permitir controlar el volumen de registros que envía, mediante filtrado por severidad, agregación de eventos o envío selectivo desde el origen, y el contratista incluirá los colectores, agentes o reenviadores de registros que su solución requiera cuando esta no pueda enviarlos directamente por Syslog o API, sin costo adicional para la UBPD.
- Garantizar el envío de eventos de seguridad, tráfico, ataques detectados, bloqueos, cambios de configuración, inicio y cierre de sesión administrativa, fallas, indisponibilidad y eventos de actualización.
- Verificar que los registros enviados contengan información suficiente para identificar la aplicación afectada, fecha y hora, dirección IP de origen, URL o recurso solicitado, regla o firma activada, acción ejecutada, severidad y demás campos técnicamente disponibles.
- Mantener la sincronización horaria de ambas soluciones con la fuente NTP que defina la Entidad, a efectos de garantizar la correlación confiable de eventos.
- Realizar pruebas de generación, envío, recepción y visualización de alertas en el SOC, al inicio del servicio, ante cambios relevantes y con la periodicidad que defina la Entidad.
- Apoyar la definición o ajuste de casos de uso, reglas de correlación, umbrales de alerta y procedimientos.

La puesta en funcionamiento se recibirá a satisfacción cuando se verifiquen, de manera objetiva y documentada por parte de la supervisión:

- Renovación del FortiWeb 1000E registrada ante el fabricante y a nombre de la Entidad (certificación del fabricante).
- Servicio WAFaaS activo para las diez (10) aplicaciones críticas identificadas, sobre una capacidad dimensionada hasta veinte (20), con redirección de tráfico operando y certificados instalados.

- Pruebas funcionales de bloqueo: ante peticiones de ataque controladas (por ejemplo, inyección SQL y XSS de prueba), la solución detecta, bloquea y registra el evento en el tablero.
- Prueba de apoyo al Sitio de Recuperación ante Desastres - DRP: conmutación del direccionamiento hacia el sitio alterno según el procedimiento de la Entidad.
- Prueba de operación activo-activo: ante un mismo ataque controlado, los dos componentes reconocen el tráfico que filtra el otro y el evento queda registrado una sola vez, con la misma severidad.
- Prueba de asunción de funciones: suspendida la disponibilidad del WAF FortiWeb 1000E en condiciones controladas, el servicio en nube mantiene el filtrado y el registro sobre las aplicaciones protegidas, sin intervención manual sobre las políticas.
- Prueba de integración: los eventos de los dos componentes llegan al Centro de Operaciones de Seguridad - SOC y se correlacionan en un solo punto.
- Prueba de restricción del origen: el servidor institucional no responde a peticiones que no provengan de la plataforma del servicio contratado.
- Matriz de escalamiento y protocolo de respuesta a incidentes entregados al supervisor.

INSTALACIÓN

- El servicio WAF SaaS se presta como servicio administrado en la infraestructura de nube del contratista, bajo arquitectura de proxy inverso, con redirección del tráfico por DNS, sin instalación de equipos físicos ni de software en las sedes de la UBPD. La implementación comprende la configuración inicial, la integración con el FortiWeb 1000E existente y con las demás soluciones de ciberseguridad de la Entidad, y la puesta en funcionamiento inicial de las diez (10) aplicaciones críticas identificadas por la Entidad y, a medida que la Entidad las valide y solicite, de las restantes hasta completar las veinte (20) aplicaciones, sin costo adicional.
- La implementación se debe ejecutar sin interrupción de los servicios en producción. Cualquier ventana de indisponibilidad requiere aprobación previa y escrita del supervisor.
- El traslado de las políticas de protección y la configuración del direccionamiento (redirección DNS y certificados) hacen parte de la implementación.
- La renovación del FortiWeb 1000E no requiere instalación física adicional; consiste en el registro del licenciamiento y del soporte ante el fabricante, a nombre de la UBPD.

FUNCIONAMIENTO

El gobierno, la dirección y la autorización sobre las soluciones permanecen en cabeza de la UBPD, y el contratista deberá ejecutar la administración técnica especializada, en los términos del preámbulo de las obligaciones específicas.

El funcionamiento comprende el monitoreo y la notificación en esquema 7×24×365 ante ataques o degradación del servicio, el cifrado de extremo a extremo en los canales de comunicación con el proveedor de nube y la entrega de la matriz de escalamiento y del protocolo de respuesta a incidentes a la suscripción del acta de inicio.

La transferencia de conocimiento se ejecutará mediante una capacitación de mínimo seis (6) horas dirigidas a dos (2) funcionarios designados por la Entidad, en idioma español, de manera presencial o virtual según lo acuerde la UBPD, con material de apoyo entregable en formato reutilizable y acta de asistencia suscrita.

El temario comprenderá como mínimo: (i) arquitectura de las dos soluciones y recorrido del tráfico protegido, en el equipo y en el servicio en nube; (ii) navegación y uso de la consola de administración, con la gestión de usuarios, roles y niveles de acceso; (iii) creación, edición y publicación de políticas de protección, y manejo de excepciones y de falsos positivos; (iv) gestión de los certificados digitales y del direccionamiento del tráfico, incluida la conmutación hacia el DRP; (v) lectura del tablero de control, interpretación de las alertas y clasificación de los eventos por severidad; (vi) generación de informes y consulta del inventario de licencias y suscripciones con sus fechas de vencimiento; y (vii) procedimiento de escalamiento ante el contratista y ante el fabricante, con la matriz de contactos y los tiempos de respuesta pactados.

SOPORTE TÉCNICO

La solución contará con soporte técnico del fabricante en esquema 7×24×365 durante toda la vigencia del soporte contratado, con actualizaciones, acceso al portal de soporte y recursos técnicos. Los Acuerdos de Nivel de Servicio que siguen son de obligatorio cumplimiento para el contratista y rigen mientras estén vigentes las coberturas contratadas, esto es, hasta el 6 de julio de 2028, con independencia de que el plazo de ejecución del contrato haya culminado. El supervisor los verificará con los medios de acreditación señalados en cada caso.

Para efectos de los tiempos de atención, se entiende por severidad 1 que el servicio de inspección esté indisponible, que una aplicación crítica no sea alcanzable, o que exista un ataque en curso sin contener; y por severidad 2, la degradación del servicio o del rendimiento sin pérdida de disponibilidad, o la falla de una función de protección sobre una aplicación no crítica.

La Disponibilidad mensual del servicio debe ser igual o superior al 99,99 %. Se acredita con el reporte mensual de disponibilidad del proveedor y con el acceso de consulta del supervisor al tablero de la plataforma, de modo que la cifra sea verificable de manera independiente.

Como mínimo, deberá cumplir con los siguientes niveles de servicio:

- Respuesta a incidente crítico (severidad 1): menor o igual a quince (15) minutos, contados desde el registro en la mesa de soporte del contratista. Se acredita con el registro de la mesa de soporte.
- Respuesta a incidente mayor (severidad 2): menor o igual a dos (2) horas, contadas desde el registro en la mesa de soporte del contratista. Se acredita con el registro de la mesa de soporte.
- Notificación de ataque detectado: menor o igual a treinta (30) minutos, contados desde la detección por la plataforma. La notificación al supervisor incluirá el análisis del evento, la validación de las acciones ejecutadas por la solución y la recomendación de las medidas de contención o de ajuste de políticas que correspondan. Se acredita con la bitácora de alertas verificable por el supervisor

- Diagnóstico de eventos de degradación o de indisponibilidad del servicio, y de los errores del servidor de origen que le impidan procesar o finalizar solicitudes mediante el protocolo HTTP/S: soporte para el análisis y el diagnóstico dentro de las dos (2) horas siguientes al reporte. Se acredita con el registro de la mesa de soporte y con el informe del caso.
- Solución o contención del incidente de severidad 1: menor o igual a cuatro (4) horas contadas desde el registro en la mesa de soporte. Cuando la causa sea imputable al fabricante, el término se suspende con la constancia del caso escalado, conforme a la obligación 19. Se acredita con el registro de la mesa de soporte y con el informe del caso.

Los tiempos deberán medirse desde la creación del caso por parte de la Entidad. Para los incidentes críticos y altos, el contratista deberá proporcionar seguimiento continuo hasta la estabilización del servicio, informar las acciones ejecutadas y entregar un informe de causa, impacto, acciones correctivas y recomendaciones de prevención.

El contratista deberá entregar, como mínimo:

- Documento de inicio que incluya plan de trabajo, cronograma, canales de soporte, matriz de escalamiento y responsables.
- Inventario técnico y línea base de ambas soluciones.
- Matriz de paridad de políticas y configuraciones entre el WAF Web y el FortiWeb 1000E.
- Documento de arquitectura e integración con el SOC.
- Bitácora mensual de actividades de administración, incidentes atendidos, cambios implementados, actualizaciones aplicadas y recomendaciones.
- Informe mensual de eventos relevantes, aplicaciones protegidas, alertas generadas, ataques bloqueados o detectados, falsos positivos, riesgos identificados y acciones pendientes.
- Respaldos de configuración y documentación actualizada de las políticas administradas.
- Informe final de transferencia de conocimiento y cierre, con el estado de las suscripciones, licencias, soporte, configuraciones e incidentes atendidos.

La Entidad aceptará los servicios previa verificación de la vigencia de las suscripciones y soportes, la operación de las soluciones, la integración efectiva con el SOC, la disponibilidad de los registros, la documentación entregada y el cumplimiento de los niveles de servicio definidos.