PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DEL SERVICIO DE GESTIÓN DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD PARA LA SOCIEDAD MERCANTIL CORPORACIÓ CATALANA DE MITJANS AUDIOVISUALS, SA

- PROCEDIMIENTO ABIERTO SIMPLIFICADO-

EXPEDIENTE N.º 2404OB03

1. SITUACIÓN ACTUAL DE LA CCMA, SA EN EL ENTORNO DE CIBERSEGURIDAD

Actualmente, la CCMA,SA y sus empresas filiales están implementando de manera progresiva acciones, herramientas y servicios para reforzar todo el entorno relacionado con la ciberseguridad.

Dentro de estas acciones, se plantea mejorar sus capacidades en materia de protección de Ciberseguridad. Es por este motivo que el objeto de este pliego es la contratación de un Centro de Operaciones de Seguridad (SOC externo), que mejore las capacidades del departamento de Ciberseguridad de la CCMA, SA, a la vez que tiene que ser elemento principal para vehicular la capacidad de protección, prevención, respuesta y orquestación bajo la gobernanza de la CCMA, SA.

CCMA, SA se plantea como objetivo crecer y mejorar las capacidades en materia de ciberseguridad, implementando la monitorización de seguridad, detección temprana de incidentes, vigilancia y análisis de varias fuentes de amenaza y vulnerabilidades y por último optimizar la capacidad de reacción, respuesta y recuperación ante cualquier incidente.

2. DESCRIPCIÓN DE LA OFERTA

El alcance del servicio, es la contratación de un servicio de ciberseguridad que incremente las capacidades actuales del área de Sistemas y Comunicaciones de la CCMA, SA a todos los niveles (proactivo, preventivo y reactivo) en los ámbitos más relevantes de la ciberseguridad.

Los servicios principales que se tendrán que contemplar y que serán detallados a lo largo de este documento serán:

- **Servicio de operación de seguridad**.
  - Monitorización continúa de logs y acontecimientos de seguridad (SIEM), capacidad de detección temprana de incidentes y amenazas y vigilancia de amenazas.
  - Despliegue de medidas de prevención y contramedidas, análisis continuo y tratamiento de las vulnerabilidades
  - Incorporar e implementar la herramienta de SIEM.
- **Servicio de inteligencia de amenazas**
  - Realización de tareas proactivas, respecto al resultado de la operación de los servicios, de prevención, protección y respuesta, incluyendo información y otras fuentes de información para identificar correlaciones entre ciberamenazas que puedan convertirse o se conviertan en un incidente de seguridad para los activos de la CCMA, SA.
- **Servicio de gestión y respuesta a incidentes de seguridad (CSIRT)**
  - Gestión de incidentes de ciberseguridad, recuperación y remediación de las operaciones después de un incidente de ciberseguridad, apoyo a las

investigaciones y requerimientos, preservación de evidencias, registro y seguimiento de actividades.

- **Servicio de apoyo a la gestión y operación del SOC**
  - Gestión centralizada de los servicios y operativa del SOC, este punto se de contacto directo con la CCMA, SA. Facilitar la integración y el buen funcionamiento, aportando valor en propuestas de mejora de la operación, definición de cuadros de mando, métricas e indicadores, todo aquello que ayude a mejorar la gobernanza de la ciberseguridad.
- **Servicio de apoyo en el área de Sistemas y Comunicaciones (Depto. Ciberseguridad)**
  - Ofrecer **propuestas de controles de seguridad**, pruebas de controles de seguridad, vulnerabilidades de la arquitectura de infraestructura y sistemas.
  - **Auditoría, pentest, reporting, informes periódicos de seguridad.**
  - **Definir plan de adecuación** al esquema nacional de seguridad (**ENS**), **asistencia técnica en la adecuación del ENS** y asistencia posterior, **auditoría interna y auditoría para la certificación en el ENS**.

El seguimiento y monitorización del servicio de ciberseguridad gestionada se hará mediante una plataforma o portal único propuesto por el adjudicatario (apertura de tickets, seguimiento, monitorización, obtención de información, estado, etc.).

El servicio prestado por el proveedor adjudicatario será flexible y estará alineado con la evolución tecnológica de la CCMA,SA, a fin de poderse adaptar a las necesidades surgidas de la implantación de nuevas infraestructuras, aplicaciones y/o proyectos tanto en CCMA, SA como en servicios de cloud.

3. SITUACIÓN ACTUAL

La CCMA, SA, gestiona internamente el servicio de seguridad desde el área de Sistemas y Comunicaciones, con la creación reciente del departamento de Ciberseguridad, donde de manera coordinada con el resto de personal técnico del área, se está coordinando y gestionando toda la vertiente de ciberseguridad.

Actualmente se están llevando a cabo las acciones de seguridad siguientes:

- Recepción, gestión y resolución de incidentes.
- Mantenimiento, administración y evolución de la infraestructura de Seguridad.
- Análisis de malware.
- Definición de configuración de seguridad, vulnerabilidades, mitigaciones, actualizaciones.
- Definiciones de seguridad en proyectos.

La CCMA, SA, quiere mejorar y dotar al servicio interno de seguridad de más capacidad y recursos especializados para poder ampliar la monitorización y vigilancia de seguridad, la detección temprana de incidentes y la rápida respuesta y recuperación ante posibles incidentes.

4. VOLUMETRÍAS

La volumetría analizada en eventos por segundo de todos los sistemas sobre los que en un principio se tendrá que recoger información para analizar es de mínimo 3700 EPS.

El número de fuentes a integrar en el sistema de recolección de logs y correlato, será de mínimo 10 fuentes, que se definirán en la fase inicial del proyecto.

El almacenamiento de logs y el mantenimiento de estos tiene que ser de dos años de retención.

5. DESCRIPCIÓN DEL SERVICIO SOLICITADO

El proveedor adjudicatario tendrá que disponer de un equipo completo de operaciones de seguridad y respuesta a incidentes en Barcelona (podrá ser visitado por CCMA,SA), dada la importancia de la actuación temprana en todos los ámbitos de la seguridad. Los detalles y condiciones quedarán especificados a lo largo de este pliego.

El proveedor adjudicatario tendrá que cubrir los siguientes servicios:

- Servicio regular
- Servicio bajo demanda

Servicio regular

El servicio regular tendrá que cubrir las siguientes tareas:

1. Servicio de operación de seguridad
2. Servicio de inteligencia de amenazas
3. Servicio de gestión y respuesta a incidentes de seguridad (CSIRT)
4. Servicio de apoyo a la gestión, orquestación y operación del SOC
5. Servicio de apoyo en el área de Sistemas y Comunicaciones (Depto. Ciberseguridad-CCMA)

Servicio de operación de seguridad

El servicio de operación de seguridad incluye la monitorización de seguridad, despliegue de medidas y análisis de vulnerabilidades, y la protección de aplicaciones cloud.

Monitorización de seguridad, detección temprana de incidentes y amenazas

El servicio de monitorización de seguridad, tiene como objetivo la detección de cualquier violación o amenaza inminente de la seguridad de la CCMA, SA, que pueda ser detectada en base al análisis continuo de los eventos o alertas de seguridad reportados por los sistemas definidos por CCMA, SA.
De manera general, este servicio tiene que cubrir:

- Monitorización contínua de los eventos y alertas en tiempo real generados por toda la infraestructura de la CCMA, SA definida. Esta monitorización se tiene que llevar a cabo en modalidad 24/7.
- Definir y desarrollar un catálogo de casos de uso documentales funcionalmente con correlación según los diferentes campos normalizados de las fuentes de datos existentes y aportadas por el servicio.
- Relación de casos de uso con categorías y taxonomías establecidas y/o propuestas por el servicio, según las buenas prácticas habituales en seguridad TI.
- Elaboración de playbooks personalizados según la detección de amenazas para ofrecer las instrucciones, las guías y recomendaciones para dar solución a incidentes y garantizar la seguridad de los sistemas de información.
- Detección, identificación, clasificación y categorización de posibles incidentes de seguridad y recolección de evidencias necesarias por análisis posteriores.
- Alertar o notificar a los responsables de la CCMA, SA. (correo electrónico, sms o llamada) y ofrecer breve información que se ha detectado y la categorización que se ha dado.

- Análisis completo de los incidentes teniendo en cuenta todas las posibles fuentes de información (evidencias, análisis de vulnerabilidades, vigilancia digital, otros incidentes, IOCs, feeds de seguridad, etc.), para obtener el impacto del incidente, activos afectados, nivel de compromiso de los servicios a los que puede afectar y cualquier información que permita optimizar la contención, la reparación y la recuperación.
- Proponer un plan de mitigación y reparación del incidente (respuesta al incidente) detectado en base a procedimientos establecidos y con el objetivo de resolver el incidente lo mejor posible y con totales garantías. También se realizarán tareas automáticas o acciones rápidas, de bloqueo, contención y respuesta (ejemplo, bloqueo automático IP de C&C detectado.....)
- Proveer una capa de orquestación automática que permita la normalización, categorización, actuación y notificación de forma automática según las necesidades definidas por CCMA, SA.

Con la detección de cualquier alerta generada por el sistema de monitorización y en base a los criterios que se hayan establecido, se realizará una categorización y notificación de toda la información significativa (configuración, cliente afectado, IPs, redes, etc.) de la alerta en los grupos de operaciones definidos (de la CCMA,SA o del proveedor adjudicatario) para atenderla lo mejor posible.

Alcance del servicio:

Concepto	Cantidad
EPS	3700 mínimo
Fuentes	10 mínimo
Disponibilidad del servicio	24h/7
Recolector de datos	Necesario para prestar el servicio
Data logger	Mantener retención 2 años

Definición de la severidad de las detecciones:

Nivel de severidad	Definición
CRITIC	Detecciones relacionados con APT o sus fases: Obtención de acceso Identificar objetivos Obtención de acceso a otros objetivos Movimientos laterales Preparación de acciones ilícitas Extracciones de datos Mantener accesos
MUY ALTO	Detecciones relacionadas con: Distribución de malware Configuración de malware Robo de información Sabotaje Interrupciones de servicio

ALTO	Detecciones relacionadas con: Sistema infectado Acceso no autorizado a la información Modificación no autorizada de información Pérdida o borrado de información Phishing Pérdida de datos Modificación no autorizada de información Conexiones C&C (Mando y Control) Compromiso de aplicaciones Compromiso de cuentas privilegiadas Ataques desconocidos DOS o DDoS. Explotación de vulnerabilidades
BAJO	Detecciones relacionadas con: Escaneo o análisis de redes/paquetes Intento de explotación de vulnerabilidades Vulneración de credenciales Sistemas vulnerables Compromiso de cuentas sin privilegio Suplantación Etc.

Los SLA que como mínimo se tienen que cumplir se especifican a continuación.

Nivel de severidad alertas	Tiempo de notificación	Tiempo de respuesta
CRÍTICO	< 30 minutos	< 15 minutos
MUY ALTO	< 45 minutos	< 15 minutos
ALTO	< 1hora	< 15 minutos
MEDIO O BAJO	< 2 horas	< 15 minutos

Concepto	Tiempo de notificación/respuesat
Revisión/Validación de los casos de uso definidos	Mensualmente
Revisión/Validación de los Playbooks asociados a los casos de uso	Mensualmente

Entrega de informe de revisiones y actualizaciones y pruebas de casos de uso y playbooks.	Mensualmente
Entrega de informe de alertas detectadas	Mensualmente

Penalizaciones:

Concepto	Valoración	Penalización
Informar en tiempo real a los responsables de la CCMA,SA de alertas con severidad CRÍTICA	Número de casos en el mes en que el tiempo al informar al responsable de la CCMA, SA > 30 minutos	3% por incidente
Informar en tiempo real a los responsables de la CCMA, SA de alertas con severidad MUY ALTA	Número de casos en el mes en que el tiempo al informar al responsable de la CCMA, SA > 45 minutos	3% por incidente
Informar en tiempo real a los responsables de la CCMA, SA de alertas con severidad ALTA	Número de casos en el mes en que el tiempo al informar al responsable de la CCMA, SA > 60 minutos	3% por incidente
Incidentes ocasionados por no gestionar alertas siguiendo el playbook asociado	Numero de incidentes mensuales >= 1	3% por incidente
Incidentes ocasionados por no revisar o actualizar casos de uso y/o playbooks.	Numero de incidentes mensuales >= 1	3% por incidente
Incidentes ocasionados por no gestionar alertas en tiempos	Tiempo de gestión de las alertas es >15 minutos	3% por incidente
No entrega de informes con el contenido y la periodicidad acordadas	Mensualmente	1%
Incumplimiento de la no disponibilidad del servicio	Si las horas no disponibilidad >=1	Importe de 2h por cada hora no dedicada o no disponible

Análisis y gestión de vulnerabilidades

Actualmente la CCMA, SA, dispone de un servicio contratado para la detección de vulnerabilidades, los servicios contratados son las amenazas inmediatas, endpoint y movimiento lateral. Se usa una herramienta del tipo BAS (Breach anb Attack Simulation), todos los análisis generan unos informes que hay que integrar en este servicio para su gestión y análisis para poder hacer un seguimiento del ciclo de vida de las vulnerabilidades detectadas (detección, corrección, verificación).

Para los activos internos, este servicio tiene que cubrir, de manera general:

- Alerta e identificación de vulnerabilidades potenciales y confirmadas: acción repetida en el tiempo periódicamente, establecida como ciclos de auditoría sobre los activos identificados.
- Propuesta de mitigación o corrección de las vulnerabilidades detectadas desde un punto de vista correctivo y preventivo. También se tendrá que tener en cuenta los falsos positivos y hacer depuración y filtrado de este para evitar su tratamiento.
- Certificar la corrección de las vulnerabilidades con un proceso de gestión del ciclo de vida de la vulnerabilidad: acción repetida en el tiempo para verificar si se han hecho las correcciones adecuadas y si estas han solucionado las vulnerabilidades detectadas.

Una vez identificadas y registradas las vulnerabilidades (etapa de identificación y descubrimiento), CCMA, SA mediante una gestión única hará el seguimiento y administración del ciclo de vida de las vulnerabilidades, asumiendo la vulnerabilidad y el riesgo, desestimando la vulnerabilidad si no es aceptada o dándola por corregida si se han llevado a cabo las medidas necesarias para mitigarla. En referencia a las vulnerabilidades corregidas, se tendrá que certificar su corrección en el siguiente análisis o auditoría programado.

- Entregar informe con el resultado del análisis/auditoría llevado a cabo en el entorno para poder evaluar el estado de seguridad de los sistemas acordados. En los documentos a entregar, se tendrá que contemplar dos tipos de informes: ejecutivo y técnico.

  Informe ejecutivo: Resumen de los hallazgos significativos además alto nivel.

  Informe técnico, informe detallado donde se reflejará como mínimo:

  Documentación de las pruebas realizadas

  Documentación de las recomendaciones de seguridad

  Descripción de vulnerabilidades encontradas con las evidencias y el estudio del impacto en términos de confidencialidad, integridad y disponibilidad.

  Detalle de la metodología para la explotación de las vulnerabilidades encontradas

  Descripción de medidas a aplicar para mitigar o eliminar los riesgos asociados a la explotación de las vulnerabilidades encontradas

Para los activos web, este servicio tiene que cubrir, de manera general:

- Pentesting persistente para los dominios web de la CCMA,SA. mínimo cada mes: lo que se pretende es obtener un análisis del estado de seguridad de los dominios web públicos de la CCMA, SA. Este pentesting se tendrá que llevar a cabo sin ningún conocimiento del entorno en las webs.

  El número de dominios que se tendrá que analizar es de mínimo 3 dominios web.

  Los objetivos esperados de estos pentests, teniendo en cuenta los requerimientos que tenemos que cubrir a nivel general, son:

- Obtener la máxima información útil de los sistemas para poder ser atacados, identificar vulnerabilidades potenciales y confirmadas focalizadas en entornos, tecnologías y aplicaciones web.
- Recomendar soluciones a las vulnerabilidades encontradas desde el punto de vista correctivo y preventivo.

- Entregar informe con los resultados de la auditoría llevada a cabo para poder evaluar la seguridad del sistema analizado. Los informes a entregar son los mismos y con el mismo detalle definidos en el documento técnico del apartado anterior.
- Certificar, tal y como se ha especificado antes, la corrección de las vulnerabilidades encontradas con un proceso completo de gestión de ciclo de vida de estas.

Este pentesting tiene que tener identificados como mínimo la siguiente tipología o metodología de ataques web:

- Detección de errores y fugas de información.
- Acceso no autorizado a archivos, directorios y zonas de administración.
- Detección de vulnerabilidades en sistemas CMS.
- Inyección de código HTML, SQL (SQLi).
- Inyecciones de pedidos de sistema operativo.
- Inyecciones de ficheros local y remota.
- Cross-Site Scripting (XSS).
- Manipulación de cookies de sesión.
- Evaluación de hábitos de navegación del cliente (DNS Snooping).

Puntualmente también tendrá que cubrir:

- Pentesting manual completo para 3 aplicaciones móviles al año: lo que se pretende es verificar la seguridad de las aplicaciones móviles intentando vulnerarlas de manera simulada cómo haría un atacante profesional, usando herramientas y recursos especializados y combinando varias vulnerabilidades encontradas.

  Los objetivos esperados de este pentesting, y teniendo en cuenta los requerimientos que tenemos que cubrir a nivel general, son:

- Identificar vulnerabilidades potenciales y confirmadas focalizadas en aplicaciones móviles.
- Recomendar soluciones a las vulnerabilidades encontradas desde el punto de vista correctivo y preventivo.
- Entregar un informe con los resultados de la auditoría llevada a cabo para poder evaluar la seguridad del sistema analizado. Los informes a entregar son los mismos y con el mismo detalle definidos en la página anterior.
- Certificar tal y como se ha especificado antes, la corrección de las vulnerabilidades encontradas a través de un proceso completo de gestión de ciclo de vida de estas.

Los modos en que se lleven a cabo las auditorías, análisis y pentest, podrán ser en cualquier modalidad (caja negra o caja negra, con intrusión externa o interna), pero siempre previo aviso y acuerdo con CCMA, SA. Del mismo modo, para verificar la explotación de cualquier vulnerabilidad, también tendrá que ser notificado y acordado con CCMA, SA.

Como consideraciones generales, se tendrá que tener en cuenta que:

- No se realizarán ataques o pruebas de denegación de servicio.
- Se tendrán que prever posibles impactos en el servicio que se puedan ocasionar a raíz de las acciones llevadas a cabo durante análisis o auditorías. Se tendrán que notificar a la CCMA, SA. antes de llevarlas a cabo, para programarlas y acordar las condiciones de las ejecuciones para así no afectar a los servicios.
- Los horarios y programaciones de las auditorías tendrán que estar supervisados y autorizados por CCMA, SA. para controlar los riesgos que se pudieran derivar y que puedan afectar al servicio ofrecido para los equipos auditados.

- Se hará énfasis en las recomendaciones de las vulnerabilidads y errores de seguridad detectados previamente pero que no han sido corregidos.
- En toda intervención, se requerirá que haya un responsable de la CCMA, SA. Que esté al corriente durante todo el tiempo de vida del análisis o auditoría.

Para la gestión de las vulnerabilidades detectadas en el proceso de identificación, éstas tendrán que ser clasificadas y documentadas según los organismos especializados y bases de datos de conocimiento como CVE (Common Vulnerabilities and Exposures) y CWE (Common Weakness Enumeration), y usando el método de cálculo estándar CVSS (Common Vulnerability Scoring System), del conocido organismo FIRST. Se tendrá que facilitar la lectura y la comprensión de las debilidades encontradas mediante este servicio.

Definición de la severidad de las detecciones:

Nivel de severidad	Definición
CRITICO	Vulnerabilidades muy graves (CVSS de 9 hasta 10), 0-day no evaluados y exploits que puedan afectar a sistemas, plataformas y software que se use en CCMA, SA Configuraciones de sistemas detectados con nivel bajo de seguridad que puedan provocar un incidente grave de seguridad Acceso no autorizado a archivos, directorios y zonas de administración Inyección de código, inyecciones de pedidos de sistema operativo o inyecciones de ficheros locales y remotas
MUY ALTO	Vulnerabilidades graves (CVSS de 7 hasta 8) y nuevas vulnerabilidades notificadas Configuraciones de sistemas detectadas con nivel bajo de seguridad que puedan provocar un incidente de seguridad Detección de errores y fugas de información Cross-Site Scripting (XSS) Manipulación de cookies de sesión
	Configuraciones de sistemas detectados con nivel bajo de seguridad que puedan provocar un incidente de seguridad Detección de errores y fugas de información Cross-Site Scripting (XSS) Manipulación de cookies de sesión
ALTO	Vulnerabilidades (CVSS de 5 hasta 6) Detección de vulnerabilidades en sistemas CMS no críticas
BAJO	Vulnerabilidades graves (CVSS <5)

Los SLA que como mínimo se tienen que cumplir se especifican a continuación.

Nivel de severidad de alertas	Tiempo de notificación	Tiempo de respuesta

CRITICO	< 120 minutos	< 240 minutos
MUY ALTO	< 180 minutos	< 360 minutos

Concepto	Tiempo de notificación/respuesta
Notificación de detecciones CRITICO, MUY ALTO y ALTO en el Servicio de Orquestación del SOC	Inmediatamente al hacer la detección
Revisión/Validación de procedimientos y protocolos de actuación	Mensualmente
Revisión/Validación de procedimientos y protocolos de elevación	Mensualmente
Entrega de informe de alertas detectadas y gestionadas	Mensualmente
Tiempo de respuesta a la petición bajo demanda de un análisis de vulnerabilidades	5 días
Entrega de los informes	7 días desde la finalización de las tareas de análisis
Disponibilidad del servicio	DS = Número escaneos/activos previstos – número escaneos/activos realizados = 0
Recurso dedicado al servicio en (8h/5)	25h/mes mínimo

Las horas de dedicación son mínimos y podrán ser modificadas y acordadas según convenga a CCMA, SA y valorando la dedicación respecto a otros servicios.

Penalizaciones:

Concepto	Valoración	Penalización
Incidentes ocasionados por no alertar o elevar el caso al Servicio de Orquestación del SOC	Numero de incidentes mensuales >= 1	15% por incidente
Incidentes ocasionados por no revisar o actualizar los protocolos y procedimientos de alerta y notificación	Numero de incidentes mensuales >= 1	10% por incidente
Incidentes ocasionados por no gestionar alertas en tiempos	Tiempo de gestión de las alertas >15 minutos	5% por incidente
No entrega de informes con el contenido y la periodicidad acordadas	Mensualmente	3%

Disponibilidad del servicio	Número de escaneos/activos planificados y no analizados. Si DS > 0	DS %
Incumplimiento del horario de dedicación mínima del servicio o la no disponibilidad del servicio	Horas de dedicación mínima mensual. Si la diferencia con las acordadas >=1 Si las horas no disponibilidad >=1	Importe de 2h por cada hora no dedicada o no disponible

Servicio de inteligencia de amenazas

CCMA, SA tiene como objetivo la protección de sus activos, procesos y reputación mediante la monitorización, notificación y respuesta ante amenazas existentes, que permita tomar decisiones de manera rapida y eficiente para minimizar o evitar impacto en los procesos y servicios corporativos.

Lo que se pretende con este servicio es tener la capacidad de evaluar la posición real que tiene CCMA, SA en el entorno digital y obtener una ventaja estratégica identificando, anticipando y respondiendo de manera rápida ante riesgos que se puedan detectar.

Este servicio de manera general tiene que cubrir:

- Detección proactiva y monitorización continua de amenazas (24/7) derivadas del entorno digital.
- Respuesta frente a estas amenazas, mitigando su impacto e incrementando la resiliencia.
- El ámbito de la monitorización a la que se hace referencia por entorno digital tendrá que hacerse a través de:
    - Internet (Surface web)
    - Internet profundo (Deep web)
    - Internet oscuro (Dark web)
- La detección, monitorización y notificación que se llevará a cabo 24/7, tendrá que incluir como mínimo los siguientes tipos de amenazas:
    - Uso no autorizado del nombre de la CCMA, SA o de las marcas asociadas.
    - Dominios sospechosos, relacionados con dominios propiedad de la CCMA, SA.
    - Exposición de información confidencial o sensible en la red.
    - Campañas, movimientos o acciones contra CCMA, SA que se puedan planificar u organizar en la web o en redes sociales. Se tendrán que contemplar, como mínimo, DDoS, “defacement”, inyecciones de código en recursos de la CCMA, SA, inyecciones de malware, etc.).
    - Identificación y notificación de toda aquella información publicada (tutoriales, publicaciones, videos, etc.) que revelen fallos o vulneraciones de mecanismos de seguridad en activos lógicos o físicos de la CCMA, SA.
    - Identificación de vulnerabilidades graves (CVSS>7), 0-day no evaluados y exploits que puedan afectar a sistemas, plataformas y software que se use en la CCMA, SA. Se notificará también a modo de avisos, boletines de seguridad y Security Advisory de los principales fabricantes, con información sobre vulnerabilidades y actualizaciones de seguridad que permitirán estar al día y tomar acciones si fuera necesario.
    - Detección de robo y compromiso de credenciales de cuentas de la CCMA, SA (brechas de información en servicios que afectan a usuarios de la CCMA, SA.).

Se facilitará un informe detallado con toda la información que se haya podido conseguir (nombre de usuario, contraseña, url del servicio afectado, etc.), así como evidencias.

- Identificar sitios web que suplanten los oficiales de la CCMA, SA. para intentar hacer campañas de phishing y pharming en nombre de la CCMA, SA.
- Dar respuesta al incidente detectado y realizar las acciones pertinentes para mitigarlo. Principalmente la respuesta será gestionar la eliminación, modificación, baja de los contenidos, webs, dominios, etc. que no sean lícitos o no estén bajo el control de la CCMA, SA. Se tienen que incluir hasta 10 actuaciones al año.

Las horas de dedicación son mínimos y podrán ser modificados y acordados según convenga a la CCMA, SA y valorando la dedicación respecto a otros servicios.

Definición de la severidad de las detecciones:

Nivel de severidad	Definición
CRITICO	Vulnerabilidades graves (CVSS > 7), 0-day no evaluados y exploits que puedan afectar a sistemas, plataformas y software que se use a CCMA, SA Robo y compromiso de credenciales de cuentas de la CCMA. SA (brechas de información en servicios que afectan a usuarios de la CCMA, SA)
MUY ALTO	Exposición de información confidencial o sensible en la red, campañas, movimientos o acciones contra la CCMA, SA que se puedan planificar u organizar en la web o en redes sociales
ALTO	Uso no autorizado del nombre de la CCMA, SA o de las marcas asociadas, dominios sospechosos, relacionados con dominios propiedad de la CCMA, SA.
BAJO	Identificación de la información que revele fallos o vulneraciones de mecanismos de seguridad en activos lógicos o físicos de la CCMA, SA. Identificar sitios web que suplanten a los oficiales de la CCMA, SA.

Los SLA que como mínimo se tienen que cumplir se especifican a continuación:

Nivel de severidad de las alertas	Tiempo de notificación	Tiempo de respuesta
CRITICO	< 30 minutos	< 15 minutos
MUY ALTO	< 45 minutos	< 15 minutos

Concepto	Tiempo de notificación/respuesta
Notificación de detecciones CRITICA, MUY ALTA y ALTA en referencia al Servicio de Orquestación del SOC	Inmediatamente al hacer la detección
Revisión/Validación de procedimientos y protocolos	Mensualmente

de actuación	
Revisión/Validación de procedimientos y protocolos de elevación	Mensualmente
Entrega de informe de alertas detectadas y gestionadas	Mensualmente
Tiempo de respuesta a la petición bajo demanda de un análisis de vulnerabilidades	5 días

Penalizaciones:

Concepto	Valoración	Penalización
Incidentes ocasionados por no alertar o elevar al Servicio de Orquestación del SOC	Numero de incidentes mensuales >= 1	3% por incidente
Incidentes ocasionados por no revisar o actualizar los protocolos y procedimientos de alerta y notificación	Numero de incidentes mensuales >= 1	3% por incidente
Incidentes ocasionados por no gestionar alertas en tiempos	Tiempo de gestión de las alertas >15 minutos	3% por incidente
No entrega de informes con el contenido y la periodicidad acordadas	Mensualmente	1%
Incumplimiento del horario de dedicación mínima del servicio o la no disponibilidad del servicio	Horas de dedicación mínima mensual. Si la diferencia con las acordadas >=1 Si las horas no disponibilidad >=1	Importe de 2h por cada hora no dedicada o no disponible

Servicio de gestión y respuesta a incidentes de seguridad (CSIRT)

La CCMA, SA requiere, en caso de sufrir un incidente grave de seguridad, de un equipo de respuesta a incidentes especializado. Este tendrá que proporcionar el apoyo y la experiencia necesarios para llevar a cabo las tareas de análisis, contención y reparación táctica enfocados a contextualizar ataques dirigidos contra CCMA, SA y minimizar su impacto siguiendo las mejores prácticas en este ámbito.

Este servicio tiene que cubrir como mínimo lo siguiente:

- Capacidades de investigación y análisis forense:
  - Evaluación inicial, validación del incidente, evidencias preliminares y contextualización del incidente.

  - Extracción de evidencias sobre sistemas comprometidos de la CCMA, SA.
  - Análisis de equipos para identificar sus capacidades (vectores de entrada, técnicas de ofuscación, métodos de propagación, técnicas de exfiltración, etc.), obtener los indicadores de compromiso (IOCs) y conocer las primeras contramedidas de mitigación.
  - Contextualizar la amenaza encontrada mediante la correlación de los equipos/sistemas encontrados en la fase forense y las fuentes de inteligencia del proveedor (propietarias, privadas o públicas), que permitan evaluar mejor acciones a llevar a cabo.
  - Evaluación del alcance del compromiso, buscando indicadores y estados previos con el fin de identificar tres activos comprometidos, movimientos laterales, escalada de privilegios y cualquier indicador de presencia de los actores del incidente.
- Respuesta y reparación del incidente:
  - Coordinación durante el incidente con el equipo de seguridad de la CCMA, SA. Y todas las partes que puedan estar involucradas (incluyente organismos oficiales donde se tiene que reportar).
  - Guía y apoyo sobre las estrategias de contención para minimizar el impacto del incidente en curso.
  - Apoyo en la erradicación, recuperación y vuelta al servicio, así como en la implementación de medidas preventivas derivadas de lecciones aprendidas para que no se vuelva a repetir el tipo de incidente sufrido.
  - Monitorización y control puesto-incidente.
- Análisis de malware :
  - Identificar los propósitos reales del ataque.
  - Identificar todos los posibles IOCs que permitan actualizar toda la infraestructura de seguridad de la CCMA, SA.
  - Identificar todos los mecanismos de propagación y todas las capacidades del equipo o sistema (vectores de entrada, técnicas de ofuscación, métodos de propagación, técnicas de exfiltración, etc.).
  - Identificar con detalle todo lo que sea susceptible de ponerse en listas de bloqueo y que estén relacionados con la actividad del artefacto (dominios, IPs, hashs, URLs, etc.).
- Redacció de informes técnicos con todo el detalle del incidente.
  - Informes periódicos sobre la actividad del servicio.
  - Informes bajo demanda sobre actuaciones/investigaciones durante la gestión de incidentes y análisis de malware.
- Recomendaciones y lecciones aprendidas.
  - Realizar análisis y recomendaciones sobre todo lo que hemos podido aprender de un incidente, enfocados a mejorar la seguridad de los sistemas con el propósito de prevenir incidentes similares.

El servicio de respuesta a incidentes y actuaciones, tendrá que contemplar las actuaciones en incidentes con criticidad media o baja con la cobertura de los servicios solicitados a lo largo de este pliego. En el caso de que el incidente tenga criticidad alta, se tendrá que activar el CSIRT (por motivo de que el primer/segundo nivel del SOC así lo solicite, o bajo demanda de la CCMA, SA) con todos los recursos necesarios.

La definición de criticidad de los incidentes será:

- Criticidad alta: incidentes que tienen un impacto considerable (afectación a la confidencialidad, disponibilidad e integridad) a información considerada crítica para la actividad de la CCMA, SA y/o sistemas TIC críticos. El incidente tiene capacidad de afectación en gran cantidad sobre información valiosa y causar la degradación de servicios vitales de la CCMA, SA. Estos incidentes pueden ser típicamente, malware

destructivo, denegación de servicios, compromiso de sistema, incidentes de hacking y violaciones de políticas que afecten a los sistemas críticos o información critica para la CCMA, SA.

- Criticidad media: incidentes que afectan a sistemas o información no crítica para la CCMA, SA, o que su impacto no repercuta directamente en servicios vitales de negocio. Estos incidentes pueden ser típicamente incidentes de hacking, phishing y/o algunas violaciones de políticas, entre otros.
- Criticidad baja: incidentes de seguridad en sistemas no críticos para la CCMA, SA. o investigaciones que impliquen hacer análisis forenses.

La metodología requerida al proveedor adjudicatario para hacer la gestión, notificación y respuesta a los incidentes de seguridad, podrá ser la aprobada por el CCN- CERT, de acuerdo con el Esquema Nacional de Seguridad (ENS) y que esté referenciada en las guías CCN-STIC403 y CCN-STIC-817. Si fuera alguna otra metodología, habrá que detallarlo en la oferta.

Los acuerdos de servicio relacionados con el servicio de CSIRT en todas las actuaciones de los diferentes niveles que contemple serán:

Descripción del indicador	Tiempo de respuesta (en horas)
Tiempo de intervención en las dependencias físicas de la CCMA, SA (solo en caso de necesidad por incidente grave de seguridad)	< 3h
Tiempo de respuesta en caso de incidencia de criticidad alta	30 minutos
Realización de análisis preliminares de los incidentes de nivel con criticidad alto.	3h
Tiempo de entrega de los informes en caso de incidencia de nivel con criticidad alta	8h después del cierre del incidente
Tiempo máximo de entrega de los informes en caso de declaración de brecha de seguridad.	40h después de que se empiece a dar respuesta
Tiempo de respuesta en caso de incidencia de criticidad media.	3h
Realización de análisis preliminares en caso de incidentes de nivel de criticidad media.	6h
Tiempo de respuesta en caso de incidencia de criticidad baja.	6h
Realización de análisis preliminares en caso de incidentes de nivel de criticidad baja.	12h
Tiempo máximo para la entrega del informe bajo demanda de análisis de malware.	48h
Tiempo máximo para la entrega del informe bajo demanda de análisis forense.	72h

El servicio tiene que contar con una dedicación de recursos, siendo la dedicación mínima de 25 horas al mes, y debe contar con un mínimo de rotación, teniendo la CCMA, SA. La potestad de pedir el cambio en el caso de que no se logren las expectativas del servicio

especificado anteriormente. Si el cambio es propiciado por el licitador, no podrá hacerse efectivo sin que haya habido un traspaso de conocimientos mínimo de dos semanas, y logra los conocimientos por parte de la CCMA, SA.

Las horas de dedicación son mínimos, y podrán ser modificado y acordados según convenga a la CCMA, SA, valorando la dedicación respecto a otros servicios.

Este recurso ha de hacer un análisis continuo (mientras no sea necesaria la intervención en un incidente identificado) de las muestras o indicadores detectados por otros servicios del SOC, previendo y detectando posibles patrones, comportamientos o evidencias que pueden dar lugar a un incidente y estableciendo las contingencias o mitigaciones necesarias.

Penalizaciones:

Concepto	Valoración	Penalización
Informar en tiempo real (t) a los responsables de la CCMA,SA de alertas con severidad CRITICA	Número de casos en el mes en que el tiempo al informar al responsable de la CCMA, SA > 30 minutos	15% por incidente
Informar en tiempo real (t) a los responsables de la CCMA, SA de alertas con severidad MUY ALTA	Número de casos en el mes en que el tiempo al informar al responsable de la CCMA, SA > 45 minutos	10% por incidente
Incidentes ocasionados por no gestionar alertas siguiendo el playbook asociado	Numero de incidentes mensuales >= 1	15% por incidente
Incidentes ocasionados por no revisar o actualizar casos de uso y/o playbooks.	Numero de incidentes mensuales >= 1	10% por incidente
Incidentes ocasionados por no gestionar alertas en tiempo	Tiempo de gestión de las alertas >15 minutos	5% por incidente
No entrega de informes con el contenido y la periodicidad acordadas	Mensualmente	3%

Servicio de apoyo a la gestión, orquestación y la operación del SOC

Servicio de apoyo a la gestión y la operación del SOC

CCMA, SA requiere un interlocutor único y con disponibilidad garantizada, responsable de todos los servicios de seguridad por parte del proveedor adjudicatario.

Este será el responsable por parte del proveedor de controlar la calidad de los servicios contratados, cumplir los compromisos adquiridos e impulsar y evolucionar estos servicios para mejorar la seguridad de la CCMA, SA., según lo que se ha establecido, y durante la duración del contrato.

Independientemente de los servicios solicitados a lo largo de este documento, el interlocutor único tiene que cubrir como mínimo las siguientes obligaciones/tareas:

- Conocer la importancia, los conceptos y las metodologías de los procesos de la seguridad informática y su implementación bajo un enfoque estratégico, que pueda apoyar a la visión y decisiones estratégicas del responsable de la CCMA, SA.
- Ser el responsable de la provisión y explotación de los servicios contratados. Gestionar, planificar y seguir la coordinación de todos los servicios de seguridad para optimizar y ofrecer los mejores resultados a los requerimientos y necesidades de la CCMA, SA.
- Velar por la correcta gestión, escalados y resolución de incidentes en que estén implicados varios equipos de servicios solicitados, optimizando las gestiones necesarias en la banda del proveedor adjudicatario para agilizar la resolución de la mejor y más rápida forma posible en todos los aspectos.
- Ser interlocutor principal ante CCMA, SA. para la gestión, el escalado y la coordinación de las necesidades o incidentes (sobre todo graves) que puedan surgir.
- Responsable de la gestión de los cambios o configuraciones de los servicios contratados para que la prestación del servicio sea la más óptima e intente mejorar en todo momento las capacidades de seguridad de la CCMA, SA.
- Responsable de la calidad del servicio contratado, del seguimiento, el control y el cumplimiento de los acuerdos de estos servicios, de la interlocución y el reporting ante la CCMA, SA.
- Aportaciones o asesoramiento sobre la constante evolución de varias tecnologías que puedan mejorar o aumentar la seguridad de la CCMA, SA.
- Aportaciones o asesoramiento sobre las mejores prácticas o recomendaciones de seguridad, la confidencialidad, la integridad y disponibilidad de la información, así como la continuidad del negocio, si fuera necesario.

Se tendrá que cumplir que el tiempo de atención de cualquier incidente o consulta por parte de la CCMA, SA. por parte del interlocutor único, no sea superior a 30 minutos. Una vez hecha esta atención, se gestionará por su parte la resolución de lo solicitado, manteniendo informada en todo momento a la CCMA, SA. de los avances en las tareas solicitadas. Si se supera este tiempo en la atención, se podrá aplicar una penalización del 1%.

Servicio de orquestación operativa

Este servicio se tiene que focalizar en apoyar la gestión operativa y táctica del SOC, siendo su finalidad principal prestar un servicio transversal en todo el SOC que permita tanto mejorar la gestión de las tareas administrativas necesarias, así medir, potenciar y presentar de manera adecuada el valor que los diferentes servicios generan con su actividad. El servicio se tendrá que encargar de:

- Liderar la orquestación operativa del SOC.
- Gestionar la información del contexto operativo, importante para la ejecución de los diferentes procedimientos establecidos al SOC.
- Definir los indicadores de valor del SOC, estableciendo los procesos necesarios para poder medir de forma continua su evolución.
- Determinar los entregables necesarios para presentar el valor que aporta el SOC a los diferentes interlocutores existentes de la CCMA, SA.

Este servicio tiene que establecer todos los procedimientos necesarios para garantizar la coordinación de todos los servicios del SOC, logrando los objetivos y focalizándose en las tareas de mayor relevancia global, la prevención, la protección, la detección y respuesta ante cualquier ciberamenaza que pueda darse en la CCMA, SA.

Este servicio deberá cubrir, de manera general:

- La coordinación **entre los servicios de operaciones**: el servicio de Orquestación Operativa se tiene que establecer como un rol de coordinación entre los diferentes

servicios del SOC, para velar porque se mantenga un alineamiento y un objetivo común entre los equipos de operaciones, así como una buena comunicación y feedback. Se tiene que encargar de definir los procesos que regirán las relaciones entre los equipos de operaciones. A la vez, el servicio de orquestación tendrá que velar por el correcto despliegue de los procedimientos establecidos, definiendo los indicadores necesarios para monitorizar el grado de despliegue. De igual forma, será función del rol de coordinación el apoyo a la resolución de conflictos operativo que se puedan dar entre los servicios, velando en todo caso por los intereses globales del SOC y la mejora de la seguridad global de la CCMA, SA.

- Tener **visión general de los servicios de operaciones** y proposición de mejoras de todos los servicios licitados, para llegar a la máxima cohesión, eficacia y precisión en la operativa global del SOC.
- **Alinear el servicio de Orquestación Operativa** con los objetivos tácticos y operativos establecidos por cada servicio del SOC. Estableciendo los procesos de coordinación necesarios con los responsables de los diferentes servicios que componen el SOC, con el objetivo de garantizar el alineamiento homogéneo con los diferentes objetivos establecidos.

Adicionalmente, habrá que garantizar en el servicio de Monitorización de seguridad, detección temprana de incidentes y amenazas descrito en el apartado "**Monitorización de seguridad, detección temprana de incidentes y amenazas"**, las actuaciones de orquestación automáticas mínimas a ofrecer:

- Envío de correo electrónico/SMS, a un grupo de contactos específicos con la especificación y detalle de la alerta encontrada para una situación concreta.
- Llamada telefónica para notificar al contacto en la CCMA, SA.
- Apertura automática de tickets de servicio para la gestión y/o resolución del altercado o incidente detectado. Posibilidad de integración con otras herramientas de ticketing que se usen en CCMA, SA (Easyvista y/o Jira).
- Envío de los informes generados referentes a alertas o incidentes, de manera automática.
- Ejecución automática de procedimientos de respuesta creados y definidos con la CCMA; SA que puedan dar respuesta automática a ciertas alertas.
- Ejecución de acciones de remediación automática (SOAR) sobre las principales tecnologías de seguridad de la CCMA, SA. (p.e: bloqueo de una IP o URL en el Firewall de perímetro por detección de alerta de intento de comunicación con un C&C en un cliente en el Firewall de perímetro).
- Incorporar capa de inteligencia en el "SIEM como servicio", incorporando feeds de IOCs propios del proveedor adjudicatario (división de ciberinteligencia propia), feeds privados (CTA, FIRST, OASIS, Fabricantes, partners, etc.) y feeds públicos (feeds opensource, listas de reputación, datos sobre amenazas, actores, etc.).

  El servicio tiene que hacer un procesamiento de toda la información completa teniendo en cuenta todas las fuentes de inteligencia posibles, para poder hacer un scoring automático, una correlación y un enriquecimiento de los resultados mediante una plataforma de threat intelligence (TIP).

- Coordinar la ejecución de los planes de mitigación y remediación iniciados hasta que se dé por cerrado el incidente con todo el equipo involucrado en el incidente en cuestión. En todo momento supeditado a la decisión del responsable de la CCMA, SA.
- Gestión del escalado, si fuera necesario, en el equipo de respuesta a incidentes especializado para la evaluación o el tratamiento del incidente completo, si fuera necesario.

- Documentar todos los casos que se den, se conviertan o no en incidente de seguridad, describiendo las evidencias e información recavada, las tareas realizadas y el análisis completo llevado a cabo.

Los SLA que como mínimo se tienen que cumplir se especifican a continuación, siendo estos la notificación de alertas o incidentes reportados por otros servicios del SOC y que tienen que gestionarse y notificar a otros servicios del SOC y/o en la CCMA, SA:

Nivel de severidad de alertas	Tiempo de notificación	Tiempo de respuesta
CRITICO	< 20 minutos	< 15 minutos
MUY ALTO	< 35 minutos	< 15 minutos
ALTO	< 50 minutos	< 15 minutos
MEDIO ó BAJO	< 1,5 horas	< 15 minutos

Penalizaciones:

Concepto	Valoración	Penalización
Incidentes ocasionados por no alertar o elevar al servicio correspondiente del SOC	Numero de incidentes mensuales >= 1	15% por incidente
Incidentes ocasionados por no gestionar alertas en tiempos	Tiempo de gestión de las alertas >15 minutos	10% por incidente
No entrega de informes con el contenido y la periodicidad acordadas	Mensualmente	3%

Servicio de apoyo en el área de Sistemas y Comunicaciones (Depto. Ciberseguridad-CCMA)

El servicio de apoyo en el departamento de Ciberseguridad de la CCMA tiene como principal función:

- Ofrecer **propuestas de controles de seguridad**, pruebas de controles de seguridad, vulnerabilidades de la arquitectura de infraestructura y sistemas.
- **Auditoría, pentest, reporting, informes periódicos de seguridad.**
- **Definir un plan de adecuación** en el esquema nacional de seguridad (**ENS**), **asistencia técnica en la adecuación del ENS** y asistencia posterior, **auditoría interna y auditoría para la certificación al ENS**.

Este servicio de manera general y no limitativa, tiene que cubrir las funciones (bajo demanda o de manera proactiva) de:

- **Evaluación de los informes de cumplimiento, riesgo y seguridad** para la definición de controles, políticas y medidas de seguridad existentes sobre los ámbitos de protección del SOC.

- **Análisis del alineamiento de la actividad del SOC** y su evolución en las directivas de seguridad de la CCMA y su estrategia, evaluando problemáticas y carencias que puedan existir para proponer medidas correctoras.
- **Definir el plan de adecuación del ENS, asistencia técnica para la adecuación del ENS y auditorías interna y auditoría para la certificación en el ENS.**
- **Dar respuesta y apoyo en la definición de tareas o dudas que puedan surgir en el departamento de Ciberserguridad de la CCMA** para incrementar la seguridad global de la CCMA.

Servicio bajo demanda

El ámbito de Ciberseguridad de la CCMA, SA, dispondrá de un cómputo de horas para la realización de tareas bajo demanda según las necesidades de cada momento y relacionadas con el servicio regular. Estas tareas irán destinadas a apoyar a CCMA, SA. tanto en la prevención, la gestión y la respuesta frente a incidentes de seguridad de la información, como otras necesidades de seguridad.

El servicio incluirá:

- Un mínimo de 15 jornadas de CSIRT: Los técnicos especializados en respuesta a incidentes (CSIRT) del proveedor adjudicatario apoyarán en incidentes graves de seguridad que lo requieran a CCMA, SA. Dado que gestión y respuesta a incidentes de nivel 1 y 2 se tiene que dar desde el SOC, el uso de estas jornadas sólo podrá estará supeditado a la necesidad del SOC por revaluación de la gravedad del incidente (previa aprobación de la CCMA, SA.) o porque CCMA, SA. lo solicite expresamente.
- Un mínimo de 10 jornadas por provisión: Los técnicos especializados del SOC del proveedor adjudicatario realizarán varias tareas de provisión según las necesidades de seguridad de la CCMA, SA.
- En estas 25 jornadas está incluida la posibilidad de desplazamiento en las dependencias de la CCMA, SA. solo en caso estrictamente necesario (incidentes graves de seguridad).

6. HERRAMIENTA SIEM. CARACTERÍSTICAS Y REQUISITOS

Relacionados con la arquitectura

- La **arquitectura** tiene que ser escalable, **sin límites de escalado.**
- **La plataforma** tiene que poder procesar las Gb de ingesta al día **sin estar limitada** a un máximo de eventos por segundo o eps.
- La plataforma SIEM tiene que darse **en modo servicio CLOUD SAAS nativo**, donde el fabricante de la solución asume la totalidad del servicio. **Esta infraestructura tiene que estar aislada de la infraestructura del proveedor para que la CCMA pueda continuar utilizándola al romper o acabar el servicio**.
- El tenant cloud proporcionado por el servicio del SIEM tiene que ser **dedicado exclusivamente por la CCMA, SA,** tiene que entregarse directamente por parte del fabricante y la propiedad **y titularidad** tienen que ser de la CCMA, SA.
- La plataforma tiene que disponer de replicación **de datos para garantizar la disponibilidad de los mismos**.
- El servicio de datos tiene que disponer de la capacidad de trabajar con bases de datos no relacionales.

- La plataforma tiene que disponer de capacidades de recopilación de datos seguros y de alto rendimiento por dispositivos Linux, MacOs y Windows. Estos **agentes tienen que ser muy ligeros y utilizar los recursos mínimos** (<2% sobre el rendimiento del servidor).

Relacionados con las capacidades y funcionalidades base de la plataforma

- La plataforma tiene que ser capaz **de ingerir cualquier dato basado en texto, preservar el acontecimiento original con total integridad y proporcionar un esquema de datos flexible para una extracción fácil de campos en tiempos de busca.**
- La solución tiene que implementar "schema on read" por los datos ingestados.
- La plataforma tiene que ser capaz de admitir la ingesta de datos mediante agente o "agentless". Tiene que soportar las **técnicas más comunes de recolección de datos sin agente**, incluyendo: TCP, UDP, WMI, recursos compartidos de ficheros de red, JDBC, ODBC, JMS, SNMP, capturas de tráfico de red, Apios, FIFO o datos provenientes de scripts personalizados.
- La solución tiene que incluir la capacidad de ingestar datos de red mediante una sonda, que permita extraer datos de más de 25 protocolos de red: IP, TCP, UDP, ICMP, HTTP, DNS…
- La solución tiene que incorporar la funcionalidad de normalización del dato basado en un **formato estándar, no propietario**.
- La plataforma tiene que **proporcionar un modelo de datos común** como estándar de normalización que facilite el análisis de los datos.
- La plataforma no tiene que depender de conectores **personalizados suministrados por el integrador para ingerir datos de diferentes fuentes**.
- El fabricante de la solución tendrá que contar con **un market o repositorio con más de 2000 conectores ya fabricados** y disponibles para facilitar la normalización y carga de los datos en la futura plataforma SIEM de la CCMA, SA.
- La plataforma tendrá que proporcionar un catálogo de casos de uso de ciberseguridad con más de 500 **reglas predeterminadas** disponibles para su implementación.
- La plataforma tendrá que ofrecer de forma nativa una herramienta que permita mapear los casos de uso de ciberseguridad con el cumplimiento del framework de ciberseguridad MITRE ATT&CK.
- Los conectores disponibles en el market tienen que tener apoyo directo de los fabricantes terceros de las soluciones a conectar o por el propio fabricante de la solución de SIEM.
- La plataforma tiene que poder **utilizar fuentes de datos externos para enriquecer** los acontecimientos en bruto, añadir contexto y/o crear análisis más completos.
- La plataforma tiene que disponer, ya implementados, de al menos **20 algoritmos de Matching Learning** mantenidos por el propio fabricante.
- La plataforma tiene que permitir la creación **y extensión de la gamma de visualizaciones personalizadas** (no se limita a los informes fijos y preestablecidos).
- Los informes y cuadros de mando de la plataforma tienen que incluir capacidades de "drilldown" que permitan a los usuarios profundizar en la información que la plataforma pone a vuestra disposición mediante clics.
- **La plataforma tiene que permitir casos de uso más allá de la ciberseguridad / desempeño** que posibilita la colaboración entre servicios y proporciona retornos de la inversión mucho más atractivos.
- La solución SIEM tiene que estar reconocida por el mercado con una posición de Leader en el Cuadrante Mágico de Gartner por al menos 5 años consecutivos.

Relativos a la arquitectura cloud

- Tiene que ser una solución ofrecida como un servicio SaaS o Software-as-a-Service, con un acuerdo de nivel de servicio o SLA del 100% de disponibilidad.
- El servicio de seguridad tiene que **disponer de un servicio de copia de seguridad** de la configuración y los datos más allá de la replicación.
- El servicio tiene que proporcionar capacidades de cifrado **en tráfico y cifrado opcional en reposo**.

Relativos a las capacidades y funcionalidades específicas de seguridad

- La solución tiene que proporcionar **actualizaciones automáticas de contenido de seguridad libradas directamente por el equipo de investigación de amenazas** para ayudar a mantener el servicio al corriente de las amenazas nuevas y emergentes.
- La solución de seguridad tiene que ofrecer funcionalidades que ayuden en todas las fases de la práctica de ciberseguridad:
    - **Monitorización de la postura de seguridad**:
        - Analizar en tiempo real el riesgo, alertas y compliance.
        - Monitorización continúa y completa de los activos.
    - **Compliance**: con los datos recogidos, analizar el estado de cumplimiento según RGPD.
    - **Detección de Amenazas Avanzadas**:
        - Detectar los sistemas y usuarios comprometidos.
        - Determinar las actividades asociadas con usuarios y atacantes.
        - Encontrar indicadores y artefactos asociados en los sistemas comprometidos.
    - **Investigación de incidentes y forense. Visibilidad de extremo a extremo** mediante una única plataforma de análisis que ayuda a detectar e investigar rápidamente las posibles amenazas de seguridad, reduciendo así sus MTTD y MTTR.

Referencias y reconocimiento del sector

- La herramienta SIEM utilizada tendrá que figurar, en alguna de sus versiones, en el Catálogo de Productos y Servicios de Seguridad de las TIC del Centro Criptológico Nacional como una herramienta cualificada para ser utilizada en sistemas de categoría ALTA de acuerdo con el Esquema Nacional de Seguridad (aprobado por el Real Decreto 3/2010).

- La herramienta tendrá que estar certificada, en alguna de las versiones, con la ISO/IEC 15408, Common Criteria u otros de naturaleza y calidad análogas, como establece la medida del Esquema Nacional de Seguridad [op.pl.5] Componentes Certificados para Categoría ALTA.

7. MODELO DE RELACIÓN CCMA, SA. – SOC

La relación estará basada en la figura del interlocutor/coordinador único (detallada en el apartado "**Servicio de apoyo a la gestión y operación del SOC**") que será el responsable de

seguridad del servicio del proveedor adjudicatario y que actuará de intermediario entre este y CCMA, SA. Este interlocutor es fundamental para el buen funcionamiento del servicio, así como para dar apoyo en el establecimiento de las políticas, buenas prácticas y controles de seguridad en el ámbito del servicio.

Lo que se pretende es conseguir un modelo de relación con el proveedor adjudicatario que dé respuesta a todas las necesidades planteadas por CCMA, SA, siguiendo el objetivo de garantizar un buen gobierno y seguimiento del servicio, así como una alineación con las necesidades estratégicas y operativas de la CCMA, SA. durante la duración del contrato.

A este objeto, se define una relación basada en tres niveles:

- **Estratégico**: como objetivo, mantener el buen gobierno y el buen funcionamiento de servicio contratado. habrán revisiones periódicas (pueden ser 3-4 por año) con los objetivos, entre otros, para hacer:
  - Seguimiento del contrato.
  - Seguimiento y evaluación del servicio prestado.
  - Validación del alcance general, objetivos y resultados esperados.
  - Validación de la planificación de las tareas previstas a realizar.
  - Verificación del cumplimiento de las especificaciones solicitadas y el cumplimiento de los acuerdos de servicio.
  - Seguimiento del consumo de jornadas del contrato.
- **Táctico**: como objetivo, llevar a cabo el seguimiento del servicio y tratamiento de puntos importantes a tratar para la evolución y mejora del servicio o de la seguridad de la CCMA, SA. Se harán revisiones que pueden ser mensuales, con los objetivos, entre otros, de:
  - Revisar el estado general del servicio. Efectuar un seguimiento/control de los servicios que se llevan a cabo, y valorar la evolución de la implantación de los servicios pendientes.
  - Revisión de principales incidencias que hayan surgido o estén activas.
  - Revisar la situación de los proyectos y tareas en curso y pendientes. Revisión del calendario previsto. Realizar análisis y priorización.
  - Revisión de informes de análisis de vulnerabilidades y amenazas. Revisión de estado de las acciones correctivas.
  - Verificación del desempeño de los acuerdos de servicio establecidos.
  - Validación de los procedimientos y acciones de mejora por parte de los Responsables de Seguridad.
  - Aprobación de la ejecución de proyectos de mejora y nuevos servicios.
- **Operacional**: tiene como objetivo llevar a cabo el seguimiento del día a día del servicio y tratar las problemáticas específicas que afecten al servicio prestado. Ofrece la visión más técnica para resolver las situaciones o temas urgentes que pueda haber. Las revisiones pueden ser semanales, con los objetivos, entre otros, de:
  - Seguimiento del día a día.
  - Propuestas de mejora y cambios.
  - Identificar riesgos o cambios significativos en la evolución del servicio para poderse trasladar a una evaluación con más detalle a nivel operativo. Si los riesgos identificados son elevados, se tratarán a niveles tácticos o estratégicos, según convenga.

En cuanto a los recursos asignados al servicio solicitado a lo largo de este pliego, el proveedor adjudicatario se tendrá que ajustar permanentemente a las necesidades de la CCMA, SA., de acuerdo con la volumetría expresada a lo largo de este pliego de prescripciones técnicas.

Cualquier modificación que el licitador quiera hacer en cualquier servicio del pliego tiene que ser debidamente notificada a la CCMA, SA, que deberá validar y aprobar si puede ser realizada.

El proveedor adjudicatario tendrá que asumir variaciones puntuales de las volumetrías previstas de hasta un 20% de incremento o decrecimiento sin necesidad de hacer ninguna modificación del contrato ni del precio.

8. PRESTACIÓN DEL SERVICIO

El proveedor adjudicatario tendrá que presentar un plan detallado que tenga en cuenta las características y fases específicas que se listan a continuación:

1. Fase de análisis.
2. Fase de inicio del servicio.
3. Fase de estabilización.
4. Fase de finalización y devolución del servicio. Este plan tendrá que ser aprobado por CCMA, SA.

Una vez se inicie la ejecución del contrato, se establecen los siguientes plazos parciales para la puesta en servicio del SOC, aplicables únicamente en el contrato inicial:

- Fase de análisis: 2 meses
- Fase de inicio del servicio: 1 mes
- Fase de estabilización: 1 mes

(Con todos los servicios contratados, no puede superar los 4 meses)

Llegada la fecha de finalización del contrato, se establece una fase de finalización y devolución del servicio establecida en 1 mes.

Fase de análisis

En esta fase, se hará un análisis para definir con detalle los procedimientos que regirán el servicio, la documentación y el soporte, así como la transferencia de conocimientos entre el equipo de seguridad de la CCMA, SA y el del proveedor adjudicatario.

Con este análisis de la información especifica recogida, los recursos, la documentación, etc. se presentará un cronograma para los objetivos a lograr en la fase de transición, que será acordado y aprobado por CCMA, SA.

Se tendrá que tener en cuenta la implantación de la herramienta de CASB y la contemplación de su fase de prueba y puesta en servicio en el cronograma que se plantee.

Esta fase no tendrá una duración mayor de 8 semanas.

Fase de inicio del servicio

En esta fase tendrían que ejecutarse todas las actividades previstas en el servicio (en base a los requerimientos especificados en este pliego), los compromisos del servicio que el adjudicatario ha incorporado a su oferta, los acuerdos y modificaciones aprobadas después de la fase de análisis, los mecanismos de control requeridos y los procedimientos de operación y gestión del servicio (así como documentarlos).

Esta fase tiene que tener en cuenta la implantación del servicio de manera evolutiva y gradual, para poder a afianzar cada uno de los servicios implantados.

Esta fase tendrá una duración estimada de 4 semanas.

Fase de estabilización

En esta fase ya está en funcionamiento el servicio gestionado por el proveedor adjudicatario.

Esta fase tiene que tener como objetivo que el servicio solicitado (especificado a lo largo de este pliego) esté funcionando con todas las garantías y de manera adecuada.

En esta fase se tienen que identificar todos los riesgos que puedan derivar en un funcionamiento no óptimo del servicio, así como todas las tareas a realizar, el tiempo de respuesta esperado, etc. para llegar al funcionamiento óptimo.

Se tendrán que detallar todas las acciones que se llevarán a cabo para que el servicio esté plenamente operativo lo antes posible.

Esta fase finalizará en el momento que el proveedor adjudicatario haya puesto en marcha o definido todas las tareas previstas en el servicio regular solicitado en este pliego técnico y la CCMA, SA haya dado su visto y aprobado.

La duración de esta fase no tiene que ser superior a 1 mes.

Fase de finalización y devolución del servicio

El objetivo de esta fase es preparar y organizar los equipos de trabajo que ofrecen el servicio para poder realizar un traspaso del servicio a la CCMA, SA., o al proveedor designado, en caso de que no haya continuidad con este.

Se tendrá que garantizar de manera correcta el **traspaso de competencias, documentación y conocimiento en la CCMA, SA. o al proveedor designado, a la finalización del contrato, y en este proceso de traspaso se tienen que devolver a la CCMA todas las personalizaciones, acciones de reparación, casos de uso y cuadros de mando de la herramienta SIEM**.

Se tendrá que contemplar un plan de traspaso de la operativa, la gestión y el control del servicio a la CCMA SA. o al proveedor designado.

La duración de esta fase no tendría que ser superior a 1 mes.

9. MEDIOS PERSONALES

El equipo profesional que el adjudicatario asignará estará integrado, como mínimo, por los siguientes perfiles:

- Coordinador del Servicio de Titulación: - Titulación universitaria en Informática, Telecomunicaciones o titulación de grado superior en Informática, Telecomunicaciones o titulación universitaria que asegure la competencia en la materia (titulación homologada en el estado español). - Acreditar la certificación CISSP - Certified Information System Security Profesional o certificaciones oficiales equivalentes. Experiencia: - 7 años de experiencia en el sector de la ciberseguridad - 5 años de experiencia como coordinador del Servicio haciendo funciones en proyectos similares al objeto del contrato. - La acreditación de 3 proyectos en 3 empresas diferentes y donde se vea que se han ejecutado proyectos de mejora de los procesos de negocio y mejoras en la seguridad.

- Técnicos Especialistas en Respuesta a Incidentes: (CSIRT) Titulación: - Titulación universitaria en Informática, Telecomunicaciones o titulación de grado superior en Informática, Telecomunicaciones o titulación universitaria que asegure la competencia en la materia (titulación homologada en el estado español). Experiencia: - 7 años de experiencia en el sector de la ciberseguridad - 4 años de experiencia efectuando funciones en proyectos similar al objeto del contrato en los últimos 7 años del sector de ciberseguridad. Se tendrá que acreditar mediante una declaración responsable que entre todos los técnicos presentados cumplen con las siguientes funciones, habilidades y conocimientos: - Gestión y Respuesta a Incidentes de Seguridad, CSIRT.
- Operación de Seguridad
  (SOC) Titulación: - Titulación universitaria en Informática, Telecomunicaciones o titulación de grado superior en Informática, Telecomunicaciones o titulación universitaria que asegure la competencia en la materia (titulación homologada en el estado español).
  Experiencia:
  5 años de experiencia en el sector de la ciberseguridad de los cuales los últimos 4 en funciones similares al objeto del contrato.
  Se tendrá que acreditar mediante una declaración responsable que entre los técnicos presentados cumplen con las siguientes funciones, habilidades y conocimientos:
  Haber realizar en el último año un mínimo de 3 tests de intrusión y 5 análisis de vulnerabilidades, utilizando metodología OSSTMM y OWASP.
  - Administración/Gestión de herramientas de análisis de vulnerabilidades.
  - Administración/Gestión de herramientas de hacking ético.
  - Desarrollo de scripts en Perl, Shell script y programación en c.
  - Administración de seguridad y diseño de red.
  - Seguridad informática en protocolos, aplicaciones y sistemas operativos.
  - Administración de sistemas Linux y Windows.
  - Administración de sistemas de seguridad (NAC, CASB, F5 Big-IP, cortafuegos).
  - Administración de equipos cortafuegos (Palo Alto, Checkpoint, Fortinet.
  - Administración de plataformas de seguridad en la endpoint (Trend Micro).
  - Hardering de servidores Windows (2003, 2008, en adelante) y Linux (SUSE, Red Hat, Ubuntu,).
  - Hardering de dispositivos de red (Routers, Switchs, Firewall).
  - Administración de Sistemas y Servicios de red .
  - Servidores web (IIS, Apache), de correo (Exchange), de aplicaciones (Weblogic, Tomcat,), BBDD (MySql, Oráculo, MSSQL).
  - Correlación de eventos cono OSSIM y RSA y monitorización de Seguridad.
  - Detección de amenazas, vulnerabilidades y ataques.
  - Administración de sistemas IDS e IPS.
  - Capacidad de respuesta a incidentes (CSIRT de 1.º y 2.º nivel).
  - Análisis y resolución de incidentes de seguridad (análisis forense, de malware).

La acreditación se realizará mediante los certificados correspondientes expedidos por los clientes del licitador y/o currículums del equipo con detalle de la experiencia profesional junto con la copia del título formativo para acreditar la solvencia. La CCMA, SA podrá requerir otra documentación adicional que acredite el cumplimiento de la experiencia requerida.

La empresa adjudicataria tendrá que mantener durante la vigencia del contrato la composición (calidad del personal) del equipo de trabajo acreditado como solvencia mínima y del equipo presentado y aportar todo el personal necesario y suficiente para la realización de los servicios.