Universitat Oberta de Catalunya

uoc.edu

CONTRATO RELATIVO AL SERVICIO DE CIBERSEGURIDAD GESTIONADA DE LA UNIVERSITAT OBERTA DE CATALUNYA

Expediente HSE00013/2019

PROCEDIMIENTO ABIERTO
Y SUJETO A REGULACIÓN ARMONIZADA

PLIEGO DE PRESCRIPCIONES TÉCNICAS

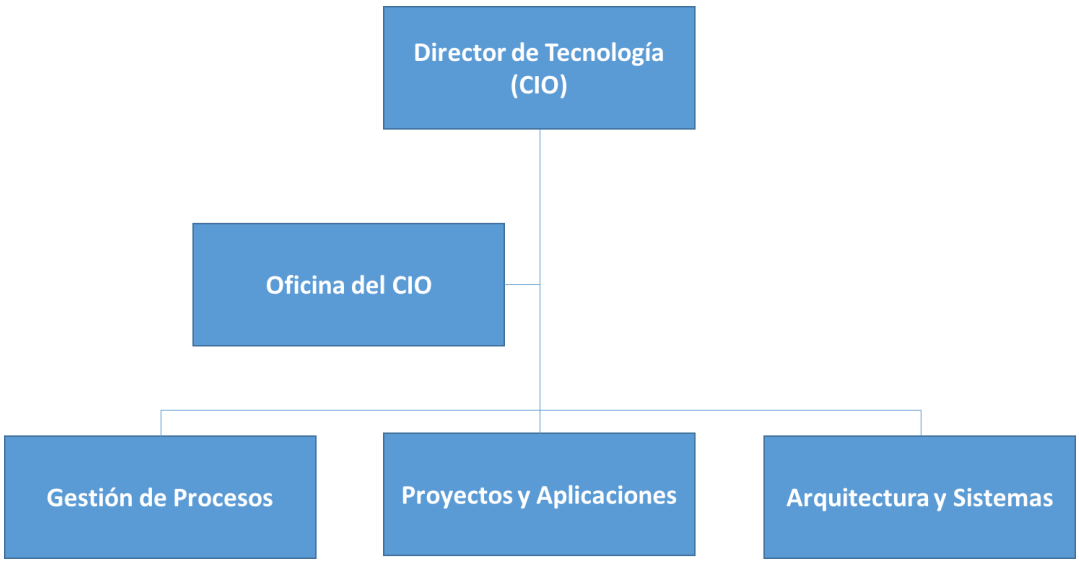
NOTA: En caso de discrepancia entre el contenido de la versión original en catalán de este documento y sus anexos y la versión traducida al castellano, la versión catalana prevalecerá sobre la versión traducida al castellano.

ÍNDICE

1. Introducción.

La Universitat Oberta de Catalunya (en adelante la UOC) es una universidad en línea que utiliza el e-learning de forma exhaustiva como canal principal para llevar a la práctica el proceso de ensañanza y aprendizaje. Toda la oferta formativa de la UOC requiere de mecanismos y elementos vinculados al e-learning que hacen posible su desarrollo.

Dentro de la universidad, el Área de Tecnología vela por la gobernabilidad de los Sistemas de Información y por la evolución tanto del Campus Virtual como de las diferentes herramientas que apoyan su gestión. A tal efecto se ha estructurado en tres grupos operativos y una oficina que dan apoyo directo al CIO, tal y como se define a continuación:



- Grupo Operativo de Proyectos y Aplicaciones: lidera la ejecución de los proyectos, así como el mantenimiento y evolución de las aplicaciones existentes. Es responsable, por tanto, del servicio de mantenimiento de las aplicaciones, tanto de gestión como de campus virtual.

- Grupo Operativo de Gestión de Procesos: es el principal referente en la interlocución con el resto de la UOC por los temas de tecnología, tiene la visión transversal de los procesos clave de la UOC, y rinde cuentas de la cartera de proyectos y evolutivos de cada área .

- Grupo Operativo de Arquitectura y Sistemas: es el responsable de la definición de la arquitectura tecnológica así como de la integración de nuevos proyectos y sistemas y de su desarrollo, de la transferencia a Tecnología de los proyectos de innovación, de la gestión de la infraestructura tecnológica en producción (CPD) y la red de telecomunicación y de su disponibilidad.

- Oficina del CIO: lidera la ejecución de los proyectos del Master Plan y está al cargo de la administración del Área de Tecnología y su seguimiento. Hace el seguimiento de los proveedores y es responsable del seguimiento de la calidad. El grupo de seguridad tecnológica forma parte de este grupo operativo.

Y es en este grupo operativo donde se ubicará el servicio objeto de la licitación para cubrir los requerimientos en materia de seguridad tecnológica con la gestión y operación de la infraestructura tecnológica de seguridad, la gestión de los incidentes de seguridad y la resolución de las tareas que le sean asignadas al proveedor adjudicatario.

2. Objeto del Contrato

El objeto de este pliego de licitación es la contratación de un Servicio de Ciberseguridad Gestionado de forma externalizada, que dé respuesta a las necesidades actuales de la UOC de acuerdo con las prescripciones que se articulan dentro del presente pliego.

3. Objetivos del Contrato

El objetivo es la contratación de un servicio de ciberseguridad gestionada, donde el proveedor adjudicatario, aporte la experiencia y especialización técnica adecuadas para garantizar el tratamiento óptimo de toda la casuística de problemáticas en las que el área de tecnología tiene que hacer frente.

La Gobernanza de la Seguridad de la Información mediante este servicio, se ocupará de gestionar la seguridad del Área de tecnología de la UOC en base a las especificaciones descritas en el presente pliego. Los objetivos que se quieren alcanzar son:

- La gestión, operación y administración de las infraestructuras de seguridad que se integran en el servicio, así como de los nuevos sistemas que se vayan incorporando, por proyectos o renovaciones, durante todo el periodo que cubra el contrato, garantizando en todo momento la disponibilidad y la continuidad del servicio.

- Apoyo a cambios, peticiones y proyectos relacionados con las infraestructuras, procedimientos, compliance tecnológico, técnicas de especialista y normativa relacionados con la seguridad tecnológica.

- Facilitar y posibilitar la focalización por parte del personal de la UOC en aspectos y proyectos más estratégicos, reduciendo la dedicación a tareas de apoyo, mantenimiento y operativas del día a día.

- Convertir el servicio actual de seguridad UOC en un servicio gestionado a través de un compromiso y una implicación por parte del proveedor adjudicatario en el servicio y en los procesos de mejora continua.

- Facilitar la medida de la calidad del servicio en relación a la seguridad tecnológica mediante Acuerdos de Nivel de Servicio específicos.

- Permitir asegurar que la UOC cumple con los requerimientos legales y normativos.

- Mejorar la satisfacción y confianza de los estudiantes de la UOC y aumentar su retención.
- Generar coherencia en los servicios y productos de la UOC.
- Gestionar y minimizar la exposición al riesgo.
- Construir una cultura interna empresarial de seguridad.
- Proteger la organización, los activos, los grupos de interés y los directivos de la UOC en frente de ciberamenazas.

3.1 Duración del contrato

La duración del contrato será la que se especifica en el Pliego de Cláusulas Particulares.

4. Alcance y descripción del servicio

El alcance del servicio es la contratación de un servicio de ciberseguridad que ayude a gestionar la Seguridad Tecnológica de la UOC a todos los niveles (proactivo, preventivo y reactivo) y en las disciplinas más relevantes del ámbito de la ciberseguridad.

Estas disciplinas o especializaciones, que se describirán en este documento son, al menos:

- **Operaciones de seguridad**: gestión de incidentes de ciberseguridad, desastres, recuperación de las operaciones después de un incidente de ciberseguridad, apoyo a las investigaciones y requerimientos, registro y seguimiento de actividades, medidas de prevención y contramedidas, tratamiento de las vulnerabilidades , preocupaciones / consultas de seguridad del personal.
- **Gestión de la seguridad y del riesgo**: gestión del riesgo, cumplimiento normativo, leyes y reglamentos, continuidad del negocio, gobernanza de la seguridad, procedimientos y directrices de seguridad, modelado de amenazas.
- **Seguridad de los activos**: controles de seguridad de los datos, protección de la privacidad.
- **Seguridad de las comunicaciones y de las redes**: estrategias de pruebas, pruebas de controles de seguridad, vulnerabilidades de la arquitectura en general.
- **Auditoría de los sistemas de información**: auditoría, reporting, informes de situación y seguimiento de las auditorías.

En general, el seguimiento y monitorización de este servicio de ciberseguridad gestionada, se hará mediante las plataformas y herramientas actualmente disponibles en la UOC (básicamente Atlassain JIRA® https://www.atlassian.com/software/jira y OneTrust® https: //www.onetrust.com/). Si así lo creen conveniente, las empresas licitadoras podrán incluir, dentro de la propuesta, herramientas adicionales a las actualmente existentes en la UOC, pero que en ningún caso sustituirán a las ya mencionadas.

El servicio prestado por el proveedor adjudicatario será flexible y alineado con la evolución tecnológica y organizativa de la UOC, con el fin de adaptarse a las necesidades surgidas de la implantación de nuevas infraestructuras, aplicaciones y / o proyectos tanto dentro de la UOC como en la nube.

El servicio estará adaptado a la transformación actual que el área de tecnología de la UOC asume para la migración progresiva a la nube, tanto de infraestructura como de servicios según el plan estratégico de la UOC.

4.1 Situación actual

La UOC actualmente gestiona el servicio de seguridad internamente mediante un equipo de dos personas y la colaboración puntual de otros técnicos del área de tecnología.

La actividad actual relacionada con la seguridad cubre los siguientes ámbitos:

- Estudios de vulnerabilidad
- Recepción, gestión y resolución de incidencias
- Análisis de malware
- Análisis forense
- Mantenimiento, administración y evolución de la infraestructura de seguridad.

La UOC quiere transformar su servicio interno de seguridad para evolucionarlo hacia un servicio gestionado que no sea dependiente de los recursos técnicos internos.

4.1.1 Infraestructura hardware de seguridad actual de la UOC

- **Descripción de los dispositivos:**

- Un ARBOR Pravail PRA-APS-2104:
  - Processor(s): 2 x Intel(R) Xeon(R) CPU E5645 @ 2.40GHz (12 total cores) (24 total threads) x 1
  - Memory: 24.00 GB
  - Inspected Throughput Limit: 2.00 Gbps

- Un TrendMicro TippingPoint IPS 660N:
  - Inspected Throughput Limit: 2.00 Gbps

- Un FW PaloAlto PA 5020:
  - 12 puertos de 10/100/1000 Gb y (8) puertos SFP
  - 5 Gbps de rendimiento del cortafuegos
  - 1x10^6 número máximo de sesiones

- Un Fortinet Fortigate 501E:
  - 2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots
  - SPU NP6 and CP9 hardware accelerated
  - 2x 240 GB onboard SSD storage

- Un IBM QRadar 3105 All-In-One en proceso de migración hacia un IBM QRadar 3129 All-In-One v7.2.8:
  - El sistema Qradar alimenta de una capa intermedia donde se procesan y centralizan los logs de diferentes dispositivos y aplicaciones. Esta capa intermedia está formada por un cluster de servidores Linux que tienen la función de agrupar logs de diferentes orígenes pero de un mismo tipo formando una única fuente, de esta manera se puede optimizar el sistema Qradar.

4.1.2. Volumetrías actuales

Ver Anexo I: Descripción de la infraestructura tecnológica actual y volumetría del servicio.

4.2 Descripción del Servicio

El proveedor adjudicatario deberá cubrir:

- Servicio regular
- Mantenimiento Evolutivo

4.2.1 Servicio regular

El servicio regular cubrirá las siguientes tareas:

1. Detección, análisis y gestión de vulnerabilidades
2. Gestión y respuesta a incidentes de seguridad de la información (CSIRT)
3. Análisis de malware
4. Análisis forense
5. Mantenimiento, revisión, administración y reporting de la infraestructura de seguridad de la UOC.

4.2.1.1 Detección, análisis y gestión de vulnerabilidades

El proveedor adjudicatario deberá llevar a cabo la gestión integral de las vulnerabilidades de los sistemas de información para protegerlos de posibles amenazas. Se realizará tanto mediante el uso de herramientas automatizadas como con técnicas de pentesting manual.

4.2.1.1.1 Requerimientos sobre la detección, análisis y gestión de vulnerabilidades.

El servicio que deberán licitar los proveedores deberá incluir:

- La identificación de las vulnerabilidades: correrá a cargo del proveedor adjudicatario la adquisición del software y la infraestructura necesaria para poderlo gestionar. La UOC facilitará acceso a su CMDB (AssetExplorer ManageEngine) de la que el proveedor adjudicatario se descargará los datos que precise. No habrá ningún sistema de sincronización entre los dos entornos (de la UOC y del proveedor adjudicatario) más allá de posibles descargas y cargas periódicas.

- La detección de las vulnerabilidades: el proveedor adjudicatario realizará escaneos periódicos de vulnerabilidades en un número mínimo de 3 al año que abarquen todas las IPs y sistemas de la UOC. El proveedor adjudicatario dispondrá de las herramientas necesarias para poder efectuar estos escaneos, los cuales deberán tener un nivel de falsos positivos muy bajo (inferior al 10% de las detecciones).

- Las metodologías: el proveedor adjudicatario utilizará metodologías reconocidas y fiables para la realización de las auditorías como: OSSTM de ISECOM y OWASP. Para la gestión de las vulnerabilidades, incluyendo las configuraciones inadecuadas y las vulnerabilidades encontradas durante el proceso del servicio, se documentarán y clasificarán de acuerdo con bases de datos del conocimiento tales como CVE, CWE, CVSS y CAPEC para facilitar a la UOC la lectura y comprensión de las debilidades encontradas.

- Mitigación de las debilidades encontradas: hará referencia a la planificación y notificación de las medidas correctoras propuestas por el proveedor adjudicatario para mitigar las debilidades detectadas. Entre otras tareas incluidas estará la depuración de los falsos positivos.

- Actividades: todas las actividades en el transcurso del proceso de detección y análisis de vulnerabilidades se hará en el modo de "Caja Negra o Caja Gris". Este módulo o apartado se compone de las siguientes tareas:
    - Planificación.
    - Presentación y aprobación a los responsables UOC.
    - Configuración de las herramientas.
    - Ejecución.
    - Análisis de los resultados.
    - Revisión detallada.
    - Descartado de falsos positivos.
    - Elaboración de los informes y presentación en la UOC.

- Consideraciones a las actividades: no se harán ataques de DoS, se deberán prever los posibles impactos en el servicio que se pudieran derivar de las acciones llevadas a cabo en la realización de la auditoría, los horarios estarán definidos por la UOC y autorizados por los responsables de servicio. La UOC proporcionará una persona o teléfono de contacto durante el tiempo que dure la realización de las pruebas. La UOC se compromete siempre que sea posible proporcionar usuarios de prueba válidos para el acceso a la aplicación.

- Entregas: para cada uno de los trabajos de detección, análisis y gestión de vulnerabilidades el proveedor adjudicatario entregará:
    - Un informe ejecutivo.
    - Un informe técnico de las debilidades encontradas y su clasificación.
    - Un informe con la documentación de las pruebas realizadas.
    - Un informe documentando las recomendaciones de seguridad.
    - Una descripción de las vulnerabilidades encontradas con su correspondiente evidencia.
    - Un estudio del impacto en la CID (confidencialidad, integridad, disponibilidad).
    - Una explicación de la metodología seguida para explotar las vulnerabilidades.
    - Un informe con la descripción de las contramedidas a aplicar que mitiguen o eliminen el riesgo asociado a la explotación de las vulnerabilidades.

- Un informe, en su caso, con los proyectos o actividades que habría que realizar para minimizar los riesgos detectados.

4.2.1.1.2 Acuerdos de Nivel de Servicio Sobre la detección, análisis y gestión de vulnerabilidades

Código	Indicador	Tiempo de respuesta (días naturales)	% Nivel de cumplimiento
ANS_4.2.1.1.a	**Tiempo de respuesta a la petición bajo demanda de ujn análisis de vulnerabilidades**	**7 días**	**> 90 %**
ANS_4.2.1.1.b	**Entrega de los informes**	**10 días desde la finalización de las tareas de análisis.**	**> 90 %**

4.2.1.2 Gestión y respuesta a incidentes de seguridad de la informació (CSIRT)

El proveedor adjudicatario hará la gestión y respuesta a incidentes de seguridad a petición de la UOC.

El proveedor adjudicatario proporcionará los recursos humanos especializados en función de la tipología del incidente, así como los procedimientos y las herramientas para mitigar de la forma más rápida y eficiente posible el ataque o la amenaza.

El proveedor adjudicatario deberá dar cobertura, como mínimo, a las siguientes tipologías de incidentes:

- Infecciones por malware en general.
- Ataques de invasión.
- DDoS.
- Defacement.
- Phising.
- Hacking: cualquier actividad o tráfico sospechoso que pueda alterar el funcionamiento del sistema y que esté relacionado con un intento de intrusión.
- Fraude utilizando medios tecnológicos.
- Violación de las políticas de seguridad.

- Intrusiones en servidores o puntos de trabajo.
- Escape de datos / fuga de información confidencial.
- Ransomware en puntos de trabajo y servidores.
- Monitorización de logs.

El servicio deberá incluir acciones especiales para el caso en que el incidente tenga afectación sobre datos personales. En caso de declaración de brecha de seguridad, siguiendo las instrucciones del artículo 33 del RGPD, el proveedor adjudicatario confeccionará o colaborará en la redacción de los informes técnicos y para el DPD UOC.

Las incidencias de nivel bajo y medio serán cubiertas únicamente en horario laboral. Las incidencias críticas serán cubiertas en horario 24x7.

4.2.1.2.1 Tipología de incidentes en función de la criticidad

1) Criticidad alta:

- **En general**: Aquellas incidencias que tienen un impacto considerable (afectación a la confidencialidad, disponibilidad e integridad) a información considerada crítica para la actividad de la organización y / o sistemas TIC críticos (elementos de seguridad perimetral de red, sistemas de autenticación centralizada, etc.). El incidente tiene capacidad de afectar información valiosa, en cantidad considerable.

- Se clasificarán con nivel crítico los casos de incidentes en los que se tenga constancia de la existencia de una amenaza que ha afectado o está afectando a los sistemas TIC de la UOC y se sabe que ha tenido un impacto más que considerable (afectación total de la confidencialidad, disponibilidad o la integridad) en información considerada crítica para la misión de la UOC y / o de los sistemas TIC críticos dentro de la arquitectura de sistemas UOC (vg. elementos de seguridad perimetral, sistemas de autenticación centralizada, fugas masivas de datos, compromiso del backoffice, infecciones masivas o de más del 80% de los equipos, etc).

  Estos incidentes suelen causar la degradación de los servicios vitales de la UOC para un gran número de usuarios, implican una grave violación de seguridad de la red, afectan a los equipos vitales o servicios, o pueden dañar la confianza pública en nuestra organización, o incluso podrían afectar a la seguridad física de las personas, causar una pérdida irreversible de los recursos de la UOC, resultando finalmente en cargas penales, sanciones y multas reglamentarias o generar una mala publicidad de forma inadecuada para la UOC.

2) **Criticidad Media**:

- **En general**: El incidente tiene un impacto medio (afectación a la confidencialidad, disponibilidad o integridad) a información considerada no crítica para la actividad de la organización y / o sistemas TIC no críticos (eg. Equipos de usuarios).

- Se clasificarán dentro de este nivel los casos de incidentes en los que se tenga constancia de la existencia de una amenaza que ha afectado o que está afectando a los sistemas TIC de la UOC y se sabe que han tenido un impacto considerable (afectación a la confidencialidad, disponibilidad o la integridad) en aquella información considerada crítica para la misión de la UOC y / o de los sistemas TIC críticos dentro de la arquitectura de sistemas UOC (vg. elementos de seguridad perimetral, sistemas de autenticación centralizada, etc).

  Estos incidentes pueden afectar a la integridad o la confidencialidad de los datos, lo que puede convertirse en la pérdida o degradación del servicio, la misión, el negocio y / o la reputación de la UOC.

  Un incidente que represente una amenaza para un número limitado de sistemas, puede poner en riesgo los sistemas considerados no críticos o sensibles y suponer un esfuerzo de gestión considerable para los responsables de los sistemas.

3) **Criticidad baja**:

- **En general**: Incidentes con impacto nulo. Los controles de seguridad implantados han funcionado y contrarrestan adecuadamente el incidente de seguridad. La afectación a un volumen apreciable de información es escasa o nula.

- O referido a incidentes con un impacto limitado a información considerada no crítica para la actividad de la organización y / o sistemas de información no críticos (equipos de usuarios), pero con un volumen de afectación de información notable o apreciable.

- Clasificaríamos con este nivel de criticidad los casos de incidentes en los que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a los sistemas TIC de la UOC y se sabe que ha tenido un impacto limitado en referencia a información considerada no crítica para la misión de la UOC y que ha podido afectar a sistemas TIC no crítica dentro de la arquitectura

de sistemas TIC UOC (vg. equipos de usuario, afectaciones mínimas en bloques o CMS no institucional, etc).

- La UOC se presupone que ya debería estar capacitada para gestionar estos incidentes y tener controles que los eliminen o limiten los riesgos.

- Son incidentes que en principio no es necesario reportar especialmente en organismos oficiales. No obstante si serán reportados de forma periódica a los órganos de dirección y coordinación UOC para poder aumentar la comprensión de los riesgos que pueden afectar a la UOC.

4.2.1.2.2 Afectación a datos de carácter personal

Siempre que haya un incidente con afectación a datos personales que pueda ser susceptible de declaración de brecha de seguridad hacia alguna de las Agencias de Protección de Datos, el proveedor adjudicatario presentará un primer informe por DPO y otro para la agencia correspondiente en un plazo máximo de 48h naturales.

El proveedor adjudicatario deberá prestar este servicio en modalidad de 24x7. Y entre otros será necesario que incluya:

- La gestión y la respuesta a los incidentes de seguridad tal y como se ha explicado anteriormente en este capítulo.

- Las actuaciones necesarias para poder dar respuesta a las agencias de protección de datos en caso de que el incidente contenga una brecha de seguridad.

- Todo el apoyo técnico y humano necesario para la resolución del incidente, las medidas de contención, erradicación y recuperación necesarias

- Todos aquellos análisis que sean necesarios.

4.2.1.2.3 Metodología

El proveedor adjudicatario utilizará la metodología propuesta por el CCN-CERT para la gestión de ciberincidentes en el marco del Esquema Nacional de Seguridad (ENS) y que está detallada en las guías CCN-STIC-403 y CCN-STIC-817.

4.2.1.2.4 Gestión de los incidentes, peticiones y tareas

La UOC dispone de una herramienta de ticketing y bug-tracking basada en Atlassian JIRA y OneTrust. Esta herramienta concentra y centraliza la recepción y gestión de todas las incidencias - en genérico - de seguridad.

El proveedor adjudicatario podrá escalar estos issues al equipo técnico UOC siempre que su conocimiento interno de UOC para poder resolverlos escape a sus posibilidades.

4.2.1.2.5 Acuerdos de nivel de servicio sobre los incidentes de seguridad

Código	Indicador	Tiempo de respuesta (horas naturales)	% Nivel de cumplimiento
ANS_4.2.1.2.a	Tiempo de intervención en las dependencias de la UOC (sólo en caso de necesidad)	< 4h	> 95 %
ANS_4.2.1.2.b	Tiempo de respuesta en caso de incidencia de criticidad alta	2h	> 90 %
ANS_4.2.1.2.c	Realización de análisis preliminares de los incidentes de nivel criticidad alto	4h	> 90 %
ANS_4.2.1.2.d	Tiempo entrega de los informes en caso de incidencia de nivel alto / crítico	8h después de cerrarse el incidente	> 95 %
ANS_4.2.1.2.e	Tiempo máximo de entrega de los informes en caso de declaración de brecha de seguridad	40h desde ANS4.2.1.2.b	> 100%
ANS_4.2.1.2.f	Tiempo de respuesta en caso de incidencia de criticidad media.	12h	> 90 %
ANS_4.2.1.2.g	Realización de análisis preliminares en caso de incidentes de nivel criticidad medio	10h	> 90 %
4.2.1.2.h	Tiempo de respuesta en caso de incidencia de criticidad baja.	18h	> 90 %
4.2.1.2.i	Realización de análisis preliminares en caso de incidentes de nivel criticidad baja	24h	> 90 %

4.2.1.3 Análisis de malware

El proveedor adjudicatario, a petición de la UOC, realizará análisis de artefactos con potencial de malware. Los artefactos podrán ser binarios y scripts de Windows, Linux, Android y iOS con los diferentes niveles de complejidad: estáticos, dinámicos, Sandboxing, reversing ... etc.

A partir de las muestras de malware proporcionadas, si así fuera el caso, el proveedor adjudicatario devolverá un análisis técnico de las muestras (IOC Indicadores de Compromiso).

4.2.1.3.1 Requerimientos sobre el análisis de malware

En el análisis de muestras de malware se incluirán:

- Los IoCs (también en forma de reglas YARA) necesarios para poder actualizar la infraestructura de seguridad de la UOC.
- Los mecanismos de propagación.
- El propósito y todo aquello susceptible de ser incluido en una lista negra:
    - Dominios.
    - IPs.
    - Firmas de código para poder ser incluidas en TrendMicro IPS 660N.
    - URLs.
    - Otros

El proveedor adjudicatario facilitará a la UOC el análisis de artefactos en modalidad 8x5.

Entregables e informes asociados al servicio de análisis de malware:

- Análisis de las URLs con posible phising o malware en general
- Análisis ligero de artefactos en plataformas de Sandboxing
- Informe e interpretación básico de los resultados del análisis, es decir, los IoCs inmediatos (hashes, dominios, URLs, IPs de C & C), análisis completo manual y estático y IOCs lo más completos posibles (hashes, dominios, IPs de C&C, protecciones detectadas, persistencia en el SO, mecanismos y filtros de limpieza, etc).

4.2.1.3.2 Acuerdos de nivel de servicio sobre el análisis malware

Código	Indicador	Tiempo máximo de respuesta (días laborables)	% Grado de cumplimiento

ANS_4.2.1.3	**Tiempo de entrega del informe bajo demanda de análisis de malware**	**2 días**	**> 90 %**

4.2.1.4 Análisis forense

El proveedor adjudicatario, a petición de la UOC, realizará análisis forenses de determinados elementos. En este sentido, deberá aplicar técnicas científicas forenses y analíticas sobre el escenario de un incidente de seguridad y que debe permitir identificar, preservar, analizar y presentar un informe con los datos que sean válidos tanto desde el punto de vista de una investigación interna como desde el punto de vista de la inmersión en un proceso penal y de peritaje.

4.2.1.4.1 Requerimientos sobre el análisis forense

- **Tipología de peticiones que habrá que cubrir por parte del proveedor adjudicatario**:

- Peticiones formales de información tanto a partir del sistema SIEM UOC como de diferentes fuentes de información estructurada o no (vg. Sistemas de archivos)
- Gestión de las cadenas de custodia.
- Clonados forenses. Entendiendo por tales aquellos que son obtenidos mediante un método certificado y donde una empresa tercera avala la obtención de los datos.
- Duplicados de información. Cuando el perito no puede realizar un clonado forense y se le han facilitado unos datos sin poder verificar su autenticidad.
- Almacenamiento y custodia de soportes de información y datos.
- Investigación de sucesos informáticos sobre las fuentes de información aportados.
- Cuantificación no sólo de los daños informáticos sufridos sino también de los económicos y reputacionales.
- Recuperación de datos borrados, corruptos, en soportes inestables o escondidos, recuperación de datos frente a desastres tipo Ransom.

- Realización de todos aquellos procedimientos orientados a la ejecución por el grupo de Sistemas necesarios para la generación de imágenes procesables (disco y / o memoria) en cualquiera de sus formas: máquina física, máquina virtual, servicio de virtualización, cloud computing, contenedores, etc.

- Realización de todos aquellos procedimientos orientados a la ejecución de la captura, recogida y preservación de evidencias forenses en estaciones de trabajo Windows, Linux o MacIntosh.

- Realización de todos aquellos procedimientos orientados a la ejecución de la captura, recogida y preservación de evidencias forenses en dispositivos móviles, tanto Android como iOS.

- **Entregables relacionados con el servicio de análisis forense**:

- Realización de informes técnicos a raíz de una investigación.

- Desarrollo y realización de informes periciales en caso de un posible delito o que se tenga que acreditar la actividad ocurrida ante un tribunal de justicia.

- Desarrollo de informes adhoc por el Delegado de Protección de Datos UOC y las agencias estatales y autonómicas de protección de datos.

- Certificaciones informáticas de hechos, acontecimientos, estados, publicaciones, etc, al estilo fe notarial, pero con los medios informáticos forenses.

4.2.1.4.2 Acuerdos de nivel de servicio sobre el análisis forense

Código	Indicador	Tiempo de respuesta (días laborables)	% Grado de cumplimiento
ANS_4.2.1.4	Tiempo de entrega del informe bajo demanda de análisis forense.	3 días	> 95 %

4.2.1.5 Mantenimiento, revisión, administración y reporting de la infraestructura de seguridad de la UOC

La UOC dispone de infraestructuras de seguridad sobre las que el proveedor adjudicatario deberá dar servicio de forma personalizada para cada tipo de dispositivo.

El proveedor adjudicatario se responsabilizará del correcto funcionamiento de la configuración de los elementos de seguridad de la UOC relacionados en el punto 4.1.1 (Infraestructura hardware de seguridad actual de la UOC).

Para garantizar este correcto funcionamiento, el proveedor adjudicatario efectuará tareas de mantenimiento y revisión de las políticas, reglas y configuración de los dispositivos. El proveedor adjudicatario, en ningún caso, operará directamente estas infraestructuras, sino que dará instrucciones hacia el servicio de operación de la UOC.

El equipo técnico de la UOC podrá realizar consultas y peticiones relacionadas con la colaboración en cambios de configuración, actualizaciones e instalaciones sobre la infraestructura de seguridad.

4.2.1.5.1 Requerimientos sobre el mantenimiento, revisión, administración y reporting de la infraestructura de seguridad de la UOC

-**Tareas mínimas a realizar por dispositivo**: El proveedor adjudicatario explicitará en su propuesta que cumple con los mínimos requerimientos explicados aquí y podrá citar tantas opciones de mejora como crea convenientes.

El proveedor adjudicatario se compromete a realizar las siguientes tareas de mantenimiento sobre la infraestructura de seguridad UOC:

1. **ARBOR Pravail:**

- El proveedor adjudicatario revisará diariamente la consola de gestión del dispositivo buscando mal funcionamientos, avisos y errores. En caso positivo generará las correspondientes órdenes de trabajo al grupo operativo o al proveedor correspondiente.

- Revisión diaria de las gráficas de bloqueos buscando anomalías en caso de que no hayan aparecido bloqueos destacables o alertas.

- Revisará semanalmente los umbrales de ancho de banda - Traffic Thresholds - los grupos de protección que tiene establecidos la UOC (6 en el momento de escribir este pliego). La corrección de los umbrales se discutirá en las reuniones semanales. Sin embargo de forma semanal elaborará informes de los eventos generados en el dispositivo que serán discutidos en las reuniones de seguimiento. El proveedor adjuducatario propondrá, si es necesario, acciones de mejora.

- Revisión bajo demanda (máximo 1 vez al mes) de la configuración de los grupos de protección - Inbound Protection Groups -.

- Revisión y actualización mensual de los Profile Capture los 6 grupos de protección en Inbound que tiene actualmente la UOC (en el momento de escribir este pliego).

- Revisión bajo demanda (máximo 1 vez bimensualmente) de los informes del servidor.

- Bajo demanda el proveedor adjudicatario se encargará de la captura de paquetes en caso de conflicto o investigación, así como de su estudio y posterior informe.

2. **TrendMicro TippingPoint 660N:**

- Revisión diaria de los eventos más destacados por nivel de severidad. El proveedor adjudicatario revisará diariamente la consola del dispositivo buscando malfuncionamientos, avisos y errores del mismo. Generará las correspondientes órdenes de trabajo al grupo operativo o proveedor en caso de avería o mal funcionamiento.

- Revisará diariamente los eventos generados por el dispositivo buscando patrones o cualquier otro tipo de indicio que pueda significar la existencia de un riesgo o vulnerabilidad. Siguiendo el procedimiento establecido, actuará en consecuencia o derivará la tarea al grupo operativo correspondiente.

- Elaboración de propuestas de cambio o mejora en las políticas del dispositivo, por tipo de tráfico. Estas propuestas podrán ser provenientes del personal de la UOC o del propio proveedor adjudicatario. Se revisarán, propondrán e implementarán a partir del comité de seguimiento y los clínicos semanales. No hay una cadencia preestablecida y se harán a medida que se detecte su necesidad.

- En caso de urgencia, el proveedor adjudicatario las implementará de forma inmediata.

- Elaboración de informes a partir de los acontecimientos generados y revisión de los mismos. La cadencia mínima para esta tarea será semanal. Estos informes

serán discutidos semanalmente en las reuniones de seguimiento y el proveedor adjudicatario deberá proponer acciones de mejora.

- Revisión de los Responders y mantenimiento de los mismos. Esta tarea no tiene cadencia y se ejecutará según necesidad. La UOC hace notar que en general esta tarea es bastante infrecuente.

- Participación en las reuniones del grupo de sistemas para poder revisar la pertenencia o no de la necesidad de recablear el dispositivo en caso de cambios en la red UOC.

3. Firewalls Palo Alto i Netscreen:

- El proveedor adjudicatario, como primera tarea, ayudará a definir un procedimiento organizativo de flujo de aprobaciones de cambios en las políticas de firewalling en la UOC.

- El proveedor adjudicatario confeccionará un mapa sencillo de reglas o catálogo fácilmente consultable. Esta tarea sólo se hará una vez por parte del adjudicatario. El adjudicatario podrá utilizar las herramientas que crea necesario para automatizar al máximo las tareas.

- Análisis y propuesta de mejora a nivel funcional de las políticas de los diferentes dispositivos.

- Realización de informes de actividad maliciosa detectada en los dos cortafuegos (NGF). Sólo a petición y en caso de necesidad.

- Análisis y captura de paquetes en los dos dispositivos en caso de detección anómala de tráfico o en combinación con tareas de detección de malware o de respuesta a incidentes de seguridad.

- El proveedor adjudicatario podrá ser solicitado para que le sean hechas consultas sobre la configuración de algunas de las reglas.

4. IBM QRadar:

- El proveedor adjudicatario revisará diariamente la consola del dispositivo buscando mal funcionamientos, avisos y errores. En caso positivo, generará las correspondientes órdenes de trabajo al grupo operativo o proveedor correspondiente.

- Revisión diaria de las ofensas que detecta el dispositivo. El proveedor adjudicatario, una vez descartado los falsos positivos, generará los tickets de trabajo necesarios para que dichas ofensas sean resueltas por el grupo operativo UOC correspondiente.

- Revisión y mantenimiento de los dashboards de QRadar bajo demanda.

- Revisión y mantenimiento de las fuentes de log. El proveedor adjudicatario se encargará de incorporar las nuevas fuentes de log que le sean notificadas desde la UOC. Esta tarea no sobrepasará nunca el número de 10 fuentes de log nuevas al mes.

- El proveedor adjudicatario se encargará del mantenimiento de los diferentes sub-sistemas y servicios de QRadar: Network Hierarchy, Index Management, Asset Profiler, Custom Asset Properties, DSM Editor, Log Sources, Custom Event Properties, Event Retention, User Behavoir. Este mantenimiento tendrá una periodicidad quincenal.

- El proveedor adjudicatario gestionará los informes que se pueden generar desde el mismo dispositivo QRadar. La propuesta de informes saldrá de las reuniones de trabajo entre el personal de la UOC y el proveedor adjudicatario. Este será el encargado de implementarlos y validarlos.

- El proveedor adjudicatario realizará las tareas de mantenimiento pertinentes sobre el sistema de pre-procesado de logs mencionado anteriormente en el párrafo 4.1.1 en la descripción de los dispositivos, garantizando de esta forma el correcto funcionamiento y proporcionando la monitorización necesaria. Estas tareas tendrán periodicidad semanal.

Parte de este equipamiento relacionado podría ser sustituido durante la prestación de este servicio, a fin de dar respuesta a necesidades técnicas o de obsolescencia. Serán sustituidos por equipos del mismo fabricante o de otro, pero siempre de la misma tipología (AntiDDOS, IPS, Firewalls, SIEM). Este hecho no conllevará ningún cambio en la prestación del servicio, debiéndose adaptar el proveedor adjudicatario para poder seguir dando el mismo servicio sobre el equipo sustituido con las mismas garantías y compromisos y sin que ello conlleve modificación de las condiciones del servicio.

4.2.1.5.2 Acuerdos de nivel de servicio sobre el mantenimiento, revisión, administración y reporting de la infraestructura de seguridad de la UOC

Estos acuerdos de nivel de servicio están fuera de la periodicidad recurrente especificada en los párrafos anteriores de este apartado 4.2.1.5.1.

Código	Indicador	Tiempo de respuesta (días laborables)	% Nivel de cumplimiento
ANS_4.2.1.5.a	**Tiempo de respuesta para peticiones de colaboración**	**2 días**	**> 95 %**
ANS_4.2.1.5.b	**Tiempo de respuesta sobre consultas**	**2 días**	**> 95 %**

4.2.2. Mantenimiento Evolutivo

El servicio de seguridad de la UOC dispondrá de una partida alzada por la realización de tareas bajo demanda según las necesidades evolutivas de cada momento y relacionadas con el servicio regular. Estas tareas irán destinadas a apoyar a la UOC en la prevención, la gestión y la respuesta frente a incidentes de seguridad de la información.

Procedimiento ante una petición:

1. La UOC hará la petición de colaboración al proveedor adjudicatario con los requerimientos particulares sobre perfiles y tareas.

2. El proveedor adjudicatario deberá hacer una propuesta en un plazo máximo de 2 semanas que posteriormente deberá ser validada por la UOC. El consumo de recursos repercutirá sobre esta partida alzada.

5. Modelo de relación

Estará basado en la figura del interlocutor / coordinador único que será el responsable de seguridad del servicio del proveedor adjudicatario y que actuará de mediador entre éste y la UOC. Este interlocutor es fundamental para acompañar y apoyar en el establecimiento de las políticas, buenas prácticas y controles de seguridad en el ámbito del servicio.

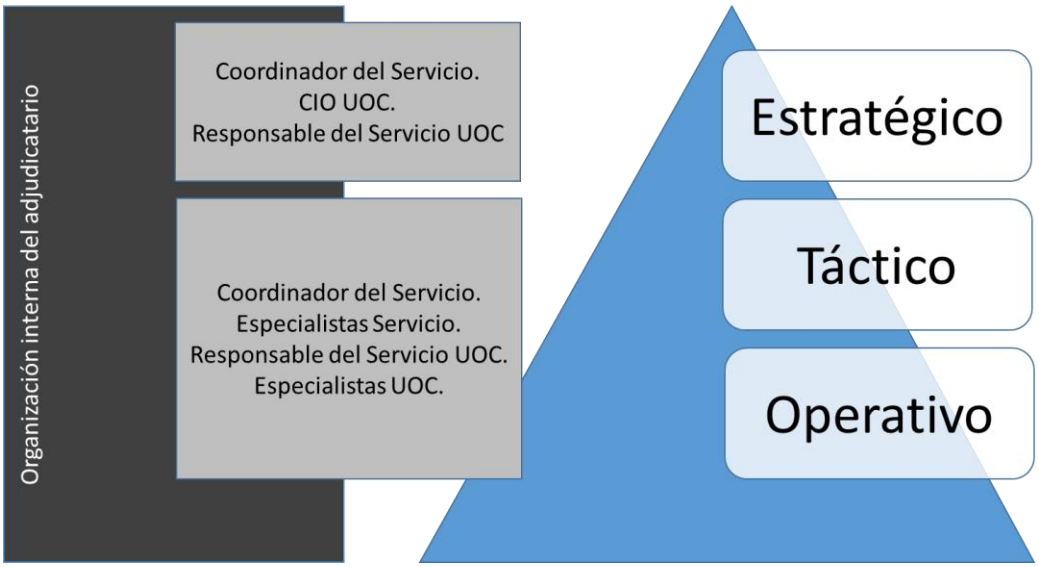
5.1 Modelo organitzativo del equipo de trabajo

El presente servicio objeto de licitación debe permitir cierta autosuficiencia a la hora de contactar, gestionar y resolver cualquier tipo de incidencias o tareas de proyectos que impliquen proveedores externos, sin que la interlocución dependa exclusivamente del responsables de la UOC.

Para dar respuesta a las necesidades planteadas por la UOC, se pide tener un modelo de relación basado en 3 niveles, con el objetivo de:

1. Garantizar el seguimiento y buen gobierno del servicio
2. Maximizar su alineamiento a las necesidades estratégicas y operativas de la UOC mientras dure la prestación del servicio.

Así pues, este modelo organizativo se basa en el establecimiento de una relación entre el proveedor adjudicatario y la UOC en tres niveles:



5.1.1. Nivel estratégico

Se define a nivel estratégico un comité ejecutivo que se reunirá con una periodicidad trimestral con el fin de mantener un punto de contacto a alto nivel para asegurar el buen funcionamiento del servicio contratado. A este nivel, se propone que por parte del proveedor adjudicatario asista un representante institucional o el coordinador del servicio, y por parte de la UOC un representante institucional que podrá ser el CIO o el responsable del servicio UOC.

Los asistentes a este comité tendrán capacidad decisoria sobre los compromisos del mismo y en aquellos aspectos que puedan originar la modificación del servicio.

5.1.2. Nivel táctico

Se proponen reuniones mensuales para poder llevar a cabo un seguimiento del servicio y poder poner en común los puntos que se consideren necesarios exponer. Por parte del proveedor adjudicatario, asistirá el coordinador del servicio y, si fuera necesario, uno o más especialistas de servicio que puedan aportar información relevante del servicio. Por parte de la UOC asistirá el responsable del servicio y los técnicos especialistas.

La finalidad de estas reuniones mensuales será exponer:

- El estado del servicio
- Las principales incidencias que hayan surgido o estén en activo
- La situación de los proyectos y tareas en curso
- Revisión del calendario previsto

5.1.3. Nivel operativo

Se propone una reunión semanal de revisión técnica tipo "clínico" para poder resolver los temas más urgentes que pueda haber y hacer seguimiento técnico de los proyectos y tareas. Por parte del proveedor adjudicatario asistirá el coordinador o los especialistas involucrados si lo desea delegar y por parte de la UOC asistirán los técnicos especialistas de seguridad.

El objetivo básico será tratar las problemáticas específicas que afecten al servicio prestado.

5.2. Funciones de los niveles del modelo organizativo:

Nivel estratégico	● Seguimiento del contrato ● Seguimiento y evaluación del servicio prestado. ● Validar el alcance general, objetivos y resultados esperados. ● Validación de la planificación de las tareas previstas a realizar ● Verificación del cumplimiento de las especificaciones solicitadas. ● Propuestas de modificaciones / ampliaciones de Acuerdos de Nivel de Servicio (ANS) ● Seguimiento económico del contrato.

Nivel táctico	● Validación de las tareas de control de la explotación e implantación de los servicios. ● Aprobación de la ejecución de proyectos y nuevos servicios. ● Verificación del cumplimiento de los ANS. ● Resolución de conflictos.

	• Revisar proyectos de implantación y valorar el grado de ejecución. • Análisis y priorización de tareas. • Validación de los procedimientos de mejora por parte de los Responsables de Seguridad. • Análisis y control del empleo de los perfiles asignados por la consecución del servicio (informe semanal y acumulado mensual). • Revisión de informes de análisis de vulnerabilidades y amenazas.

Nivel operativo	• Seguimiento rutinario. • Propuestas de mejora y cambios. • En caso de identificarse riesgos o cambios significativos en la evolución del servicio se convocan las reuniones operativas para tratar el tema en cuestión. • En caso de evidenciar un riesgo elevado, se procederá a convocar el Comité Estratégico o al Comité Táctico según se considere. • Análisis de incidencias detectadas de los operadores que implican solicitar una reunión operativa. • Análisis de peticiones que impliquen un control detallado debido a un impacto técnico, económico, de ejecución, etc. • El comité podrá ser convocado por iniciativa tanto de UOC como del proveedor adjudicatario. El comité se constituirá en un máximo de 24h desde el momento de la convocatoria.

5.3. Gestión del servicio: planificación y demanda

El objetivo es poder asegurar que el servicio está definido en función de la demanda, que sea correcto en su planificación, capacidad y esté desplegado con los recursos técnicos y humanos necesarios. Podemos considerar la planificación y el control como la gestión del tiempo y la capacidad en su sentido más amplio.

El proveedor adjudicatario pactará con la UOC la entrega de los servicios, tanto en lo que se refiere a los proyectos evolutivos como por las actividades recurrentes o de mantenimiento.

Para la planificación de proyectos la UOC hará llegar al proveedor adjudicatario, en su caso, cada dos meses una planificación con la previsión de proyectos a ejecutar.

5.3.1. Gestión de los incidentes, peticiones y tareas

La UOC dispone de una herramienta de ticketing y bug-tracking basada en Atlassian JIRA y OneTrust. Estas herramientas concentran y centralizan la recepción y gestión de todas las incidencias - en genérico - de seguridad.

La UOC clasifica estos issues en 4 tipos:

- **Incidentes de seguridad:** generados desde el equipo de seguridad o por cualquier otra persona que alerta o notifica de un posible incidente.

- **Notificaciones:** cuando algún otro grupo operativo, especialmente Arquitectura y Sistemas, informa sobre algún cambio notable o que es necesario que desde el rol de ciberseguridad sea conocido.

- **Tarea**: cuando se pide al grupo de seguridad del área de tecnología la elaboración de algún tipo de documento, procedimiento o dictamen.

- **Petición:** Consulta o tarea poco elaborada y de solución rápida.

El proveedor adjudicatario podrá escalar estos issues al equipo técnico UOC siempre que su conocimiento interno de la UOC para poder resolverlos escape a sus posibilidades.

5.3.2. Seguimiento, control y revisión.

- Actividades de control y seguimiento: Son el conjunto de tareas que se harán de forma periódica, mínimo 1 vez cada 15 días y de forma alternada con las tareas de revisión, entre el coordinador único del proveedor adjudicatario y el equipo de seguridad UOC:

- Generación y seguimiento de los indicadores de cumplimiento acordados en la anterior fase.
- Seguimiento de las planificaciones a largo plazo.
- Gestión del apoyo a la formación, definición y elaboración del material de apoyo, en su caso.
- Seguimiento del progreso de las peticiones de cambio. Gestión del riesgo.
- Re-asignación de tareas, ajuste de hitos y reconsideración del alcance de las tareas.
- Informes de seguimiento a nivel ejecutivo y a nivel técnico para la UOC.

- Revisión: Conjunto de tareas que se harán de forma periódica. Mínimo 1 vez cada 15 días y de forma alternada con las tareas de control y seguimiento, entre el coordinador único del proveedor adjudicatario y el equipo de seguridad UOC:

- Evaluación de los resultados obtenidos.
- Recogida, clasificación y aprendizaje.
- Propuestas de acciones de mejora a partir de la evaluación de resultados.

5.3.3. Gestión de la documentación.

El servicio proporcionado por el proveedor adjudicatario se encargará de garantizar la estabilidad y permanencia del conocimiento generado durante el tiempo de prestación del servicio.

Toda la documentación generada y obtenida será tratada según los acuerdos de confidencialidad. Será también propiedad intelectual de la UOC y siempre estará almacenada en los servidores de la UOC.

El área de tecnología proporcionará las herramientas más adecuadas para la gestión de esta documentación.

5.4 Horario

El proveedor adjudicatario deberá cubrir los horarios de lunes a viernes entre las 9:00 AM y las 18:00 PM, incluido el periodo vacacional donde se mantendrá operativo el servicio.

El proveedor adjudicatario cubrirá fuera del horario laboral definido la recepción y resolución de incidentes de nivel crítico alto.

El calendario laboral de los servicios será el mismo que el de la UOC.
Enlace al calendario laboral de la UOC:

http://cv.uoc.edu/webapps/intrauoc2/documents/10530/2813754/Calendari+laboral+SEUS+UOC+2019_Festius+estatals%2C%20auton%C3%B2mics+i+locals/96291554-15d6-4e04-b14c-8bac3ad2448a

5.5 Localización física

Preferentemente, los profesionales que formen parte del servicio estarán ubicados en las oficinas del propio proveedor adjudicatario. Es voluntad de la UOC poder facilitar que el proveedor adjudicatario realice la mayor parte de las tareas y las reuniones de forma

virtual utilizando herramientas de videoconferencia, herramientas colaborativas o de conectividad segura tipo VPN.

Sólo serán de presencialidad obligada en alguna de las dependencias de la UOC:

- Las reuniones de nivel estratégico, táctico y operacional.
- Las incidencias de seguridad de nivel alto.
- Las tareas que requieran la realización de entrevistas o recogida de evidencias físicas.
- Y todas aquellas tareas en que no sea posible el uso de la virtualidad para la realización de las mismas.

En cualquier momento durante la ejecución del contrato, la UOC se reserva el derecho de solicitar que la prestación temporal del servicio se ubique en sus instalaciones o bien en alguna ubicación designada por la UOC.

En caso de presencialidad, el servicio cubrirá alguna de las siguientes direcciones, pero preferentemente el llamado Edificio de Castelldefels:

- Edificio Castelldefels. Parque Mediterráneo de la Tecnología. Avenida Carl Friedrich Gauss 5, 08860 Castelldefels.
- Edificio Tibidabo. Avenida Tibidabo 39-43, 08035 Barcelona.
- Edificio 22 @. Rambla del Poblenou 156, 08018 Barcelona.

En caso de que la UOC, durante la vigencia del contrato, haga un cambio de sede, de alguna de las anteriores a otro edificio, y siempre que esta nueva ubicación esté dentro de la provincia de Barcelona, el proveedor adjudicatario se compromete a cubrir el servicio sin repercutir ningún coste adicional a la UOC.

5.6. Recursos asignados al servicio

El número de recursos asignados por parte del proveedor adjudicatario deberá ajustarse permanentemente a las necesidades de la UOC, de acuerdo con la volumetría del servicio de seguridad expresada en el punto 4.1.2 y el Anexo I de este pliego de prescripciones técnicas.

El proveedor adjudicatario deberá 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.

Las horas detalladas a la volumetría del anexo I constituyen las horas mínimas a las que el proveedor adjudicatario deberá comprometerse por tipología de tarea.

A continuación se detallan los perfiles que el proveedor adjudicatario deberá asignar al servicio:

- Coordinador del servicio de seguridad.
- Especialistas.

5.6.1 Coordinador del servicio de seguridad:

Será el interlocutor único ante la UOC y será el responsable de garantizar que la prestación del servicio es correcta. Es decir, garantizará el servicio asegurando la optimización del mismo y por tanto minimizando los posibles riesgos.
Deberá realizar principalmente siguientes funciones:

- Garantizar la entrega del servicio, tal y como se especifica en este pliego, asegurando todos y cada uno de los tiempos de respuesta solicitados y que la UOC pueda requerir.
- Coordinar y supervisar de forma periódica el equipo a su cargo, comunicando en su caso los posibles cambios en éste, así como sus causas.
- Gestión de los riesgos detectados así como la presentación del plan de mitigación de los mismos.
- Detectar oportunidades de mejora.
- Participar en las reuniones de seguimiento y reporting.

Para las tareas a realizar se condiera una dedicación promedio de:

Requerimiento.	Periodicidad promedio.	Horas/año.
Coordinación del servicio	3 horas/semana	156

5.6.2 Especialistas:

Los especialistas serán los técnicos asignados al servicio por el proveedor adjudicatario que llevarán a cabo las tareas y actuaciones que requieran una especialización técnica para poder garantizar un resultado satisfactorio.

El equipo del proveedor adjudicatario que prestará el servicio a la UOC contará con trabajadores que tengan perfiles de especialista al menos en los siguientes ámbitos:

- Técnico especialista en hacking ético y pentesting.
- Auditor en seguridad de la información y continuidad de negocio.
- Profesional certificado en seguridad de la información.
- Técnico especialista en respuesta a incidentes de seguridad de la información.
- Técnico especialista en gestión y administración de sistemas SIEM.

Tanto el coordinador del servicio como los perfiles especialistas asignados al servicio deberán cumplir los requerimientos expresados en el apartado de solvencia técnica del PCP.

6. Fases de la prestación del servicio

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

1. Auditoría
2. Transformación del servicio
3. Evolución del servicio. Fase de ejecución
4. Devolución del servicio

6.1. Auditoría

Esta auditoría se inciará inmediatamente después de la formalización del contrato y deberá haber finalizado en un plazo máximo de 30 días naturales desde la fecha de la formalización.

La UOC facilitará al proveedor adjudicatario toda la información de los activos y recursos implicados, detalle de los servicios actuales, tecnologías, redes, infraestructuras, conocimiento del negocio, etc. Igualmente, la UOC organizará el proceso de acceso a los usuarios con el fin de coordinarlo de la forma más eficaz posible.

Los resultados y las conclusiones de esta auditoría serán entregadas en la UOC, que podrán incorporar, de forma suficientemente justificada en función de los resultados, cambios en:

- Las volumetrías
- Las planificaciones y los plazos

La UOC mostrará su acuerdo o desacuerdo con las conclusiones y los cambios propuestos. En cualquier caso será la UOC la que decida, finalmente, qué cambios y qué consideraciones considera aceptadas. Estas conclusiones o consideraciones podrán ser incorporadas al contrato.

A la finalización de esta auditoría, el proveedor adjudicatario deberá disponer de un plan, aprobado por la UOC, que implementará durante la fase de transformación del servicio.

6.2. Transformación del servicio

En esta fase, el proveedor adjudicatario procederá a ejecutar:

- Todas las actividades previstas dentro de este servicio, en base a los requerimientos de este pliego.
- Los compromisos incorporados por el proveedor adjudicatario en su oferta
- Los acuerdos post-auditoría entre el proveedor adjudicatario y la UOC.
- Los mecanismos de control requeridos en este pliego más los comprometidos en la oferta.
- Escribir y ejecutar los procedimientos de operación y gestión del servicio.

El proveedor adjudicatario ejecutará dentro del primer mes de esta fase y de forma previa a la ejecución real de las tareas del Servicio Gestionado de Seguridad:

- La definición de los objetivos, los ámbitos de servicio objeto de la prestación y la revisión y consolidación de los niveles de servicio definidos en este pliego.
- El desarrollo de estos objetivos dentro de las actividades definidas en este pliego.
- La identificación de los riesgos, las medidas apropiadas y valorar la capacidad disponible y necesaria.
- La elaboración del documento de planificación integrada de todo el servicio.
- Los protocolos para la gestión de cambios en el alcance funcional o tecnológico.

La UOC quiere transformar su servicio interno de seguridad para evolucionarlo hacia un servicio más gestionado que no sea tan dependiente de los recursos técnicos dedicados.

En esta línea, la UOC pedirá al proveedor adjudicatario, dentro del proceso de mejora continua, propuestas para la transformación de parte de la actividad, que actualmente sea dependiente de personal técnico interno, en procesos automáticos o en actividad asumida por los equipos del proveedor adjudicatario. El proveedor adjudicatario implementará estas propuestas una vez sean validadas por la UOC.

La línea de trabajo del proveedor adjudicatario debe ser simplificar progresivamente las tareas, procedimientos y protocolos con la intención de que estos puedan ser asumidos o ejecutados por personal no dedicado al servicio. Sin embargo, se espera la procedimentación y la automatización del máximo número de tareas regulares.

Esta fase finalizará en el momento que el proveedor adjudicatario haya puesto en marcha o definido todas las tareas previstas en el servicio regular relacionadas en el apartado 4.2.1 de este pliego y cuando la UOC haya dado su visto bueno.

La duración de esta fase no será superior a 2 meses.

6.3. Evolución del servicio. Fase de ejecución

El proveedor adjudicatario deberá presentar mecanismos que permitan asegurar la evolución del servicio tanto desde el punto de vista tecnológico, como de gobernanza o incorporación de nuevas funcionalidades y tareas.

Los mecanismos de evolución deben incluir información detallada sobre las pautas de activación, instrumentos de seguimiento, integración de tareas y procedimientos de forma tanto reactiva como proactiva por parte del proveedor adjudicatario.

Además de los criterios generales, los mecanismos de evolución deben tener en cuenta la incorporación de nuevas funcionalidades que no se hayan previsto inicialmente o que la evolución del mercado y de la demanda hagan que la UOC decida incorporarlas (nuevos servicios en la nube, nuevas aplicaciones, etc).

6.4. Devolución del servicio

El proveedor adjudicatario incluirá en su propuesta un plan de devolución del servicio detallado que incluya y describa:

1. Las obligaciones y tareas que deberán ser desarrolladas por cada una de las partes en relación con la devolución.
2. Los términos y condiciones en que se realizará esta devolución.

El plan de devolución deberá cumplir con los siguientes principios y contenidos:

- El plazo de ejecución será de 2 meses desde la notificación oficial de expiración o cancelación, total o parcial, del servicio. El proveedor adjudicatario deberá poner en práctica el plan de devolución que haya incluido en su oferta. La UOC se reserva el derecho de poder reducir el plaso de ejecución según considere necesario.

- Deberá incluir medodología de transferencia y conocimiento de los aspectos fundamentales de operaciones y proyectos en curso y que, como mínimo, describirá:

    - La asistencia, formación y documentación sobre los procedimientos de negocio o sistemas de seguridad de la UOC al nuevo proveedor adjudicatario.
    - El acceso al hardware, el software, la información, la documentación y demás material utilizado por el proveedor adjudicatario o la UOC en la provisión del servicio.
    - La formación práctica tutelada, en la que el personal designado por la UOC realice los trabajos propios de cada proceso o funcionalidad, tutelados por el personal del proveedor adjudicatario.

- El proveedor adjudicatario deberá ofrecer toda la ayuda en la transferencia a la UOC, o a terceras partes nombradas por él mismo, de los servicios subcontratados, garantías o contratos de mantenimiento existentes, hasta el momento de la terminación en los mismos términos pactados con los adjudicatarios de este.

- Durante el primer mes de la fase devolución el proveedor adjudicatario será completamente responsable de mantener los mismos niveles de servicio que en la fase regular del servicio.

- Durante el segundo mes de la fase de devolución el proveedor adjudicatario saliente acompañará al nuevo proveedor adjudicatario y dará soporte con los siguientes recursos mínimos, garantizando la cobertura en todos los ámbitos tecnológicos actuales:

    1 x Especialista

- El proveedor adjudicatario deberá ofrecer un plan para definir las responsabilidades y gestionar la resolución de problemas entre el nuevo proveedor adjudicatario y la UOC.

- Durante el primer mes del periodo de devolución del servicio, el proveedor adjudicatario saliente seguirá siendo responsible del cumplimiento de los acuerdos de nivel de servicio. El plan de devolución no debe causar ninguna discontinuidad en el servicio.

Anexo I: Descripción de la infraestructura tecnológica actual y volumetría del servicio.

El servicio actual que dispone la UOC tiene como finalidad la explotación de los recursos tecnológicos (recursos informáticos, infraestructuras de sistemas, comunicaciones y aplicaciones informáticas) ubicados en los diferentes centros de la UOC.

La descripción de las infraestructuras tecnológicas actuales de la UOC, y la volumetría del servicio asociado a su explotación se detallan a continuación.

AI.1. Descripción de la Infraestructura tecnológica

La infraestructura tecnológica relacionada es la más representativa en la actualidad, y en cualquier caso, esta relación es dinámica y susceptible a ampliaciones o modificaciones en función de la evolución tecnológica de la UOC y que el proveedor adjudicatario se comprometerá a asumir.

AI.1.1 Infraestructura física

La UOC tiene actualmente dos CPDs, los cuales se citan a continuación:

- El CPD principal se encuentra en el Campus de Castelldefels, con 25 racks, donde están los entornos de Producción (PRO) y Desarrollo (DEV).
- El CPD secundario se encuentra en el edificio de la UOC ubicado en Av. Tibidado, con 10 racks, donde se encuentra el entorno de contingencia (CON). Acualmente se está en fase de trasladar este CPD secundario a un CPD externo.

AI.1.2 Hardaware servidores y sistemas operativos:

- La UOC dispone del siguiente hardware:
    - Servidores físicos (Standalone): 100
    - Servidores virtuales: 530
        - Ubuntu: 350
        - Red Hat: 30
        - SUSE: 50
        - CENTOS: 25
        - Windows: 75

AI.1.2 Almacenamiento:

- Espacio disco: Total espacio para datos: 250 TB + 150 TB (Contingencia)
- Ocupación datos críticos en backup regular: 80 TB

AI.1.3 Aplicaciones y Bases de Datos:

- Jboss: 33x3 (PRO-PRE-DEV) (instancias diferentes, un cluster de servidores)
- Apache: 18x3 (PRO-PRE-DEV) (instancias diferentes, un cluster de servidores)
- Tomcat: 13x3 (PRO-PRE-DEV) (instancias diferentes, un cluster de servidores)
- Oracle: 7x3 (PRO-PRE-DEV)
- MySql: 9x3 (PRO-PRE-DEV)

AI.1.4 Red:

- Sistemas de red: Avaya, Cisco, Enterasys, F5, Juniper
- Número de sub-redes: 200

- Número de elementos de red: Aprox 100 (Routers, Switches)
- Firewalls: 3 Palo Alto (frontend), 3 Nokia y 4 F5 (backend)
- Balanceadores: 4 F5
- Wireless: Sistema centralizado Cisco. Access Points: 92
- Conexiones edificios: Conexiones Anella científica (1Gb) redundada con Macrolan (1Gb)
- Conexión Internet: Acceso Internet anella (1 Gb) redundada con Orange (1 Gb).

AI.1.4 Herramientas:

- Herramientas de gestión de procesos y documentación: JIRA, Confluence, Plone
- Herramientas de administración Cloud: API Manager, OpenShift
- Herramientas de gestión de seguridad: Ya descrito en el apartado 4.2.1.5.1

AI.2. Volumetría del servicio actual.

Actualmente la explotación de la infraestructura tecnológica descrita en el punto anterior, supone la siguiente volumetría del servicio:

Requerimiento.	Periodicidad promedio	Horas/año.
Detección, análisis y gestión de vulnerabilidades.	3 veces/año	240
Gestión y respuesta a incidentes de seguridad de la información (CSIRT).	4 incidentes / mes	480
Servicios de análisis de malware.	5 veces/año	48
Servicio de análisis forense.	5 veces/año	96
Mantenimiento ARBOR.	11.5 horas / mes	138
Mantenimiento IPS.	11.5 horas / mes	138
Revisión Firewall.	8.6 horas / mes	104
Mantenimiento QRadar.	25.1 horas / mes	302
		1544