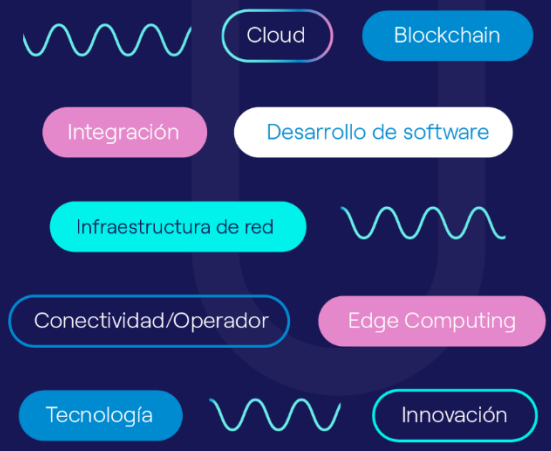
SUBMINISTRO DE EQUIPOS INFORMÁTICOS Y DE SERVICIOS ASOCIADOS CON DESTINO A LAS ENTIDADES LOCALES DE CATALUÑA

LOTE 38 - SERVICIOS DE CIBERSEGURIDAD – PONIENTE

Expediente núm. 2024.01

Pasión por la tecnología



Consorci Català pel Desenvolupament Local

Servicio de Ciberseguridad

Contenido

27313335F ALFREDO ESTIRADO (R: B79513156)

Firmado digitalmente por 27313335F ALFREDO ESTIRADO (R: B79513156)
Fecha: 2025.05.29 10:41:32 +02'00'

1. ALCANCE

El presente documento tiene como objetivo definir las acciones y servicios propuestos por TRC para el desarrollo del presente lote en el marco de los servicios de ciberseguridad requeridos por el pliego. El servicio ofrecido abarca dos líneas principales diseñadas para proporcionar al **Consorci Català pel Desenvolupament Local**, en adelante**, CLIENTE**, un marco robusto de seguridad que permita identificar, mitigar y prevenir riesgos, así como capacitar a su personal en las mejores prácticas y normativas aplicables.

TRC proporciona una solución que incluyen los siguientes servicios:

- **Consultoría en Ciberseguridad:** Incluye un diagnóstico detallado del estado actual de la infraestructura tecnológica, la identificación de vulnerabilidades y riesgos, y la elaboración de un plan de mejora adaptado a las necesidades del CLIENTE. Este servicio contempla recomendaciones específicas orientadas a mitigar amenazas, fortalecer los controles técnicos y organizativos, y asegurar el cumplimiento de normativas como ENS, LOPD-GDD, ISO/IEC 27001 y NIS2.
- **Formación Especializada en Ciberseguridad:** Programa formativo dirigido tanto al personal técnico como al personal no técnico, centrado en la adquisición de conocimientos prácticos sobre seguridad digital. Incluye temáticas como prevención de amenazas (phishing, malware, ransomware), buenas prácticas en el uso de tecnologías, y actuación ante incidentes, todo ello adaptado al perfil del alumnado.

Ambos servicios se ejecutarán dentro del horario previamente establecido al momento de la adjudicación por cada entidad local, asegurando una ejecución eficiente y alineada con los objetivos del cliente. Las actividades se adaptarán plenamente a los requerimientos operativos y logísticos establecidos por el CLIENTE.

Asimismo, se dará cumplimiento al requisito estipulado en el pliego, garantizando la disponibilidad para atender consultas relacionadas con el plan elaborado, indicado en el apartado de compromisos post-contrato.

2. COORDINACIÓN CON LA ENTIDAD LOCAL CONTRATANTE

Con el objetivo de garantizar una ejecución eficiente y alineada con las necesidades operativas del cliente, TRC implementará un modelo de coordinación basado en buenas prácticas de gobernanza, comunicación fluida y control operativo. Este modelo responde a los principios del Esquema Nacional de Seguridad (ENS) y se ajusta a las normativas aplicables, asegurando trazabilidad, eficiencia y adaptabilidad.

2.1. Modelo de gobierno

TRC designará un interlocutor único para la gestión del servicio, quien actuará como punto de contacto principal frente al órgano de contratación y las entidades locales adheridas. Este responsable liderará la coordinación operativa, supervisará el cumplimiento de los compromisos contractuales y gestionará las incidencias, asegurando una visión global y centralizada del servicio.

Gobiernos clave de la infraestructura

El modelo de gobernanza de TRC contempla:

- **Definición de roles y responsabilidades:** Se asignarán funciones específicas tanto al equipo técnico como al interlocutor del CLIENTE, permitiendo una trazabilidad clara y evitando ambigüedades en la ejecución de tareas.
- **Control de acceso y trazabilidad (RBAC):** La gestión de los entornos se realizará bajo un esquema de control de accesos basado en roles, garantizando que solo el personal autorizado acceda a elementos críticos.
- **Monitorización centralizada:** se habilitará monitorización del avance a través de herramientas colaborativas de gestión (como Microsoft Planner o equivalentes).

Modelo de Comités

Basándose en su experiencia en la prestación de servicios similares, TRC propone un modelo de comités como marco de gobernanza que facilitará una coordinación eficaz, seguimiento del servicio y toma de decisiones. La constitución, periodicidad y alcance de cada comité serán definidos de mutuo acuerdo entre el CLIENTE y TRC, y podrán modificarse durante la vigencia del contrato, siempre que se mantenga dentro del alcance previamente establecido.

1. Comité de Dirección

Este comité tiene como propósito supervisar la gestión integral del contrato, revisando el cumplimiento de los objetivos estratégicos, los indicadores clave y mediando en la resolución de conflictos críticos. Su convocatoria se realizará a solicitud de cualquiera de las partes cuando se considere necesario, especialmente en casos que requieran una revisión de alto nivel, resolución de incidencias relevantes o evaluación de ajustes estratégicos en el servicio. La periodicidad de estas reuniones será flexible y se acordará en función de las necesidades detectadas durante la ejecución del contrato.

Las funciones de este comité incluyen:

- Evaluar el servicio prestado y el cumplimiento de los objetivos de los indicadores de supervisión.
- Resolver conflictos escalados desde otros niveles.
- Hacer seguimiento del cumplimiento económico del contrato.
- Acordar estrategias, ajustes y nuevos objetivos.
- Aprobar cambios significativos y nuevos compromisos contractuales.

Estará compuesto por representantes del órgano de contratación que aseguren la visión estratégica del cliente, junto con los responsables de coordinación y gestión de TRC, así como directivos relevantes de ambas partes para decisiones clave.

2. Comité de Seguimiento

El Comité de Seguimiento tiene como objetivo revisar, cuando sea necesario, los indicadores clave del servicio, verificar el cumplimiento de las condiciones pactadas y gestionar incidencias operativas específicas que puedan surgir durante la ejecución. Su convocatoria será ad-hoc, a solicitud del CLIENTE o de TRC, cuando se considere necesario para analizar situaciones concretas, validar entregables o proponer mejoras, siempre dentro del alcance establecido

Las funciones de este comité incluyen:

- Supervisar el cumplimiento de los compromisos acordados en cuanto a calidad de servicio y tiempos de respuesta.
- Gestionar incidencias técnicas y operativas surgidas durante la ejecución del servicio.
- Planificar y proponer mejoras en base a las necesidades detectadas.
- Supervisar el estado de las actividades del servicio.
- Evaluar riesgos asociados a cambios o nuevas solicitudes.
- Escalar decisiones críticas al Comité de Dirección cuando sea necesario.

Este comité estará compuesto por representantes técnicos del CLIENTE y miembros del equipo de supervisión de TRC con capacidad de análisis y toma de decisiones sobre aspectos operativos vinculados al servicio.

3. Comité Técnico

El Comité Técnico vela la correcta ejecución operativa del servicio, atendiendo y resolviendo problemas técnicos que puedan surgir. Las reuniones pueden ser periódicas o convocarse bajo demanda según las necesidades del servicio y el alcance del contrato.

Las funciones de este comité incluyen**:**

- Planificar y realizar seguimiento de las actividades técnicas asociadas a las solicitudes de servicio.
- Identificar mejoras y riesgos operativos, escalándolos al nivel superior si procede.

- Resolver conflictos técnicos puntuales y colaborar en la toma de decisiones sobre configuraciones o entregables específicos.

Estará integrado por responsables técnicos de TRC y del CLIENTE, así como por especialistas designados en función del tipo de tarea a ejecutar o del ámbito tecnológico involucrado.

2.2. Canales de comunicación

Para una interacción efectiva con el CLIENTE y los distintos responsables designados (Responsable del Acuerdo Marco, Oficina de Seguimiento y Comisión de Apoyo), se habilitarán los siguientes canales:

1. **Correo Electrónico Corporativo**
   - Listas distribuidas diferenciadas por perfil (operativo, técnico, administrativo).
   - Responder a solicitudes clasificadas como urgentes por el CLIENTE en un plazo máximo de 4 horas laborables, siempre que estas estén relacionadas con aspectos críticos de la auditoría en curso o con incidentes de seguridad detectados durante la misma
2. **Llamadas y Videoconferencias**
   - Líneas directas para coordinación técnica inmediata.
   - Uso de Microsoft Teams u otra herramienta designada por el CLIENTE para sesiones de trabajo colaborativo y revisión de entregables
3. **Libro de Órdenes y Actas Digitales**
   - Registro de instrucciones y acuerdos generados durante la prestación.
   - Acceso compartido entre las partes a través de una carpeta segura (SharePoint, OneDrive, etc.)

4. **Automatización y eficiencia operativa**
   - En aquellas actividades que incluyan configuraciones técnicas o implantación de medidas recomendadas, se podrá aplicar herramientas de automatización (scripts, plantillas o procesos CI/CD) con el fin de agilizar la entrega, reducir errores manuales y asegurar una configuración coherente, todo ello manteniendo la trazabilidad y los niveles de seguridad requeridos.

2.3. Reuniones de coordinación

TRC participará en las reuniones en reuniones convocadas por el órgano de contratación cuando así se requiera, para revisar el estado del servicio, resolver incidencias relevantes o evaluar aspectos específicos del contrato.

Además, se propone:

- **Reunión inicial de arranque (kick-off)**: Sesión celebrada tras la adjudicación, para establecer los procedimientos operativos y validar los canales de comunicación y escalado.
- **Reunión anual (si es requerida):** En caso de que el Responsable del Acuerdo Marco o la Comisión de Apoyo convoque una sesión formal de revisión, TRC participará para abordar posibles incidencias acumuladas, validar los compromisos ejecutados y revisar, si fuera necesario, el enfoque del servicio.
- **Reuniones ad-hoc:** Podrán ser convocadas en cualquier momento por el CLIENTE, el PMO si aplicase o cualquier parte implicada, cuando sea necesario tratar temas urgentes, validar entregables o coordinar nuevas solicitudes dentro del alcance. Su frecuencia y contenido dependerán de las necesidades reales del servicio y lo acordado en el contrato.
- **Informes de intervención:** TRC elaborará y entregará informes específicos al finalizar cada actividad o intervención, detallando los trabajos realizados, hallazgos detectados y recomendaciones propuestas. La entrega de dichos informes estará sujeta a lo solicitado en cada requerimiento de servicio.

2.4. Entrega de informes y seguimiento

TRC entregará informes específicos por cada intervención, solicitud o actividad ejecutada, detallando los trabajos realizados, los hallazgos identificados y las recomendaciones propuestas. Estos informes podrán incluir anexos técnicos o documentación de apoyo, según corresponda a la naturaleza del servicio prestado.
En caso de que una entidad local o el órgano de contratación solicite consolidar un seguimiento general del servicio, TRC podrá generar un informe resumen, adaptado a los requerimientos y al volumen de intervenciones realizadas hasta el momento.
Todas las comunicaciones relevantes, acuerdos y entregables quedarán documentados mediante actas, correos electrónicos o registros en la plataforma de gestión acordada, garantizando la trazabilidad y la alineación con los objetivos del contrato.

2.5. Metodología específica para consultoría y formación

2.5.1. Consultoría

La consultoría ofrecida se fundamenta en una metodología orientada a resultados, basada en el análisis técnico riguroso, la adaptación a las necesidades específicas del CLIENTE y la entrega de recomendaciones viables y accionables. Esta metodología incluye tres fases clave:

- **Evaluación técnica:** Se realiza un diagnóstico detallado del entorno tecnológico del CLIENTE, incluyendo infraestructuras, políticas de seguridad, controles actuales y configuraciones críticas, con el objetivo de identificar vulnerabilidades, deficiencias de cumplimiento y áreas de mejora.
- **Recomendaciones prácticas:** Se entregan recomendaciones prácticas, priorizadas según la criticidad del riesgo, la facilidad de implementación y las necesidades operativas del CLIENTE. Las soluciones propuestas estarán alineadas con buenas prácticas reconocidas (ENS, ISO/IEC 27001, NIS2, etc.) y adaptadas al contexto específico de cada entidad local.
- **Seguimiento:** TRC ofrecerá soporte puntual para facilitar la interpretación e implementación de las recomendaciones, dentro de los márgenes del contrato por horas y conforme a lo acordado en cada solicitud. En caso de requerirse un acompañamiento más extenso, podrá ser objeto de una solicitud adiciona

2.5.2. Formación

La formación en ciberseguridad ofrecida por TRC combina teoría y práctica mediante un enfoque flexible y adaptado a las necesidades específicas del CLIENTE. El objetivo es capacitar al personal —técnico y no técnico— en el fortalecimiento de la cultura de seguridad, la prevención de riesgos y la respuesta ante incidentes.

- **Contenido personalizado:** Los programas formativos se diseñan en función del nivel de conocimiento del grupo destinatario y los objetivos definidos por el CLIENTE. Se ofrece formación diferenciada para personal técnico (profundización en normativas, gestión de incidentes, configuraciones seguras) y no técnico (concienciación, buenas prácticas, detección de amenazas comunes).
- **Material actualizado:** Todos los contenidos incluyen documentación y ejercicios prácticos actualizados, alineados con las principales normativas y marcos de referencia (ENS, LOPD-GDD, NIS2, ISO 27001), así como con las tendencias más recientes en ciberamenazas.
- **Modalidad remota:** La formación se impartirá de forma remota, garantizando una experiencia formativa de alta calidad adaptada a las posibilidades y restricciones logísticas de cada entidad local.

3. ASPECTOS CLAVE EN MATERIA DE CIBERSEGURIDAD Y PROCEDIMIENTO DE ACTUACIÓN ANTEDESASTRES

En TRC comprendemos los crecientes desafíos que enfrentan las organizaciones públicas para garantizar la seguridad de la información y la continuidad operativa en un entorno digital dinámico y expuesto a ciberamenazas cada vez más sofisticadas.
Nuestro enfoque se basa en la aplicación de estrategias avanzadas de protección, metodologías probadas de gestión de incidentes y un servicio integral de consultoría y formación. Todo ello alineado con los marcos normativos de referencia como el Esquema Nacional de Seguridad (ENS), la ISO/IEC 27001, la NIS2, y la LOPD-GDD, asegurando así la adecuación a los estándares más exigentes en materia de ciberseguridad.

3.1. Procedimiento de actuación ante desastres

El enfoque ante desastres se basa en una estrategia integral que combina prevención, preparación, respuesta y recuperación, con el objetivo de garantizar la continuidad operativa ante incidentes graves y minimizar el impacto en los servicios críticos del CLIENTE.
Las fases clave del procedimiento son:

1. **Plan de Continuidad de Negocio y Recuperación ante Desastres (BCP/DRP)**
   - Diseño de planes que contemplen distintos escenarios de contingencia, con criterios claros de prioridad y tiempos de recuperación (RTO/RPO).
   - Identificación y clasificación de activos críticos, así como definición de estrategias de mitigación de interrupciones.
2. **Definición de roles y responsabilidades**
   - Establecimiento de un equipo de Respuesta a Incidentes (**CSIRT**), con roles claramente asignados.
   - Designación de un responsable principal que coordine las acciones durante situaciones de crisis y actúe como interlocutor con el CLIENTE.
3. **Detección y notificación de incidentes**
   - Procedimientos estandarizados para identificar y reportar incidentes en etapas tempranas.
   - Establecimiento de canales de comunicación inmediatos con equipos internos y autoridades competentes, conforme a la normativa vigente.
4. **Evaluación y contención**
   - Análisis rápido del impacto y alcance del incidente para permitir una toma de decisiones efectivas.
   - Aplicación de medidas técnicas de contención para evitar la propagación y reducir el daño.
5. **Recuperación y restauración**
   - Ejecución de acciones técnicas para reestablecer servicios, priorizando operaciones críticas.
   - Verificación exhaustiva de la integridad del sistema antes de reanudar actividades.
6. **Revisión post-incidente**
   - Realización de un análisis retrospectivo para identificar causas raíz y mejorar estrategias de prevención.
   - Actualización de planes, procedimientos y controles en base en las lecciones aprendidas.

3.2. Servicio de asesoría en ciberseguridad

En TRC, Ofrece un servicio de consultoría en ciberseguridad orientado a fortalecer la postura defensiva del CLIENTE mediante auditorías técnicas exhaustivas, planes de mejora personalizados y estrategias adaptadas a los marcos normativos vigentes

3.2.1. Auditoría y consultoría inicial

El proceso comienza con una auditoría detallada de la infraestructura tecnológica actual, con el objetivo de identificar vulnerabilidades, riesgos y áreas de mejora. Los elementos clave son:

- **Evaluación de infraestructura actual:** Análisis de los entornos tecnológicos para detectar configuraciones inseguras, componentes obsoletos o carencias en las medidas de protección
- **Identificación de vulnerabilidades**: Revisión técnica de sistemas críticos con el fin de detectar puntos débiles en seguridad, tanto a nivel de hardware como de software.
- **Revisión de controles de acceso**: Validación de los esquemas de autenticación, asignación de permisos y políticas de acceso, asegurando que solo el personal autorizado pueda acceder a los activos críticos
- **Evaluación de políticas de encriptación y seguridad**: Análisis de la eficacia de los mecanismos de encriptación, así como de las políticas aplicadas para la protección de información sensible y cumplimiento de la normativa vigente.
- **Detección de Riesgos Específicos:** Identificación de exposiciones frente a amenazas comunes como ransomware, phishing, ataques de día cero, y revisión de posibles brechas derivadas de la interoperabilidad entre sistemas.
- **Análisis de buenas prácticas**: se analizará a nivel de implementación de buenas prácticas de seguridad alineadas con normativas y estándares internacionales, incluyendo recomendaciones específicas para su adopción si no están presentes, identificando posibles brechas en su aplicación.

Entregables de la auditoría inicial

- Informe detallado con hallazgos clasificados por nivel de criticidad.
- Recomendaciones iniciales para mitigar riesgos inmediatos.

3.2.2. Plan de mejora

A partir de los hallazgos obtenidos durante la auditoría inicial, TRC elabora un plan de mejora personalizado, orientado a fortalecer la postura de seguridad del CLIENTE. Este plan se estructura en torno a una hoja de ruta priorizada, que contempla tanto medidas técnicas como organizativas, alineadas con las mejores prácticas y las normativas vigentes

Hoja de ruta para una infraestructura más segura

- **Recomendaciones técnicas de hardware:** Sugerencias específicas de hardware, como la actualización de dispositivos críticos (firewalls, switches, servidores, etc.) con el objetivo de mejorar la resiliencia y el rendimiento de la infraestructura.
- **Sugerencias de software especializado:** Propuesta de herramientas avanzadas de ciberseguridad, incluyendo sistemas de detección y respuesta (EDR/XDR), plataformas de análisis de vulnerabilidades, y soluciones para la gestión de identidades y accesos (IAM).

Prevención de ciberamenazas

- **Medidas contra ransomware y amenazas avanzadas:** Propuestas concretas para mitigar riesgos de ataques avanzados como ransomware mediante tecnologías de respaldo y recuperación rápida.
- **Protección contra phishing y fraude digital:** Estrategias para combatir el phishing a través de soluciones de autenticación multifactor (MFA) y filtrado avanzado de correos electrónicos.

Cumplimiento normativo

- Diseño de un plan de acción para alineamiento regulatorio:

Elaboración de un plan de trabajo con hitos claros para garantizar el cumplimiento de las normativas aplicables

  - Esquema Nacional de Seguridad (ENS): Implementación de medidas organizativas y técnicas para cumplir con los niveles de seguridad exigidos.

- NIS2: Adaptación de la infraestructura y los procesos para cumplir con los requisitos de esta directiva europea.
- ISO 27001: Fortalecimiento del sistema de gestión de seguridad de la información.

Desarrollo de indicadores clave que permitan medir el avance en la implementación de las recomendaciones y facilitar el seguimiento continuo.

3.2.3. Estrategias clave de ciberseguridad

Como parte del servicio de consultoría, TRC promueve un enfoque holístico y proactivo en materia de ciberseguridad, garantizando que el CLIENTE disponga de las capacidades necesarias para anticiparse a amenazas, mitigar riesgos y mantener una postura de seguridad alineada con los estándares más exigentes.
Las estrategias clave que se contemplan son:

Defensa en profundidad

Diseño e implementación de un modelo de seguridad multicapa, que combine distintas tecnologías y controles para una protección integral:

- Integración de soluciones multicapas como firewalls de próxima generación (NGFW), sistemas EDR, segmentación de red y monitorización continua.

Gestión proactiva de vulnerabilidades

- Uso de herramientas avanzadas para realizar análisis regulares y priorizar la remediación de vulnerabilidades críticas.

Políticas y procedimientos actualizados

- Asistencia en la redacción y actualización de políticas de seguridad alineadas con las mejores prácticas y regulaciones.

Capacitación y concienciación

- Formación del personal técnico y general en buenas prácticas de seguridad, incluyendo simulacros de incidentes.

3.3. Servicio de formación en ciberseguridad

El servicio de formación en ciberseguridad de TRC está diseñado para dotar al cliente de conocimientos prácticos y estratégicos, fomentando una cultura de seguridad sólida a todos los niveles de la organización. Este servicio incluye capacitación específica para el personal general y formación técnica avanzada para responsables TIC, con el objetivo de fortalecer la resiliencia ante ciberamenazas y garantizar el cumplimiento de normativas aplicables.
La metodología combina teoría y práctica, impartiéndose en modalidad remota. Incluye material didáctico actualizado y ejercicios prácticos, diseñados para adaptarse al nivel técnico y los objetivos específicos de cada grupo, asegurando un aprendizaje efectivo y aplicable.

3.3.1. Formación general en ciberseguridad

Dirigida a todo el personal de la organización, esta formación se centra en la concienciación sobre las amenazas cibernéticas y la adopción de prácticas seguras en el uso de herramientas digitales. Sus objetivos principales son:

- **Reconocimiento de amenazas comunes:**
  - Identificación de riesgos habituales, como el phishing, el ransomware y el malware.
  - Capacitación para evitar interacciones que puedan comprometer la seguridad de la organización.
- **Fomento de buenas prácticas:**
  - Gestión segura de contraseñas y autenticación.
  - Protección adecuada de datos sensibles en el entorno laboral y remoto.
  - Uso responsable de herramientas y recursos corporativos.
- **Análisis de casos reales de ciberseguridad:**
  - Estudio de incidentes reales para ilustrar el impacto de las amenazas cibernéticas.

- Discusión interactiva sobre las mejores prácticas de prevención y respuesta.

3.3.2. Formación especializada para responsables TIC

Diseñada específicamente para personal técnico y responsables de infraestructura, esta formación aborda los desafíos avanzados de ciberseguridad y su aplicación en entornos críticos. **Incluye:**

Gestión de infraestructuras seguras

- Diseño, configuración y monitoreo de sistemas críticos con medidas avanzadas de protección.
- Implementación de políticas de segmentación de red y defensa en profundidad.

Gestión proactiva de vulnerabilidades

- Estrategias para la identificación, análisis y mitigación de amenazas en tiempo real.
- Procedimientos para contener y erradicar brechas de seguridad.

Cumplimiento normativo avanzado

- Actualización detallada sobre regulaciones como ENS, NIS2, ISO 27001 y LOPD.
- Orientación práctica para su implementación y gestión continua en la organización.

Talleres y simulaciones técnicas

- Ejercicios prácticos en un entorno controlado, diseñados para perfeccionar habilidades críticas.
- Simulaciones de incidentes para evaluar y fortalecer la capacidad de respuesta del equipo técnico.

4. COMPROMISOS POST-CONTRATO

TRC garantiza su compromiso de acompañamiento al CLIENTE una vez finalizada la ejecución de cada servicio o intervención, conforme a los requisitos establecidos en el pliego.

En particular, se establece lo siguiente:

- **Disponibilidad para consultas:**

TRC estará disponible durante un período de hasta un año tras la contratación para atender consultas específicas relacionadas con el contenido del plan o los entregables presentados, según lo requerido en el pliego de condiciones.