PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DEL SUMINISTRO EN MODALIDAD DE SUSCRIPCIÓN CON SERVICIOS GESTIONADOS DE UNA HERRAMIENTA BAS DENTRO DEL ENTORNO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA TI.

- PROCEDIMIENTO ABIERTO -

EXPEDIENTE NÚM. 2606OB01

1. INTRODUCCIÓN

El presente Pliego de Prescripciones Técnicas (PPT) tiene por objeto definir y establecer las condiciones, las funcionalidades y los requisitos técnicos que deben regir la contratación de un suministro, en modalidad de suscripción, de una plataforma de simulación de ataques y brechas (Breach and Attack Simulation - BAS), junto con los servicios gestionados necesarios para su correcta implantación, operación y explotación. Esta contratación busca proporcionar a la CCMA, S. A. una capacidad avanzada de validación continua de su postura de ciberseguridad.

En el contexto actual, donde las ciberamenazas son cada vez más complejas, persistentes y numerosas, las estrategias de defensa basadas únicamente en la prevención y reacción postincidente resultan insuficientes. Es imprescindible evolucionar hacia un modelo de seguridad proactivo, inteligente y predictivo, que permita identificar y corregir las debilidades antes de que puedan ser explotadas por actores maliciosos. La validación manual y periódica de los controles de seguridad, como las pruebas de penetración tradicionales, no ofrece la frecuencia ni cobertura necesarias para hacer frente a un panorama de amenazas en constante cambio.

La implementación de una solución BAS como servicio gestionado permite abordar este reto mediante la automatización de pruebas de seguridad. Estas pruebas simulan, de forma segura y controlada, las Técnicas, Tácticas y Procedimientos (TTP) utilizados en ataques reales. El objetivo es evaluar de forma continua y objetiva la eficacia de los controles de seguridad desplegados en la infraestructura tecnológica, incluyendo los sistemas de protección perimetral, estaciones de trabajo (endpoints) y mecanismos de control de la red interna.

A través de este servicio, se busca obtener una visibilidad clara y accionable sobre las posibles brechas de seguridad, configuraciones incorrectas y vulnerabilidades en la cadena de defensa, permitiendo priorizar los esfuerzos de remediación basándose en evidencias tangibles y mejorando de forma demostrable la resiliencia de la organización frente a ciberataques.

2. ANTECEDENTES Y JUSTIFICACIÓN

El entorno digital actual se caracteriza por una constante evolución y una creciente sofisticación de las ciberamenazas. Los actores maliciosos desarrollan continuamente nuevas técnicas, tácticas y procedimientos (TTP) para eludir las defensas y

comprometer la seguridad de las organizaciones. En este contexto, la estrategia de ciberseguridad de esta organización se ha basado en el despliegue de un ecosistema de controles de seguridad perimetrales e internos, incluyendo cortafuegos de nueva generación, sistemas de detección y respuesta en el endpoint (EDR), soluciones de seguridad para el correo electrónico y herramientas de gestión de eventos e información.

A pesar de la significativa inversión realizada en estas tecnologías de defensa, la validación de su eficacia operativa ha dependido, en gran medida, de metodologías tradicionales como las auditorías de seguridad periódicas y las pruebas de penetración (pentesting). Aunque estas evaluaciones son valiosas, presentan limitaciones inherentes: son análisis puntuales en el tiempo que no ofrecen una continua visibilidad sobre el estado de la seguridad. La ventana temporal entre evaluaciones puede ser aprovechada por atacantes para explotar nuevas vulnerabilidades o errores de configuración introducidos en la operativa diaria. Este enfoque reactivo no permite garantizar que los controles de seguridad estén correctamente configurados y funcionen de forma óptima en todo momento.

Por este motivo, resulta imprescindible evolucionar hacia un **modelo proactivo y continuo de validación de la seguridad**. Es necesario adoptar una estrategia que no sólo asuma que las defensas funcionan, sino que verifique su efectividad de forma automatizada y sistemática frente al escenario de amenazas real.

La contratación de una plataforma de Simulación de Ataques y Brechas (BAS) en modalidad de servicio gestionado se justifica como la solución idónea para cubrir esta necesidad. Una herramienta BAS permite **simular de forma segura y controlada un amplio abanico de ataques reales** a través de toda la cadena de ataque (Kill-Chain), desde el perímetro hasta el endpoint y los movimientos laterales dentro de la red. Esta capacidad ofrece una evaluación continua y basada en la evidencia de la eficacia de los controles de seguridad desplegados, identificando brechas, errores de configuración y rutas de ataque potenciales antes de que puedan ser explotadas. La implementación de esta solución permitirá optimizar el retorno de la inversión en ciberseguridad, priorizar las acciones de remediación en base al riesgo real y, en definitiva, fortalecer la resiliencia de la organización frente a ciberataques cada vez más avanzados.

3. OBJETO Y ALCANCE DEL SUMINISTRO

El objeto de este contrato es la definición de las condiciones y los requisitos para la contratación del suministro, en régimen de suscripción, de una plataforma de simulación de ataques y brechas (BAS – Breach and Attack Simulation), junto con los servicios gestionados necesarios para su implantación, configuración, operación y mantenimiento.

La finalidad de esta contratación es dotar a la CCMA, S. A. de una capacidad de validación continua y automatizada de su postura de ciberseguridad. El servicio permitirá evaluar de forma proactiva y segura la efectividad de los controles de

seguridad existentes frente a un amplio espectro de amenazas, identificar debilidades en la configuración de las defensas y obtener recomendaciones accionables para su remediación. El alcance del servicio cubrirá las infraestructuras tecnológicas de la organización, incluyendo sistemas de usuario final, servidores y otros elementos de la red corporativa.

3.1. DESCRIPCIÓN GENERAL DEL SERVICIO

El servicio objeto del contrato proporcionará una solución integral que combine una plataforma tecnológica avanzada con la experiencia necesaria para su gestión. Esta solución debe permitir la realización de simulaciones de ciberataques de forma controlada y no disruptiva, abarcando diferentes vectores y fases de un ataque real.

Como mínimo, la plataforma tecnológica debe incluir los siguientes módulos o funcionalidades esenciales:

- **Módulo de endpoint:** Debe permitir la ejecución de simulaciones directamente sobre los equipos de usuario final y servidores. El objetivo es validar la eficacia de las soluciones de seguridad del endpoint (como EDR, XDR, antivirus y políticas de sistema) en la detección y el bloqueo de malware, ransomware, exploits y otras técnicas de ataque dirigidas a estos activos.
- **Módulo de movimiento lateral:** La solución debe ser capaz de simular las técnicas que un atacante utilizaría para expandirse a través de la red interna una vez comprometido un activo inicial. Este módulo debe probar la resiliencia de los controles de red internos, como la microsegmentación, los cortafuegos internos y las políticas de control de acceso, para contener a un atacante dentro de un segmento de red limitado.
- **Módulo de simulación de amenazas inmediatas:** La plataforma debe disponer de una funcionalidad específica para simular las amenazas más recientes y activas a nivel mundial. Este módulo debe ser actualizado de forma continua, preferiblemente diaria, para incorporar indicadores de compromiso (IoC) y tácticas, técnicas y procedimientos (TTP) de campañas de ataque emergentes, lo que permitirá evaluar la preparación de la organización frente a amenazas de día cero o de gran impacto mediático.
- **Módulo automatización y remediación:** La plataforma debe disponer de la funcionalidad de poder ejecutar acciones de remediación de forma automática, controlada y verificable sobre los sistemas de la organización. Este módulo es esencial para garantizar un ciclo completo de detección, validación, corrección y revalidación.

3.2. MODALIDAD DEL SUMINISTRO

El suministro deberá prestarse bajo una **modalidad de servicio gestionado**, basado en una plataforma en la nube (**Software as a Service - SaaS**).

La modalidad de **servicio gestionado** implica que la empresa adjudicataria será la responsable de la totalidad del ciclo de vida del servicio. Esto incluye el despliegue inicial de la plataforma y sus agentes, la configuración personalizada según las

características del entorno de la organización, la planificación y ejecución de las campañas de simulación, el análisis de los resultados obtenidos, la generación de informes técnicos y ejecutivos, y el soporte continuo. La organización actuará como consumidora de los resultados y recomendaciones del servicio, sin necesidad de dedicar recursos internos a la operación de la herramienta.

La modalidad **SaaS (Software as a Service)** exige que la plataforma esté alojada y mantenida por el proveedor de la tecnología. Esto garantiza que la organización siempre disponga de la última versión de la plataforma, incluyendo las actualizaciones de funcionalidades y de la librería de ataques, sin requerir inversiones en infraestructura propia ni esfuerzos de mantenimiento. El acceso a la consola de gestión y a los cuadros de mando deberá realizarse de forma segura a través de un navegador web.

4. REQUISITOS TÉCNICOS DE LA PLATAFORMA BAS

Esta sección establece los requisitos técnicos y funcionales mínimos que debe cumplir la plataforma de Simulación de Ataques y Brechas (BAS) y los servicios asociados. El objetivo es garantizar que la solución seleccionada sea capaz de validar de forma continua, automatizada y segura la eficacia de los controles de seguridad de la organización, proporcionando una visibilidad completa sobre la postura de ciberseguridad y la resiliencia frente a amenazas reales. Los licitadores tendrán que garantizar el cumplimiento de todos los requisitos que se detallan a continuación, describiendo en su oferta técnica cómo su solución satisface cada uno de ellos.

4.1. REQUISITOS GENERALES

La plataforma BAS debe ser una solución moderna, eficiente y diseñada para operar con un impacto mínimo en la infraestructura tecnológica existente, ofreciendo la máxima flexibilidad y escalabilidad.

La arquitectura de la solución debe ser obligatoriamente en modalidad **Software as a Service (SaaS)**, completamente gestionada por el proveedor en una infraestructura en la nube. Este modelo libera a la CCMA, S. A. de las tareas de gestión, mantenimiento, actualización y escalado del hardware y software subyacentes. La consola de gestión debe ser accesible a través de un navegador web seguro, sin necesidad de instalar software cliente en los equipos de los administradores.

La plataforma debe garantizar un sistema de **actualizaciones automáticas y transparentes**. El proveedor será el único responsable de aplicar las actualizaciones de seguridad de la plataforma, las nuevas funcionalidades y, de forma crítica, las actualizaciones de la librería de simulaciones de ataque. Estas actualizaciones deben realizarse sin interrupciones del servicio y sin requerir intervención por parte del personal de la organización.

Para la ejecución de simulaciones en los sistemas internos, la solución debe disponer de un **agente único, universal y ligero**. Este agente debe ser el vehículo para ejecutar las diferentes simulaciones requeridas (endpoint, movimiento lateral) y debe ser

diseñado para tener un consumo de recursos (CPU, memoria, I/O de disco y red) insignificable, de forma que no afecte al rendimiento de los sistemas productivos donde se instale. El agente debe ser compatible con las versiones más extendidas de los sistemas operativos de escritorio y servidor utilizados en la CCMA, S. A., como Windows, Windows Server, y las principales distribuciones de Linux. El despliegue, la configuración y la gestión del ciclo de vida de estos agentes deberán poder realizarse de forma centralizada desde la consola de gestión de la plataforma.

4.2. REQUISITOS FUNCIONALES

La plataforma debe proporcionar un conjunto completo de funcionalidades que permitan una evaluación exhaustiva y realista de la postura de seguridad de la organización.

La solución debe ofrecer una **amplia cobertura de vectores de ataque y controles de seguridad**. Debe ser capaz de simular amenazas a través de múltiples dominios para validar la eficacia de las distintas capas de defensa. Como mínimo, deberá cubrir los siguientes vectores:

- **Seguridad del endpoint**: Ejecución de muestras de malware (troyanos, ransomware, keyloggers) de forma segura, técnicas de evasión de defensas, escalada de privilegios y explotación de vulnerabilidades conocidas.
- **Movimiento lateral**: Simulación de técnicas utilizadas por los atacantes para moverse dentro de la red corporativa una vez comprometido un equipo inicial, como Pass-the-Hash, Pass-the-Ticket, uso de herramientas como PsExec, explotación de protocolos de red y robo de credenciales.
- **Seguridad del correo electrónico**: Envío de correos de phishing, mensajes con adjuntos maliciosos (ejecutables, documentos con macros) y enlaces a sitios web fraudulentos para evaluar la respuesta de los filtros antispam, antimalware y la sensibilización de los usuarios.
- **Seguridad de la navegación web**: Simulación de descargas "drive-by-download", ataques a través de aplicaciones web (WAF) y validación de la capacidad de bloqueo de tráfico hacia dominios maliciosos conocidos (C2).
- **Exfiltración de datos**: Intentos controlados de extraer información sensible a través de varios canales (HTTP/S, DNS, ICMP) para poner a prueba las soluciones de prevención de pérdida de datos (DLP).

Es un requisito indispensable que la plataforma soporte la **validación end-to-end (Full Kill-Chain)**. No es suficiente con ejecutar pruebas aisladas; la solución debe ser capaz de lanzar campañas que simulen la cadena de ataque completa, desde el vector de entrada inicial hasta la exfiltración de datos, pasando por el movimiento lateral y la escalada de privilegios. Esto permite evaluar la resiliencia global de la organización e identificar dónde se rompe la cadena de ataque (o dónde no se rompe).

Todas las simulaciones, técnicas y tácticas deben estar rigurosamente alineadas con el marco de referencia **MITRE ATT&CK**. La plataforma debe mapear cada simulación con las tácticas, técnicas y procedimientos (TTP) correspondientes del framework. Los

informes y cuadros de mando deben permitir visualizar la cobertura y eficacia de los controles de seguridad directamente sobre la matriz ATT&CK, facilitando la identificación de lagunas y la priorización de mejoras.

La plataforma debe permitir tanto **simulaciones programadas como bajo demanda**. Debe ser posible configurar ejecuciones continuas y automatizadas (diarias, semanales, mensuales) para una validación constante, así como lanzar evaluaciones específicas de forma inmediata para verificar la eficacia de una nueva herramienta de seguridad, validar la correcta aplicación de un parche o comprobar la defensa contra una amenaza emergente.

La solución debe contar con una **librería de ataques extensa y actualizada a diario**. Esta librería debe incluir miles de simulaciones basadas en amenazas reales, incluyendo las más recientes y prevalentes. Es obligatorio que la plataforma disponga de un módulo específico de **"Amenazas Inmediatas" (Immediate Threats)** o funcionalidad equivalente, que permita lanzar simulaciones basadas en las campañas de ataque activas y las vulnerabilidades de día cero más recientes, pocas horas o días después de su descubrimiento público. Todas las simulaciones deben ser llevadas a cabo de **forma segura y sin disrupción** para la organización, garantizando que no existe ningún riesgo para los servicios, la integridad de los datos o la disponibilidad de la infraestructura.

4.3. REQUISITOS DE INTEGRACIÓN

La plataforma BAS debe poder integrarse de forma nativa y fluida con el ecosistema de ciberseguridad existente en la organización, para maximizar su valor y automatizar los ciclos de validación. La solución debe proporcionar una API RESTful completa y bien documentada, además de conectores preconfigurados para las principales herramientas del mercado. Se requiere, al menos, la capacidad de integración con:

- **SIEM (Gestión de información y eventos de seguridad)**: La plataforma debe enviar los registros y las alertas generadas durante las simulaciones (tanto las bloqueadas como las exitosas) al SIEM de la organización. Esto es fundamental para validar que las reglas de detección y correlación del SIEM funcionan correctamente y que los analistas de seguridad reciben las alertas pertinentes.
- **SOAR (Orquestación, Automatización y Respuesta de Seguridad)**: La plataforma BAS **debe permitir una integración bidireccional y completa con una plataforma SOAR** mediante API, con el objetivo de automatizar el ciclo de mejora continua de la seguridad. A tal efecto:
    - El **SOAR debe poder iniciar de forma automática simulaciones o campañas de la plataforma BAS**.
    - La **plataforma BAS debe devolver los resultados de las simulaciones de forma estructurada y consumible vía API por el SOAR**, incluyendo evidencias de detección, bloqueo o fallo de los controles de seguridad.

- En caso de que el resultado de una simulación evidencie una brecha, carencias o ineficiencias en un control de seguridad, el **SOAR podrá orquestar automáticamente una o varias acciones de remediación sobre los sistemas afectados**, sin intervención manual.

A título **meramente ejemplificativo y no limitativo**, estas acciones de remediación pueden incluir la aplicación o modificación de políticas en dispositivos de seguridad (como cortafuegos, EDR/XDR, pasarelas de correo, WAF o sistemas similares).

Una vez ejecutada la remediación, el **SOAR debe ser capaz de relanzar automáticamente la misma simulación BAS** para:

- Verificar la efectividad real de la medida correctora aplicada.
- Disponer de evidencia objetiva de la mejora lograda.

Este mecanismo debe permitir **cerrar de forma automática, repetible y auditable el ciclo completo**: **"hallazgo→ acción de remediación → re-test → validación"**.

- **EDR/XDR (Endpoint/Extended Detection and Response)**: La integración es necesaria para validar la eficacia de las soluciones de endpoint a la hora de detectar y bloquear técnicas de ataque específicas. La plataforma BAS debe poder correlacionar sus acciones con las alertas generadas por el EDR/XDR.

4.4. REQUISITOS DE SEGURIDAD Y CUMPLIMIENTO DE LA PLATAFORMA

La propia plataforma BAS, al ser un elemento crítico que interactúa con los sistemas de la organización, debe cumplir con los más altos estándares de seguridad y cumplimiento normativo.

Además, el proveedor del servicio SaaS deberá demostrar el cumplimiento de normativas y estándares de seguridad internacionalmente reconocidos. Tendrá que poseer la certificación del **ENS** mínimo categoría Media, otras certificaciones **ISO/IEC 27001**, que garantiza la existencia de un Sistema de Gestión de la Seguridad de la Información (SGSI) maduro para la prestación del servicio.

La plataforma deberá implementar controles de acceso robustos, incluyendo la obligatoriedad de uso de **autenticación de múltiple factor (MFA)** para todos los usuarios que accedan a la consola de gestión. Asimismo, debe disponer de un sistema de **control de acceso basado en roles (RBAC)** granular, que permita definir permisos específicos para distintos perfiles de usuario (administradores, operadores, consultores). Todas las acciones realizadas en la plataforma deben quedar registradas en un sistema de auditoría (audit log) completo e inalterable.

5. DESCRIPCIÓN DE LOS SERVICIOS GESTIONADOS

El objeto de este contrato no se limita al simple suministro de una licencia de software, sino que incluye un conjunto integral de servicios gestionados que garanticen la correcta implantación, operación, mantenimiento y aprovechamiento de la plataforma de

Simulación de Ataques y Brechas (BAS). El adjudicatario será el responsable de asumir la gestión completa del ciclo de vida del servicio, desde el despliegue inicial hasta la operación diaria y el soporte, permitiendo a la organización focalizarse en el análisis de los resultados y la implementación de mejoras en su postura de seguridad.

Estos servicios deben ser prestados por personal técnico cualificado y con experiencia demostrable en la gestión de herramientas BAS y en el ámbito de la ciberseguridad ofensiva y defensiva. El adjudicatario deberá garantizar que el servicio se ejecuta de forma eficiente, proactiva y alineada con las necesidades y objetivos de seguridad de la organización.

5.1. IMPLANTACIÓN Y CONFIGURACIÓN INICIAL

Esta fase comprende todas las actividades necesarias para la puesta en marcha completa y operativa de la solución BAS en la infraestructura de la organización. El adjudicatario será responsable de la ejecución de las siguientes tareas:

En primer lugar, deberá elaborarse y presentar un **Plan de Despliegue detallado**. Este documento deberá incluir, al menos, un cronograma de actividades, la definición de los recursos técnicos y humanos implicados, la matriz de responsabilidades (RACI), los procedimientos de comunicación y un plan de gestión de riesgos durante la implantación. Este plan deberá ser consensuado y aprobado por la organización antes del inicio de cualquier labor técnica.

Una vez aprobado el plan, el adjudicatario procederá con el **despliegue de la plataforma en la nube (SaaS)**, incluyendo el aprovisionamiento del entorno dedicado (tenant) para la organización y la configuración inicial de los parámetros de seguridad y red necesarios.

Posteriormente, se llevará a cabo la **instalación y configuración de los agentes** necesarios para la ejecución de las simulaciones en los "puntos de test" designados. Estos puntos serán definidos conjuntamente con el equipo técnico de la organización y cubrirán una muestra representativa de los sistemas (servidores, estaciones de trabajo) para validar la seguridad de los controles de endpoint y movimientos laterales. El adjudicatario deberá coordinarse con los administradores de sistemas para garantizar un despliegue fluido y sin impacto en la operativa.

La configuración de la plataforma deberá incluir:

- **Activación y ajuste de los módulos contractuales**: Deberán configurarse de forma específica los módulos de seguridad de endpoint, movimiento lateral y amenazas inmediatas, adaptando sus particularidades al entorno tecnológico de la organización.
- **Definición de perfiles de usuario y control de acceso (RBAC)**: Se crearán los perfiles de usuario necesarios (administradores, analistas de seguridad, consultores) con los permisos adecuados para garantizar un acceso seguro y segmentado a la plataforma, siguiendo el principio de mínimo privilegio.

- **Configuración de las políticas de simulación**: Se establecerán las políticas iniciales para las simulaciones programadas, definiendo su periodicidad, alcance y objetivos, en línea con lo descrito en el apartado de gestión continua.
- **Integración con sistemas de terceros**: Si es necesario y se considera necesario, se configurará la integración de la plataforma BAS con otras herramientas de seguridad de la organización, como el SIEM o el SOAR, para la correlación de eventos y la automatización de respuestas.

Por último, esta fase concluirá con la realización de unas **Pruebas de Aceptación del Servicio (SAT)** para validar el correcto funcionamiento de la plataforma y la entrega de un **Dossier de Configuración Final** que documente todos los parámetros aplicados.

5.2. GESTIÓN Y OPERACIÓN CONTINUA

El adjudicatario será responsable de la operación diaria de la plataforma BAS, asegurando su ejecución continua y el análisis proactivo de los resultados. Este servicio es el núcleo de la propuesta de valor gestionada y debe incluir las siguientes tareas:

La **ejecución programada y bajo demanda de simulaciones de ataque** constituye la actividad principal. El adjudicatario deberá gestionar un calendario de simulaciones que garantice una constante validación de los controles de seguridad. Como mínimo, deberá cumplirse la siguiente periodicidad:

- **Módulo de amenazas inmediatas**: Ejecución continua o diaria para validar la defensa contra las amenazas más recientes y activas a nivel global (Zero-Days, nuevas campañas de malware).
- **Módulo de movimiento lateral**: Ejecución programada con una periodicidad mínima mensual para evaluar la capacidad de detectar y bloquear desplazamientos no autorizados en la red interna.
- **Módulo de endpoint**: Ejecución programada con una periodicidad mínima mensual para verificar la eficacia de las soluciones EDR/EPP contra distintos tipos de malware, ransomware y técnicas de evasión.
- **Módulo automatización y remediación:** Asegurar que se están aplicando las remediaciones que los módulos anteriores indiquen para proteger la información de la CCMA, S. A.

Además, el adjudicatario deberá realizar el **monitoraje proactivo de la salud de la plataforma**, verificando el estado de los agentes, la correcta ejecución de las tareas programadas y el rendimiento general de la herramienta. Cualquier anomalía en la plataforma deberá ser gestionada como incidencia técnica.

Una parte fundamental del servicio es el **análisis y la interpretación de los resultados** de las simulaciones. No es suficiente con ejecutar los ataques; el adjudicatario deberá analizar los hallazgos, correlacionarlos con el framework **MITRE ATT&CK**, identificar los controles de seguridad que han fallado y priorizar las vulnerabilidades detectadas en función de su riesgo potencial. Este análisis deberá materializarse en recomendaciones claras y accionables para su remediación.

Por último, el adjudicatario será responsable de la **gestión de la inteligencia de amenazas (Threat Intelligence)**, asegurando que la librería de ataques de la plataforma esté permanentemente actualizada con las últimas técnicas, tácticas y procedimientos (TTP) e indicadores de compromiso (IOC) utilizados por los actores maliciosos.

5.3. APOYO TÉCNICO Y MANTENIMIENTO

El adjudicatario deberá proporcionar un servicio de soporte técnico robusto y eficaz para atender cualquier incidencia relacionada con la plataforma BAS o para resolver consultas operativas. Este servicio deberá estructurarse en torno a un punto único de contacto (Service Desk).

El servicio deberá garantizar la **gestión de incidencias con disponibilidad 7x24** para su recepción y registro, con un compromiso de **respuesta y tratamiento en horario laboral de 8x5** (de 9:00 a 17:00, de lunes a viernes no festivos). Las incidencias podrán ser de naturaleza técnica (p. ej., un agente no responde, una simulación falla) o de seguridad (por ejemplo, detectar una vulnerabilidad que podría ser atacada, avisar para aplicar la remediación o estar atentos al posible agujero de seguridad). La priorización y los tiempos de respuesta deben ajustarse al Acuerdo de Nivel de Servicio (ANS) definido en la sección 6 de este pliego.

Además de la gestión reactiva de incidencias, el servicio de soporte deberá atender **peticiones de servicio** como la creación de nuevos usuarios, la modificación de políticas de simulación o la ejecución de evaluaciones bajo demanda ante la aparición de una vulnerabilidad notoria.

El adjudicatario será también responsable del **mantenimiento evolutivo y correctivo de la plataforma**. Dado que se trata de una solución SaaS, se espera que el proveedor de la tecnología gestione las actualizaciones de versión y los parches de seguridad. Sin embargo, el adjudicatario del servicio gestionado deberá supervisar este proceso, planificar las ventanas de mantenimiento, comunicarlas a la organización con la suficiente antelación y validar que las nuevas versiones no introducen regresiones ni afectan negativamente a la operativa.

El servicio deberá incluir el acceso a **personal experto en ciberseguridad** para sesiones de consulta, donde se puedan discutir en profundidad los resultados de los informes, evaluar las recomendaciones de remediación y asesorar a la organización sobre las mejores estrategias para fortalecer su postura de seguridad a partir de las evidencias recogidas por la plataforma BAS.

6. ACUERDO DE NIVEL DE SERVICIO (ANS)

Este Acuerdo de Nivel de Servicio (ANS) establece los parámetros objetivos de calidad y compromisos de rendimiento que el adjudicatario deberá garantizar durante la prestación del servicio de suministro de la plataforma BAS y los servicios gestionados asociados. El objetivo de este ANS es definir un marco medible para la evaluación

continua del servicio, asegurando que la calidad y rapidez en la gestión y respuesta a incidencias se alinean con las necesidades operativas y de seguridad de la organización. El cumplimiento de estos acuerdos será fundamental para la correcta ejecución del contrato y será objeto de seguimiento a través de informes periódicos.

6.1. DEFINICIÓN DE SEVERIDADES DE INCIDENCIAS

Todas las incidencias y alertas de seguridad gestionadas en el marco de este servicio se clasificarán según su nivel de severidad, determinado por el impacto potencial o real sobre los sistemas, datos y operativa de la organización. Esta clasificación permitirá priorizar los recursos y las acciones de respuesta de forma eficiente. Se establecen las siguientes categorías de severidad:

- **Crítica**: Se refiere a una incidencia que tiene un impacto severo en la seguridad o en la disponibilidad de los servicios críticos de la organización. Se considera crítica una alerta que indique una intrusión confirmada, un ataque en curso con éxito, una exfiltración de datos sensibles o cualquier evento que comprometa de forma grave la confidencialidad, la integridad o la disponibilidad de activos estratégicos. Requiere una acción de respuesta inmediata para contener su amenaza y minimizar los daños.
- **Alta**: Corresponde a una incidencia con impacto significativo, pero no catastrófico, sobre los servicios o la seguridad. Incluye situaciones como la detección de actividad maliciosa que ha sido parcialmente contenida por los controles existentes, vulnerabilidades explotables en sistemas relevantes que podrían derivarse en un incidente crítico, o la notable degradación del rendimiento de un servicio importante. Aunque el servicio puede continuar operativo, el riesgo de propagación o escalada es elevado y exige una actuación urgente.
- **Media**: Se asigna a incidencias con un impacto limitado o moderado que no afectan de forma directa a la continuidad de los servicios críticos. Puede incluir alertas sobre intentos de ataque bloqueados con éxito, anomalías de configuración que reducen el nivel de seguridad, o el incorrecto funcionamiento de funcionalidades no esenciales de la plataforma BAS. Estas incidencias requieren un análisis y una corrección planificada para evitar problemas futuros.
- **Baja**: Esta categoría se aplica a eventos de bajo impacto, consultas informativas o problemas menores que no representan un riesgo inminente para la seguridad ni afectan a la funcionalidad del servicio. Incluye a este nivel, por ejemplo, solicitudes de cambios de configuración menores que no serían una amenaza inmediata, peticiones de informes personalizados o alertas informativas que no requieren acciones correctoras inmediatas.

6.2. TIEMPO DE RESPUESTA Y NOTIFICACIÓN

Para cada nivel de severidad se definen unos tiempos máximos de respuesta y notificación que el adjudicatario está obligado a cumplir. Estos tiempos se contabilizarán dentro del horario de servicio definido (atención 7x24 con respuesta en horario laboral 8x5 de lunes a viernes, excepto festivos nacionales).

Se definen los siguientes conceptos:

- **Tiempo de Respuesta**: Tiempo transcurrido desde que se genera una alerta o se registra una incidencia en el sistema del adjudicatario hasta que un técnico cualificado inicia formalmente su análisis y diagnóstico.
- **Tiempo de Notificación Detallada**: Tiempo transcurrido desde que se genera la alerta hasta que el adjudicatario envía a la organización una notificación formal y detallada sobre la incidencia, que debe incluir un análisis inicial, el impacto evaluado y, en su caso, las primeras acciones de contención recomendadas o ejecutadas.

Los tiempos máximos comprometidos son los siguientes:

Severidad	Tiempo de Respuesta Máximo	Tiempo de Notificación Detallada Máximo
Crítica	15 minutos	1 hora
Alta	30 minutos	2 horas
Media	1 hora	6 horas
Baja	2 horas	12 horas

6.3. INDICADORES CLAVE DE RENDIMIENTO (KPIS)

Con el fin de evaluar de forma objetiva la calidad del servicio prestado, se establecen los siguientes Indicadores Clave de Rendimiento (KPI), que serán medidos mensualmente y reportados en los informes de seguimiento:

- **Disponibilidad del servicio de la plataforma BAS**: Mide el porcentaje de tiempo que la plataforma BAS ha estado operativa y accesible para la ejecución de simulaciones y la consulta de resultados. El objetivo de disponibilidad mensual será del **99,5% o superior**. Este cálculo excluirá las ventanas de mantenimiento programadas y notificadas previamente con un mínimo de 48 horas de antelación.
- **Porcentaje de Cumplimiento del Tiempo de Respuesta**: Indica el porcentaje de incidencias en las que el adjudicatario ha iniciado el análisis dentro del tiempo de respuesta máximo establecido en el ANS para cada nivel de severidad. El objetivo de cumplimiento mensual será:
  - Incidencias de severidad **Crítica y Alta**: ≥ 98%
  - Incidencias de severidad **Media i Baja**: ≥ 95%
- **Porcentaje de Cumplimiento del Tiempo de Notificación Detallada**: Mide el porcentaje de incidencias para las que se ha enviado la notificación detallada dentro del plazo máximo establecido en el ANS. El objetivo de cumplimiento mensual será:
  - Incidencias de severidad **Crítica y Alta**: ≥ 98%
  - Incidencias de severidad **Media i Baja**: ≥ 95%

La no consecución reiterada de estos KPI podrá ser considerado un cumplimiento defectuoso del contrato, de acuerdo con lo que se establezca en el Pliego de Cláusulas

Administrativas Particulares. El adjudicatario deberá proporcionar las herramientas y el acceso necesarios para la verificación de estos indicadores.

7. INFORMES Y CUADROS DE MANDO

La visibilidad sobre el estado de la seguridad y la eficacia de los controles es un elemento fundamental del servicio contratado. Para garantizar una comunicación fluida, transparente y útil para la toma de decisiones en todos los niveles de la organización, el adjudicatario deberá proporcionar un sistema completo de informes periódicos y un cuadro de mando con acceso en tiempo real. Estos elementos deben permitir no sólo conocer los resultados de las simulaciones, sino también entender la evolución de la postura de seguridad y priorizar las acciones de mejora.

El adjudicatario entregará, con una periodicidad mensual, dos tipos de informes diferenciados: un informe ejecutivo y un informe técnico detallado.

El **informe ejecutivo** estará orientado a la dirección y a los responsables del área, ofreciendo una visión de alto nivel de la postura de seguridad de la organización. Este documento deberá incluir, como mínimo: un resumen de la puntuación de seguridad global y su evolución respecto a períodos anteriores, los principales riesgos identificados, un análisis de tendencias y un resumen de las recomendaciones estratégicas más relevantes para la mejora continua de la seguridad.

El **informe técnico** estará destinado al equipo de ciberseguridad y deberá contener información exhaustiva sobre las actividades realizadas. Este informe incluirá los resultados detallados de todas las simulaciones de ataque ejecutadas durante el período (endpoint, movimiento lateral, amenazas inmediatas), identificando qué controles de seguridad han funcionado correctamente y cuáles han fallado. Detallará las brechas y vulnerabilidades detectadas, su severidad, y proporcionará **recomendaciones técnicas concretas y accionables** para su remediación. Además deberá contener métricas de rendimiento, como el porcentaje de penetración por vector de ataque, y su evolución histórica. Los resultados deben presentarse alineados con marcos de referencia como MITRE ATT&CK, mostrando claramente las técnicas, tácticas y procedimientos (TTP) probados y el estado de cobertura.

Adicionalmente a los informes mensuales, el adjudicatario deberá proporcionar acceso a un **cuadro de mando online (dashboard)** accesible vía web de forma segura. Esta herramienta debe permitir la consulta en tiempo real de la información generada por la plataforma BAS. El cuadro de mando debe ser intuitivo y personalizable, permitiendo al equipo técnico explorar los datos con diferentes niveles de detalle. Deberá visualizar, como mínimo: la puntuación de seguridad actualizada, los resultados de las últimas simulaciones, un mapa de calor o matriz de cobertura según framework MITRE ATT&CK, alertas sobre vulnerabilidades críticas descubiertas y la capacidad de generar informes bajo demanda. La plataforma debe garantizar la historización de los datos para poder realizar análisis comparativos y de tendencias a lo largo del tiempo.

8. SEGURIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El adjudicatario está obligado a adoptar todas las medidas técnicas y organizativas necesarias para garantizar la seguridad, integridad y confidencialidad de la información y los datos a los que tenga acceso o que sean generados durante la ejecución del contrato. Esta obligación se extiende a todo su personal, así como a cualquier subcontratista que pueda intervenir en la prestación del servicio.

El tratamiento de los datos de carácter personal que se derive de la ejecución del contrato se someterá a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD). A estos efectos, el adjudicatario tendrá la consideración de **Encargado del Tratamiento** y actuará en todo momento siguiendo las instrucciones documentadas del poder adjudicador, que ostentará la posición de Responsable del Tratamiento. El adjudicatario no podrá utilizar los datos para finalidades distintas de las especificadas en este pliego y deberá implementar las medidas de seguridad adecuadas para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Para acreditar su solvencia y capacidad en materia de seguridad de la información, el adjudicatario deberá demostrar el cumplimiento de los siguientes requisitos:

- **Esquema Nacional de Seguridad (ENS):** El adjudicatario deberá estar en posesión del Certificado de Conformidad con el Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022, de 3 de mayo, para sistemas de **categoría MEDIA** al menos. Este certificado deberá estar vigente durante toda la duración del contrato y cubrir el alcance de los servicios objeto de esta licitación.
- **Certificación ISO/IEC 27001:** El adjudicatario tendrá que disponer de un certificado vigente de la norma ISO/IEC 27001 relativo a su Sistema de Gestión de la Seguridad de la Información (SGSI). Esta certificación garantiza la adopción de un enfoque sistemático para la gestión de la seguridad de la información sensible.

Todo el personal del adjudicatario que participe en el servicio estará sujeto a un deber de secreto profesional y confidencialidad respecto a la información a la que tenga acceso. Esta obligación subsistirá incluso después de la finalización del contrato. En caso de un incidente de seguridad que afecte a los datos del organismo, el adjudicatario deberá notificarlo sin dilación indebida. Una vez finalizado el contrato, el adjudicatario deberá proceder a la devolución o supresión de todos los datos, según las indicaciones del responsable, certificando su eliminación completa.

9. PLAZO DE EJECUCIÓN E IMPLANTACIÓN

El plazo de ejecución del contrato se establece en una duración inicial de **treinta y seis (36) meses**, a contar a partir de la fecha de aceptación de la puesta en marcha del servicio. Este período podrá ser objeto de prórrogas expresas, previo acuerdo entre las

partes. Se prevé un máximo de una (1) prórroga anual, por un período de doce (12) meses adicionales, hasta alcanzar una duración máxima total del contrato de treinta y seis (36) meses. Cualquier prórroga se formalizará de acuerdo con la normativa de contratación pública vigente y estará condicionada al mantenimiento de las necesidades del organismo y la correcta ejecución del servicio por parte del adjudicatario.

El adjudicatario dispondrá de un plazo máximo e improrrogable de **cuatro (4) semanas** para la implantación y puesta en funcionamiento completa de la solución y los servicios gestionados asociados. Este plazo empezará a contar desde el día siguiente a la fecha de formalización del contrato.

Dentro de este plazo de implantación, el adjudicatario deberá realizar todas las tareas necesarias para dejar el servicio plenamente operativo, incluyendo el despliegue de la arquitectura SaaS, la instalación y configuración de los agentes en los "puntos de test" acordados, la configuración inicial de las simulaciones para los módulos contratados (endpoint, movimiento lateral y amenazas inmediatas), la definición de perfiles de usuario y la integración con las herramientas requeridas por el organismo.

Una vez finalizada la implantación, se realizará una fase de pruebas de aceptación para verificar que el servicio cumple con todos los requisitos técnicos y funcionales definidos en este pliego. La fecha de inicio del cómputo del plazo de ejecución del contrato será la correspondiente al acta de conformidad que certifique la correcta puesta en marcha del servicio.

Sant Joan Despí, junio de 2026