PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD Y CUMPLIMIENTO NORMATIVO DE LOS SISTEMAS INFORMÁTICOS Y LAS INFRAESTRUCTURAS ASOCIADAS (HARDWARE Y SOFTWARE DE BASE) QUE DAN SOPORTE TELEMÁTICO A FOMENTO DE SAN SEBASTIÁN

1. CONDICIONES BÁSICAS DEL SERVICIO

El objeto del contrato lo constituye la prestación de los servicios de ciberseguridad y cumplimiento normativo, es decir, la contratación de un servicio que satisfaga los requisitos de cumplimiento normativo del Reglamento General de Protección de Datos (RGPD) y Esquema Nacional de Seguridad (ENS) de los sistemas informáticos y las infraestructuras asociadas (hardware y software de base) que dan soporte telemático a Fomento de San Sebastián.

Al comienzo de la prestación del servicio, la empresa adjudicataria mantendrá una reunión inicial de Comienzo de Prestación del Servicio con Fomento, en la que se contrastarán todos los términos de la prestación del mismo, concretando cualquier punto necesario por parte de la empresa adjudicataria y acordando los términos y el Plan de trabajo definitivo.

En concreto, en la prestación del objeto del contrato, la empresa adjudicataria deberá realizar las siguientes actuaciones:

1.1 Servicio de asesoramiento y apoyo al cumplimiento tanto en materia del RGPD como del ENS.

1.1.1 Apoyo en la definición del modelo de Gobernanza en materia de RGPD y ENS, en concreto, definiendo los siguientes aspectos:

- Cumplimiento legal y normativo, que permitan la adaptación al Esquema Nacional de Seguridad.
- Definición de indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- Despliegue de herramientas para la mejora de la ciberseguridad y cumplimiento normativo, incluyendo tanto soluciones como la definición y carga de protocolos.
- Asesoramiento en labores de cumplimiento RGPD/LOPD-GDD

1.1.2 Plan de Adecuación integral al RD 311/2022

La puesta en marcha del Plan de adecuación se orientará a mejorar el grado de seguridad de la entidad, alineado a conseguir la conformidad con el Esquema Nacional de Seguridad de forma progresiva en todos sus sistemas de información. El plan determinará la hoja de ruta de adaptación de Fomento de San Sebastián. Se deberán considerar, al menos, las siguientes actividades:

- Se certificarán los diferentes sistemas de forma progresiva hasta disponer de una conformidad integral.

- Carga de la valoración, atendiendo a las dimensiones de seguridad, de los servicios prestados y de la información que manejan, con especial atención en la incidencia en los datos de carácter personal.
- Carga de la categorización del Sistema. Con carácter general los sistemas a certificar serán de categoría media, sin perjuicio de la existencia de sistemas segregados en categoría básica o alta.
- Carga de la Declaración de Aplicabilidad Provisional: aplicación de medidas por categorización.
- Carga del preceptivo Análisis de Riesgos, integrando las medidas de seguridad y la posibilidad de refuerzos. Para ello se utilizará la herramienta PILAR.
- Carga de la Declaración de Aplicabilidad definitiva.
- Implementación de soluciones de seguridad que permitan dar cumplimiento a los marcos organizativos, operacionales y de protección, conforme a las medidas del Anexo II del Real Decreto 311/2022.

1.1.3 Herramientas para la gestión de la gobernanza

Se prestará especial atención en la puesta en marcha de un sistema de gestión de seguridad de la información que permita obtener la conformidad con el ENS, a través de las soluciones del CCN-CERT:

- Despliegue de las herramientas del CCN (INES) que permitan la carga de contenidos particularizados, incluyendo el Plan de Adecuación y el Sistema de Gestión de Seguridad de la Información.
- Desarrollo de protocolos de cumplimiento con flujos de aprobación que permitan integrarse de forma efectiva con las herramientas de gestión municipal.
- Puesta en marcha de soluciones que permitan la generación de todas las evidencias que serán necesarias para conseguir la conformidad con el ENS.
- Desarrollo de una auditoría interna previa a la certificación, incluyendo el soporte de acciones correctivas.

1.2 Auditorías de las Páginas WEB tanto en materia del RGPD como del ENS.

En diciembre de 2024 se realizará una auditoría de certificación (Coste no incluido en el contrato). La certificación se realizará incluyendo en categoría MEDIA conforme al RD 311/2022. En los sucesivos años se ampliará el alcance de forma que se extienda de forma global en toda la entidad.

En previsión, la empresa adjudicataria pondrá en marcha y llevará a cabo auditorias para la detección y prevención de incidentes de seguridad, incluyendo todo el equipamiento y licencias que sean necesarias para su funcionamiento. En particular se realizarán los siguientes ejercicios:

- Hacking interno, analizando el estado actual de las vulnerabilidades de los servidores, debilidades en los protocolos de conexión, así como un test de intrusión, identificando el nivel de riesgo y plan de remediación.
- Hacking de todas las aplicaciones municipales, en formato caja negra y gris de las diferentes soluciones desplegadas en la entidad.

Se auditarán las siguientes aplicaciones y páginas webs:

Aplicaciones:

1. Aplicación monitorización fotovoltaica.
2. Airwave: Aplicación de gestión de equipos de red Wifi
3. ClearPass: Aplicación de gestión de usuarios de red Wifi
4. SIFOM: Sistema de Información de Fomento San Sebastián que recoge la información obtenida en la tramitación de nuestros servicios con la ciudadanía.

Páginas web

1. www. smartKalea.eus
2. https://sansebastian-gipuzkoafilmcommission.eus/es/
3. www.fomentosansebastian.eus.

En caso de necesitar conocer mayor detalle sobre el alcance de los sistemas a auditar y bastionar, se solicitará previo acuerdo de confidencialidad a la siguiente dirección de correo fomentoss@donostia.eus en el plazo de 5 días hábiles desde la publicación de los Pliegos.

1.3 Despliegue de una solución de básica de monitorización:

La solución de monitorización se deberá desplegar en alta disponibilidad en formato Cloud, y deberá cubrir todos los elementos objeto de la certificación ENS.

Las soluciones contempladas deberán cumplir los siguientes requisitos generales:

- Detectar y prevenir intrusiones en cualquier protocolo y aplicación utilizados.
- No repercutir en una degradación del rendimiento de las aplicaciones y servicios.
- Detectar temprana y respuesta ante incidentes.
- Proporcionar servicios de *Threat Hunting* sobre los eventos supervisados.
- Analizar eventos basado en firmas, comportamientos, logs, procesos e IOCs.
- Disponer de técnicas de IA para la detección de anomalías.
- Posibilidad de definir reglas de alerta adaptadas a la particularidad de la organización.
- Centralizar, salvaguardar y correlación de eventos multifuente.
- Disponer de Sistema de detección de intrusiones a nivel de red.
- Integrar de servicios externos vía syslog/api.
- Contemplar soporte experto ante los incidentes notificados.
- Generar informes mensuales de estado con indicadores.
- Disponer de un servicio de Vigilancia digital.

Para realizar las funciones referidas, la empresa adjudicataria deberá implementar una solución SIEM. Dicha solución debe cumplir los siguientes requisitos:

- Formará parte del catálogo CPSTIC-105 del CCN.
- Ser capaz de capturar y recopilar todos los eventos de seguridad que se producen en la red de forma centralizada, de recibir información desde una gran cantidad de

fuentes, de correlacionar los datos recogidos y de mostrar una amplia variedad de información en paneles. La infraestructura que soporta la solución será proporcionada por la empresa licitadora en formato Cloud en alta disponibilidad.

- Capacidad de retención de eventos para su correlación. Se almacenará eventos durante 12 meses, de los cuales, al menos 2 meses deberán realizarse *en caliente*.
- La solución SIEM propuesta permitirá la ingesta de todos los sistemas objeto de la certificación. Se estima al menos 10 tipos fuentes diferentes.
- Asimismo, a lo largo del contrato, previo modificado, podrá incorporar progresivamente nuevas fuentes, atendiendo a su vez a las recomendaciones que pueda realizar la Oficina Técnica de Seguridad y/o a las nuevas soluciones de ciberseguridad que adquiera la entidad.
- Para la funcionalidad de análisis de eventos, el producto deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos o actividades maliciosas, registrando el resultado de los análisis.
- La solución propuesta deberá contar con una copia de seguridad diaria del conjunto total de logs ingestados para asegurar su disponibilidad y cubrir posibles contingencias que pudieran suponer una pérdida de los registros. Dicho backup deberá ser alojado en una ubicación externa proporcionada por la empresa licitadora, diferente a la ubicación de la propia herramienta de SIEM, acreditando la seguridad de dicha ubicación. Las copias de seguridad deberán permitir una recuperación completa de los logs con un plazo de retención de 1 año.

Todos los servicios se prestarán previa solicitud por parte de la persona responsable de Fomento de San Sebastián y en todos los casos, la empresa adjudicataria deberá de dar una valoración del coste en horas, que deberá ser aprobada, antes de su ejecución, por Fomento de San Sebastián. Este trámite se realizará siempre por correo electrónico y deberá existir evidencia de la aprobación para la facturación de cualquier actuación referida a los diferentes servicios objeto de esta licitación. De acuerdo a esto, tras la solicitud por parte de Fomento San Sebastián, la empresa adjudicataria deberá informar de la **valoración en horas para la realización de la actuación** concreta en un **plazo máximo de 24 horas para el servicio 1** y en un **plazo máximo de 7 días hábiles, para los servicios 2 y 3**. En relación a la prestación de estos dos últimos servicios, la empresa adjudicataria deberá además presentar un **Documento de Análisis Funcional**, que recogerá de forma técnica, los requerimientos de la actuación concreta solicitada, así como su valoración en horas de producción y los plazos aproximados de realización para su posterior control de cumplimiento.

Tras la revisión conjunta entre Fomento y la empresa adjudicataria del Documento de Análisis Funcional, se pactarán las modificaciones necesarias entre ambos para que responda a los requerimientos reales, desarrollando un documento definitivo de Análisis Funcional que será el que recoja concretamente el desarrollo a llevar a cabo por la empresa adjudicataria.

Una vez validado el **documento definitivo de Análisis Funcional**, así como la valoración en horas para su ejecución, la empresa adjudicataria tiene el visto bueno para comenzar con la ejecución del trabajo solicitado de acuerdo a dicho documento. La empresa adjudicataria **deberá comenzar con los trabajos un plazo máximo de 24 horas para el servicio 1** y en un **plazo máximo de 7 días hábiles, para los servicios 2 y 3.** En relación con el servicio 1, cabe

indicar que la empresa adjudicataria tendrá un plazo máximo de 72 horas en la resolución de consultas en materia de RGPD, (se entienden el plazo de 24 horas por una jornada comprendida de 9 de la mañana a 17 horas de la tarde, de lunes a jueves y viernes de 9 a 14:00 h)

Cualquier modificación al Documento de Análisis Funcional aprobado que se proponga durante el desarrollo, deberá de ser registrada por escrito, así como estimar es su caso si requiere alguna desviación en las horas estimadas. La empresa adjudicataria deberá realizar la prestación del servicio de acuerdo a la planificación realizada en el Documento de Análisis Funcional y acordada por Fomento San Sebastián.

La empresa adjudicataria reportara **mensualmente un informe de ejecución** para el seguimiento del avance de los **servicios 2 y 3** por parte de Fomento San Sebastián, así como del número de asesoramientos llevados a cabo en relación al servicio 1. Asimismo, a la **finalización de la prestación del servicio 2** entregará a Fomento San Sebastián un **informe** acerca del resultado de las auditorias, que contendrá asimismo las medidas correctoras a acometer por Fomento San Sebastián. En relación al **servicio 3** deberá poner a disposición de Fomento San Sebastián un **acceso en Cloud** para poder validar y testear el correcto funcionamiento de la **solución de monitorización.**

Se requiere que la empresa adjudicataria tenga disponibilidad para la realización de los servicios objeto de esta contratación, en horario de oficina de 9 de la mañana a 17 horas de la tarde, de lunes a jueves y viernes de 9 a 14:00 h.

En Donostia/San Sebastián a 22 de junio de 2023

MARIA SOLEDAD GARMENDIA BELOQUI - 15968224Z

Marisol Garmendia Beloqui
Vicepresidente de Fomento de San Sebastián, S.A.