PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGULAN EL ACUERDO MARCO DEL SUMINISTRO DE SOLUCIONES Y SERVICIOS GESTIONADOS DE SEGURIDAD TIC

ÍNDICE

1 Objeto del acuerdo marco 5
2 División en lotes 5
2.1 Seguridad de la información 7
3 Modalidad de contratación de las soluciones y servicios gestionados de seguridad TIC 9
4 Lote 1: Soluciones de seguridad TIC incluidas al CPSTIC 9
4.1 Alcance y requerimientos 11
4.2 Asistencia técnica para el despliegue de los servicios de seguridad TIC 12
4.3 Soporte técnico 12
4.4 Organización del servicio 14
4.5 Capacitación de los administradores 15
4.6 Agrupación de productos ofrecidos 15
4.6.1 Grupo 1: Básico 15
4.6.2 Grupo 2: Medio 16
4.6.3 Grupo 3: Avanzado 17
4.6.4 Otros grupos 17
4.6.5 Resumen 19
5 Lote 2: Servicios de auditoría técnica de ciberseguridad 20
5.1 Descripción del servicio 20
5.2 Plan de ejecución: 21
5.3 Alcance 22
5.4 Documentación a entregar 24
5.5 Organización del servicio 26
6 Lote 3: Servicios de gestión de la ciberseguridad 27
6.1 Funciones a realizar 28
6.1.1 Descubrimiento, análisis e interlocución en materia de ciberseguridad 28
6.1.2 Gestión operativa de la ciberseguridad 29
6.1.3 Análisis y gestión de incidentes de ciberseguridad 31
6.2 Organización del servicio 32
6.3 Gestión y ejecución del Plan de Seguridad 34
6.3.1 Gestión del Plan de Seguridad 35

6.3.2 Adecuación normativa prevista en el Plan de Seguridad 36
6.3.3 Actuaciones y proyectos específicos en el marco del Plan de Seguridad .. 37
6.4 Acuerdos de Nivel de Servicio (SLA) 38
7 Lote 4: Servicios de Centro de Operaciones de Seguridad (ZOCO) 40
7.1 Implantación del ZOCO 41
7.2 Funciones y capacidades del ZOCO..... 44
7.2.1 Disponibilidad del servicio 45
7.2.2 Capacidades de prevención 45
7.2.3 Capacidades de detección 46
7.2.4 Capacidades de protección 48
7.2.5 Capacidades de respuesta a incidentes..... 49
7.3 Plataforma de correlación de acontecimientos de seguridad de la información (SIEM) 50
7.4 Organización del servicio 51
7.5 Acuerdos de Nivel de Servicio (SLA) 53
8 Lote 5: Servicios de adecuación al Esquema Nacional de Seguridad (ENTE)..... 55
8.1 Plan de adecuación..... 56
8.1.1 Política de Seguridad y normativa interna..... 56
8.1.2 Identificación de los servicios presentes y categorización de los sistemas de la entidad contratante, con la valoración de la información tratada. 57
8.1.3 Análisis de riesgos..... 57
8.1.4 Elaboración de la Declaración de Aplicabilidad..... 58
8.1.5 Plan de mejora 58
8.2 Tareas relacionadas con la protección de datos. 59
8.3 Gobernanza de la seguridad. 59
8.4 Gestión del cambio y formación. 60
8.5 Acompañamiento a la obtención de la conformidad. 60
8.6 Entregables..... 61
8.7 Equipo de trabajo..... 62
9 Lote 6: Servicios de formación y concienciación en ciberseguridad ad hoc 63
9.1 Niveles de formación..... 64
9.1.1 Nivel básico de formación..... 64

9.1.2 Nivel avanzado de formación 66
9.2 Itinerarios de perfiles especializados de ciberseguridad 67
9.3 Otras secciones formativas complementarias 68
10 Lote 7: Servicios de CSIRT (Computer Security Incidente Response Team) 68
10.1 Características del servicio 69
10.2 Cumplimiento Normativo y Confidencialidad. 71
10.3 Modalidad de prestación del servicio. 71
10.4 Organización del servicio 74
11 Devolución del servicio 76
12 Plazos y modelo de relación 77
13 Facturación 78
14 Gastos de Impulso 78

ANEXO 10 – Descripción de las actuaciones previstas en el modelo de ciberseguridad de la Agencia de Ciberseguridad de Cataluña.
ANEXO 11. CCN-STIC-105 CPSTIC – Catálogo de productos y servicios de seguridad de las tecnologías de la Información y la comunicació.
ANEXO 12. CCN-STIC-140 – Taxonomía de referencia para productos y servicios de seguridad TIC.

1 OBJETO DEL ACUERDO MARCO

El acuerdo marco tiene por objeto el suministro, instalación y soporte de productos y la prestación de servicios destinados a la seguridad TIC de los organismos y entidades del sector público local catalán.

El objeto del acuerdo marco se define según las funcionalidades concretas que se pretenden satisfacer.

El acuerdo marco pretende construir una oferta de productos y servicios con capacidad suficiente para dar respuesta a las necesidades actuales y futuras de la ciberseguridad de las entidades locales, dando soporte el despliegue de cualquier plan de seguridad de la información que requiera tecnología aprobada por el Centro Criptográfico Nacional (CCN).

La finalidad del acuerdo marco es que las entidades beneficiarias puedan lograr los objetivos siguientes:

- Adquirir productos y servicios destinados a la mejora de la seguridad de sus infraestructuras TIC.
- Implementar mecanismos de ciberseguridad que incorporen las funcionalidades necesarias para obtener un mejor escenario de protección ante posibles ataques e incidentes de seguridad TIC.
- Politizar, monitorizar y supervisar las aplicaciones, las conexiones y, si se tercia, los datos, que empleen la red de la entidad local.
- Desarrollar capacidad de respuesta ante ciberincidentes en términos de recuperación de la información y del buen funcionamiento de los sistemas informáticos en caso de infección.
- Adoptar las medidas necesarias para adaptar el funcionamiento de las infraestructuras TIC a las necesidades inherentes propias de este acuerdo marco.

Los beneficiarios potenciales del acuerdo marco son todas las entidades que, durante la vigencia del acuerdo marco, formen el Consorcio Localret (https://www.localret.cat/qui-som/ens-adherits/), así como sus entes dependientes y aquellos en que las entidades que forman el Consorcio tienen una participación mayoritaria, previa su adhesión específica al acuerdo marco.

2 DIVISIÓN EN LOTES

Atendiendo a los diferentes tipos de soluciones y servicios de seguridad TIC que tienen que ser proveídos en el marco del presente pliego, los productos objeto del acuerdo marco se han agrupado en los lotes siguientes:

- Lote 1: Soluciones de seguridad TIC incluidas al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN (CPSTIC) .

  Suministro de productos, licencias o suscripciones de software, instalaciones y mantenimientos incluidos en el CPSTIC relacionadas con la seguridad TIC. Adicionalmente, tienen que ofrecer servicios de implantación.

Los siguientes lotes conforman servicios gestionados de ciberseguridad que tienen que contemplar todos los elementos necesarios para la gestión, monitorización, administración y ejecución de todas las tareas necesarias a fin de cubrir su ejecución.

A continuación se detallan cada uno de los servicios que forman parte del acuerdo marco. Cada servicio gestionado conforma un lote en sí mismo. Estos servicios gestionados contemplarán todos los elementos necesarios para la gestión, monitorización y administración de todas las tareas necesarias a fin de cubrir su ejecución. Los requerimientos y sus descripciones serán de obligado cumplimiento por parte del adjudicatario, sin menoscabo de ampliar las funcionalidades y ofrecer mejores prestaciones que las descritas. Del mismo modo, una empresa adjudicataria se podrá presentar a cualquier de los servicios presentes en estos lotes.

- Lote 2: Servicios de auditoría técnica de ciberseguridad.
  Engloba los requerimientos para la realización de una auditoría técnica a fin de establecer el grado de madurez de la entidad contratante en términos de seguridad TIC.

- Lote 3: Servicios de gestión de la ciberseguridad.
  Gestión de los servicios de ciberseguridad de manera integral por el licitador a fin de proveer de capacidades de ciberseguridad al ente público contratante.

- Lote 4: Servicios de Centro de Operaciones de Seguridad (ZOCO).
  Servicio SOC a proporcionar por el licitador así como de su operativa tanto a nivel técnico como organizativo.

- Lote 5: Servicio de adecuación al Esquema Nacional de Seguridad (ENTE).
  El servicio incluye los trabajos necesarios para la adecuación de todos los sistemas de información del ente contratante al Esquema Nacional de Seguridad.

- Lote 6: Servicios de formación y concienciación en ciberseguridad ad hoc .
  Servicio encargado de la generación de actividades y contenidos diseñados para educar y concienciar usuarios y organizaciones sobre las mejores prácticas, amenazas y riesgos relacionados con la seguridad informática y así minimizar el riesgo de incidentes.

- Lote 7: Servicios de CSIRT (Computer Security Incidente Response Team). Servicio de gestión y respuesta a incidentes de ciberseguridad, así como en el análisis forense digital para investigar y comprender estos incidentes. Este servicio tiene como objetivo minimizar el impacto de los incidentes, restaurar las operaciones normales y proporcionar información crítica para mejorar las defensas de seguridad de las entidades contratantes.

Las empresas licitadoras deberán adjuntar a sus propuestas el detalle de la plataforma o plataformas que ofrezcan (especificaciones técnicas, funcionalidades...), y de los diferentes niveles de suscripción, en su caso, para ofrecer los servicios de los lotes 2 a 7.

Las empresas velaran porque la entidad obtenga el servicio requerido con el mínimo coste, proponiendo los productos que mejor se adecuen a las necesidades del ente, y deberán asesorar proactivamente los clientes para optimizar la adquisición de productos.

Los servicios de ciberseguridad descritos (lotes 2 a 7) contemplan todos los elementos y servicios necesarios para su ejecución. Serán los contratos basados los que definirán el alcance del servicio que requiera cada ayuntamiento.

La empresa adjudicataria asumirá el servicio contratado de seguridad TIC durante la vigencia de los contratos basados, responsabilizándose de la buena ejecución del servicio contratado. Tendrá que disponer de los recursos técnicos, humanos y materiales adecuados para la prestación del servicio contratado garantizando los tiempos de respuesta y resolución de incidencias detallados al apartado de Acuerdos de Nivel de Servicio (SLA).

2.1 Seguridad de la información

Las empresas adjudicatarias del acuerdo marco serán responsables de la seguridad de los sistemas de información utilizados para la ejecución del contrato. Las empresas tendrán que contar, al menos, con una política de seguridad aprobada y, en todo momento, actualizada, que se pondrá a disposición del órgano de contratación, si este lo solicita.

Considerando el impacto que tendría un incidente que afectara la seguridad de la información o de los servicios, con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, los sistemas de información en que se sustentan los servicios prestados por las empresas adjudicatarias de contratos basados, tendrán que cumplir, como mínimo, los requisitos establecidas en el Real Decreto

311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENS), para la categoría que establece este mismo pliego por cada lote. No obstante, los órganos de contratación de los contratos basados podrán elevar la categoría de seguridad –a media o alta según el caso– de los sistemas de información exigibles para la ejecución del contrato.

El cumplimiento de estos requisitos se acreditará mediante la declaración de conformidad con el ENS, cuando se trate de sistemas de categoría básica, o la certificación de conformidad con el ENS, cuando se trate de sistemas de categoría media o alta, o la justificación de tener implementadas las medidas de tipo organizativo, operacional y de protección previstas en el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el ENS, que le permitan obtener estas certificaciones. Entre los sistemas de información cubiertos por la declaración o certificación de conformidad se tendrán que encontrar, necesariamente, aquellos que resulten necesarios para realizar el objeto del contrato.

En caso de que la empresa adjudicataria del acuerdo marco no disponga de la declaración o certificación de conformidad, exigida en el momento de la adjudicación, dispondrá de un plazo de cuatro meses por, al menos, implementar las medidas de tipo organizativo, operacional y de protección previstos en el Real Decreto 311/2022, que le permitan obtener la declaración y las certificaciones de conformidad correspondientes a la categoría exigida. Transcurrido este plazo, la empresa comunicará al órgano de contratación las medidas adoptadas para garantizar la seguridad de los sistemas de información utilizados para la ejecución de los contratos.

Este plazo de cuatro meses se aplica a todos los lotes con servicios que requieren certificación del ENS, para garantizar que todas las empresas adjudicatarias cumplan con los requerimientos de seguridad establecidos.

Igualmente, la empresa adjudicataria de un contrato basado en este acuerdo marco tendrá que cumplir, al menos, las siguientes obligaciones:

- Persona de contacto. Comunicar al responsable del contrato el nombre y los datos de contacto de la persona designada como responsable de la seguridad de la información.
- Cadena de suministro. En caso de que se autorice la subcontratación de actuaciones que impliquen el uso de sistemas de información, la empresa adjudicataria trasladará a las empresas subcontratistas cualquier requisito de seguridad en relación con la ejecución del contrato, así como monitorizará el correcto cumplimiento de los mismos. En cualquier caso, la adjudicataria asumirá cualquier responsabilidad en que incurran sus subcontratistas.
- Notificación y gestión de incidentes. La empresa adjudicataria del contrato

basado notificará a la entidad contratante cualquier incidente de seguridad que pueda redundar directa o indirectamente en la seguridad de los sistemas de información. Además, dispondrá de procedimientos de gestión de incidentes de seguridad, así como copias de seguridad para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

- Resolución de vulnerabilidades. La empresa adjudicataria del contrato basado tendrá que reparar toda vulnerabilidad que afecte a los sistemas de información utilizados durante la ejecución del contrato.
- El órgano de contratación de los contratos basados en el acuerdo marco podrá verificar, en cualquier momento, el cumplimiento de las medidas de seguridad requeridas.

3 MODALIDAD DE CONTRATACIÓN DE LAS SOLUCIONES Y SERVICIOS GESTIONADOS DE SEGURIDAD TIC

Las soluciones y servicios de seguridad TIC del presente acuerdo marco podrán ser contratados en las diferentes modalidades que ofrezca el fabricante o licitador, como por ejemplo:

- Adquisición de licencias perpetuas y mantenimientos (con pago mensual o anual).
- Adquisición de hardware con servicio de instalación y registro de alta de la entidad contratante hacia el fabricante.
- Modo de suscripción o pago por uso (con pago mensual, anual o plurianual).
- Servicio gestionado (con pago mensual o anual).

En los contratos basados se podrá establecer un modelo de tarificación según los parámetros y características que el licitador considere para responder a las necesidades del ente contratante.

En caso de que la solución contemple el pago por uso, los parámetros de pago y los precios correspondientes serán definidos a la propuesta del licitador del contrato basado.

En el caso de los servicios gestionados y monitorizados se definirá un precio por servicio según los parámetros establecidos en el presente pliego y los requerimientos concretos que defina el contrato basado.

4 LOTE 1: SOLUCIONES DE SEGURIDAD TIC INCLUIDAS AL CPSTIC

Las empresas adjudicatarias del lote 1 tendrán que proveer las licencias o suscripciones de software de seguridad TIC presentes a las guías publicadas al CPSTIC, ofreciendo los servicios siguientes:

- Tareas de suministro, instalación, configuración y soporte técnico a los usuarios/operadores.
- Traspaso de licencias.
- Gestiones con el fabricante para dar de alta los equipos y licencias así como para activar los servicios de soporte y mantenimiento ofrecidos por los fabricantes.
- Suministro de maquetas de instalación y configuración necesarias durante el periodo de vigencia del contrato.
- Soporte técnico a los usuarios operadores durante el periodo de vigencia del contrato.
- Se realizará un seguimiento de la utilización de los diferentes productos, ya sea con una herramienta de monitorización o en base a los logs de acceso del servidor de licencias.

La solución presentada podrá estar formada por productos de diferentes fabricantes y se podrá proveer más de una solución.

Se permitirá la creación de paquetes (*bundles*) de productos siempre que su precio final sea menor a la suma del precio de adquisición por separado. En este caso el tiempo de duración de la suscripción del software y servicio de soporte o mantenimiento será por el conjunto y no por los elementos por separado.

Las empresas tienen que adjuntar a sus ofertas el detalle de su solución (fabricantes de los diferentes componentes, especificaciones técnicas, funcionalidades...) y de los diferentes niveles de suscripción.

Las empresas licitadoras tienen que adjuntar, igualmente, el detalle de productos y mantenimiento, y de los diferentes niveles de suscripción.

Las empresas tendrán que ofrecer el servicio de monitorización de las licencias contratadas estableciendo métodos de seguimiento de las renovaciones de las mismas, la expiración de garantías y el soporte de los productos contratados, siempre velando por el uso correcto de las mismas.

Adicionalmente, las empresas pueden ofrecer servicios de asistencia técnica para el despliegue del servicio de seguridad TIC, que podrán ser facturados según la oferta presentada como servicios de implantación.

Para la instalación y configuración de los productos, los licitadores tendrán que seguir las instrucciones, siempre que el producto disponga, de la guía de configuración aprobada y publicada a las guías del CCN dedicada a tal efecto.

Para facilitar la elige de la solución, se ofrecerá el acceso a una demostración de la solución propuesta, un enlace a una web explicativa o cualquier otro medio que lo posibilite.

4.1 Alcance y requerimientos

El primer lote comprende el suministro de productos, instalaciones y mantenimientos calificados por el CCN, que cumplen los requisitos de seguridad exigidos por el ENS y que, por lo tanto, se encuentren incluidos dentro del CPSTIC, dadas las garantías de seguridad contrastadas de que disponen. Se entiende que estos productos y servicios pueden ser físicos o virtuales y de diferentes fabricantes.
Se adjunta el documento como anexo núm. 11.

Del mismo modo, también serán aceptados aquellos productos que estén en proceso de calificación y que ya aparecen como productos cualificados o aprobados por el CPSTIC.

Mediante la adquisición de estos productos y tecnologías, las entidades beneficiarias del acuerdo marco tendrán que poder cubrir las necesidades relacionadas con la ciberseguridad a sus sistemas.

En la misma línea, los productos que responden a la anterior taxonomía de referencia se podan consultar y descargar en formato PDF y *xlsx* al ""Catálogo de productos CPSTIC".

La clasificación y descripción de las familias de productos objete de este lote se encuentra a la "Guía de seguridad de las TIC CCN-STIC 140", que tiene el objetivo de describir la taxonomía de referencia para productos y servicios de seguridad TIC.
Se adjunta el documento como anexo 12.

Dada la evolución tecnológica constante de los productos y tecnologías incluidos al listado CPSTIC se prevé su actualización periódica y consecuentemente la actualización de productos y tecnologías del presente lote. La incorporación de productos y fabricantes nuevos al listado CPSTIC permitirá que las empresas puedan ofrecerlos dentro del presente acuerdo marco.

Cada elemento se dimensionará de acuerdo con las necesidades de la entidad que se establecerán en el contrato basado. El software, hardware y servicio de mantenimiento ofrecido por el licitador debe estar incluido al CPSTIC.

El licitador facilitará un listado de los productos incluidos al CPSTIC que ofrece a su oferta según el modelo de presentación de oferta del anexo 9. Estos productos podrán ser de diferentes fabricantes, igual que los del listado CPSTIC.

Existen productos catalogados que incorporan componentes que no están incluidos al listado del CPSTIC. Un ejemplo de esta casuística bote ser un cortafuegos (calificado) que incluya WAF (*Web Application Firewall*) o *antispamanti-spam* (no calificados).

De acuerdo con esto, el contrato basado podrá incluir productos no incluidos en el CPSTIC (o no calificado por el CPSTIC), que sean complementarios o auxiliares, y siempre que su coste no supere el 20 por ciento del valor total del contrato.

4.2 Asistencia técnica para el despliegue de los servicios de seguridad TIC

La empresa adjudicataria de un contrato basado en el acuerdo marco velará para garantizar las funcionalidades requeridas y optimizar el coste de la suscripción. También asegurará que las entidades adquieran una solución de seguridad que garantice el buen funcionamiento y las funcionalidades necesarias, proponiendo la suscripción más adecuada a sus necesidades y ofreciendo un asesoramiento suficiente y adecuado.

Los proyectos de implantación serán requeridos en los contratos basados con la definición y el alcance de los servicios demandados, y la empresa licitadora tendrá que presentar una oferta ajustada a estos requerimientos particulares.

En cualquier caso, se seguirán las instrucciones de la guía de configuración aprobada y publicada a las guías del CCN, siempre que el producto disponga.

4.3 Soporte técnico

Soporte básico

El soporte básico estará incluido en el precio del contrato.

Los licitadores de un contrato basado tendrán que ofrecer un soporte básico que incluirá los aspectos siguientes:

a) Creación (y baja) del cliente.
b) Registro y alta de la suscripción a nombre de la entidad.
c) Dar acceso y soporte a todas las actualizaciones y novedades sobre las aplicaciones contratadas que tengan lugar durante el plazo de vigencia del contrato,
d) Soporte en el proceso de facturación.

En los casos que se requieran tareas de administración avanzada, se podrá solicitar los servicios de espaldarazo a la implantación de nuevas funcionalidades que desarrolle el fabricante o que por modificación de la arquitectura de los nos sean necesarios realizar sobre el entorno actual del fabricante. En líneas generales se considerarán bajo este

epígrafe todas aquellas tareas que no sean consideradas una incidencia y suponga una modificación de la configuración y/o parametrización de los servicios.

Las empresas adjudicatarias del acuerdo marco tendrán que tener un centro de soporte donde las entidades que adjudiquen un contrato basado puedan comunicar incidencias, solicitar información y resolver dudas. Las empresas adjudicatarias proporcionarán soporte telefónico, al menos, entre las 9.00 h. y las 14.00 h. los días laborables de lunes a viernes, además de una dirección de correo electrónico donde poder dirigir las consultas. El tiempo de respuesta máximo desde la petición de la entidad hasta la recepción de la respuesta será de 8 horas laborables. El tiempo de respuesta podrá ser mejorado por la oferta del licitador.

Opcionalmente, el licitador podrá ofrecer un espacio donde se registren las comunicaciones de las incidencias o peticiones de soporte. Esta herramienta tendrá que conservar el histórico de las incidencias reportadas por la entidad y los tiempos de respuesta por cada una de ellas con su estado (abierta, resuelta, cerrada....).

Los contratos basados podrán tener como requerimiento el suministro de esta herramienta de *ticketing*.

Soporte del fabricante

El soporte de fabricante estará incluido en el precio del contrato.

Las empresas adjudicatarias tendrán que garantizar el servicio de soporte del fabricante:

a) Resolución de incidencias en caso de quiebra del servicio, *bug* del producto y actualización por resolución de vulnerabilidades.
b) Acceso al servicio de asistencia del propio fabricante, por teléfono o mediante dirección de correo electrónico.
c) Acceso en la base de conocimientos del fabricante, si dispone, por consulta y resolución de dudas relacionados con el producto.

Estas incidencias serán gestionadas por el contratista a petición de la entidad, sin ningún coste.

4.4 Organización del servicio

Estructura organizativa

Por parte de la entidad, se establecerá la figura del responsable del servicio, que será el encargado de dirigir y coordinar la relación con el adjudicatario.

Por parte del adjudicatario, del mismo modo, se establecerá un responsable del servicio, encargado de coordinar y garantizar el cumplimiento de los requisitos del servicio, asignando los medios adecuados para la correcta prestación del servicio.

Equipo de trabajo

Los integrantes del equipo de trabajo se concretarán en cada contrato basado en función del servicio requerido.

El personal incluido a la propuesta de la empresa licitadora del contrato basado deberá reunir los requisitos mínimos establecidos como requerimiento del contrato basado para la categoría profesional concreta y función a desarrollar y, además, que los mismos perfiles coincidan con los presentados a la propuesta efectuada por el adjudicatario en su oferta del presente acuerdo marco .

Si durante la ejecución del contrato surge la necesidad de sustitución de algún miembro del equipo de trabajo, el adjudicatario tendrá que motivar la solicitud con al menos dos semanas de antelación, y ser autorizada, si se tercia, por la entidad. Dado el elevado impacto que supone la rotación de perfiles, el adjudicatario velará para que esta rotación sea baja una vez aprobado el equipo de trabajo de cada contrato basado.

En general, si se produjera la sustitución de un miembro del equipo de trabajo, habrá un proceso de traspaso del conocimiento o solapamiento entre el recurso saliente y los recursos que asumen las tareas ejercidas por el recurso saliente, de 10 días hábiles mínimo para asegurar el traspaso de conocimiento interno.

Las empresas deberán disponer, como mínimo, de un equipo de trabajo formado por los siguientes perfiles:

- Responsable del servicio, las funciones del cual es garantizar servicio y gestionar la relación con la entidad.
- Un experto técnico en seguridad. Las principales funciones serán las correspondientes a la prestación del servicios de asistencia técnica para el despliegue de los servicios de seguridad TIC y el soporte técnico del presente lote.

Todos los perfiles tendrán que tener como mínimo **3 años** de experiencia en proyectos similares.

4.5 Capacitación de los administradores

Las entidades podrán solicitar la formación o planes de capacitación por los usuarios administradores de la plataforma de seguridad, ligados a los servicios contratados. Estos servicios tendrán que estar incluidos en el precio del producto o servicio y no tendrá que suponer un cargo económico adicional por la entidad.

Lo nos podrá solicitar un plan de capacitación para que su administrador pueda gestionar los dispositivos, los puntos de conexión y la seguridad de forma centralizada desde la consola de administración, según los productos adquiridos.

Esta formación tendrá una duración mínima de dos horas.

En caso de hacer la formación telemática el licitador tendrá que proveer los medios telemáticos para hacer la formación y tendrá que incluir la presencia del formador.

En caso de hacer la formación presencial esta será a la ubicación designada por la entidad local.

4.6 Agrupación de productos ofrecidos

Los productos que pueden ser ofrecidos por las empresas licitadoras se clasifican en tres grupos diferenciados, según el nivel de exigencia y complejidad de las demandas de los ente contratantes.

Si las empresas licitadoras son directamente los fabricantes de una solución que pertenece a una familia específica, no estarán obligadas a ajustarse a las agrupaciones descritas más adelante. Así, podrán ofrecer su solución sin necesidad de tener que proveer el resto de familias del grupo.

4.6.1 Grupo 1: Básico

Las empresas adjudicatarias tienen que proporcionar productos de todas las categorías y familias que se describen a continuación:

Categoría	Familia
Monitorización de la seguridad	IDS, IPS y AntiDDoS
Protección de las Comunicaciones	Cortafuegos
Protección de las Comunicaciones	Redes privades virtuales: IPSec
Protección de las Comunicaciones	Redes privades virtuales: SSL

Seguridad de la explotación	Antivirus / EPP (Endpoint Protection Platform)
Seguridad de la explotación	EDR (Endpoint Detection and Response)

Las empresas adjudicatarias que quieran ser homologadas en este grupo tienen que poder ofrecer la totalidad de los productos presentes a la tabla anterior. Además, tienen que cumplir con los siguientes requerimientos:

- Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 8x5 (laborables de lunes a viernes).
- Servicio de reposición: opcionalmente se puede ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.

4.6.2 Grupo 2: Medio

Las empresas adjudicatarias tienen que proporcionar productos de todas las categorías y familias del Grupo 1 (básico) y, como mínimo, 6 de las 10 familias que se describen a continuación:

Categoría	Familia
Conformidad y gobernanza de la seguridad	Formación y concienciación
Control de acceso	Control de acceso en la red (NAC)
Control de acceso	Servidores de autenticación
Protección de equipos y servicios	Protección de correo electrónico
Protección de la información y los soportes de la información	Hardware Security Modulo (HSM)
Protección de las comunicaciones	Dispositivos de red inalámbricas
Protección de las comunicaciones	Rúter
Protección de las comunicaciones	Proxy
Protección de las comunicaciones	Switch
Seguridad en la explotación	Herramientas de gestión de red

Las empresas adjudicatarias que quieran ser homologadas en esta categoría tienen que poder ofrecer, como mínimo, 6 de las 10 familias de productos presentes a la tabla anterior además de todos los presentes al **Grupo 1 (básico)**. Adicionalmente, tienen que cumplir con los siguientes requerimientos:

- Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 8x7.
- Servicio de reposición: tiene que ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.

4.6.3 Grupo 3: Avanzado

Las empresas adjudicatarias tienen que proporcionar productos de la siguiente familia además de heredar las obligaciones de los grupos 1 y 2.

Categoría	Familia
Seguridad en la explotación	Sistemas de gestión de incidencias e información de seguridad (SIEM)

Las empresas que quieran ser homologadas en esta categoría tienen que poder ofrecer la familia de esta categoría, como mínimo, 6 de las 10 familias de productos presentes a la tabla de la categoría del Grupo 2 (medio), además de todas las presente al Grupo 1 (básico). Adicionalmente, tienen que cumplir con los siguientes requerimientos:

- Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 24x7.
- Servicio de reposición: tiene que ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.

4.6.4 Otros grupos

Adicionalmente, existen una serie de categorías presentes al CPSTIC que contienen familias de productos aceptados y que pueden complementar las soluciones basadas en los grupos anteriormente expuestos en este documento.

En este sentido, las empresas licitadoras podrán complementar las soluciones ofrecidas con los elementos presentes en la lista que se muestra a continuación:

Categoría	Familia
Comunicaciones tácticas seguras	Soluciones para protección de las comunicaciones tácticas
Comunicaciones tácticas seguras	Plataformas y dispositivos tácticos confiables
Conformidad y gobernanza de la seguridad	Notificación y gestión de ciber incidentes
Conformidad y gobernanza de la seguridad	Gobernanza y planificación de la seguridad
Conformidad y gobernanza de la seguridad	Normativa de seguridad y conformidad
Conformidad y gobernanza de la seguridad	Análisis y gestión de riesgos
Control de acceso	Gestión de identidades (IM)
Control de acceso	Gestión de acceso privilegiado (PALMO)

Herramientas para el desarrollo de productos de seguridad	-
Monitorización de la seguridad	Captura, monitorización y análisis de tráfico
Monitorización de la seguridad	Herramientas de entorno controlado de pruebas (*sandbox*)
Otras herramientas	Otras herramientas
Protección de equipos y servicios	Sistemas operativos
Protección de equipos y servicios	Herramientas de video identificación
Protección de equipos y servicios	Dispositivos móviles
Protección de equipos y servicios	Sistemas de gestión de bases de datos (DBMS)
Protección de equipos y servicios	Conmutadores KVM
Protección de equipos y servicios	Hiperconvergència
Protección de equipos y servicios	Balanceadores de carga
Protección de la información y los soportes de la información	Almacenamiento cifrado de datos
Protección de la información y los soportes de la información	Herramientas para la firma electrónica
Protección de la información y los soportes de la información	Cifrado y compartición segura de datos
Protección de la información y los soportes de la información	Herramientas de borrado seguro
Protección de la información y los soportes de la información	Sistemas para prevención de fugues de dades
Protección de las comunicaciones	Herramientas de mensajería instantánea (IM)
Protección de las comunicaciones	Herramientas de voz IP
Protección de las comunicaciones	pasarelas seguras de intercambio de datos
Protección de las comunicaciones	Diodos de datos
Protección de las comunicaciones	Herramientas de videoconferencia
Protección de las comunicaciones	Cifradores IP
Protección de las comunicaciones	Redes definidas por software (SDN)
Protección de las comunicaciones	Redes privadas virtuales: otros
Protección de las comunicaciones	Herramientas para comunicaciones móviles seguras
Seguridad en la explotación	Dispositivos para la gestión de claves criptográficas
Seguridad en la explotación	Herramientas de filtrado de navegación
Seguridad OT	Seguridad OT

TEMPEST	Servidor
TEMPEST	Armarios apantallados
TEMPEST	Periféricos
TEMPEST	Monitores
TEMPEST	Impresoras
TEMPEST	CPU

4.6.5 Resumen

Grupos	Obligaciones
Grupo 1: Básico Productos y servicios Grupo Básico	• Ofrecer totes las familias del Grupo 1. • Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 8x5 (laborables de lunes a viernes). • Servicio de reposición: opcionalmente se puede ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.
Grupo 2: Medio (Grupo 1: Básico + Grupo 2: Medio)	• Ofrecer como mínimo 6 familias del Grupo 2 y todas las del Grupo 1. • Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 8x7. • Servicio de reposición: tiene que ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.
Grupo 3: Avanzado (Grupo 1: Básico + Grupo 2: Medio + Grupo 3: Avanzado)	• Ofrecer la familia del Grupo 3, 6 del Grupo 2 y todas las del Grupo 1. • Nivel de asistencia: tienen que ofrecer un servicio de asistencia técnica 24x7 • Servicio de reposición: tiene que ofrecer el servicio de reposición temporal (en forma de préstamo) en caso de avería de un dispositivo.

5 LOTE 2: SERVICIOS DE AUDITORIA TÉCNICA DE CIBERSEGURIDAD

El servicio de auditoría técnica interna y supervisión en ciberseguridad tendrá que analizar el estado de la entidad: detectar e informar de todas las posibles vulnerabilidades y riesgos, incluyendo un análisis de los usuarios existentes con acceso a los sistemas y la actualización del software utilizado, que puedan comprometer la integridad, confidencialidad y disponibilidad de la información y de los sistemas informáticos del ente contratante que la contienen mediante la simulación de intrusiones reales y controladas. También incluirá la revisión del plan de seguridad que tenga la entidad y la exposición de los datos de carácter personal.

La prestación del servicio se llevará a cabo a las instalaciones de la empresa adjudicataria, sin menoscabo de desarrollarlo a las instalaciones de ente contratante si las necesidades del servicio así lo determinan.

Las empresas deberán garantizar que sus sistemas de información que sustentan los servicios prestados al ser adjudicatarias de contratos basados del presente lote aplican las medidas de seguridad establecidas en el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el ENS. El adjudicatario tendrá que disponer de un certificado de desempeño del ENS de nivel MEDIO, y aportar el certificado correspondiente y que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

5.1 Descripción del servicio

El servicio se ejecutará de acuerdo con la metodología prevista en el Modelo de ciberseguridad de la Agencia de Ciberseguridad de Cataluña, para la fase de diagnóstico y la revisión del plan de seguridad. Esta metodología, disponible al anexo 10, determina el enfoque, criterios y entregables a tener en cuenta durante la ejecución de los test de penetración, la evaluación de controles en el proceso de consultoría y la elaboración de informes de diagnóstico.

En términos generales, el servicio de auditoría técnica interna de ciberseguridad estará vertebrado en el análisis de ls procedimientos relacionados con la gobernanza de los circuitos de ciberseguridad, del equipo disponible a la entidad en cuanto a software y hardware y en la simulación de diferentes ciberataques, con una duración a establecer con el ente contratante, en los cuales los atacantes tratarán de acceder a activos o sistemas de información del ente público, aprovechando debilidades tanto en el ámbito tecnológico como en el físico y en el de la ingeniería social.

En cuanto al análisis de la gobernanza de los circuitos relacionados con ciberseguridad y el análisis de la equipo de la entidad, la auditoría tendrá que cumplir, como mínimo, los siguientes puntos:

- Identificación e inventariado de los activos presentes a los sistemas del ente.
- Identificación de los usuarios con acceso a los activos y a los datos.

- Revisión del Plan de Seguridad (conjuntamente con las normativas, procedimientos principales y evaluación de riesgos) para asegurar su estricto cumplimiento posterior y actualización.
- Identificación de las medidas de seguridad técnicas, legales y organizativas necesarias para la protección de los sistemas de información en todos los entornos existentes a la entidad.

En cuanto a la simulación de ataques para determinar el grado de robustez de los sistemas de la entidad contratante, el proveedor diseñará y pondrá en marcha un conjunto de escenarios realistas que muestren métodos de ciberataques dirigidos a los ámbitos correspondientes al ente contratante.

5.2 Plan de ejecución:

El licitador, de acuerdo con la metodología indicada, tendrá que seguir la siguiente estructura para llevar a cabo el servicio:

- Planificación:
  - Análisis de la organización.
  - Aplicación de procesos de identificación y modelo de amenazas.
  - Determinar el alcance final y los objetivos.
  - Determinar los tiempos de inicio y final de la fase de ejecución.
  - Establecer los requerimientos iniciales para las pruebas e interlocutores.
- Ejecución de la auditoría:
  - Ejecutar los supuestos para conseguir los objetivos establecidos previamente.
  - Registrar las observaciones de las áreas de revisión y la evidencia de los objetivos conseguidos.
- Presentación de informes:
  - Presentación e informe: documentar las observaciones en un informe de diagnóstico final junto con un resumen-informe ejecutivo.
  - Presentación de los resultados a los responsables de las áreas revisadas a fin de discutir las debilidades encontradas.
  - Documentar los problemas identificados para cada observación, con una valoración de su gravedad y las recomendaciones adecuadas.
- remediación:
  - Proponer acciones para la remediación de las debilidades identificadas basado en recomendaciones, que tendrá que ser consensuado con los responsables del ente contratante.
  - Priorizar las acciones a tomar en función de la suya criticidad.
- Soporte puesto-auditoría:
  - Una vez aceptado el informe de auditoría, se tomarán medidas para corregir las vulnerabilidades según su relevancia. Después de que la

entidad contratante ejecute las acciones de remediación, habrá que confirmar que las vulnerabilidades se han solucionado con éxito.
    - El adjudicatario verificará que las correcciones hayan sido realizadas y redactará un Informe de Confirmación de remediación. Si la solución implementada por la entidad afectada no cumple con los requisitos para remediar la vulnerabilidad especificada, el adjudicatario proporcionará nuevas recomendaciones para la correcta resolución de las vulnerabilidades detectadas.
    - El soporte puesto-auditoría tendrá que contar como mínimo con reuniones quincenales con la entidad ofreciendo las soluciones para la resolución de los problemas detectados. El soporte tendrá una duración mínima de 2 meses. Se valorará la ampliación de este soporte.
- Borrado de información
    - Al finalizar el servicio, el adjudicatario tendrá que eliminar de sus sistemas o archivos todos los códigos fuente, certificados u otra información que pertenezca a la entidad contratante y que haya recibido para la ejecución de su trabajo.

Las empresas deberán proponer, para cada contrato basado, una planificación inicial de los servicios a proveer: plazo, horas, plan de revisión, programas de pruebas a realizar y el procedimiento de supervisión y seguimiento del servicio.

La entidad contratante estará en el día sobre las pruebas realizadas en cada momento, además de facilitar el establecimiento de la cooperación para la facilitación de información necesaria para llevar a cabo las pruebas. Las áreas concretas sujetas a la auditoría técnica en ciberseguridad, en términos de personal, no tienen que recibir información sobre las pruebas realizadas y sus resultados hasta el acabado de estas, a fin de elevar la complejidad y la efectividad de los intentos de intrusión.

Se establecerá un plan de reuniones de seguimiento donde el adjudicatario tendrá que presentar un informe de seguimiento con los trabajos realizados y la planificación prevista.

5.3 Alcance

Para llevar a cabo las tareas de auditoría técnica se hará un trabajo de campo en las instalaciones municipales que constituyan el centro de trabajo que se basará en los siguientes puntos:

- Visitar y supervisar el sistema de información de la entidad.
- Asignar responsables de auditoría interna de protección de datos y ciberseguridad.
- Mantener entrevistas con los responsables o bien con las personas designadas de las entidades.
- Recoger evidencias por parte de la comisión o responsable de seguridad.

- Revisión de la documentación de la gestión de la seguridad de la información.
- Definición de registros e indicadores, y realización práctica de los mismos.

En cuanto a la determinación de la robustez de los sistemas ante ataques, los vectores de ataque tendrán que emplear los ámbitos digital, físico y social para detectar vulnerabilidades tan técnicas como humanas. Las técnicas de intrusión específicas tendrán que ser propuestas por el adjudicatario y ser empleadas según los escenarios y vectores posibles para cada caso. Se podrán contemplar los siguientes:

- Intrusión física:
  - Análisis perimetral de seguridad.
  - Identificación de accesos alternativos.
  - Análisis de redes inalámbricas.
  - Control remoto de CCTV (si se tercia).
- Intrusión digital:
  - Análisis de sistemas perimetrales.
  - Análisis de servidores públicos y activos presentes en la red.
  - Intrusión y control de dominios internos.
  - Obtención de información crítica.
  - Infraestructura Wi-Fi.
  - Simulación de ataques avanzados:
    Incorporación de técnicas de ataque modernos, como *ransomware simulation*, para evaluar la capacidad de respuesta de la entidad ante amenazas complejas y avances.
    Simular ataques de movimiento lateral y persistencia dentro de la red para detectar debilidades en la capacidad de contención y respuesta.
  - Análisis del entorno Cloud:
    Si la entidad utiliza servicios a la nube (AWS, Azure, Microsoft 365, Google Cloud, etc.), se realizará una revisión detallada de las configuraciones, exposición y medidas de seguridad para garantizar que no existen vulnerabilidades derivadas de este entorno.
  - Auditoría de las políticas de recuperación y continuidad:
    Revisión de los planes de recuperación ante desastres (DRP) y continuidad del negocio (BCP) para asegurar que pueden mitigar adecuadamente los efectos de un ciberataque o desastre.
  - Análisis de la eficacia de las alertas y monitorización:
    Se llevará a cabo, en caso de que la entidad tenga, una evaluación de los sistemas de monitorización y respuesta a incidentes (SIEM/SOAR) para verificar que estos detectan y responden con eficiencia ante incidentes críticos de seguridad.
  - Indicadores de exposición a Internet:
    Análisis detallado de la exposición pública de los sistemas y activos de la entidad, incluyendo open puertos, configuraciones DNS, y posibles filtraciones de información en repositorios públicos (como GitHub u otras plataformas).

- Ingeniería social:
  - Despliegue de dispositivos cebo (*Media dropping*).
  - Envío de malware controlado a un conjunto de equipos reducido.
  - *Phising, Vishing,...*
  - Suplantación de identidades (*spoofing*).

En todo caso, las pruebas ejecutadas no tienen que suponer una interrupción o degradación de la operativa del ente contratante, ni se realizarán fuera del horario marcado por la entidad con objeto de no comprometer la operativa y tener capacidad de recuperar el funcionamiento de los servicios si resulta necesario. Aun así, estas pruebas tienen que permitir revertir cualquier modificación y recuperar el estado original de los sistemas o los datos.

Del mismo modo, la empresa adjudicataria tiene que informar al ente contratante de las pruebas que sean susceptibles de afectar los sistemas o los datos a fin de aprobar su ejecución.

5.4 Documentación a entregar

La empresa adjudicataria deberá dejar constancia de los trabajos realizados en los siguientes informes, que serán presentados a las reuniones con el adjudicatario:

- Informe técnico:
  - Adecuación de las medidas y controles existentes.
  - Descripción de las pruebas realizadas.
  - Alcance de las pruebas.
  - Medidas de protección identificadas.
  - Detalle de la intrusión.
  - Listado de hallazgos, vulnerabilidades, debilidades o riesgos obtenidos.
  - Método para reproducir las vulnerabilidades detectadas.

Para la puntuación y clasificación de las vulnerabilidades obtenidas, se utilizará el sistema de puntuación y métricas Sistema de Puntuación de Vulnerabilidades Comunes o *Common Vulnerability Scoring System* (CVSS, por las siglas en inglés) CVSS 3.1. Aun así cada una de estas vulnerabilidades dispondrá de una ficha con una descripción completa, su riesgo asociado, los sistemas afectados y una serie de recomendaciones para su solución.

Complementariamente al sistema de puntuación y métricas CVSS por cada vulnerabilidad obtenida se reforzará con el análisis de factores adicionales para una gestión más efectiva:

- Impacto organizativo: Se valorará como las vulnerabilidades pueden afectar los procesos críticos y la continuidad operativa, identificando ajustes necesarios para minimizar los riesgos asociados.
- Esfuerzo de remediación: Cada vulnerabilidad se categorizará en baja, media o alta según la complejidad de la solución requerida, detallando brevemente las acciones necesarias para abordarla.
- Impacto económico y de recursos: Se calculará el coste material, el tiempo necesario y los recursos implicados para implementar las soluciones, priorizando las acciones en función del riesgo y el análisis coste-beneficio.

Si se encuentran vulnerabilidades críticas o de alto riesgo de fuga de datos durante las auditorías, se emitirá una alerta al responsable del servicio auditado. Esta alerta incluirá un informe con la descripción de la vulnerabilidad, el tipo de impacto y una solución o medida temporal para mitigarla si no hay una solución disponible.

- Informe final:
  - Descripción del trabajo realizado.
  - Conclusiones y recomendaciones con los datos, hechos y observaciones sobre las que se basan.
  - Revisión del Plan de Seguridad.
  - Identificación de las acciones y proyectos a realizar que permitan reducir las debilidades y riesgos identificados en el ente contratante.
  - Clasificación de activos según el ENS. El informe incluirá una revisión de la clasificación de los activos de la entidad, siguiendo los principios de confidencialidad, integridad y disponibilidad del ENS, para garantizar que cada activo tiene el nivel de protección adecuado.
- Formación:
  - Adicionalmente se valorará que el adjudicatario ofrezca un plan de concienciación y formación adaptado a la entidad y el resultado obtenido de la auditoría técnica.

Todos los informes y los datos que en estos puedan aparecer, que hayan sido generados como consecuencia de la prestación del servicio constituyen información confidencial y se mantendrán bajo custodia del ente contratante.

La empresa adjudicataria se comprometerá a guardar absoluta confidencialidad sobre todos los datos y conocimientos que se deriven de la ejecución del servicio de auditoría interna de ciberseguridad y los datos manejados.

Todos los documentos generados serán confidenciales y no podrán ser total ni parcialmente reproducidos en ningún medio, o librados a terceras personas sin la exprés autorización del ente contratante por escrito.

5.5 Organización del servicio

Estructura organizativa

Por parte de la entidad, se establecerá la figura del Responsable del Servicio, que será el encargado de dirigir y coordinar la relación con el adjudicatario.

Por parte del adjudicatario, del mismo modo, se establecerá un Responsable del Servicio, encargado de coordinar y garantizar el cumplimiento de los requisitos del servicio, asignando los medios adecuados para la correcta prestación del servicio.

Equipo de trabajo

Los integrantes del equipo de trabajo se concretarán en cada contrato basado en función del servicio requerido.

El personal incluido a la propuesta del licitador del contrato basado deberá reunir los requisitos mínimos establecidos como requerimiento del contrato basado para la categoría profesional concreta y función a desarrollar y, además, que los mismos perfiles coincidan con los presentados a la propuesta efectuada por el adjudicatario en su oferta del presente acuerdo marco .

Si durante la ejecución del contrato surge la necesidad de sustitución de algún miembro del equipo de trabajo, la empresa adjudicataria tendrá que motivar la solicitud con al menos dos semanas de antelación, y ser autorizada, si se procede, por la entidad. Dado el elevado impacto que supone la rotación de perfiles, la empresa adjudicataria velará para que esta rotación sea baja una vez aprobado el equipo de trabajo de cada contrato basado.

En general, si se produjera la sustitución de un miembro del equipo de trabajo, habrá un proceso bisiesto del conocimiento o solapamiento entre el recurso saliente y los recursos que asumen las tareas ejercidas por el recurso saliente, de 10 días hábiles mínimo para asegurar el traspaso de conocimiento interno.

Las empresas deberán de disponer, como mínimo, de un equipo de trabajo formado por los siguientes perfiles:

- Responsable del servicio, las funciones del cual es garantizar servicio y gestionar la relación con la entidad.
- Un experto técnicos en Seguridad. Las principales funciones serán las correspondientes a la prestación del servicio.

Todos los perfiles tendrán que tener como mínimo **3 años** de experiencia en proyectos similares.

6 LOTE 3: SERVICIOS DE GESTIÓN DE LA CIBERSEGURIDAD

El servicio de gestión de la ciberseguridad englobará todas las actuaciones relacionadas con la ciberseguridad y, por lo tanto, contemplará todos los elementos y servicios necesarios para la implantación, administración y mantenimiento de la ciberseguridad de la entidad.

Una vez implementada el ecosistema que regula la ciberseguridad del ente local, el proveedor será el responsable de gestionar todos los trabajos de configuración, mantenimiento, monitorización, prevención de incidentes y de actuación ante ataques en el cariz de la ciberseguridad, según la política establecida por la entidad.

Del mismo modo, la empresa adjudicataria asumirá los trabajos necesarios para la recuperación del buen funcionamiento de todos los sistemas informáticos así como el software y los datos afectados por un incidente de seguridad con el fin de recuperar el normal funcionamiento de la entidad en el menor tiempo posible.

El proveedor escogido asumirá el servicio encargado de la ciberseguridad durante la vigencia de los contratos basados, responsabilizándose de la gestión de las incidencias relacionadas con el sistema. Tendrá que disponer de los recursos técnicos, humanos y materiales adecuados para la prestación del servicio contratado garantizando los tiempos de respuesta y resolución de incidencias detallados al apartado correspondiente a los acuerdos de nivel de servicio.

En el supuesto de que el ente contratante requiera incorporar nuevas soluciones o software, este software y/o hardware tendrá que estar incluido en el catálogo CPSTIC, tal y como se establece al lote 1 de este mismo pliego.

En el supuesto de que la entidad contratante ya disponga de un software en funcionamiento, la empresa adjudicataria del servicio tendrá que poder acreditar que posee experiencia con este software y un equipo técnico humano con los conocimientos necesarios para operar con la plataforma establecida.

En cualquier caso, la empresa adjudicataria del servicio de operación de la ciberseguridad tendrá que poder acreditar que opera con un software reconocido y homologado en el catálogo CPSTIC y que está capacitada a tal efecto.

La empresa adjudicataria tendrá que garantizar que sus sistemas de información que sustentan los servicios prestados al ser adjudicatarias de contratos basados del

presente lote aplican las medidas de seguridad establecidas en el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENS). El adjudicatario tendrá que disponer de un certificado de desempeño del Esquema Nacional de Seguridad de nivel MEDIO, y aportar el certificado correspondiente y que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

6.1 Funciones a realizar

Los servicios ofrecidos estarán incluidos en los siguientes puntos que se detallan a continuación y que las entidades podrán solicitar total o parcialmente en los contratos basados:

6.1.1 Descubrimiento, análisis e interlocución en materia de ciberseguridad

Se incluyen en este apartado todos los servicios orientados a realizar un descubrimiento y diagnóstico inicial de los activos, servicios y nivel de cumplimiento de la entidad que permitan planificar y ejecutar auditorías y evaluaciones técnicas de seguridad, de controles normativos y de cumplimiento legal:

- Configuración, monitorización y mejora/ampliación de los activos relacionados con la seguridad de operaciones.
- Descubrimiento, identificación, catalogación y mantenimiento del inventario de los activos, dispositivos, comunicaciones, servicios y sistemas de información de la entidad, para obtener una visión completa y detallada de los recursos, servicios e infraestructuras TIC y de seguridad. Esta información tendrá que permitir facilitar las auditorías técnicas y evaluaciones en ciberseguridad, planificar estrategias de seguridad más eficientes, responder de manera más efectiva a incidentes de seguridad, y favorecer el cumplimiento de los requisitos de cumplimiento y auditoría. La catalogación seguirá las directrices y clasificaciones establecidas al Esquema Nacional de Seguridad (ENS)
- Ejecución o soporte en la ejecución de pruebas y análisis técnicos de seguridad llevadas a cabo por la Agencia de Ciberseguridad de Cataluña, personal interno u otros actores (SOC operativo que se define al lote 4).
- Ejecución o soporte en la ejecución de revisiones y evaluaciones de controles técnicos y de cumplimiento normativo llevados a cabo por la Agencia de Ciberseguridad de Cataluña, personal interno o externo de la entidad.
- Interlocución técnica en materia de ciberseguridad con los proveedores, entidades públicas o privadas que estén ejecutando o proveyendo servicios de ciberseguridad y procedimientos de auditoría.

- Trabajos necesarios para la realización de un diagnóstico preliminar del nivel de adecuación de los sistemas de información al Esquema Nacional de Seguridad, que permita identificar el correcto cumplimiento de los aspectos tanto generales como específicos del ENS tales como, el nivel de categorización de los sistemas de información y declaración de aplicabilidad, el nivel de cumplimiento de las medidas del marco organizativo, operacional y de protección, y la disponibilidad y calidad de toda la documentación asociada a su cumplimiento.
- Trabajos necesarios para la realización de un diagnóstico preliminar del nivel de cumplimiento de la entidad en materia de protección de datos de acuerdo con aquello establecido por la normativa vigente.
- Capacidad para describir los requerimientos y características técnicas de las herramientas y servicios en ciberseguridad que el ente local requiera adquirir mediante los procedimientos de contratación y licitación que se determinen.
- Actualización y seguimiento del plan de adecuación y monitorización de la implantación de las medidas definidas en el plan.

6.1.2 Gestión operativa de la ciberseguridad

En este apartado se describen el conjunto de actuaciones y servicios destinados a ofrecer el soporte necesario para que las herramientas y servicios de protección del ente local estén integrados en el SOC correspondiente, bien sea el SOC Operativo de la entidad o el de la Agencia de Ciberseguridad que se referencia al Lote 4:

- El servicio por parte de la empresa adjudicataria se tendrá que encargar de la gestión de las operaciones de seguridad diarias, en la medida de aglutinar en un mismo punto tanto las alertas emitidas -en caso de existir- por el servicio de monitorización de la seguridad descrito más adelante en este documento (SOC) como aquellas provenientes de las sondas SAT-INET, organismos CERT u otro tipo de sondas que estén presentes a la entidad.
- Monitorizar en tiempo real todos los dispositivos que el ente contratante defina como críticos.
- Mantener debidamente actualizados a las últimas versiones los software y el firmware del hardware vinculados al perímetro de seguridad de la entidad.
- El servicio de ciberseguridad contratado tendrá que garantizar que el sistema de copias de seguridad funcione de manera óptima, asegurando que todas las copias se realicen correctamente y que incluyan todos los elementos críticos configurados de manera adecuada. Además, se tendrán que llevar a cabo pruebas periódicas de restauración, que permitan verificar la integridad y fiabilidad de las copias, garantizando así la capacidad de recuperación de los datos en caso de incidente.

- Instalación, configuración, mantenimiento y mejora/ampliación de las herramientas, software y servicios de ciberseguridad vinculados al perímetro de seguridad de la entidad necesarios para proteger la información y sus sistemas y equipos informáticos:
  - En el supuesto de que el ente contratante no disponga del software necesario o desee operar con el software de la empresa adjudicataria, esta tendrá que implantar el software y/o hardware pertinente.
  - En el supuesto de que la entidad contratante ya disponga de un software en funcionamiento, este tendrá que ser integrado por la empresa adjudicataria del servicio y su equipo técnico humano suya tendrá que llevar a cabo la operación y mantenimiento.
- Asumir los trabajos necesarios para la integración y monitorización, en el SOC correspondiente de las alertas generadas por las herramientas, software y servicios de ciberseguridad descritos anteriormente.
- Notificar las amenazas e incidentes identificados, al SOC correspondiente, y a los interlocutores que formen parte del proceso de escalado y toma de decisiones, para su evaluación y tratamiento.
- Con las indicaciones y espaldarazo del SOC correspondiente, realizar las tareas necesarias por:
  - Detectar amenazas y riesgos tales como la identificación de comportamientos anómalos, dispositivos y usuarios comprometidos, y descubrimiento de potenciales rendijas de ciberseguridad, entre otros.
  - Clasificar y priorizar las alertas de seguridad que se puedan detectar en el ámbito.
  - Realizar las tareas necesarias para preservar los logs de la entidad según las políticas acordadas y la normativa vigente.
- Asumir la gestión de las incidencias relacionadas con los software, servicios y equipos de ciberseguridad desplegados a la entidad, disponiendo de los recursos técnicos, humanos y materiales adecuados para atender las incidencias relacionadas con estos, garantizando los tiempos de respuesta y resolución de incidencias detallados al apartado de Acuerdos de Nivel de Servicio (SLA).
- Recogida de evidencias en caso de incidente de seguridad.
- Adoptar medidas de contención para los incidentes de seguridad, o dar indicaciones precisas porque estas sean implementadas por el personal del área TIC de la entidad, según los protocolos establecidos, así como verificar la eficacia.
- Estudio de impacto de incidentes, activos afectados y nivel de compromiso de los servicios.
- Proposición del plan de mitigación y remediación o adopción del plan propuesto por el SOC Operativo o de referencia de la entidad. Coordinación con la entidad sobre la ejecución de los planes de mitigación y remediación iniciados hasta la finalización.

6.1.3 Análisis y gestión de incidentes de ciberseguridad

En este apartado se describen el conjunto de actuaciones y servicios destinados a habilitar las capacidades de respuesta en incidentes de seguridad del ente local, con el soporte y supervisión del SOC correspondiente:

- Asumir, siguiendo las estrategias de respuesta del SOC correspondiente, y bajo su dirección y supervisión, los trabajos necesarios derivados de la materialización de un incidente de seguridad, con el objetivo de lograr el restablecimiento y el buen funcionamiento de todos los sistemas informáticos y de los datos, para recuperar la normal actividad de la entidad en el menor tiempo posible.
- Desarrollar políticas y procedimientos de respuesta y recuperación ante acontecimientos de destrucción de información o interrupción del funcionamiento del sistema informático del ente contratante.
- Capacidad para la recogida y preservación segura de evidencias relativas al incidente de seguridad, bajo la dirección y supervisión del SOC correspondiente, garantizando en todo momento el mantenimiento de la cadena de custodia para asegurar su validez e integridad en posibles procesos de investigación o legales.
- Coordinar con la entidad y los actores que correspondan, la ejecución de los planes de mitigación y remediación acordados hasta la finalización del incidente de seguridad, bajo la dirección y supervisión del SOC correspondiente.
- En la ejecución de estos trabajos y en caso de incidentes graves de ciberseguridad, el adjudicatario tendrá que ofrecer una disponibilidad y capacidad de trabajo en formato 24x7 hasta que el SOC correspondiente lo determine en el marco de la estrategia de respuesta. A tal efecto tendrá que poder participar en los diferentes comités y salas de crisis que se convoquen durante el episodio.
- Soporte en la evaluación del impacto, y en la clasificación y priorización de los incidentes de seguridad.
- Establecer y mantener procedimientos para investigar y documentar los incidentes de seguridad.
- Investigación de acontecimientos de seguridad para notificar las amenazas e incidentes identificados, al SOC correspondiente, y a los interlocutores que formen parte del proceso de escalado y toma de decisiones, para su evaluación y tratamiento.
- Registrar y preservar la información relativa a los acontecimientos asociados a los incidentes y llevar a cabo el análisis forense del incidente de seguridad.
- Realización de análisis forense para determinar las causas y las responsabilidades del incidente, con el soporte del SOC correspondiente

- Realización de evaluaciones y revisiones una vez superada el incidente, para analizar y desarrollar un plan de acción que permita corregir las deficiencias identificadas durante el incidente de ciberseguridad.
- Soporte técnico a las acciones comunicativas que pueda requerir la entidad, en el marco del gobierno y la comunicación de un incidente de ciberseguridad.

En lo posible la detección y respuesta de incidencias tienen que estar automatizadas para reducir el tiempo de respuesta ante las amenazas.

El registro, el control y el seguimiento de la actividad se llevará a cabo, si dispone, utilizando la herramienta interna de gestión (*ticketing*) del adjudicatario, así como las herramientas de notificación de ciber incidentes que se establezca por parte de las autoridades nacionales (del CCN-CERT o de la Agència de Ciberseguretat de Catalunya).

La entidad determinará los canales de comunicación con el proveedor que será a todo caso a través de teléfono, dirección de correo electrónico y/o de la herramienta interna de gestión de incidencias de la entidad en modo no automatizado.

También tendrá que recoger aquellas alertas emitidas por el CAU (Centro Atención Usuarios) u otras fuentes internas en el supuesto de que estas no hayan sido identificadas por la herramienta de monitorización de la empresa adjudicataria.

La empresa adjudicataria, a petición del ente, impartirá formación a los técnicos de la entidad que sean designados, sobre las herramientas y metodologías implantadas al proyecto. La misma se realizará de forma telemática y tendrá un carácter básico incluyendo el uso de la aplicación, la configuración y la instalación de los sistemas desplegados.

6.2 Organización del servicio

Estructura organizativa

Por parte de la entidad, se establecerá la figura del Responsable del Servicio, que será el encargado de dirigir y coordinar la relación con el adjudicatario.

Por parte del adjudicatario, del mismo modo, se establecerá un Responsable del Servicio, encargado de coordinar y garantizar el cumplimiento de los requisitos del servicio, asignando los medios adecuados para la correcta prestación del servicio.

Equipo de trabajo

Los integrantes del equipo de trabajo se concretarán en cada contrato basado en función del servicio requerido.

El personal incluido a la propuesta del licitador del contrato basado deberá reunir los requisitos mínimos establecidos como requerimiento del contrato basado para la categoría profesional concreta y función a desarrollar y, además, que los mismos perfiles coincidan con los presentados a la propuesta efectuada por el adjudicatario en su oferta del presente acuerdo marco .

Si durante la ejecución del contrato surge la necesidad de sustitución de algún miembro del equipo de trabajo, la empresa adjudicataria tendrá que motivar la solicitud con al menos dos semanas de antelación, y ser autorizada, si se procede, por la entidad. Dado el elevado impacto que supone la rotación de perfiles la empresa adjudicataria velará para que esta rotación sea baja una vez aprobado el equipo de trabajo de cada contrato basado.

En general, si se produjera la sustitución de un miembro del equipo de trabajo, habrá un proceso bisiesto del conocimiento o solapamiento entre el recurso saliente y los recursos que asumen las tareas ejercidas por el recurso saliente, de 10 días hábiles mínimo para asegurar el traspaso de conocimiento interno.

Las empresas tendrán que disponer, como mínimo, de un equipo de trabajo formado por los siguientes perfiles:

- Consultor de Gobierno de Seguridad, las funciones del cual estarán relacionadas con el servicio de Gobernanza de la Ciberseguridad, que engloba la gestión de la Oficina Técnica de Seguridad.
- Un experto técnico en Seguridad. Las principales funciones serán las correspondientes a la prestación de los siguientes servicios:
    - La instalación, configuración y mantenimiento de herramientas que apoyen al servicio de seguridad de operaciones de ciberseguridad.
    - Servicio de Gestión de Incidentes de Seguridad de la Información, mediante la detección, contención, análisis, respuesta y recuperación a acontecimientos de ciberseguridad.
    - Interlocución, si existe, con el Centro de Operaciones de Seguridad (SOC) y el CERT.

  Todos los perfiles tendrán que tener como mínimo 3 años de experiencia en proyectos similares.

Seguimiento del servicio

A las reuniones de seguimiento participaran, al menos, el Responsable del Servicio de la entidad y del adjudicatario.

Durante las fases iniciales de puesta en marcha y de devolución del servicio se llevarán a cabo reuniones de seguimiento con periodicidad mensual. En estas reuniones, se llevará un seguimiento de la planificación y tareas realizadas, así como un análisis de riesgos por parte del adjudicatario.

Durante la fase de prestación del servicio se establece una periodicidad semestral para las reuniones de seguimiento, aunque la entidad podrá solicitar reuniones extraordinarias por la existencia de circunstancias que lo hagan necesario.

El adjudicatario librará un informe mensual de actividad (que a la vez servirá para dar conformidad a las facturas) que recoja:

- Avance en el cumplimiento del objeto del contrato.
- Incidentes de seguridad que hay que destacar.
- Riesgos existentes y previstos.
- Otros aspectos relevantes en materia de seguridad de la información detectados y que tengan que ser conocidos por la entidad.

En caso de que, por cuestiones relacionadas con la prestación del servicio, fuera necesario el desplazamiento del personal del equipo técnico a cualquier ubicación, este desplazamiento iría a cargo de la empresa adjudicataria, sin que suponga un coste adicional.

Las reuniones de seguimiento se llevarán a cabo a las instalaciones de la entidad o en línea si la entidad está de acuerdo.

Horario del servicio

El servicio se prestará por el equipo de trabajo especializado con disponibilidad diaria de 8 horas, de lunes a viernes (modelo 8x5), con un servicio de resolución de incidencias con horario 24x7 (24 horas, de lunes a domingo) para proveer de un servicio de operaciones de seguridad gestionada a la entidad.

6.3 Gestión y ejecución del Plan de Seguridad

La gestión del servicio de operación tiene que englobar, por parte de la empresa adjudicataria, la gestión de la Oficina Técnica de Seguridad del ente local, el mantenimiento del marco normativo y de procedimientos de seguridad además del análisis y la presentación de resultados de manera recurrente y programada o debajo petición explícita. Esta gestión tendrá que asegurar el cumplimiento de las medidas de seguridad establecidas al ENS.

Con el objetivo de ejecutar el Plan de Seguridad, se tendrán que ofrecer servicios y funciones orientadas a la ejecución de las medidas y acciones identificadas en el Plan, y a su seguimiento y actualización.

El servicio ofrecido por el licitador tendrá que incluir las prestaciones divididas en los siguientes ámbitos:

6.3.1 Gestión del Plan de Seguridad

- Implementación, seguimiento y Gestión del Plan de Seguridad impulsando todas aquellas acciones generales y específicas para lograr su consecución.
- Revisión y evaluación del Plan de Seguridad para entender y valorar dentro del contexto de la entidad, los riesgos identificados y medidas compensatorias propuestas.
- Evaluación de los riesgos y de las medidas propuestas para determinar su viabilidad, impacto, y priorización ante los órganos de decisión de la entidad.
- Implementación de las medidas propuestas en el plan, coordinándose con los actores pertinentes, y ejecutando un seguimiento de su ejecución hasta su finalización.
- Elaboración de planes de acción específicos para la implementación de medidas de elevada complejidad
- Actualización y documentación del Plan de Seguridad para su trazabilidad, auditoría y mejora continua.
- Medida, interpretación y seguimiento de indicadores y métricas de seguridad, y la agrupación de los mismos en la confección de Cuadros de Mando.
- Soporte a la dirección de la entidad en la convocatoria del Comité de Seguridad de la Información y preparación de la documentación para el desarrollo de las sesiones.
- Asesoramiento técnico y jurídico de primer nivel en materia de ciberseguridad y cumplimiento normativo, con la posibilidad de elevar cuestiones complejas a otras entidades o autoridades con un alto nivel de conocimiento y competencia en la materia.
- Soporte en las acciones de comunicación que se deriven de la gestión del Plan de Seguridad.
- Atención y respuesta a consultas técnicas y jurídicas en materia de seguridad de la información.

6.3.2 Adecuación normativa prevista en el Plan de Seguridad

La implementación de las medidas y actuaciones previstas en el Plan de Seguridad comportan progresivamente a la adecuación normativa de la entidad al Esquema Nacional de Seguridad.

La operativa de adecuación normativa se fundamenta en la implementación del Plan de Seguridad y en el despliegue de las capacidades y recursos necesarios para gobernar el cumplimiento normativo de la entidad, con el objetivo de lograr de manera satisfactoria los futuros procesos de certificación de los servicios escogidos a tal fin por la entidad. A tal efecto, las principales tareas a desarrollar serán las siguientes:

- Apoyar activo y constando, en el despliegue del modelo de ciberseguridad, durante las diferentes fases, respecto a las diferentes actividades y tareas relacionadas con el cumplimiento y la adecuación normativa.
- Impulsar y gobernar la implantación de las iniciativas y proyectos, asociados al cumplimiento normativo, definidos en el Plan de Seguridad.
- Identificar y establecer, conjuntamente con la dirección de la entidad, el objetivo de implantación de las normativas, legislaciones y estándares de buenas prácticas a implantar en la entidad, así como el servicios susceptibles de pasar los futuros procesos de certificación.
- Realizar evaluaciones periódicas del estado de implantación de los requerimientos normativos de la entidad, tanto desde el punto generalista, a nivel de entidad, como específico, de los servicios que se quieren adecuar, y posteriormente certificar, para identificar las carencias respecto al cumplimiento, que hay que dirigir.
- referencia a las evaluaciones periódicas realizadas, definir las iniciativas y proyectos que habría que abordar, de manera coordinada y consensuada con la estrategia del Plan de Seguridad, e impulsar su implantación.
- Coordinar la generación de las evidencias necesarias, velar por su mantenimiento actualizado, y realizar la operativa para hacer su entrega a la Agencia de Ciberseguridad de Cataluña o a la entidad certificadora correspondiente cuando se requiera durante el proceso de certificación.
- Llevar a cabo los trabajos necesarios, para elaborar, adaptar y mantener la documentación y procedimientos relacionados con el marco organizativo, normativo y de cumplimiento del ENS siguiendo, cuando estén disponibles, las indicaciones, guías y modelos de referencia que la entidad local pueda facilitar.
- Colaborar y realizar los trabajos necesarios de soporte en el proceso de auditoría externa y certificación en el ENS.
- Llevar a cabo las tareas necesarias asociadas en el gobierno y mantenimiento de

la certificación.

6.3.3 Actuaciones y proyectos específicos en el marco del Plan de Seguridad

La implementación del Plan de Seguridad puede suponer la ejecución y gobernanza de proyectos, tanto de rápida ejecución, como de actuaciones más complejas que requieran de un análisis y planificación para su consecución. A tal efecto el adjudicatario tendrá que proveer de los recursos, capacidades y conocimiento técnico necesarios para llevarlos a cabo. A título orientativo, los proyectos podrán alcanzar las siguientes tipologías sin descartar otros de homólogas en el ámbito de la ciberseguridad:

- Proyectos de transformación para enmendar la obsolescencia tecnológica de los entornos, sistemas de información y puesto de trabajo de la entidad.
- Proyectos de gestión vulnerabilidades y mejora de configuraciones, tales como la protección de servicios configurados por defecto, la aplicación de parches de seguridad, mitigación de vulnerabilidades asociadas a soluciones propias o de terceros, y la realización de escaneos de seguridad internos y gestión de vulnerabilidades.
- Proyectos de adquisición y despliegue de herramientas de seguridad y perimetrales, proyectos de gestión centralizada de logs y mejora de las configuraciones de las herramientas de seguridad.
- Proyectos de elaboración de políticas y procedimientos vinculados al cumplimiento y en el cuerpo normativo de la entidad.
- Proyectos para implementar una gestión de usuarios y control de acceso, tales como las restricciones de acceso a servicios y activos de la entidad, gestión de las bajas de los usuarios inactivos, despliegue de soluciones de MFA (factor de autenticación múltiple), implementación de políticas de mínimos privilegios, configuraciones seguras de las soluciones de acceso remoto, e implementación de mejoras de la seguridad y detección de ataques a los directorios activos.
- Proyectos de seurización de la red, tales como la mejora de la seguridad de los protocolos y servicios de la red, segmentación segura, securización de redes Wifi y configuración adecuada de las soluciones NAC.
- Proyectos de mejora en la protección y securización de los equipos de trabajo y dispositivos móviles.
- Proyectos en el ámbito de la criptografía y relativos a la implementación de certificados reconocidos y seguros, y de configuración segura de la firma electrónica.
- Proyectos orientados a la mejora de la gestión y protección de las copias de

seguridad.

- Proyectos de análisis de riesgos de los sistemas utilizando la herramienta PILAR u otra en caso de que el Supervisor de Seguridad de las Tecnologías de la Información y las Comunicaciones (SSTIC) así lo determinara. Este análisis de riesgos tiene que ser completa, de forma que permita validar el conjunto de medidas de seguridad implantada, detectar la necesidad de medidas adicionales y justificar el uso de medidas de protección alternativas.
- Proyecto de elaboración del plan de contingencia y continuidad de negocio. Se llevará a jefe un plan de continuidad de los servicios y de la infraestructura de soporte a los sistemas de información y telecomunicaciones ante posibles contingencias.

Las entidades podrán solicitar la totalidad de las prestaciones o una parte de ellas.

6.4 Acuerdos de Nivel de Servicio (SLA)

Los SLA de los contratos basados podrán ser especificados en el propio contrato, o establecer como genéricos los que se describen en este apartado. Aun así, en los contratos basados se establecerán los medios con los que se harán las comunicaciones (como por ejemplo correo electrónico, llamadas telefónicas, herramienta de ticketing, etc..).

Todas las comunicaciones relacionadas con los servicios o con el correspondiente acuerdo de nivel de servicio se tendrán que realizar por las áreas o departamentos de la entidad contratante.

Obligatoriamente, la entidad adjudicataria dispondrá de un registro operativo de las peticiones o notificaciones realizadas por la entidad contratante, empleando, en su caso, la herramienta señalada a tal efecto al contrato basado. A todos los efectos este registro tendrá que ser también el registro de incidencias y peticiones, y tendrá que cumplir las premisas establecidas a la normativa de protección de datos.

Las incidencias y las peticiones de servicio mantendrán un flujo con el comunicante, procediendo a su cierre cuando se hubiera comunicado al mismo y no se considere ninguna acción adicional.

Será de obligatoria inclusión al registro:

- Hora de inicio de la incidencia y hora de finalización (incluyendo la hora en la que se produce la incidencia, la hora de notificación y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.

- Tiempo de resolución.
- Conclusiones y mejora.

En este sentido se tendrán en cuenta los puntos requeridos por la normativa aplicable, para la identificación, gestión y registro de incidencias, que puedan afectar al servicio , que serán acordados con la entidad contratante.

Ante las incidencias producidas y comunicadas correctamente, la entidad adjudicataria dispondrá de un tiempo de respuesta para la resolución de las mismas, así como las penalidades derivadas su incumplimiento, que estarán definidas en el correspondiente acuerdo basado según la criticidad:

- Alta: incidencias que suponen una parada de los sistemas de información de la entidad o que generan un impacto reputacional significativo.
- Media: incidencias que afectan al funcionamiento de más de un 5% de los empleados de la entidad.
- Baja: incidencias que generan un funcionamiento incorrecto, pero permite continuar trabajando a los empleados de la entidad.

Nivel de criticidad	Tiempo de respuesta	Tiempo de resolución
Alta	60 minutos	4 horas
Media	4 horas	48 horas
Baja	48 horas	5 días

En cuanto a las pruebas necesarias después de un incidente, y en su caso, después de acordarlo con la entidad contratante, se programarán generando el menor impacto posible en la operatividad del servicio. Todas las paradas técnicas del servicio serán en horarios previamente acordados con la entidad contratante.

Se tiene que tener en cuenta que el tiempo de resolución es el tiempo transcurrido entre la detección de la incidencia por el sistema de monitorización o comunicación de la incidencia a la empresa contratista por el canal previsto y la resolución documentada de la incidencia por parte de la empresa contratista.

Los tiempos de respuesta y de resolución de incidencias no se podrán ver afectados por aumentos esporádicos del número de incidencias.

7 LOTE 4: SERVICIOS DE CENTRE DEOPERACIONS DE SEGURIDAD (SOC)

Este lote del presente acuerdo marco tiene por objeto la contratación de un SOC operativo para la entidad contratante. El SOC tendrá que proporcionar servicios de monitorización, detección, prevención y respuesta a incidentes de seguridad, bajo la supervisión, directrices, soporte y acompañamiento de la Agencia ~~de Ciberseguretat de Catalunya~~ AgènciaAgencia de Ciberseguridad de Cataluña (en lo sucesivo, Agencia).

Del mismo modo, el SOC implantado tendrá que formar parte de la Red Nacional de Centros de Operaciones de Seguridad y compartir información con esta, que integrará el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y los de las otras administraciones públicas de ámbito nacional.

La Agencia es la entidad que coordina la protección y seguridad de la información y las infraestructuras de Cataluña ante las ciber amenazas, y la respuesta efectiva ante los mismos, siempre bajo el amparo de la colaboración y coordinación con diferentes actores a nivel local, nacional e internacional.

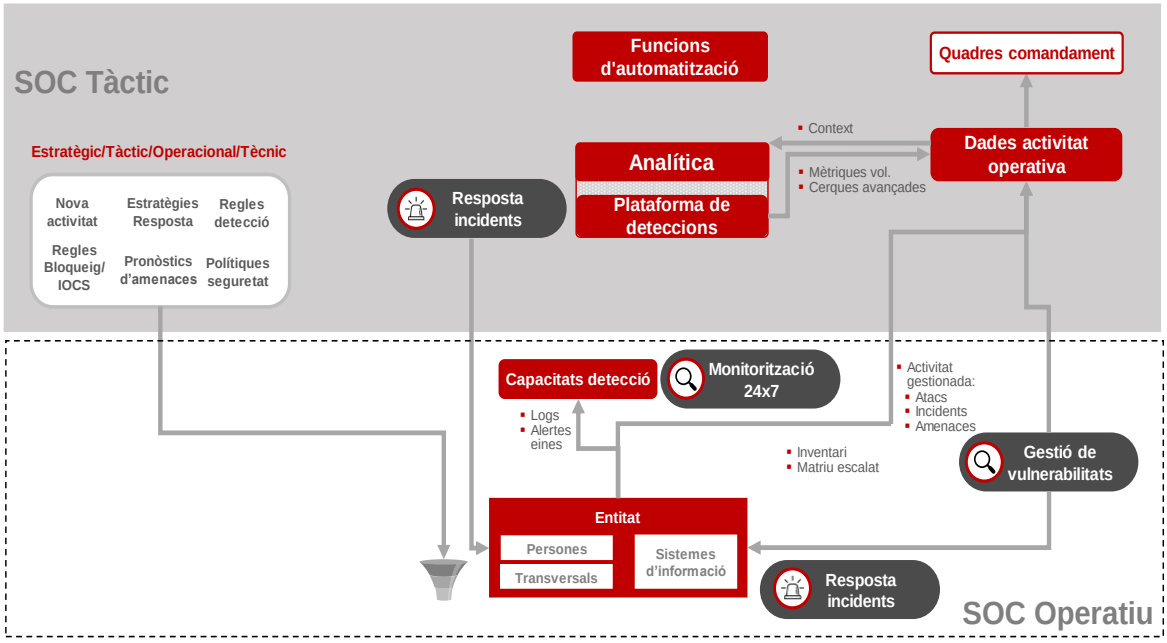
Una de las funciones principales de la Agencia es ejercer como SOC Táctico dentro del modelo de integración y gobierno operativo de los diferentes SOC's Operativos, definiendo la estrategia de prevención, detección, protección y respuesta ante amenazas, que estos tienen que tener como referencia para adaptar sus propias.

La estructura funcional del modelo de Integración y Gobierno Operativo pretende satisfacer los cuatro ejes fundamentales de la seguridad de la información frente a amenazas e incidentes de seguridad (detección, prevención, protección y respuesta) en un modelo de Integración con responsabilidad y operación distribuida, dónde:

- **El SOC Táctico** tiene las competencias de definir la estrategia de prevención, detección, protección y respuesta ante amenazas y acompañar a los Zocos Operativos en su adaptación. Para facilitar esta adaptación, el SOC Táctico propondrá reglas de correlación para detectar las principales amenazas a la entidad, políticas de seguridad a desplegar, contramedidas a desplegar a las herramientas de detección/protección de la entidad sobre amenazas activas, y estrategias de respuesta ante incidentes e información de inteligencia operativa. Igualmente liderará la respuesta a incidentes complejos segundos se establece a la Esquema Nacional de Seguridad (ENS).
- **El SOC Operativo** tiene la responsabilidad de dotar de visibilidad al SOC Táctico respecto a la actividad gestionada de la entidad, y el grado de exposición a la amenaza de forma que dote a la Agencia de disponer del conocimiento del entorno y el contexto necesario para hacer frente a las amenazas, ataques e incidentes, haciendo más productiva y operativa la estrategia definida por la entidad. Por eso es imprescindible la coordinación operativa con el SOC Táctico

con un seguimiento periódico según el que se establezca al modelo de integración del SOC Operativo de la entidad.

El siguiente esquema muestra a grandes rasgos el modelo de Gobierno Operativo de relación entre el SOC Táctico y los SOC's Operativos:



Las funciones, a modo de ejemplo no limitativo, que tendrán que ejecutar los SOC's Operativos en términos de integración operativa son:

- Adaptación de la estrategia definida por el SOC Táctico, mediante la definición y aplicación de los procedimientos e instrucciones operativas internas que apliquen a la entidad en cada caso, así como su actualización continúa, según los procesos de mejora continua que se puedan acontecer durante el servicio.
- Coordinación operativa con el SOC Táctico con seguimiento periódico según lo establecido al modelo de integración del SOC Operativo de la entidad, aportando en cualquier caso información actualizada que permita para asegurar la visibilidad de la actividad gestionada y el grado de exposición desde el SOC Táctico.

7.1 Implantación del SOC

La entidad adjudicataria se encargará de implantar el SOC así como de su operativa tanto a nivel técnico como organizativo.

Durante la fase embrionaria del proyecto de implantación del SOC, la entidad adjudicataria realizará un estudio preliminar por parte de un técnico propio in situ, a fin de establecer los siguientes hitos:

- Conocimiento de la infraestructura tecnológica de la entidad pública para la implantación del SOC y todas las herramientas que lo tienen que constituir.
- Identificación de los procesos, procedimientos y políticas de operación para una correcta adecuación del SOC a la entidad pública.
- Definición de la estrategia de implantación de las herramientas necesarias.

En el momento de la detección de un incidente a través del servicio de monitorización, o bien este sea comunicado por alguno de los canales establecidos, el SOC procederá a la gestión completa del incidente realizando, al menos, las actividades siguientes:

- Registrar, clasificar, valorar, priorizar y escalar los incidentes de seguridad que sean detectados a través del servicio de monitorización, que sean comunicados por el personal de seguridad o TIC de la entidad.
- Emitir las alertas oportunas ante acontecimientos de seguridad, tanto internas como terceros (autoridades nacionales y/u otras organizaciones).
- Realizar la notificación y documentación de los incidentes de seguridad según la Guía nacional de notificación y gestión de ciber incidentes y los protocolos establecidos conjuntamente con la entidad.

El ciclo de vida del incidente se gestionará según los procedimientos y la estrategia definida por el SOC Táctico.

Adicionalmente el adjudicatario tendrá que mantener actualizados y probados los procedimientos de respuesta ante incidentes.

Para la atención al servicio de Gestión de Incidentes de Seguridad el adjudicatario tendrá que contar al menos con un Punto Único de Contacto al intervalo de servicio ofrecido por la atención a incidencias, consultas, peticiones y gestión de notificaciones.

El responsable del contrato designado por la entidad contratante controlará el desempeño de los plazos acordados así como la calidad de la instalación y su adecuación a los requerimientos técnicos.

La empresa adjudicataria destinará una persona como responsable único durante todo el proceso de implantación y más adelante durante toda la vigencia del contrato. En caso de cambio de la persona responsable del contrato, se comunicará por escrito al responsable designado por el ente.

Todo el hardware y software necesario por el proyecto, que tendrá que estar homologado en el catálogo del CPSTIC, será por anticipado del adjudicatario y tendrá

que estar correctamente dimensionado con la infraestructura del ente público para poder ofrecer el servicio con garantías durante la duración del contrato, incluyendo las actualizaciones y/o ampliaciones oportunas.

El adjudicatario tendrá que tener en cuenta la existencia de uno en torno a alta disponibilidad en caso de existencia de máquinas virtuales a la entidad. Si se da el caso, todo aquello necesario (hardware, software y licencias) para estos recursos será proporcionado por la empresa adjudicataria.

Las tareas de licenciamiento, implantación, integración, configuración, automatización y pruebas tendrán que ser realizadas por el adjudicatario íntegramente, incluyendo todas las tareas a realizar hacia el equipamiento de la entidad pública que sean requeridas, y estarán basadas en el estudio de implantación previamente generado.

El adjudicado configurará y desplegará a través de la infraestructura de la entidad todas aquellas instalaciones y/o actualizaciones susceptibles de ser automatizadas. Estas tareas tendrán que ser desarrolladas, siempre que sea posible, de forma presencial a las dependencias de la entidad pública.

Las herramientas a implantar y desplegar que tiene que incluir la oferta del licitador su las siguientes, sin menoscabo de ampliar el catálogo según las necesidades del ente público:

- **Plataforma de correlación de acontecimientos de seguridad de la información (de ahora en lo sucesivo SIEM):**
  La empresa adjudicataria ofrecerá la implantación y despliegue de una plataforma dedicada a la recolección y análisis de datos a tiempo real de las alertas generadas por los componentes que conforman los diferentes sistemas de información de la entidad. Esta plataforma tendrá que estar calificada en el catálogo CPSTIC.

  Se recogerán y se centralizarán los registros y *logs* que contengan información y acontecimientos relacionados con la seguridad de la entidad, detectando incidentes y generando las alertas pertinentes.

  El periodo de retención de los *logs* será acordado con la entidad, y siempre será más grande de treinta (30) días para la operación de acontecimientos e incidentes y de seis (6) meses por el archivado.

- **Herramienta de intercambios**
  El adjudicatario del contrato ofrecerá la implantación y despliegue, en modo federado, la herramienta pertinente a fin de permitir el intercambio automático y fluido de los ciber incidentes con la Plataforma Nacional de Notificación y Seguimiento de ciber incidentes.

- **Sistema de Alerta Temprana de internet (SAT INET)**
  La empresa adjudicataria del servicio ofrecerá la implantación y despliegue del SAT-INET desarrollado por el CCN-CERT mediante la instalación de una sonda en la red de la entidad pública contratante.

- **Herramienta MicroCLAUDIA**
  La empresa contratante ofrecerá la instalación del agente ligero MicroCLAUDIA a la infraestructura de la entidad contratante con el fin de descargar y ejecutar las vacunas que lo CCN-CIERTO haya desarrollado.

- **Sistema de detección de ataques avanzados**
  La empresa contratante tendrá que ofrecer la implantación de las herramientas del CCN-CIERTO Carmen y Claudia de análisis y gestión de incidentes para identificar el compromiso de la red por amenazas persistentes avanzadas (APT).

El adjudicatario también se encargará de la instalación y/o automatización de la instalación de los diferentes agentes en el equipamiento de la entidad objeto de monitorización y de las actualizaciones necesarias que requiera la entidad contratante en su contrato basado. Este equipamiento y/o software tendrán que estar incluidos en el catálogo de productos del CPSTIC.

La implantación y despliegue de estas herramientas se realizará a las mismas condiciones que el resto del equipamiento a implantar sin intervención del personal municipal.

A la fase final de la implantación del servicio de SOC, el adjudicatario hará una evaluación de la seguridad de la entidad con las pertinentes pruebas que considere oportunas y se aplicarán las metodologías, procedimientos y actividades previstas al modelo de servicio.

7.2 Funciones y capacidades del SOC

Los siguientes apartados describen las funciones y capacidades principales requeridas al SOC Operativo en las áreas de prevención, detección, protección y respuesta dentro del modelo de Gobierno expuesto anteriormente.

Estas funciones se deberán ir adaptando para garantizar la óptima ejecución del contrato. En todo caso, estas tareas no eximen en ningún caso de la realización otras tareas adicionales necesarias para garantizar la ciberseguridad de la entidad contratante.

En todos los casos, permanecerá como base la adaptación de la estrategia definida por el SOC Táctico para cada materia, mediante la definición de procedimientos e instrucciones operativas internas y adaptación de herramientas que apliquen a la

entidad, para garantizar una óptima gestión, asegurando la visibilidad gestionada y el grado de exposición desde el SOC Táctico.

7.2.1 Disponibilidad del servicio

Atendiendo a la naturaleza del servicio de SOC, se puede requerir que su prestación se lleve a cabo en un horario 24x7 365 días en el año.

En estos casos se indicará esta necesidad en la contratación basada. Adicionalmente, se informa que los servicios incluidos en este Acuerdo marco pueden implicar la necesidad de llevar a cabo guardias y trabajos fuera de horario. En este sentido:

- Se considera guardia la disponibilidad por atención telefónica y actuación presencial en horario no laboral en el caso de actuaciones especiales o que la importancia de la incidencia lo requiere.
- A petición exprés de la entidad, se podría pedir la realización de algunas tareas fuera del horario de días laborables para garantizar el correcto desarrollo del servicio.

7.2.2 Capacidades de prevención

La prevención tiene como objetivo analizar y aplicar medidas que permitan anticiparse a la posible materialización de las amenazas a los activos, mitigando o eliminando el riesgo y el impacto a la entidad. Por eso acontece un factor clave conocer el estado de los activos en materia de seguridad, las vulnerabilidades y las amenazas que los pueden afectar, y actuar de forma preventiva.

En el modelo de integración y de Gobierno Operativo, se tendrá que prever que el SOC Táctico (SOC/CET de la Agencia), elaborará pronósticos de amenazas y alertas tempranas, y ejecutará tareas relacionadas con el servicio de vigilancia/monitorización digital (escapes de información, credenciales, suplantación de identidad, etc.), así como ejercicios de exposición a la amenaza, o pruebas técnicas de intrusión sobre los sistemas críticos.

En este contexto, el SOC Operativo implantado tendrá que ejecutar las siguientes funciones:

- Inventario y clasificación en base a la criticidad de los activos objeto de monitorización y gestión en aspectos relativos a la seguridad, para poder hacer un correcto diagnóstico de la seguridad y una gestión preventiva de los mismos. El SOC Operativo facilitará estos informes actualizados al SOC Táctico.
- Análisis y gestión de vulnerabilidades de los activos y sistemas de la entidad, ejecuciones de escaneos de vulnerabilidades y clasificación mediante *scoring* CVE, CVSS 3.1, etc. aplicando las implantaciones y despliegue de contramedidas a los

activos bajo su responsabilidad, que permitan evitar o minimizar el impacto de las vulnerabilidades mencionadas.

El SOC Operativo se coordinará con el SOC Táctico, informando de los resultados obtenidos, identificando especialmente los casos complejos y participante en el proceso de gestión de los casos, incluidos el seguimiento y el soporte en la gestión de estos.

- Análisis de la superficie de exposición externa de la entidad, revisando de forma activa las configuraciones, infraestructuras, y activos de la entidad expuestos a Internet, para identificar desde la perspectiva de un atacante externo, vulnerabilidades y debilidades que puedan ser explotadas, poder priorizarlas, gestionarlas y mitigarlas. Dentro de esta función se contemplan, escaneos de vulnerabilidades, auditorías técnicas y pruebas de intrusión necesarias, como pueden ser *pentests*, análisis de código fuente, tests de *phishing*, entre otros; los que generen resultados y diagnóstico de seguridad, que serán compartidos con el SOC Táctico de la Agencia. Igualmente propondrán pruebas de concepto y planos de acción para mitigar los aspectos identificados, realizando el seguimiento de las acciones correctivas.
- Determinación del grado de exposición de amenaza de la entidad según solicitud del SOC Táctico de los organismos competentes, aportando información actualizada respecto a activos de la entidad, información relevante del último análisis de seguridad, indicadores de compromiso relevantes por la amenaza y su evolución, e informas de grado de exposición, de forma que se pueda mantener el relato de la entidad respecto a la amenaza.
- Dar visibilidad de la actividad gestionada a los organismos competentes con seguimiento periódico según lo establecido al modelo de integración del ZOCO Operativo de la entidad, aportando en cualquier caso inventarios actualizados de los activos de la entidad, informas de actividad gestionada con exportaciones de las herramientas que se integrarán en un repositorio del SOC Táctico de la Agencia, y cuadros de mando accesibles. Igualmente se reportarán indicadores e informes que permitan evidenciar la eficacia de los planes de despliegue y contramedidas relativas a la prevención de amenazas. Se podrán solicitar igualmente informes detallados o ejecutivos según el tipo de amenaza.
- Mantener y evolucionar las herramientas y los procedimientos que sean objeto de su ámbito de responsabilidad y que necesarios para llevar a cabo estas tareas.

7.2.3 Capacidades de detección

La detección de amenazas tiene como objetivo identificar ciber amenazas y permitir aplicar medidas de mitigación y contención antes de que estas que causen un daño significativo a la entidad. En este sentido, las operaciones del SOC/CERT de la Agencia

giran alrededor del concepto de “perímetros de ciberseguridad” que, mediante un conjunto de actividades y tecnologías desplegadas y gestionadas, ayudan a mejorar la ciberseguridad de los sistemas de información, las infraestructuras transversales y las personas.

En el marco de la integración del modelo, el SOC Táctico tendrá que identificar a alto nivel los casos de uso para la detección de amenazas en base a los marcos de referencia como por ejemplo MITTRE ATT&CK, elaborará reglas de detección para nuevas amenazas y propuestas para misiones de ThreatHunting, y proporcionará indicadores de inteligencia operativa a fin de poder hacer una gestión de la seguridad efectiva.

En este contexto, el SOC Operativo implantado tendrá que ejecutar las siguientes funciones:

- Detección de actividad relacionada con ciber amenazas basándose en una monitorización y detección automática 24x7 de actividad relacionada con ciber amenazas, mediante herramientas de correlación tipo SIEM/XDR. Será responsabilidad del SOC Operativo el correcto mantenimiento, configuración y actualización de estas herramientas y sus fuentes integradas para permitir identificar potenciales amenazas, ataques o incidentes de seguridad sobre los activos dentro de su ámbito de responsabilidad.
- Implementación de reglas de detección de amenazas o casos de uso en las herramientas de correlación tipo SIEM/XDR, indicadas por el SOC Táctico y que sean de aplicación a la entidad, así como aquellas que, según el análisis de información de la actividad y contexto disponible, el SOC Operativo considere adecuados para permitir identificar potenciales amenazas, ataques o incidentes de seguridad sobre los activos dentro de su ámbito de responsabilidad.
- Monitorización de indicadores de compromiso sobre las herramientas de ciberseguridad para la búsqueda continúa de actividad relacionada con las amenazas.
- Análisis y gestión priorizada de las alertas de detección de amenazas, aplicando las implantaciones y despliegue de contramedidas a las herramientas perimetrales y activos bajo su responsabilidad, que permitan evitar o minimizar el impacto de las amenazas mencionadas.
- Ejecución de las misiones de ThreatHunting sobre la entidad a la que se da servicio, en base a los indicadores de inteligencia de amenazas, así como aquellas que, según el análisis de información de la actividad y contexto disponible, el SOC Operativo considere adecuados para detectar posibles exposiciones a las amenazas y actuar de forma preventiva sobre los activos dentro de su ámbito de responsabilidad.
- Elaboración y monitorización de cuadros de actividad en tiempo real y accesibles

de forma que permitan disponer de información en tiempo real del grado de exposición de la amenaza, evolución de los indicadores de compromiso, activos afectados y grado de adaptación de los planes de actuación y contramedidas, de cara a que el SOC Táctico pueda mantener el relato de la entidad respecto a las amenazas.

- Dar visibilidad de la actividad gestionada al organismos competentes con seguimiento periódico, aportando en cualquier caso informas de actividad gestionada y cuadros de mandos, accesibles. Por eso el SOC Operativo tendrá que ser capaz de recopilar, inventariar, registrar y documentar las evidencias de amenazas gestionadas, y extraer indicadores que permitan al SOC Táctico tener un relato de la entidad respecto a amenazas. Igualmente se reportarán indicadores e informes que permitan evidenciar la eficacia de los planes de despliegue y contramedidas relativas a la detección de amenazas. Se podrán solicitar igualmente informes detallados o ejecutivos según el tipo de amenaza.
- Mantener y evolucionar las herramientas y los procedimientos que sean objeto de su ámbito de responsabilidad y que necesarios para llevar a cabo estas tareas.

7.2.4 Capacidades de protección

La protección tiene como objetivo dar respuesta a aquellos acontecimientos significativos que supongan o puedan suponer un potencial incidente de seguridad. Esto incluye: aplicación o solicitud de aplicación de contramedidas, así como la participación en todo el proceso de gestión de los casos, incluidos el seguimiento y el soporte en comités de crisis cuando sea necesario.

Dentro del modelo de integración y de Gobierno Operativo, hay que tener en cuenta que el SOC Táctico prescribirá las políticas de detección/protección a desplegar sobre las herramientas de Ciberseguridad (mediante libros blancos o guías de configuración), así como acciones de protección enfrente a nuevos ataques y amenazas.
En este contexto, el SOC Operativo implantado tendrá que ejecutar las siguientes funciones:

- Operación de las herramientas de ciberseguridad de la entidad, configurándolas para que funcionen según las políticas de detección/protección prescritas, y administrándolas gestionando todo su ciclo de vida (mantenimiento y posta a punto, optimizaciones, actualizaciones, licenciamiento, etc.)
- Aplicación de contramedidas sobre las herramientas de ciberseguridad, para evitar o reducir el impacto sobre los activos de la entidad, el escalado de casos complejos a otros grupos resolutorios, así como la participación en todo el proceso de gestión de los casos, incluidos el seguimiento y el soporte correspondiente.

- Despliegue de indicadores de compromiso sobre las herramientas de protección/detección por la búsqueda continúa de actividad relacionada con las amenazas.
- Automatización de las tareas más concurrentes, de forma que se dé una rápida respuesta de ejecución y evitando errores debido a la acción humana.
- Dar visibilidad de la actividad gestionada al SOC Táctico con seguimiento periódico según lo establecido al modelo de integración del SOC Operativo de la entidad, aportando en cualquier caso informas de actividad gestionada y cuadros de mando, accesibles, que permitan monitorizar el despliegue de las fuentes de inteligencia. Por eso el SOC Operativo tendrá que ser accedido en modo auditoría y vía API en la configuración de las herramientas gestionadas.
- Mantener y evolucionar las herramientas y los procedimientos que sean objeto de su ámbito de responsabilidad y necesarios para llevar a cabo estas tareas.

7.2.5 Capacidades de respuesta a incidentes

La respuesta a incidentes tiene como objetivo hacer frente a los incidentes de seguridad, tanto de manera proactiva como reactiva. Adicionalmente tiene que garantizar la gestión correcta de las evidencias y la validez jurídica, así como proveer el conocimiento y los planos de actuación necesarios para reducir de manera efectiva y eficiente el impacto de las ciber amenazas dentro de los ámbitos de actuación.

Dentro del modelo de integración y de Gobierno Operativo, hay que tener en cuenta que el SOC Táctico definirá las estrategias de respuesta para incidentes de Ciberseguridad, y establecerá el modelo de relación y matriz de responsabilidades de los equipos de respuesta, liderando la respuesta ante incidentes críticos y apoyando al SOC Operativo en incidentes no críticos

En este contexto, el SOC Operativo implantado tendrá que ejecutar las siguientes funciones:

- Respuesta ante incidentes no críticos, en tiempos y en forma, minimizando el impacto, asegurando la erradicación y garantizando que no se puedan volver a repetir del mismo modo. Por eso se encargará de la gestión del incidente, así como de proveer el relato necesario respecto a la investigación para la toma de decisiones en el contexto de un incidente.
- Búsqueda proactiva de amenazas (Threat Hunting), para detectar posibles incidentes no detectados por los sistemas de detección desplegados, pero que pueden ser visibles vía la detección de anomalías o correlación avanzada de acontecimientos, o ejecutando los análisis forense posteriores. Así, búsqueda proactiva de amenazas proporcionaría información en el análisis forense para

enfocar la investigación, mientras que el segundo aportaría pruebas al Threat Hunting para confirmar las amenazas identificadas.

- Coordinación con el SOC Táctico para la respuesta ante incidentes críticos, ejecutando un primer análisis de la afectación, proveyendo el contexto necesario que ayude a la toma de decisiones del SOC Táctico a los diferentes comités. Por eso tendrá que recopilar, analizar las evidencias siguiendo un proceso que garantice la integridad de estas y de su cadena de custodia garantizando la validez ante un posible proceso judicial, así como aplicar las medidas de contención iniciales establecidas o aquellas indicadas desde el SOC Táctico como propuesta de contención, erradicación y/o recuperación.
- Dar visibilidad de la actividad gestionada al SOC Táctico con seguimiento periódico según lo establecido al modelo de integración del SOC Operativo de la entidad, aportando en cualquier caso informas de actividad gestionada y cuadros de mando, accesibles. Por eso el SOC Operativo tendrá que ser capaz de recopilar, inventariar, registrar y documentar las evidencias e incidentes gestionados e investigaciones realizadas, y extraer indicadores que permitan al SOC Táctico tener un relato de la entidad respecto a incidentes. Igualmente se reportarán indicadores e informes que permitan evidenciar la eficacia de planes de mejora o erradicación relativos a la respuesta a incidentes.
- Mantener y evolucionar las herramientas y los procedimientos que sean objeto de su ámbito de responsabilidad y que necesarios para llevar a cabo estas tareas.

7.3 Plataforma de correlación de acontecimientos de seguridad de la información (SIEM)

En el supuesto de que el ente contratante no disponga o desee operar con el sistema de gestión de acontecimientos de información de la empresa adjudicataria, esta tendrá que implantar un SIEM que esté reconocido en el catálogo CPSTIC, tal y como se establece al lote 1 de este mismo pliego.

En el supuesto de que la entidad contratante ya disponga de un SIEM, la empresa adjudicataria del servicio tendrá que poder acreditar que posee experiencia con el software y un equipo técnico humano con los conocimientos necesarios para operar con la plataforma establecida.

En cualquier caso, la empresa adjudicataria del servicio de monitorización de la seguridad tendrá que poder acreditar que opera con un software reconocido y homologado en el catálogo CPSTIC y que está capacitada a tal efecto.

El servicio tiene que permitir la monitorización y la correlación de acontecimientos de seguridad, integrando las fuentes de datos que generen todos los dispositivos y sistemas de red ofrecidos así como los sistemas preexistentes en el ente contratante, a

fin de detectar anomalías de seguridad y generar alertas que permitan la adecuada clasificación del nivel de amenaza de cualquier de los incidentes de seguridad detectados. El sistema tendrá que soportar la creación de tickets en el sistema de *helpdesk* del ente contratante, si se tercia, para aquellas actividades que tengan que ser atendidas por el personal de este.

El licitador detallará la arquitectura de componentes del sistema SIEM propuesto, incluyendo todos los elementos de recolección, agregación y procesamiento de acontecimientos, así como la ubicación de los mismos (en las instalaciones del ente público contratante, en las infraestructuras del propio licitador u otros a este efecto).

El licitador indicará las métricas de licenciamiento que sean aplicables al sistema SIEM ofrecido, justificando adecuadamente su dimensionado para las fuentes de datos de los sistemas que formen parte de su oferta, así como de las fuentes de los sistemas preexistentes en el ente contratante, durante toda la duración del contrato.

Se valorarán las automatizaciones y correlaciones a implantar en el SIEM, por lo cual, para su correcta valoración, se tendrán que detallar los casos de uso a implantar en la propuesta. También se valorará la inclusión de elementos que faciliten la integración con las herramientas del ecosistema del Centro Criptológico Nacional y el envío de tráfico de red de manera selectiva a estas.

El adjudicatario proporcionará, como mínimo cada tres meses, los registros de actividad completos de los sistemas ofrecidos en formato interoperable.

7.4 Organización del servicio

Estructura organizativa

Por parte de la entidad, se establecerá la figura del Responsable del Servicio, que será el encargado de dirigir y coordinar la relación con el adjudicatario.

Por parte del adjudicatario, del mismo modo, se establecerá un Responsable del Servicio, encargado de coordinar y garantizar el cumplimiento de los requisitos del servicio, asignando los medios adecuados para la correcta prestación del servicio.

Equipo de trabajo

Los integrantes del equipo de trabajo se concretarán en cada contrato basado en función del servicio requerido.

El personal incluido a la propuesta del licitador del contrato basado deberá reunir los requisitos mínimos establecidos como requerimiento del contrato basado para la categoría profesional concreta y función a desarrollar y, además, que los mismos

perfiles coincidan con los presentados a la propuesta efectuada por el adjudicatario en su oferta del presente acuerdo marco .

Si durante la ejecución del contrato surge la necesidad de sustitución de algún miembro del equipo de trabajo, el adjudicatario tendrá que motivar la solicitud con al menos dos semanas de antelación, y ser autorizada, si se procede, por la entidad. Dado el elevado impacto que supone la rotación de perfiles el adjudicatario velará para que esta rotación sea baja una vez aprobado el equipo de trabajo de cada contrato basado.

En general, si se produjera la sustitución de un miembro del equipo de trabajo, habrá un proceso bisiesto del conocimiento o solapamiento entre el recurso saliente y los recursos que asumen las tareas ejercidas por el recurso saliente, de 10 días hábiles mínimo para asegurar el traspaso de conocimiento interno.

Las empresas tendrán que disponer, como mínimo, de un equipo de trabajo formado por los siguientes perfiles:

- Responsable del servicio, las funciones del cual es garantizar servicio y gestionar la relación con la entidad.
- Un experto técnico en Seguridad. Las principales funciones serán las correspondientes a la prestación del servicios SOC:
    - Gestión de vulnerabilidades.
    - Monitorización y operación de la seguridad
    - Gestión de incidentes.
    - Generación de nuevas reglas, automatización e integración de despliegues ad hoc.
- Un experto en el despliegue de las herramientas SIEM propuestas a la oferta presentada.

Todos los perfiles tendrán que tener como mínimo **3 años** de experiencia en proyectos similares.

Seguimiento del servicio

En las reuniones de seguimiento participaran, al menos, el Responsable del Servicio de la entidad y del adjudicatario.

Durante las fases iniciales de puesta en marcha y de devolución del servicio se llevarán a cabo reuniones de seguimiento con periodicidad mensual. En estas reuniones, se llevará un seguimiento de la planificación y tareas realizadas, así como un análisis de riesgos por parte del adjudicatario.

Durante la fase de prestación del servicio se establece una periodicidad semestral para las reuniones de seguimiento, aunque la entidad podrá solicitar reuniones extraordinarias por la existencia de circunstancias que lo hagan necesario.

La empresa adjudicada entregará un informe mensual de actividad (que a la vez servirá para dar conformidad a las facturas) que recoja:

- Avance en el cumplimiento del objeto del contrato.
- Incidentes de seguridad que hay que destacar.
- Riesgos existentes y previstos.
- Otros aspectos relevantes en materia de seguridad de la información detectados y que tengan que ser conocidos por la entidad.

En caso de que, por cuestiones relacionadas con la prestación del servicio, fuera necesario el desplazamiento del personal del equipo técnico a cualquier ubicación, este desplazamiento iría a cargo del adjudicatario, sin que suponga un coste adicional.

Las reuniones de seguimiento se llevarán a cabo a las instalaciones de la entidad o en línea si la entidad está de acuerdo.

7.5 Acuerdos de Nivel de Servicio (SLA)

Las penalidades y los SLA de los contratos basados podrán ser especificados en el propio contrato, o establecer como genéricos los que se describen en este apartado:

Métrica	Objetivo	Descripción
Tiempo de detección	< 5 minutos	Tiempo en el que el SOC tiene que detectar un incidente de seguridad.
Tiempo de respuesta	< 30 minutos	Tiempo desde que se detecta el incidente de seguridad hasta que el SOC responde el incidente.
Tiempo de resolución de incidencias no críticas	24h	Tiempo desde que se detecta el incidente de seguridad hasta que se resuelve la incidencia no crítica.
Comunicación de incidentes	30 minutos	El tiempo máximo en el cual el SOC tiene que comunicar incidentes críticos a la dirección de la organización.

Los valores indicados a la mesa se podrán personalizar según las necesidades y recursos del ente contratante.

Los SLA's se revisarán y se actualizarán regularmente para garantizar que continúen siendo efectivos a medida que cambian las amenazas y las necesidades de seguridad del ente contratante.

Todas las comunicaciones relacionadas con los servicios o con el correspondiente acuerdo de nivel de servicio se tendrán que realizar por las áreas o departamentos de la entidad contratante.

Aun así, en los contratos basados se establecerán los medios mediante los cuales se harán las comunicaciones (como por ejemplo correo electrónico, herramienta de ticketing, llamadas telefónicas, etc..).

Obligatoriamente, la entidad adjudicataria dispondrá de un registro operativo de las peticiones o notificaciones realizadas por la entidad contratante, empleando, en su caso, la herramienta señalada a tal efecto a contrato basado. A todos los efectos este registro tendrá que ser también el registro de incidencias y peticiones, y tendrá que cumplir las premisas establecidas a la normativa de protección de datos.

Las incidencias y las peticiones de servicio mantendrán un flujo con el comunicante, procediendo a su cierre cuando se hubiera comunicado al mismo y no se considere ninguna acción adicional.

Será de obligatoria inclusión al registro:

- Hora de inicio de la incidencia y hora de finalización (incluyendo la hora en la que se produce la incidencia, la hora de notificación y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.
- Conclusiones y mejora.

En este sentido se tendrán en cuenta los puntos requeridos por la normativa aplicable, para la identificación, gestión y registro de incidencias, que puedan afectar al servicio , que serán acordados con la entidad contratante.

Anualmente, se remitirán estos valores en un informe a la entidad contratante.

Los tiempos de respuesta y de resolución de incidencias no se podrán ver afectados por aumentos esporádicos del número de incidencias.

8 LOTE 5: SERVICIOS DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD (ENTE)

La adecuación al Esquema Nacional de Seguridad, es un proceso que se podrá culminar a través de la ejecución y seguimiento del Plan de Seguridad generado en el lote 2 del presente Acuerdo marco. Sin embargo por aquellas entidades que requieran un proceso de adecuación específico al ENS se prevé este servicio que tendrá como objetivo la confección de los trabajos necesarios para la realización de una consultoría a la organización para la adecuación de sus sistemas de información al Esquema Nacional de Seguridad, estableciendo la política de seguridad en la utilización de los medios electrónicos así como los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información en el ámbito de la administración electrónica.

Aquellos sistemas que traten ficheros, ya sean o no automatizados, que contengan datos de carácter personal, también se analizarán desde los puntos de vista de la actual normativa en materia de protección de datos con carácter personal.

En todo caso, el objetivo final del servicio de adecuación al ENS es preparar adecuadamente los sistemas, el tratamiento de los datos y la organización del ente contratante para la certificación por parte de la Agencia de Ciberseguretat de Cataluña o por otras entidades de certificación acreditados este listado.

Objetivos y alcance

El proceso de implantación del ENS empezará con la elaboración del Plan de Adecuación, que será la base por el proceso de gestión continuada de la seguridad de la entidad contratante mediante la designación de roles, la constitución de órganos de seguridad, además de la adquisición de los compromisos de seguridad y de implantación, que se verán reflejados a la Política de Seguridad de la Información y el Plan de Adecuación, respectivamente.

La empresa adjudicataria tendrá que garantizar que sus sistemas de información que sustentan los servicios prestados al ser adjudicatarias de contratos basados del presente lote aplican las medidas de seguridad establecidas en el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENS). El adjudicatario tendrá que disponer de un certificado de desempeño del Esquema Nacional de Seguridad de nivel MEDIO, y aportar el certificado correspondiente y que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

8.1 Plan de adecuación

El Plan de Adecuación será el punto inicial por el proceso de implantación del ENS y estará compuesto por las siguientes actuaciones:

- Elaboración de la Política de Seguridad y la normativa correspondiente.
- Identificación de los servicios presentes y categorización de los sistemas de la entidad contratante, con la valoración de la información tratada.
- Realización de un análisis de riesgos.
- Elaboración de la Declaración de Aplicabilidad.
- Desarrollo de un Plan de Mejora de la seguridad a partir de las deficiencias que se hayan detectado.

El Plan de adecuación identificará tanto las personas y órganos responsables involucrados en la futura implantación como en la definición de las medidas de seguridad a implantar, conjuntamente con sus hitos y los recursos necesarios para llevar-las a término.

8.1.1 Política de Seguridad y normativa interna

La Política de Seguridad se sublimará en un documento de alto nivel, mediante el cual, la entidad definirá su compromiso al respecto de la seguridad de la información y los servicios que pueda prestar. En esta política se describirán los mecanismos implementados para una gestión continuada de la seguridad así como sus responsables. Estos contenidos, sin menoscabo de ser ampliados, serán los siguientes:

- Compromiso de cumplimiento de la totalidad del Real Decreto del ENS (principios básicos y requerimientos mínimos).
- Marco legal y regulatorio.
- Indicadores de cumplimiento de la normativa de protección de datos.
- Roles de seguridad y funciones designadas. Como mínimo serán los siguientes:
    - Responsable de la Información, y Responsables de los Servicios para todos aquellos sistemas que sean operados directamente por la entidad contratante.
    - Responsable de Seguridad y Responsable de Sistema, estructura del comité de seguridad y sus funciones o, según el caso, la estructura simplificada que prevé el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (PCE-RES).
- Detalle de los mecanismos implementados para la resolución de los conflictos entre los diferente roles asignados.
- Indicación sobre cómo se desarrollará, las revisiones previstas indicando la periodicidad de las mismas.

La Normativa Interna será un compendio de normas de carácter interno que se habrán definir e instaurar de cara al comportamiento de los usuarios de los sistemas presentes a la entidad contratante.

8.1.2 Identificación de los servicios presentes y categorización de los sistemas de la entidad contratante, con la valoración de la información tratada.

La empresa adjudicataria tendrá que categorizar los sistemas de información del ente contratante y realizar una declaración de aplicabilidad de acuerdo con la categorización realizada. C cambio que se realice en la categorización de los sistemas se tendrá que reflejar en la declaración de aplicabilidad, así como en el plan de mejora de la seguridad.

Con esta identificación se procederá a identificar la información tratada y su tipología, así como los servicios prestados por la entidad contratante y se procederá a su valoración tal y como establecen los principios del Anexo Y del Esquema Nacional de Seguridad.

En caso de adherirse a un perfil de cumplimiento específico, la adecuación se realizará intermediando microCENS, y se seguirá la metodología y plataforma prevista a tal efecto.

8.1.3 Análisis de riesgos

La empresa adjudicataria hará las tareas necesarias para asegurar que se cumplen las medidas del marco operacional según el definido en el artículo 14 y Anexo II del ENS para la categoría establecida por el sistema.

En base a esto, el análisis de riesgos se desarrollará bajo la metodología MAGERIT –metodología de análisis y gestión de riesgos elaborada por el "*Consejo Superior de Administración Electrónica*"-, determinando los riesgos que comportan los sistemas de información involucrados. Las herramientas a utilizar serán las previstas bajo esta metodología: PILAR bajo cualquier de sus versiones, además de la plataforma INÉS en caso de ser en línea.

En base a los riesgos, se desarrollarán una serie de tasques técnicas y medidas de protección por parte de la empresa adjudicataria para asegurar que se cumplen las medidas de protección según el definido en la declaración de aplicabilidad. A título indicativo y no exhaustivo, se señalan las tareas requeridas en este ámbito de trabajo:

- Implantar un registro de e/s de equipamiento.
- Realizar el etiquetado de soportes.
- Hacer tareas de concienciación y formación.
- Asegurar la inclusión y cumplimiento de los requisitos de seguridad en los aplicativos a desarrollar.
- Verificar uso correcto de los certificados digitales.
- Determinar y revisar los perfiles de seguridad a implantar en cada tipo de componente de los sistemas de información.

En caso de adherirse a un perfil de cumplimiento específico, la adecuación se realizará intermediando microCENS, y se seguirá la metodología y plataforma prevista a tal efecto.

8.1.4 Elaboración de la Declaración de Aplicabilidad.

En respondida al resultado del análisis de riesgos, la empresa a contratar deberá de elaborar una relación de las medidas recogidas al ENS que son de aplicación a los sistemas de la entidad contratante.

Para tal cuestión, se recurrirá a todo aquello detallado al Anexo II del ENS, teniendo que justificar la no aplicación de todas aquellas medidas que no puedan ser aplicadas debido a la casuística de la entidad.

La Declaración de aplicabilidad se tendrá que reflejar en un documento aprobado por el Responsable de Seguridad designado y estará basado en el perfil de categoría o perfil de cumplimiento específico que corresponda

En caso de adherirse a un perfil de cumplimiento específico, la adecuación se realizará intermediando microCENS, y se seguirá la metodología y plataforma prevista a tal efecto.

8.1.5 Plan de mejora

La empresa adjudicataria hará tareas de análisis y consultoría que permitan verificar el correcto cumplimiento de los aspectos tanto generales como específicos del ENTE, se detectarán las deficiencias que tenga el sistema y se realizará la propuesta de mejoras que se verán reflejadas en un plan de acción. A título indicativo y no exhaustivo, se señalan las tareas requeridas en este ámbito de trabajo:

- Realizar el análisis de vulnerabilidades de webs y aplicaciones.
- Realizar pruebas de intrusión en sistemas.
- Hacking ético.
- Asesoría en contratación y despliegue de componentes de seguridad (*web application firewall*, antivirus de pasarela, antivirus de servidores, sistema de gestión de incidentes de seguridad, sistemas de cifrado de soportes, sistemas de seguridad física, etc.).
- Mejora continua. Se harán tareas sistemáticas orientadas a la mejora continua de la adaptación al ENS.

El Plan de Mejora tendrá que mostrar qué deficiencias mejora en cada actuación, con su plazo de ejecución y las fechas de inicio y fin, y el coste aproximado que supondrá.

En caso de adherirse a un perfil de cumplimiento específico, la adecuación se realizará intermediando microCeENS, y se seguirá la metodología y plataforma prevista a tal efecto.

8.2 Tareas relacionadas con la protección de datos.

La empresa adjudicataria realizará las tareas de soporte necesarias por la adaptación del ente contratante al RGDP y la normativa derivada. A tal efecto, se tendrá que dar cumplimiento a los requerimientos previstos en el propio ENS en su Anexo II, según la guía CCN-STIC 808. Con carácter indicativo y no exhaustivo se realizarán las siguientes tareas:

- Análisis situación actual. La empresa adjudicataria realizará un análisis de la situación actual respecto a los requisitos marcados en materia de protección de datos.
- Hoja de ruta. La empresa adjudicataria establecerá las deficiencias entre la situación actual y la situación requerida para adaptarse a la normativa de protección de datos y realizará la hoja de ruta con las acciones necesarias para adaptarse.
- Ejecución de tareas de adaptación. La empresa adjudicataria hará las tareas necesarias para adaptarse a los requisitos definidos en materia de protección de datos.
- Colaboración con el Delegado de Protección de Datos del ente contratante. La empresa adjudicataria asumirá el asesoramiento sobre las funciones del subdelegado de protección de datos de la entidad contratante, si se tercia, según la normativa vigente.
- Mejora continua. Se harán las tareas necesarias para establecer un ciclo de mejora continua en materia de protección de datos.

8.3 Gobernanza de la seguridad.

La empresa adjudicataria hará las tareas necesarias para poder realizar una gobernanza eficiente de la seguridad y adaptación al RGPD, así como el cumplimiento y gestión de la información requerida por las aplicaciones actuales y futuras que lo CCN-CERT pose a disposición de las administraciones públiques. Con carácter indicativo y no exhaustivo se harán las siguientes tareas:

- Rellenar la información requerida en el informe anual de seguridad por la aplicación INES o cualquier que la sustituya.
- Realizar la gestión de incidentes. Incluyendo la gestión a través de la aplicación LUCIA o la correspondiente de la Agencia de Ciberseguridad de Cataluña.
- Revisar y mantener actualizado el sistema de indicadores.
- Mantener y actualizar el plan de adecuación

8.4 Gestión del cambio y formación.

La empresa adjudicataria realizará la gestión del cambio y formación necesaria en temas de seguridad y protección de datos. La formación será, como mínimo, la requerida por la normativa de aplicación. Se incluye formación específica en el ámbito del ENS y la protección de datos.

- Se harán las tareas necesarias de difusión y formación a todos los usuarios de la entidad contratante en temas de seguridad y protección de datos. La empresa adjudicataria aportará un Plan de Comunicación y un Plan de Formación, en este sentido, que incluirá como mínimo las acciones planteadas a continuación, y que será aprobado previamente por el Responsable del Contrato.
- Se realizará formación al personal designado por la entidad contratante durante 15 días hábiles presenciales, al menos, cada año del contrato, tanto en temas de seguridad como en protección de datos.

8.5 Acompañamiento a la obtención de la conformidad.

La empresa adjudicataria acompañará a la entidad contratante en el proceso de obtención de la certificación de conformidad con el ENS. Con carácter indicativo y no exhaustivo se harán las siguientes tareas:

- Preauditoria. La empresa adjudicataria tendrá que realizar una auditoría previa interna que permita analizar el grado de implantación y prepare la entidad para la auditoría de obtención de la conformidad. A partir del resultado de la misma se establecerán las tareas a realizar para resolver las no conformidades detectadas y los puntos de mejora.
- Soporte al proceso de auditoría. La empresa adjudicataria tendrá que dar el soporte necesario en el proceso de auditoría para asegurar que esta se pueda realizar en las mejores condiciones, ayudará en las gestiones con la empresa certificadora y acompañará presencialmente en el proceso de auditoría externa.
- No conformidades. Una vez realizada la preauditoria y la auditoría de conformidad, se analizará y establecerá el plan de trabajo para resolver las no conformidades detectadas, así como los puntos de mejora u otros aspectos que se consideren en estos procesos. Este plan de trabajo se tendrá que llevar a cabo por parte de la empresa adjudicataria.

Por el seguimiento del servicio se nombrarán los interlocutores necesarios a nivel de áreas funcionales que la entidad contratante crea oportunas a fin de poder participar en las reuniones adyacentes al proyecto y que llevarán a un informe final con análisis de las no-conformidades respete el modelo de seguridad propuesto por el ENS.

El ente público recibirá un plan de formación y sensibilización, generado por el adjudicatario, para el personal implicado en los procedimientos afectados por el ENS,

dando énfasis a la formación impartida al personal técnico que gestionará la seguridad informática y que velará por su seguimiento y cumplimiento.

En todo caso, estos trabajos representan una especificación de la "**Guía CCN-STIC 806 – Plan de adecuación al ENS"**.

8.6 Entregables

Como resultados de los trabajos realizados, la empresa adjudicataria tendrá que entregar al ente contratante como mínimo los siguientes entregables, durante la ejecución del contrato.

Tareas relacionadas con el ENS

- Documentación generada en las tareas del ENS.
- Planes de adecuación e informes de seguimiento.
- Informas de tareas realizadas.

Tareas relacionadas con la protección de datos

- Documentación generada en las tareas de protección de datos.
- Planes de adecuación e informes de seguimiento.
- Informas de tareas realizadas.

Gobernanza de la seguridad

- Documentación generada en las tareas de gobernanza.

Gestión del cambio y formación

- Plan de formación detallado. Independientemente del plan de formación propuesto en la propuesta técnica, el plan de formación final se tendrá que consensuar y aprobar por parte del ente contratante.
- Plan de comunicación detallado, con las acciones de comunicación y difusión a realizar.
- Informas de las acciones de comunicación y formación realizadas (sesiones, asistentes, contenido, incidencias, encuesta de satisfacción...).
- Documentación utilizada para realizar las acciones de comunicación y formación.

Acompañamiento a la obtención de la conformidad

- Preauditoria.
- Planes de resolución de no conformidades y puntos de mejora.
- Documentación de seguimiento de los planes de resolución.

La documentación generada durante la ejecución del contrato es de propiedad exclusiva del ente contratante sin que el adjudicatario pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la exprés autorización del ente público, que la daría en su caso previa petición formal del contratista con expresión del fin. La documentación se librará en formato editable y en formato pdf.

A la presentación de los resultados se intentará diferenciar claramente los ámbitos del Esquema Nacional de Seguridad y del cumplimiento de normativa en materia de protección de datos de carácter personal.

8.7 Equipo de trabajo

La empresa de consultoría adjudicataria aportará el personal que sea necesario para el mejor cumplimiento del objeto del contrato. Este personal contará con las competencias, conocimientos y calificaciones necesarios según la vigente, y posterior si hubiera, normativa sobre este tema; y su designación tendrá que ser aprobada por el Responsable del Contrato, quién a lo largo del desarrollo del mismo podrá solicitar su relevo o sustitución.

El personal de la empresa adjudicataria que desarrolle el servicio objete de esta contratación actuará, junto con los recursos humanos designados por la entidad, en cada una de las fases que acontezcan necesarias.

Los licitadores tendrán que describir en sus ofertas el equipo de trabajo propuesto para la prestación del servicio, basándose en los perfiles detallados en este apartado. En general, tendrán que presentar:

- Perfiles que forman parte del equipo de trabajo.
- Funciones específicas de cada uno de los perfiles dentro del equipo.
- Currículum de los perfiles propuestos, así como dedicaciones y funciones de estos.
- En su caso, copias de las certificaciones solicitadas.

Los perfiles que realicen los servicios detallados en el presente pliego, tendrán que adecuarse a los propuestos por el adjudicatario. Estos perfiles serán los siguientes:

Cabe de proyecto:

- Dirección, seguimiento y control del proyecto.
- Generación de la documentación de control.
- Revisión de la documentación generada por el equipo de trabajo.
- Coordinar y organizar las relaciones del equipo de trabajo con los responsables de la entidad en forma de reuniones periódicas de seguimiento.

Un consultor experto en adecuación al ENS:

- Dirección y ejecución de las tasques técnicas y operativas.
- Documentación técnica.
- Seguimiento y corrección de los planes de acción.
- Propuestas de mejora continua.
- Dirección de la gobernanza de seguridad.
- Coordinación con el DPD de la entidad contratante.

Todos los perfiles tendrán que tener como mínimo 3 años de experiencia en proyectos similares.

La falsedad en el nivel de conocimientos técnicos de los perfiles que se incorporen, deducida del contraste entre la información especificada en la oferta y los conocimientos reales demostrados en la ejecución de los trabajos, implicará la sustitución del recurso por otro en un plazo no superior a 15 días laborables.

Además, en el supuesto de que sea necesario realizar una sustitución de un recurso, las empresas se comprometen a reemplazar este recurso por otro de igual perfil en un plazo no superior a 15 días laborables.

9 LOTE 6: SERVICIOS DE FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD AD HOC

Para impulsar una cultura de ciberseguridad, las entidades locales tienen la necesidad de disponer y ejecutar un plan de formación donde se identifiquen las necesidades de las habilidades y conocimientos en ciberseguridad para cada puesto de trabajo.

La empresa adjudicataria, definirá las acciones formativas necesarias por la capacitación y concienciación por la totalidad de la plantilla de la administración pública que permita diseñar y desplegar las fases de actuación del Plan de concienciación y formación usando diferentes niveles de contenidos previamente definidos, con una personalización y adaptación sobre contenidos existentes.

Las actividades prácticas de concienciación tienen que poder incluir la realización de campañas simuladas de estafas digital utilizando los medios disponibles (correo electrónico, Intranet, SMS..).

El objetivo de los aprendizajes de la formación tiene que ser capacitar las personas trabajadoras a utilizar las herramientas de ciberseguridad que los permite garantizar la confidencialidad de la información que utilizan durante su actividad profesional (con especial énfasis en el trabajo a distancia), así como conocer en detalle los protocolos y metodologías que el ente local ha adoptado para garantizar la seguridad y la privacidad de la información.

En este sentido, la formación en Ciberseguridad tiene que tener como objetivos de alto nivel el logro, por parte del alumnado, de las siguientes capacidades, sin menoscabo de ampliar el alcance del conocimiento impartido a voluntad del ente contratante:

- Autoprotegerse en el uso de las redes.
- Protegerse del *malware*.

- Protegerse del *phishing* y los engaños de Internet.
- Mejorar la seguridad de las herramientas ofimáticas y mensajería.
- Evitar el *hacking* de los sistemas de información.

El plan de formación se tiene que dirigir a personas trabajadoras que quieran proteger documentos confidenciales y conocer en detalle los sistemas y metodologías a seguir para garantizar la seguridad y la privacidad de la información.

En esta línea, se tienen que presentar las medidas de seguridad TIC que hay configuradas a la organización (herramientas y dispositivos) además de indicar como se garantiza la protección de los datos del ente local y las personas usuarias de los servicios informáticos del municipio.

El contenido se tiene que trabajar mediante lecturas, videos, ejercicios y cuestionarios los protocolos a seguir para mejorar las prácticas en ciberseguridad y tiene que apoyar mediante servicios de transcripción para personas sordas.

El adjudicatario proporcionará material de formación y concienciación, y se encargará de su actualización.

9.1 Niveles de formación

La empresa adjudicataria definirá las acciones formativas necesarias por la capacitación y concienciación de la totalidad de la plantilla del ente contratante utilizando diferentes niveles de contenido previamente definidos, con una personalización y adaptación sobre los contenidos que se describirán a continuación.

9.1.1 Nivel básico de formación

Los contenidos de formación y concienciación considerados de nivel básico en ciberseguridad que se dirigen a todos los empleados públicos precisen de una identificación/validación continua de la Agencia de Ciberseguridad y se estructuran en unos módulos (del conocido como *Curs de Ciberseguretat i Protecció de Dades en el lloc de treball*) y que como a referencia se disponen de la siguiente estructura de contenidos:

1. El puesto de trabajo

    - Conocimiento y presa de conciencia del hábitos y acciones cotidianas que pueden afectar la seguridad de la información.
    - Concienciación de las buenas prácticas en el uso de cuentas personales y el trato de las credenciales de acceso.
    - Fomento del uso del bloqueo de la estación de trabajo.
    - Conocimiento de los diferentes niveles de confidencialidad de la información.

- Conocimiento de los puntos principales de la política de seguridad de la información
- Conocimiento de buenas prácticas por atención ciudadana por medios digitales.

2. Contextos de seguridad

- Concienciar sobre el rol activo de los trabajadores para favorecer la seguridad a los equipamientos públicos.
- Conocer medidas de protección en el marco del trabajo a distancia: uso de VPN o redes wi-fi.
- Conocer herramientas autorizadas para videoconferencias.
- Conocer buenas prácticas con herramientas de e-administración: por ejemplo, IdCat.

3. Prevención de riesgos

- Conocer las principales técnicas de ciberataques referidas a las principales amenazas en el mundo local: malware-ransomware, phishing...
- Aprender a identificar las peculiaridades de cada herramienta de ataque en el contexto de herramientas de ofimática/ mensajería usado.
- Conocer los protocolos de organización y técnicos en caso de ser víctimas de un ataque exitoso.
- Conocer las principales medidas para hacer frente a los principales ciberincidentes y herramientas que aseguran el acceso a las aplicaciones.

4. Tratamiento de datos personales

- Conocer el concepto de datos confidenciales en el marco de la Administración pública.
- Conocer las bases y el marco normativo de la LOPDGDD.
- Conocer las tipologías de datos y las medidas de protección asociadas.
- Conocer como aplica el Esquema Nacional de Seguridad (ENS) y los perfiles de cumplimiento previstos al mundo local.
- Conocer las principales formas de cifrado de la información.

5. Evitar pérdidas de datos y cumplir las normas:

- Ser consciente de la importancia de notificar los incidentes de seguridad y analizar algunos casos.
- Ser consciente de la destrucción de la información obsoleta y conocer el mejor sistema para hacerlo.
- Conocer medidas de seguridad basadas en las copias de seguridad y ser conscientes de la importancia.

- Conocer riesgos de las memorias USB externas y los dispositivos móviles.

Se recomienda la modalidad formativa en un entorno virtual de aprendizaje propio o de un tercero (Diputaciones o Consejos comarcales que dispongan del curso).

Esta formación tiene que comportar las siguientes acciones formativas que la empresa adjudicataria tendría que proponer, asociadas de cara al aprovechamiento y consolidación de los conocimientos impartidos:

- Dinamización del curso, con dedicaciones temporales de hasta 5 horas
- Talleres de sensibilización basados con dosieres didácticos sobre los contenidos básicos
- Difusión y comunicación de píldoras (infográficas) referentes a este contenido estructurado, para acompañar el contenido auto formativo, en intranets, correo corporativo...
- Desarrollo de ejercicios de habilidad
- Ejercicios prácticos donde se simulen casos de uso de las situaciones expuestas en el curso
- Cuestionario/quiz/test que permita detectar aprovechamiento, comprensión y evaluación del contenido desarrollado en el curso

9.1.2 Nivel avanzado de formación

Los contenidos de formación y concienciación considerados de nivel avanzado en ciberseguridad estarán dirigidos a empleados públicos que tienen que desarrollar capacidades técnicas o legales en relación a la materia a fin de contar con un abanico más amplio de conocimientos y habilidades.

En los últimos años, el Área de Cultura de Ciberseguridad de la Agencia, conjuntamente con entidades municipalistas y las Diputaciones, han desplegado un catálogo de cursos de ciberseguridad de este nivel que pueden servir de base por la reutilización para que la empresa adjudicataria tenga que hacer una adaptación mínima pero que no represente un rediseño significativo del contenido.

Estas capacidades se adaptarán en cursos que tengan una dedicación mínima de 5 horas y podrán estar estructurados en los siguientes temas:

- Modelo de análisis de riesgos de ciberseguridad de la protección de datos.
- Análisis y gestión de riesgos de sistemas de información.
- Aproximación al µCeENS (adecuación para la obtención de la Certificación de Conformidad).
- Seguridad en entorno Cloud.
- Hacking ético: herramientas de auditoría y OWASP.
- Respuesta a incidentes.
- Bastionado de redes y sistemas.

- Gestión de las vulnerabilidades.
- Seguridad en las aplicaciones web.

Se recomienda la modalidad formativa mixto, presencial y en entorno virtual de aprendizaje propio o de un tercero. Y también que combine contenido teórico de los conceptos que se desarrollan y práctico con uso de herramientas o casos de uso que aplican en el mundo local. En este sentido es exigible una evaluación final que permita documentar el aprovechamiento y aplicabilidad en las entidades del mundo local donde provienen los usuarios/se solicitantes del curso.

La empresa adjudicataria deberá hacer propuestas de nuevos contenidos de cursos pero requiere una validación de la Agencia de Ciberseguridad para poder ser también compartida en el catálogo de cursos de ciberseguridad disponibles por el mundo local.

9.2 Itinerarios de perfiles especializados de ciberseguridad

La empresa adjudicataria tiene que ofrecer una propuesta de cara a colaborar/participar en la actividad que desarrolla la Ciber academia de la Agencia de Ciberseguridad, para desplegar diferentes itinerarios formativos que se dirigen específicamente a los técnicos del mundo local que quieren profundizar y ampliar conocimientos, en habilidades y competencias, requerido por ejemplo por una promoción interna.

Los perfiles de itinerarios previstos a desarrollar cursos se encuentran descritos al documento "European Cybersecurity Skills Framework (ECSF)" de "*The European Union Agency for cybersecurity" (ENISA)*.

Los contenidos formativos organizados van desde cimientos de ciberseguridad hasta un desarrollo operativo de herramientas específiques. Estos itinerarios tendrán cursos en diferentes niveles que permiten:

- N1: Conversar /iniciación.
    - Se dispone del conocimiento general sobre la competencia y sus implicaciones en la seguridad pudiendo realizar tareas sencillas relacionadas.
- N2: Hacer / Creación y ejecución de acciones.
    - Tiene conocimiento suficiente sobre procesos concretos y como la competencia se implementa en los sistemas, es capaz de ejecutar las tareas propias del puesto de trabajo y además sigue metodologías y procesos de trabajo
- N3: Modificar / Participación en los cambios.

Dispone de conocimientos avanzados sobre la mayoría de procesos del alcance de la competencia, configuraciones e integraciones con el resto de sistemas relacionados. Trabajo autónomo.

- N4: Liderar / Toma de decisiones.
    - El conocimiento profundo de la competencia también a nivel teórico y de buenas prácticas, diseña nuevos procesos seguros desde su concepción, modifica metodologías existentes y establece nuevas políticas y estrategias en su campo.

En este sentido, se requerirán formadores que puedan desarrollar los cursos en sesiones teóricas (síncronas/asíncronas en streaming), en la definición de actividades ad hoc o en el desarrollo o corrección de prácticas por los alumnos, en entornos presenciales o en espacio virtual.

9.3 Otros secciones formativas complementarias

La empresa adjudicataria realizará propuesta de actividades prácticas de concienciación y complementarias a los niveles e itinerarios descritos con anterioridad, que se vincularán al propio Plan de concienciación y formación previsto, como por ejemplo:

- Campañas simuladas de estafas digital utilizando los medios disponibles por el ente local.
- Esquemas de gamificación o sensibilización para las personas que desarrollan funciones directivas del mundo local.
- Elementos comunicativos que involucran la participación de la ciudadanía como usuarios activos por la mejora en ciberseguridad de los servicios prestados por el ente local.

Estas actividades también requerirán la inscripción y registro en un catálogo de actividades compatibles.

10 LOTE 7: SERVICIOS DE CSIRT (COMPUTER SECURITY INCIDENTE RESPONSE TEAM)

El presente lote del acuerdo marco tiene por objeto la contratación de un servicio de CSIRT (*Computer Security Incidente Response Team*) que tendrá como misión la gestión y respuesta a incidentes de ciberseguridad, así como en el análisis forense digital para investigar y comprender estos incidentes. Este servicio tiene como objetivo minimizar el impacto de los incidentes, restaurar las operaciones normales y proporcionar información crítica para mejorar las defensas de seguridad de las entidades contratantes.

El servicio de CSIRT tendrá que coordinarse con las capacidades de respuesta en incidentes del SOC que apoye a la entidad, bien sea el SOC Operativo de la misma entidad o el de la Agencia de Ciberseguridad.

Con el funcionamiento de este servicio, los objetivos a cumplir a nivel organizativo son los siguientes:

- Reducción del Impacto de los Incidentes: Una respuesta rápida y efectiva, desde el minuto cero, minimiza el mal causado por los incidentes de seguridad.
- Mejora de la Seguridad: El análisis forense proporciona información crítica para fortalecer las defensas y prevenir futuros ataques.
- Cumplimiento Normativo: Asegura que la organización cumpla con las normativas y regulaciones de protección de datos.
- Recuperación Rápida: Dota al ente contratante de procedimientos dedicados muy definidos que permiten una rápida restauración de la operativa normal.

10.1 Características del servicio

El servicio de CSIRT ofrecido por la empresa contratada tendrá que tener, sin menoscabo de ampliar el catálogo, las siguientes características:

- Preparación (esta fase se prevé en caso de contratar el servicio antes de sufrir un incidente de ciberseguridad)
  - Identificación y documentación de la información de contexto de la entidad, potencialmente necesaria durante la gestión de un incidente.
  - Evaluación de la entidad y su infraestructura, desde el punto de vista de la gestión de un incidente, para mesurar y mejorar las capacidades de respuesta disponibles.
  - Mantenimiento de las matrices de escalado relevantes en caso de incidente.
  - Elaborar un procedimiento de respuesta a incidente según el ENS estableciendo el protocolo de comunicación en caso de incidente (equipo de respuesta).
  - Capacidad de integración del servicio en un Plan de Continuidad de Negocio basado en el ENS.
- Monitorización y Detección (esta fase se prevé en caso de contratar el servicio antes de sufrir un incidente de ciberseguridad)
  - En caso el caso que sea necesario, despliegue puntual de herramientas de detección, respuesta y con capacitado forense, tipo EDR, para ganar visibilidad y capacidad de detección y respuesta a amenazas durante el incidente.
- Respuesta a Incidentes

  - Disponibilidad de un Equipo de Respuesta a Incidentes (IRT) especializado 24/7.
  - Determinación de la gravedad de los incidentes.
  - Desarrollo e implementación de un Plan de Respuesta a Incidentes.
  - Procedimientos y actuación para la contención de amenazas luego que sea adecuado y evitar así la propagación del incidente aislando los sistemas comprometidos y/o bloqueando accesos no autorizados.
  - Medidas para la erradicación de amenazas identificadas a fin de limpiar los sistemas afectados y asegurar su integridad.
  - Capacidad de coordinación con otros equipos y partes interesadas durante incidentes.
  - Investigación activa de atacantes dentro de los sistemas del ente contratante.
- Análisis Forense Digital
  - Recolección de evidencias: Se recopilaran evidencias digitales de todos los sistemas por los que sea necesario de manera meticulosa para asegurar su integridad y validez legal.
  - Análisis forense: Utilizando herramientas avanzadas, se analizará la evidencia recopilada para determinar el origen, la metodología y el impacto del ataque. Este análisis incluye la identificación de vulnerabilidades explotadas y la reconstrucción de la cronología del incidente.
  - Elaboración de informes forenses detallados y comprensibles.
- Mitigación y recuperación
  - Procedimientos para la restauración de sistemas: Se llevaran a término procedimientos para restaurar los sistemas afectados en su estado operativo normal de manera segura. Esto incluye la reinstalación de sistemas, la aplicación de parches y la actualización de configuraciones de seguridad que sean necesarios.
  - Aseguramiento de la continuidad del negocio durando y después de un incidente.
  - Implementación de soluciones para prevenir la recurrencia de incidentes, que pueden incluir la mejora de configuraciones y la aplicación de soluciones tecnológicas adicionales.
- Revisión post incidente y mejora continúa
  - Evaluación post incidente: Se realiza una evaluación detallada del manejo del incidente para identificar lecciones aprendidas y áreas de mejora. Esto incluye la revisión de la efectividad de la respuesta y la identificación de cualquier brecha en los procedimientos de seguridad.
  - Creación de informes: Los investigadores tendrán que elaborar un informe donde se detalle el evento de seguridad tratado, y si se tercia, la identificación

de los atacantes. En estos entregables se entregarán también las recomendaciones de cara a la actualización de políticas y procedimientos.
- Asesoría legal en temas relacionados con la ciberseguridad, gestión de la conformidad con leyes y regulaciones, soporte en la preparación de informes y evidencias para procedimientos legales.
- Evaluación y gestión de riesgos de seguridad, aseguramiento del cumplimiento con normativas y estándares de seguridad.
- Desarrollo y ejecución de planes de recuperación de desastres, aseguramiento de la continuidad del negocio durando y después de un incidente.

10.2 Cumplimiento Normativo y Confidencialidad.

El servicio de CSIRT propuesto por parte del la empresa tendrá que proporcionar protección legal en base al cumplimiento de las normativas legales y estándares. En base a este precepto, tendrá que cumplir con las siguientes normativas y estándares:

- Normativa de Protección de Datos Personales (GDPR)
- Compliance Corporativo: Todas las operaciones realizadas al servicio de CSIRT tendrán que estar alineadas con las políticas de seguridad, confidencialidad y privacidad del ente contratante.
- La empresa adjudicataria tendrá que garantizar que sus sistemas de información que sustentan los servicios prestados al ser adjudicatarias de contratos basados del presente lote aplican las medidas de seguridad establecidas en el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENTE). El adjudicatario tendrá que disponer de un certificado de desempeño del Esquema Nacional de Seguridad de nivel MEDIO, y aportar el certificado correspondiente y que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

10.3 Modalidad de prestación del servicio.

La adjudicación del servicio CSIRT se formalizará mediante un **contrato de servicios por suscripción** que cubra todas las necesidades de preparación, monitorización, respuesta a incidentes, análisis forense y recuperación puesto-incidente. Este contrato, establecido a largo plazo (anual o plurianual), garantizará la cobertura de los servicios CSIRT para la entidad contratante, asegurando la disponibilidad 24x7 del servicio y una respuesta inmediata ante cualquier incidente de ciberseguridad. Este modelo resulta especialmente adecuado para entidades con requisitos elevados de seguridad y necesidad de respuesta ágil.

El adjudicatario tendrá que ofrecer la contratación del servicio con la modalidad de pago de servicios por suscripción según las necesidades específicas de la entidad:

> Un contrato de suscripción anual o plurianual que tendrá que cubrir todos los servicios de preparación, monitorización, respuesta a incidentes, análisis forense y recuperación post incidente. Este tipo de contrato garantizará la disponibilidad continua del servicio y ofrecerá al CSIRT un conocimiento en profundidad de la entidad, mejorando la calidad y rapidez de la respuesta.

Las empresas licitadores de este servicio CSIRT tendrán que ofrecer un catálogo de tarifas según la medida de la entidad y el nivel de los incidentes que se cubren. Este catálogo, consta de dos niveles de incidencia y se segmenta según el número de trabajadores de la entidad.

Catálogo de tarifes propuesto

El catálogo se basa en una estructura que combina:

- **Volumen de la entidad contratante** según el número de trabajadores:
  - Menos de 15 trabajadores.
  - Entre 15 y 50 trabajadores.
  - Entre 50 y 100 trabajadores.
  - Entre 100 y 500 trabajadores.
  - Más 500 trabajadores.
- **Nivel de complejidad del incidente** gestionado:
  - Nivel 1: Incidentes leves y moderados

    Este nivel incluye incidentes que afectan servicios no críticos pero que pueden tener impacto operativo significativo, con potencial de escalar. Incluye, por ejemplo, infecciones por malware en estaciones de trabajo o anomalías de seguridad en redes internas que impactan a un pequeño número de dispositivos o usuarios. Incluye problemas como intentos de phishing detectados y ataques de baja complejidad que no han comprometido sistemas.

  - Nivel 2: Incidentes críticos

    Este nivel incluye los incidentes de nivel 1 y también los incidentes con afectación grave para la infraestructura crítica o que comprometen datos sensibles u operaciones esenciales o que generan un impacto reputacional significativo. Incluye ataques de ransomware, robo de datos, acceso no autorizado a sistemas o denegaciones de servicio o sabotaje digital que impiden la continuidad operativa.

Tarifes de suscripción

A continuación se proponen diferentes tarifas ajustadas a las dimensiones del municipio, garantizando un modelo escalable y adecuado a las necesidades específicas de cada entidad que las empresas licitadores tendrán que ofrecer:

Nivel de incidencia	Tipo de entidad	Tarifa propuesta (€/año)
Nivel 1: Incidentes leves y moderados	< 15 trabajadores	
	15 – 50 trabajadores	
	50 – 100 trabajadores	
	100 – 500 trabajadores	
	> 500 trabajadores	
Nivel 2: Incidentes críticos	< 15 trabajadores	
	15 – 50 trabajadores	
	50 – 100 trabajadores	
	100 – 500 trabajadores	
	> 500 trabajadores	

Servicio adicional de consultoría post incidente y mejora continúa

Adicionalmente a las tarifas de suscripción se ofrecerá un precio de servicio de consultoría post incidente. Este servicio complementario se podrá requerir fuera de la cobertura básica de respuesta a incidentes contratada como suscripción:

Este servicio adicional se centra en la evaluación y mejora de los procesos de seguridad después de la resolución de un incidente para evitar que incidentes similares se repitan. Incluye el análisis del manejo global del incidente para identificar áreas de mejora, la evaluación de la eficacia de la respuesta, la rapidez de la detección y la capacidad de recuperación, y se proponen mejoras para aumentar la seguridad y evitar posibles futuros incidentes.

El precio del servicio de consultoría será por sesión de revisión puesto-incidente (con una duración máxima de 4 horas/sesión).

10.4 Organización del servicio

Estructura organizativa

Por parte de la entidad, se establecerá la figura del Responsable del Servicio, que será el encargado de supervisar y coordinar la actuación y la relación con la empresa que desarrolla el servicio.

Por parte del adjudicatario, del mismo modo, se establecerá un Responsable del Servicio, que será el Director de Seguridad de la Información (SISO) encargado de la supervisión y coordinación, además de garantizar el cumplimiento de los requisitos, asignando los medios adecuados para la correcta prestación del servicio.

Equipo de trabajo

El equipo de CSIRT tendrá que estar compuesto por profesionales altamente cualificados y especializados para gestionar eficazmente los incidentes de ciberseguridad y llevar a cabo análisis forenses digitales.

La combinación de varias especializaciones permitirá una respuesta integral y coordinada, asegurando la protección de los activos digitales de la organización contratante y la rápida recuperación de los incidentes de seguridad.

El licitador tendrá que incluir a su propuesta los perfiles siguientes:

- Gerente de Respuesta a Incidentes
  - Coordinación y liderazgo del equipo de respuesta a incidentes, y desarrollo del plan de respuesta a incidentes.
- Uno analista Forense Digital
  - Recolección y preservación de evidencias digitales, realización de análisis forense detallado y documentación de los hallazgos.

Todos los perfiles tendrán que tener como mínimo 3 años de experiencia en proyectos similares.

Seguimiento del servicio

Una vez se ha activado el servicio por la detección de un incidente de ciberseguridad, se tiene que hacer un seguimiento detallado, coordinado y transparente entre la empresa que realiza el servicio y la entidad contratante, y debe llegar hasta la resolución del incidente e implementación de medidas preventivas.

En caso de que, por cuestiones relacionadas con la prestación del servicio, fuera necesario el desplazamiento del personal del equipo técnico a cualquier ubicación, este desplazamiento iría a cargo del adjudicatario, sin que suponga un coste adicional.

En estas reuniones se realizará un seguimiento diario durante el incidente para mantener la entidad contratante debidamente informada del progreso de la investigación, las medidas tomadas y los pasos a seguir. Los participantes de estas reuniones serán, entre otros *stakeholders* relevantes, entre lo SISO de la empresa que realiza el servicio y lo SISO o responsable de la entidad.

Las comunicaciones podrán ser efectuadas por llamada telefónica, videoconferencia, correos electrónicos o presenciales, siente en este último supuesto posible que las reuniones se lleven a término a las instalaciones de la entidad si esta está de acuerdo y así lo pide.

El seguimiento de la ejecución del servicio de CSIRT seguirá los siguientes pasos a partir de la notificación inicial del incidente:

- **Identificación e investigación**
  - Valorar las alertas y acontecimientos obtenidos a partir de la monitorización disponible o del SOC correspondiente, para determinar la existencia de un incidente de seguridad.
  - Colaboración coordinada con otros Ciertos o equipos de ciberseguridad potencialmente involucrados.
- **Contención**
  - Aislar sistemas comprometidos para prevenir la propagación del ataque.
  - Utilizar soluciones temporales para mitigar el impacto inmediato.
  - Coordinar con otros equipos de IT u otros equipos CERT's involucrados en la gestión del incidente para aplicar medidas de contención.
- **Erradicación**
  - Realizar un análisis exhaustivo para encontrar la causa raíz.
  - Eliminar todo rastro de la amenaza del entorno.
  - Aplicar parches y actualizaciones para cerrar las vulnerabilidades explotadas.
- **Análisis forense y preservación de evidencias**
  - Recolección y preservación de evidencias garantizando en todo momento el mantenimiento de la cadena de custodia para asegurar su validez e integridad en posibles procesos de investigación o legales.
  - Análisis de logs, ficheros y sistemas comprometidos.
  - Identificación de vectores de ataque y actores de amenaza.
- **Recuperación**
  - Restaurar sistemas y datos a partir de copias de seguridad seguras.
  - Revisar y validar la integridad de los sistemas antes de ponerlos en producción.

  - Implementar monitorización continua para asegurar que no haya reinfecciones.
- **Lecciones apresas**
  - Realizar una sesión de revisión puesto-incidente con todos los involucrados (*tabla-mortem*).
  - Documentar todas las etapas del incidente y las acciones tomadas.
  - Actualizar el plan de respuesta a incidentes basado en los aprendizajes.
- **Reporte y cumplimiento**
  - Generar informes detallados para el alta dirección y partes interesadas.
  - Asegurar que todas las acciones cumplen con las regulaciones aplicables.
  - Preparar comunicados públicos si es necesario.

Horario del servicio

El servicio se prestará por el equipo de trabajo especializado con disponibilidad 24x7 (24 horas, de lunes a domingo) para proveer a la entidad de respuesta inmediata a cualquier incidente detectado.

11 DEVOLUCIÓN DEL SERVICIO

Según el servicio contratado y a determinación del contrato basado, en el supuesto de que sea de aplicación la devolución del servicio, seis (6) meses antes de su finalización, la empresa contratista tendrá que presentar el plan de devolución del servicio en cuestión que incluya los mecanismos necesarios para traspasar toda la información relacionada con el servicio prestado.

La devolución del servicio no tendrá un coste adicional por la entidad y garantizará el traspaso del servicio al nuevo adjudicatario. La duración máxima de la migración será 1 mes desde la finalización del contrato.

La finalización del contrato exigirá también la eliminación segura de toda la información que se haya utilizado para la ejecución del contrato.

Con el objetivo de evitar que la empresa contratista que esté dando el servicio pueda hacer un uso indebido de su posición dominante, durante el proceso de relevo por cambio de prestamista del servicio tendrá que facilitar toda la información tanto técnica como administrativa requerida por la entidad contratante. Así mismo, la empresa contratista no podrá dificultar el proceso de cambio ni degradar los SLA pactados.

12 PLAZOS Y MODELO DE RELACIÓN

Las empresas adjudicatarias del acuerdo marco tendrán que designar, durante los 15 primeros días del acuerdo marco, sus interlocutores:

- Un interlocutor único para mantener directamente la interlocución con el Consorcio Localret. Tendrá las responsabilidades siguientes:
  - Velar por el cumplimiento de los compromisos contractuales adquiridos.
  - Seguimiento y resolución de las incidencias.
  - Envío de informes periódicos.

- Un centro de soporte para las entidades beneficiarias del acuerdo marco:
  - Soporte telefónico con horario mínimo de 9.00 h. a 14.00 h. en el lote 1 y de 9.00 h. a 18.00 h. en el resto de lotes, a excepción de aquellos que tienen que tener servicio 24h (lotes 3, 4 y 7).
  - Soporte mediante una dirección de correo electrónico.
  - Herramienta de ticketing para comunicar incidencias en línea si la empresa lo ofrece.

En los contratos basados, la empresa adjudicataria designará una persona responsable que actuará como persona de contacto con el ayuntamiento o entidad, y será la persona encargada de planificar, gestionar y coordinar todo el proceso de adquisición y mantenimiento de las licencias o del servicio gestionado de copias.

Atendiendo a la naturaleza de algunos de los servicios incluidos en este acuerdo marco, se puede requerir que su prestación se lleve a cabo en un horario 24x7 365 días en el año. En estos casos, la ampliación del horario quedará indicado en el posterior contrato basado.

Adicionalmente, se informa que los servicios incluidos en este acuerdo marco pueden implicar la necesidad de llevar a cabo guardias y trabajos fuera de horario. En este sentido:

- Se considera guardia la disponibilidad por atención telefónica y actuación presencial en horario no laboral en el caso de actuaciones especiales o que la importancia de la incidencia lo requiere.
- A petición exprés de la entidad contratante, se podría pedir la realización de algunas tareas fuera del horario de días laborables para garantizar el correcto desarrollo del servicio.

Dado que los periodos de finalización de los contratos de los ayuntamientos son diferentes para cada uno de ellos, habrá que gestionar la renovación de los servicios de licenciamiento y mantenimiento dentro de los plazos impuestos por el fabricante y siempre antes de la finalización del periodo de licenciamiento.

13 FACTURACIÓN

La facturación será en formato digital e-FACT. El contratista tendrá que facilitar la facturación electrónica a cada entidad y la plataforma a utilizar será FACe o e-FACTh o las que indique la normativa vigente. También se podrá entregar en formado papel si las entidades así lo pidieran y sin ningún coste adicional. A esta factura se tendrá que anexar el documento de detalle que se corresponda con el importe facturado. En caso de no anexarse el documento de detalle, las entidades podrán devolver la factura por carencia de información por su pago.

14 GASTOS DE IMPULSO

La cláusula QUINCUAGÉSIMA del pliego de cláusulas administrativas particulares (PCAP) establece los gastos de impulso, seguimiento y coordinación de los contratos basados en el presente acuerdo marco que irán a cargo de los adjudicatarios.

Eva Guijarro
Cabe del Área de Transformación Digital y Tecnologies