PLIEGO DE CONDICIONES TÉCNICAS

PROCEDIMIENTO ABIERTO SIMPLIFICADO Y TRAMITACION ORDINARIA PARA LA CONTRATACIÓN DEL SERVICIO CONSISTENTE EN LA "ELABORACIÓN DEL PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN DE GESTIÓN Y PLANEAMIENTO TERRITORIAL Y MEDIOAMBIENTAL, S.A." INFORME DE CONTRATACIÓN NÚMERO 202/24

1. OBJETO DEL CONTRATO.

El presente pliego tiene por objeto establecer las prescripciones técnicas que han de regir en la realización del Plan de Acción propuesto en el diagnostico de Ciberseguridad.
Dentro de las actuaciones del Plan Director que la empresa está desarrollando, se ha realizado un diagnóstico de ciberseguridad que como resultado establece en varios años la realización de proyectos para incrementar el nivel de madurez en materia de seguridad.
El plan de acción propuesto incluye 18 proyectos para abordar en tres años, el objeto del siguiente contrato se centra en la realización de los 7 proyectos propuestos para el primer año.
Los proyectos referidos se agrupan en cuatro bloques de Gobierno, Protección, Vigilancia y Resiliencia.

2. CONTENIDO Y PRESCRIPCIONES TÉCNICAS.

Los proyectos son los siguientes:

- Elaboración de un cuerpo normativo de seguridad (Fase I)
- Definición y despliegue del proceso de gestión de riesgos de terceras partes
- Diseño estructura de Gobierno de seguridad (TOM)
- Definición arquitectura de seguridad
- Definición de plan de Pentesting
- Despliegue y gestión de herramienta de escaneo de vulnerabilidades
- Servicio Cyber Emergency Management Service (CEMS)

2.1 Elaboración de un cuerpo normativo de seguridad (Fase I)

Esta línea de trabajo consiste en el desarrollo del Marco de Ciberseguridad teniendo en cuenta las nuevas normativas y buenas prácticas en materia de Ciberseguridad. Dicho

alcance será desarrollado como un mecanismo de protección, pero también como un elemento base para la continuidad de negocio.

A continuación, se enumeran las fases y principales tareas a desarrollar para la elaboración del Marco de Ciberseguridad:

- **Preparación**
    - Planificación inicial:
        - Definición y validación de la metodología de trabajo a seguir.
        - Establecimiento de las fechas tentativas para la elaboración de cada uno de los documentos que conformarán el Cuerpo Normativo de Ciberseguridad.
    - Recopilación de información
        - Solicitud de información para acotar el desarrollo del Cuerpo Normativo de Ciberseguridad.
        - Entrevistas con el personal clave para identificar responsabilidades y aspectos a tener en cuenta en el desarrollo de los documentos.
    - Definición del alcance
        - Identificación de las normas y estándares de la industria que son de aplicación para la compañía.
        - Elaboración de un marco de control donde se identifique la aplicabilidad de los controles implantados frente a dichos estándares.
- **Objetivo:** La finalidad principal de la fase de planificación es la preparación y puesta en marcha de las líneas de trabajo. Realizar una preparación de cara a la correcta gestión, el seguimiento y control de las actividades y de los equipos de Trabajo y materiales que intervienen en el proyecto.
- **Actividades clave**: La maximización de la calidad y del beneficio obtenido en los servicios involucrados en la presente propuesta es objetivo fundamental de las

actividades desarrolladas a lo largo de los mismos servicios, entre ellas las que corresponden a la planificación del proyecto.

- **Actividades principales de esta fase**
  - Establecer modelo de gobierno y seguimiento
  - Preparar la gestión del Equipo de Trabajo
  - Identificación de los medios requeridos (reuniones, etc.)
  - Establecimiento del calendario detallado
  - Identificación y gestión de sinergias e interdependencias
  - Identificación de los factores que puedan provocar desviaciones

- **Desarrollo**

  - Desarrollo de los documentos
    - Definición del índice a incluir en cada procedimiento en función del contenido propuesto.
    - Desarrollo de los documentos tomando como referencia estándares internacionales y guías específicas de ciberseguridad.
  - Revisión y mejora de los documentos
    - Realimentación, identificando los ajustes a realizar durante el desarrollo de los documentos.
    - Reuniones puntuales para completar aspectos precisos de los documentos.
  - Validación
    - Validación de los documentos elaborados, e identificación de potenciales ajustes a realizar.

  Dentro del alcance de este proyecto se deben desarrollar documentos los cuales están comprendidos principalmente en las siguientes áreas o dominios de seguridad:

  - Ciberseguridad ligada al personal
  - Gestión de activos
  - Clasificación, tratamiento y regulación del intercambio de la información
  - Control de acceso a los sistemas
  - Cifrado de la información y las comunicaciones
  - Seguridad física de los sistemas y del entorno
  - Seguridad ligada al mantenimiento y administración
  - Protección y gestión del software
  - Protección y gestión de redes

- Seguridad en el ciclo de vida de los sistemas
- Gestión de incidentes de ciberseguridad
- Ciberseguridad en la relación con terceros
- Gestión de la continuidad de negocio
- Auditoria de ciberseguridad

Durante las primeras fases del desarrollo del Marco de Ciberseguridad una vez analizado la información, se validará y priorizará el contenido del primer nivel de normativas que apliquen a los puntos descritos.

Para el desarrollo de los documentos se deberá tomar como referencia **estándares internacionales y guías específicas de seguridad industrial,** así como la información recopilada durante las entrevistas mantenidas y la documentación aportada.

- **Plazo ejecución:** 3 meses

2.2 Definición y despliegue del proceso de gestión de riesgos de terceras partes.

Los riesgos que conlleva la externalización de servicios se encuentran en el foco de atención de las entidades y reguladores. Esto es así debido a que se ha difuminado el perímetro de las organizaciones, aumentando la dependencia de terceras partes, y cambiando de manera radical el escenario de los riesgos que afectan a la organización.

Esta línea de trabajo **consiste en** el desarrollo de un modelo de gestión segura de proveedores que permita controlar adecuadamente los riesgos de seguridad asociados a los servicios externalizados., para el cual a continuación, se enumeran las **fases y principales tareas** a desarrollar:

- **Fase I: Definición de un Modelo de Third Party Cyber Risk Management**
    - Analizar la situación actual (As-Is)
        - **Actores involucrados:** Identificación de áreas y personal relevantes para los flujos de gestión de la externalización de servicios IT.
        - **Marco normativo:** Requisitos regulatorios y de normativa interna establecidos en relación a la contratación de servicios desde la perspectiva de riesgos IT.

- **Escenario actual:** Situación de la organización, incluyendo las recomendaciones abiertas referentes a la gestión del outsourcing, los proveedores ya homologados, etc.

- Establecer el modelo de gobierno (roles y responsabilidades)
  - **Roles y responsabilidades:** Definición de roles y responsabilidades asociados al cumplimiento de las tareas necesarias para la gestión del outsourcing, la realización de análisis de riesgos, el reporte de indicadores, etc.

- Definir el modelo operativo de 3rd party Cyber Risk Assessment, incluyendo entre otros procesos, modelo de controles, cuestionarios, categorización de peticiones, etc.
  - **Revisión norma de seguridad en terceras partes:** Revisión de la política alineada con los requisitos regulatorios e integrada con el cuerpo normativo.
  - **Definición del modelo:** Identificación de los **procedimientos necesarios** para soportar el modelo de externalización basada en riesgos.
  - **Cuestionarios**: Definición de cuestionarios a completar por la propia entidad para la clasificación de proveedores.
  - **Criterios de clasificación**: Definición de los criterios en función de los cuales se **clasificarán a los proveedores: criticidad, tipología, etc. y que servirán para establecer el triaje.**
  - **Tipos de revisión**: Definición de las **tipologías de revisión según su clasificación**
  - **Controles:** Definición de los **requerimientos** sobre los proveedores según su clasificación.

- Establecer KPIs y mecanismos de reporting
  - **Objetivos**: Identificación de objetivos y aspectos a reportar considerados relevantes en relación a la gestión de servicios externalizados.
  - **Indicadores:** Propuesta de indicadores de seguridad que reflejen el estado y evolución de la función de seguridad.
  - **Modelo de reporte:** Propuesta de canales de reporte a los distintos interlocutores identificados.

- **Fase II: Introducción del modelo en el flujo de peticiones de proyecto/compras**

  - Revisar propuesta de mejoras sobre el clausulado legal
    - **Clausulado:** Revisión y propuesta de mejoras sobre el clausulado legal de ciberseguridad requerido a los proveedores.

- Establecer el flujo de relación con compras
  - **Flujo de peticiones de proyectos:** Entendimiento del flujo de petición de nuevos proyectos o renovación de existentes y la relación con el departamento de compras.
  - **Establecer modelo de relación con compras:** Definir el modelo de relación con compras con el objetivo de que ciberseguridad pueda ejecutar el modelo operativo definido con éxito (ie. información sobre los servicios, contratos, contactos de los proveedores, etc.)

- **Fase III: Piloto de ejecución del modelo implantado**

  - Identificar y seleccionar proveedores a incluir en la prueba piloto
    - En función de la criticidad, se identificarán diferentes proveedores para la ejecución del piloto (**2-3 proveedores de diversas criticidades**)
  - Ejecutar las revisiones del piloto
    - **Revisión:** siguiendo el modelo formalmente establecido, ejecución de la revisión.
    - **Mejora continua:** Implementar las mejoras identificadas sobre el modelo definido.

  - **Plazo ejecución:** 3 meses

2.3 Diseño estructura de Gobierno de seguridad (TOM)

Esta línea de trabajo consiste en el análisis del actual modelo operativo y de gobierno del área de seguridad de la información para posteriormente diseñar un modelo operativo aspiracional, para el cual a continuación, se enumeran las fases y principales tareas a desarrollar:

- **Fase I: Análisis de situación**

  - Entendimiento de los objetivos del área de seguridad, el negocio y su estrategia
  - Identificación del modelo de relación actual
  - Análisis del Modelo de Gobierno y Operativo actual
  - Actividades para esta fase:
    - **Entendimiento de los objetivos del área de seguridad, el negocio y su estrategia**. Para ello es necesario entender la estrategia específica de seguridad, como esta está siendo implementada actualmente por el Plan

Director de Ciberseguridad y como se alinea esta a los objetivos de negocio.

- Para entender bien el contexto de la organización será necesario analizar previamente algunos elementos:
- **Riesgos contemplados y activos a proteger**: será necesario identificar los principales activos de la organización (*Crown jewels*) de [Nombre de la empresa] para conocer cuáles son las prioridades de protección de los procesos clave de negocio. El objetivo es solo llegar al nivel de identificación a alto nivel y no realizar un inventario de activos como tal.
- **Modelo organizativo y cobertura**: El entendimiento del organigrama de la organización, los roles y responsabilidades, los órganos de gobierno y control existentes, entre otros, son elementos clave para poder entender correctamente el modelo organizativo. Al mismo tiempo, es necesario conocer cuál es el alcance de las diferentes funciones de Seguridad de la Información y cuáles son las herramientas de gobierno y control a nivel geográfico para de esta forma conocer el alcance real y la delegación de responsabilidades a nivel territorial (en caso de que las hubiese).
- **Servicios de seguridad y relación con los negocios**: Será necesario conocer cuál es el catálogo de servicios que actualmente se está proveyendo desde el área de seguridad de la información. Para ello, se analizará dicho catálogo y como estos se relacionan con el negocio (principales actividades) y cuales es la cobertura que se les da a cada uno de ellos, así como el modelo existente (normalmente cliente-proveedor interno).
- **Modelo de relación con otras áreas de seguridad**: el modelo de relación requiere del conocimiento de los mecanismos de relación entre áreas implicados, indicadores definidos, modelos de reporting, comités, etc.
- **Visión futura**: identificación de las declaraciones del modelo aspiracional del área de seguridad de la información y su posible implementación en los posibles escenarios futuros de seguridad.

- Para llevar a cabo esta fase será necesario contar con cierta información a analizar:
  - Modelo de Gobierno actual de la función de seguridad corporativa, así como su relación/dependencias con el resto de áreas
  - Organigrama, con roles y responsabilidades del actual Modelo Operativo (TOM)

- Principales drivers identificados por Gesplan para realizar un Plan de Transformación
- Principales Comités de Seguridad (miembros y funciones, periodicidad de reunión y responsabilidades)
- Identificación del personal externo, su modalidad de contratación (servicio o proyecto), roles y responsabilidades
- Personal interno, con sus roles y responsabilidades
- Relación de proveedores actuales y su función actual
- Modelo financiero: CAPEX y OPEX actual y su desglose por capacidades y servicios
- Plan Estratégico actual y framework de seguridad
- Cualquier otro documento de trabajos anteriores que pueda ayudar al equipo experto: Análisis de riesgos, PDSI, certificaciones actuales, normativas aplicables, BIA, etc.

- **Fase II: Evaluación del modelo**
  - Evaluación del Modelo actual
  - Workshop comparativo entre varios modelos
  - Definición aspiracional del Modelo Operativo

En esta fase se evaluará en base a toda la información analizada en el modelo anterior cual debe ser el modelo operativo futuro para cubrir las necesidades y los GAP identificados, a partir de los siguientes acciones:

Actividades

- Se identificarán las **fortalezas y debilidades** del modelo.
- Se identificará cuales son las **capacidades / servicios** de seguridad de la información **no cubiertos** actualmente **o que puedan haber sido delegados excesivamente a un tercero** sin existir un gobierno efectivo.

- Se analizará el **dimensionamiento del área de ciberseguridad** en base a sus funciones actuales.
- Se identificará cuales son los **comités** existentes y **si estos cubren todas las necesidades** específicas del área de seguridad de la información.

El objetivo es tener identificado todos aquellos aspectos a tener en cuenta en la definición de un nuevo modelo operativo.

El modelo Operativo definido en esta fase incluirá:

- **Dependencia jerárquica** organizacional de la **función** del área de **ciberseguridad** (normalmente, el CISO).
- **Áreas de ciberseguridad del nuevo modelo**: estas pueden ser el resultado de añadir nuevas competencias a las ya existentes, modificar capacidades, crear nuevas áreas o dividir alguna ya existente en dos, etc. Todo ello, buscando siempre la eficiencia de recursos, las necesidades reales y los modelos más prácticos basados en las buenas prácticas.
- **Responsabilidades no tratadas** o **gestionadas** por los comités actuales
- Etc.

Se realizará un **Workshop** a través de un experto en la materia, se conducirá una sesión presentando las principales tendencias y **Modelos Operativos** actuales de las compañías, realizando un brainstorming experto para tomar decisiones sobre aspectos que se podrían incorporar y mejorar.

El **Workshop** irá dirigido tanto a interlocutores que puedan participar y contribuir por su conocimiento y visión de cada área, así como a interlocutores de otras áreas si el cliente lo decide.

Una vez definido el **Modelo Operativo** y, tomando como referencias las necesidades y palancas de seguridad asociadas al negocio y contexto se analizará el GAP existente entre el modelo actual y el modelo objetivo planteado para generar un **Modelo de transición** (en la siguiente fase del proyecto) a través del cual se podrá gestionar de forma controlada por fases y ciertos mecanismos de aseguramiento de la calidad para llegar al **aspiracional**.

El objetivo no es lograr que se implante directamente su nuevo modelo una vez este haya sido definido, sino que lo haga a través de un modelo transicional que permite una

fácil y controlada toma de control del nuevo modelo y manejo de posibles desviaciones sin impactar en el modelo de negocio.

- **Fase III: Diseño del Modelo**
  - Diseño en detalle del Modelo Operativo
  - Plan de acción a través de un modelo de transición

Actividades

Definición de la **misión y objetivos** para cada una de las áreas de seguridad de manera alineada con el framework de seguridad definido en la Fase I.

- Diseño del **catálogo de servicios para cada uno de los dominios del modelo**. Dicha definición deberá tener en cuenta aspectos como:
  - Servicios y capacidades existentes actualmente
  - Requerimientos internos (necesidades de los negocios, planes estratégicos de la Organización) y requerimientos externos (normativa, regulación).
  - Panorama actual de amenazas, así como tendencias en el corto y medio plazo.
  - Catálogo de activos y geografías – particularidades.
  - Exposición al riesgo de los activos de la empresa.
  - Conocimiento y experiencia de otras organizaciones comparables – sectores relevantes.
- Presentación y ajuste de catálogo de servicios y mapeo con el modelo organizativo de transición (y aspiracional).
- Generación del listado de comités incluyendo las modificaciones necesarias para cubrir las necesidades del área de ciberseguridad.
- Matriz RACI, de roles y responsabilidades.

Definición conceptual de cada uno de los servicios de seguridad incluidos en el catálogo, mediante **el desarrollo de fichas específicas para cada uno** de ellos. Estas fichas detallarán, al menos, la siguiente información:

- **Definición y objetivos** del servicio.

- **Identificación de las unidades encargadas del delivery** implicadas en las prestación del servicio, así como los **mecanismos de coordinación** entre ellos.
- **Presupuesto teórico** del servicio (si es posible).
- Definición de las **actividades que deben desarrollarse dentro del servicio**, así como los requisitos de seguridad.
- **Modelo de madurez** basado en CMMI adaptado a la casuística del servicio, que permita evaluar a lo largo del tiempo las capacidades relacionadas con dicho servicio, así como un umbral objetivo de madurez para cada servicio.
- Indicadores a alto nivel **que permitan medir, tanto la calidad y rendimiento de los servicios de seguridad**, como la eficacia y eficiencia en el cumplimiento de las objetivos marcados.
- Modelo de relación entre **métricas y modelo de madurez** que permita establecer objetivamente el nivel de cada uno de los servicios.
- Matriz de **roles y responsabilidades** implicados en la gestión del servicio.

Se realizará un Plan de Acción basado en un Modelo transición para cubrir el GAP identificado, incluyendo:

- **Plan de actividades**
- Evaluación de **criticidad** y **priorización** de actividades
- **Estimación** de costes de los planes
- **Calendario** y estimación temporal
- **Roles y responsabilidades** para la ejecución del plan
- **Necesidades** tecnológicas

- **Plazo de ejecución:** 3 meses

2.4 Definición arquitectura de seguridad

Esta línea de trabajo **consiste en** la revisión y definición de un modelo de referencia para la arquitectura de red de la entidad, que proporcione nuevas capacidades de control, sea más resiliente y escalable, para el cual a continuación, se enumeran las **fases y principales tareas** a desarrollar:

- Entrevistas con los responsables de las comunicaciones para entender en profundidad la arquitectura de red, la infraestructura y conexiones entre CPDs.
- Entrevistas con las áreas técnicas necesarias para entender la estrategia de segmentación de la organización, las VLANs definidas o las zonas de seguridad utilizadas, entre otros.
- Análisis técnico de los elementos de seguridad perimetral (Firewalls e IDS/IPS).
- Evaluación desde el punto de vista de bastionado de una muestra de elementos de electrónica de red (Switches o Routers)
- Análisis de cómo se realiza el inventariado y categorización de activos según topología.
- Evaluación del modelo de arquitectura de red donde se incluye el nivel de segmentación y segregación de redes, la visibilidad entre redes a través de los distintos flujos de comunicación, cómo se realizan las conexiones de acceso remoto, de terceros o en nubes públicas y en general cómo es el modelo de gobierno de la red.
- Identificación de capacidades de seguridad adicionales existentes en las diferentes herramientas de seguridad de la organización.
- Verificación de aspectos relacionados con la trazabilidad, monitorización o redundancia.

- **Plazo de ejecución:** 10 meses

2.5 Definición de plan de Pentesting

Esta línea de trabajo **consiste en** la revisión y definición de un modelo de Pentesting y hacking, compuesto por:

- Pentesting perimetral
- Hacking Externo: objetivo identificar todas las vulnerabilidades siendo un atacante real en los activos expuestos a internet.

- Hacking Interno: simulando ser un atacante que ha conseguido acceso o siendo un Insider, identificar las vulnerabilidades dentro de la red organizativa.

Para dicho plan, se enumeran las **fases y principales tareas** a desarrollar:

- **Fase I: Planificación y diseño**
    - Definición de objetivos y alcance
        - Como primera actividad de preparación, se verifica el plan de trabajo propuesto por el cliente, revisando de forma detallada las tareas y fechas de realización. Se provee al cliente de un documento con la planificación del encargo, metodología a usar, aspectos que se van a revisar, dedicación prevista y relación de técnicos que realizarán el encargo.
    - Validación de escenarios y verificación de requerimientos
        - Una vez que sea confirmada la planificación el equipo designado para las pruebas validarán los aspectos de conectividad requeridos para las tareas previstas. Como conclusión de esta actividad, el líder de proyecto designado, validará la vigencia de los accesos y reportará cualquier limitación o inconveniente que sea identificado.
- **Fase II: Ejecución**
    - Reconocimiento
        - Durante esta fase, el pentester realizará los ataques necesarios para hacer un reconocimiento de la organización, algunas de las pruebas a realizar son:
            - Búsqueda de subdominios en fuentes públicas (FDNS, motores de búsqueda...) para los nombres de dominio principales
            - Búsqueda de rangos IP adicionales a través de Whois, prefijos exportados por ASN
            - Búsqueda de activos por certificados
            - Descubrimiento de activos potenciales mediante palabras clave
            - Servicios públicos mediante motores de búsqueda de servicios
            - Búsqueda de posibles adquisiciones de dominios
            - Información sensible sobre servicios web mediante motores de búsqueda
            - Búsqueda de credenciales filtradas
            - Fuerza bruta de subdominios mediante permutaciones y listas de palabras

- Escaneo de servicios con escáneres de red
- Rastreo de sitios web y búsqueda de rutas mediante diccionarios.
- Identificación de tecnología web
- Detección automática de vulnerabilidades mediante scripts nmap y escáneres de vulnerabilidades
- Búsqueda de configuraciones inseguras

  - Análisis y explotación de vulnerabilidades
    - El objetivo de esta fase es la de confirmar la veracidad de las vulnerabilidades detectadas y la eliminación de falsos positivos, así como de acceder a recursos internos de la red, a la información almacenada o toma de control de los activos, mediante el aprovechamiento de las vulnerabilidades detectadas. Se incluye dentro de este apartado la investigación cuya finalidad es encontrar o desarrollar las herramientas necesarias para comprobar activamente las vulnerabilidades y demostrar su grado de impacto. Esto implica la búsqueda en bases de datos y listas de correo, públicas y privadas, generales o específicas de los sistemas que están siendo investigados. En caso de identificar una vulnerabilidad crítica que pueda estar comprometiendo la seguridad del cliente, se notificará inmediatamente sin esperar a la entrega de los resultados del trabajo en curso.

- **Fase III: Reporting y conclusiones**

  - Informes ejecutivo y técnico
    - Resumen ejecutivo. Un resumen ejecutivo donde se presenta a nivel gerencial, el resultado de las pruebas desarrolladas, incluyendo:
      - Descripción y objeto de las pruebas
      - Resumen de problemas identificados, agregados por riesgo
      - Priorización de las actividades correctoras en base al riesgo
    - Informe técnico y Plan de recomendaciones. Un resumen donde se presenta a nivel técnico el resultado de las pruebas desarrolladas:
      - Vulnerabilidades encontradas (descripción, referencia CVE/BID, nivel de criticidad, si se ha conseguido verificar/explotar, posible riesgo / impacto…), junto a su/s correspondiente/s contramedida/s.
      - Pruebas realizadas.
      - Logros y resultados obtenidos.
      - Detalle de la intrusión (explicación paso a paso de cómo se ha logrado la intrusión: vulnerabilidades explotadas, código fuente de los exploits utilizados, diferentes etapas de la intrusión, etc.).
      - Capturas de pantalla que ilustren los puntos anteriores (evidencias).
      - Propuestas de mejora y recomendaciones.
      - Mapas de red.

- Evidencias. en forma de captura de pantalla e incluidas en el informe técnico, para ilustrar la vulnerabilidad o paso de la intrusión concreto.

- **Plazo de ejecución:** 3 meses

2.6 Despliegue y gestión de herramienta de escaneo de vulnerabilidades

Esta línea de trabajo **consiste en** el despliegue y gestión de herramienta de escaneo de vulnerabilidades basado en el riesgo definido por el cliente, para el cual a continuación, se enumeran las **fases y principales tareas** a desarrollar:

- Reunión Kick-Off y toma de información
- Propuesta y validación del diseño de arquitectura
- Instalación y configuración de herramientas
- PoC: Primera política y escaneo
- Realizar escaneos de red para los sistemas no identificados
- Definir y ajustar políticas y escaneos
- Programar y lanzar escaneos
- Puntuación de las vulnerabilidades asociadas al riesgo del activo
- Explotación de la información y creación de Dashboards
- Crear reportes acorde a la priorización

Para la ejecución de los escaneos de vulnerabilidades nos basaremos en 3 pilares:

- Escaneos automáticos: Obtención de todas las vulnerabilidades, abarcando las siguientes tareas:
  - Calendarización, ejecución y seguimiento de los proyectos relacionados con la identificación de vulnerabilidades mediante escaneos
  - En esta etapa, el escaneo se llevará a cabo con el objetivo de identificar posibles vulnerabilidades en cualquier capa de activos (sistema operativo, aplicación, etc.) en función del alcance del proyecto y las herramientas elegidas.
  - Estas son las acciones que se realizarán para esta tarea:

- Ejecutando herramientas de escaneo generalistas y herramientas específicas de identificación de vulnerabilidades
- Re-escaneo con el propósito de asegurar la correcta remediación de la vulnerabilidades identificada
- Escaneo de seguridad para aquellos sistemas previo paso a producción.

Como resultados se obtendrá:

- Gestión de proyectos de escaneos de vulnerabilidades
- Listado de vulnerabilidades

- Revisiones manuales: Revisión manual de los resultados obtenidos por las herramientas y test para detectar errores y obtener un resultado más preciso, abarcando las siguientes tareas:
  - En estas etapas, las tareas tienen como objetivo analizar los resultados proporcionados por las herramientas utilizadas después de finalizar la ejecución del escaneo automático.
  - Las siguientes tareas se llevarán a cabo en esta etapa por un experto en seguridad:
    - Categorización de vulnerabilidad por impacto de riesgo.
    - Priorización de vulnerabilidades mediante la identificación de riesgos prioritarios y amenazas que pueden afectar la disponibilidad, integridad y confidencialidad de la información según la información disponible. Se indicará cuando se necesite tomar medidas inmediatas, acciones intermedias y acciones a largo plazo.
    - La categorización de la vulnerabilidad por equipos críticos proporcionó información de activos disponible.
    - Identificación de malas prácticas.
    - Descarte de falsos positivos

  Como resultados se obtendrá:

  - Lista de todas las vulnerabilidades identificadas en todos los activos que pertenecen al alcance.
  - Borrado de todas las vulnerabilidades duplicadas y falsas positivas obtenidas durante el escaneo automático por las herramientas.

- Plan de Acción: Entregables, Reporting y seguimiento de las vulnerabilidades hasta su cierre, abarcando las siguientes tareas:

  - Esta etapa cubre el estudio de toda la documentación generada a lo largo de todos los trabajos técnicos recopilados en las etapas previas. Las acciones que se llevarán a cabo son las siguientes:
    - Documentación de toda la información extraída sobre las vulnerabilidades y las pruebas realizadas.

- Categorización de vulnerabilidad por tipo y gravedad, de acuerdo con los estándares principales.
- Estudio y evaluación de vulnerabilidad para proporcionar recomendaciones de mitigación correspondientes.
- Recomendación de los diferentes errores detectados y malas prácticas en términos de configuración e implementación.
- Inclusión de evidencia, como capturas de pantalla de pruebas y vulnerabilidades detectadas.
- Elaboración del informe de resultados, tanto a nivel ejecutivo y técnico con el formato bugblast
- Seguimiento.

Como resultados se obtendrá:

- Documentación y entregables del servicio.

- **Plazo de ejecución:** 12 meses

2.7 Servicio Cyber Emergency Management Service (CEMS)

Esta línea de trabajo **consiste en** un servicio de asesoramiento frente a ciberincidentes que deberá cubrir la preparación, la respuesta y la recuperación ante estos, alineado con los principales estándares internacionales (NIST 800-61R2, SANS Security, ENISA, etc.), que ofrezca disponibilidad en caso de incidentes críticos de 24x7.

- Descripción del servicio:

Se requiere un servicio de asesoramiento frente a ciberincidentes que deberá cubrir la preparación, la respuesta y la recuperación ante estos, alineado con los principales estándares internacionales (*NIST 800-61R2, SANS Security, ENISA, etc.).*

El servicio deberá contar con un equipo de primera respuesta, que ofrezca disponibilidad en caso de incidentes críticos de 24x7.

Tras una primera respuesta, el servicio deberá contar con capacidades DFIR que permitan entender la actividad del atacante, el escenario, la amenaza y las hipótesis posibles para desarrollar un análisis ágil, identificar *findings* relevantes y diseñar las medidas técnicas que permitan contener el incidente y limitar los daños.

Además, si el escenario así lo requiere, el proveedor deberá proveer una figura de Gestor del Incidente, que coordine las actuaciones y asesore la toma de decisiones a nivel técnico y táctico.

El licitador deberá especificar el alcance de las labores de análisis, contención, remediación y recuperación incluidas dentro de un servicio de retainer en el que la bolsa de horas ofertada pueda utilizarse en cualquiera de las capacidades incluidas.

En resumen, se busca:

- Un servicio que cuente con recursos y personal experto suficiente para ampliar las capacidades internas, que identifique y lleve a cabo mejoras en materia de preparación táctica y técnica de cara a la gestión de las ciber contingencias.
- Un servicio flexible y que se adapte al escenario para dar una respuesta lo más ágil posible y que proporcione capacidades de forense digital avanzado que permitan conocer los detalles de lo ocurrido.
- Un servicio que preste asistencia en la recuperación de entornos tecnológicos y seguimiento de tareas post-incidente.

- **Reporting**

Es necesario elaborar documentación para el seguimiento del servicio, así como para el análisis y posterior aplicación de mejoras y revisión evolutiva del mismo:

- En tiempo de incidente:
    - Creación y mantenimiento de elementos de *reporting* del caso con diferente recurrencia que ayuden en el entendimiento de los trabajos realizados de forma diaria, esfuerzos asociados, situación actual del incidente (visión ejecutiva y/o técnica), cumplimiento del plan de acción general asociado al incidente, etc.
    - Composición de informe de cierre de incidente que abarque entre otros conceptos: visión técnica, táctica y ejecutiva de la situación inicial que presentó el incidente, las medidas tomadas bajo una variable temporal para la contención y erradicación de la amenaza, la causa raíz y una serie de recomendaciones extraídas de las lecciones aprendidas durante el incidente.

- Durante la ejecución del servicio:
    - Sesión de seguimiento mensual: donde se expondrán los cumplimientos, las desviaciones, así como un análisis de tendencias del servicio, detección de problemas, mejoras de procedimientos, etc.
    - Acta de sesión mensual: reporte de la sesión donde se recogerán los principales asuntos tratados en la reunión mensual.

- **Nivel del servicio**

Este Apartado establece los indicadores y niveles de servicio específicos que el Proveedor deberá entregar al Cliente para los servicios descritos en el Apartado Descripción de los Servicios:

- SLA de respuesta: <1h desde el levantamiento del caso, es decir, en menos de una hora desde que el Cliente active el servicio, un especialista en Respuesta a Ciber incidentes deberá atenderlo y comenzar la gestión del mismo.

- **Plazo de ejecución:** 12 meses.

3. ENTREGA DE LOS TRABAJOS.

A la finalización de cada uno de los proyectos se entregará la documentación propia de los trabajos realizados, descritos en el contenido y prescripciones técnicas del presente pliego técnico.

4. PRESUPUESTO

Se deberá respetar el precio máximo de cada proyecto, si se supera en algún proyecto, no se valorará la oferta.
Se establece un presupuesto de ciento quince mil euros (115.000,00 €), a los que incluidos ocho mil cincuenta euros (8.050,00 €) correspondientes al 7% de IGIC, hacen un total de ciento veintitrés mil cincuenta euros (123.050,00 €)

Proyecto	IMPORTE sin IGIC	IGIC	IMPORTE con IGIC
Elaboración de un cuerpo normativo de seguridad (Fase I)	10.000,00 €	700,00 €	10.700,00 €
Definición y despliegue del proceso de gestión de riesgos de terceras partes	18.000,00 €	1.260,00 €	19.260,00 €
Diseño estructura de Gobierno de seguridad (TOM)	17.000,00 €	1.190,00 €	18.190,00 €
Definición arquitectura de seguridad	20.000,00 €	1.400,00 €	21.400,00 €
Definición de plan de Pentesting	5.000,00 €	350,00 €	5.350,00 €
Despliegue y gestión de herramienta de escaneo de vulnerabilidades	25.000,00 €	1.750,00 €	26.750,00 €
Servicio Cyber Emergency Management Service (CEMS)	20.000,00 €	1.400,00 €	21.400,00 €
TOTAL	**115.000,00 €**	**8.050,00 €**	**123.050,00 €**

FORMA DE ABONO.

Se presentarán las facturas a la finalización de los proyectos indicados en el presente pliego.

El pago se realizará contra facturas, que se presentarán en formato electrónico, si ello fuera posible, dentro de los 30 días siguientes a la fecha de entrega de los trabajos, y habrá de reunir los requisitos exigidos en la normativa aplicable. Para realizarlo será necesario que el Responsable del Servicio de Tecnologías de la Información e Instalaciones dé el visto bueno a la factura presentada.