Expediente:	**2021/00001391A**
Procedimiento:	**Expedientes de Contratación de Servicios**
Asunto:	**Proyecto de auditoría LOPDGDD/RGPD y ENS.Plan de Adecuación al ENS y consultoría de implantación.**
INFORMÁTICA	

PRESCRIPCIONES TÉCNICAS

Asunto: Proyecto de auditoría LOPDGDD/RGPD y ENS.

1. **Objeto del contrato.**
   El proyecto consiste en dar cumplimiento en la legislación vigente en materia de protección de datos según las normas vigentes:
   - LOPDGDD 3/2018 de 5 de diciembre
   - RGPD (UE) 2016/679 de 27 de abril
   - LISSCE 34/2002

2. **Código CPV.**
   Código CPV: 79212000-3 (Servicios de Auditoría)

3. **Descripción del proyecto a realizar.**
   3.1)LOPDGDD/RGPD
   a) **Análisis.**
   Esta es la primera parte de las tareas a realizar presencialmente, si es posible según la situación de pandemia actual, en las distintas sedes del ayuntamiento (**Anexo I**). En estos puntos se examinarán los siguientes aspectos:
   - Ubicación de las instalaciones físicas, distribución y configuración física de los sistemas informáticos. Donde se encuentran ubicados el/los servidores, el sistema de copias de seguridad, la visibilidad de las pantallas de los usuarios por parte de terceros, etc.
   - Sistema de video-vigilancia, se revisará el sistema sobre el que está configurado, las zonas de grabación, en especial si se capta vía pública o no, etc.
   - Aplicaciones utilizadas para el tratamiento de datos personales y con qué fines legítimos se tratan.
   - Relación de usuarios que acceden a diferentes tratamientos.
   - Relación de terceros que acceden a los datos de carácter personal, en su calidad de encargados del tratamiento.
   - Identificación de:
     - Responsable de la información. Determinará los requisitos de la información tratada.
     - Responsable del servicio. Determinará los requisitos de los servicios prestados.
     - Responsable de seguridad. Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios

   Análisis de la página web corporativa y/o URL titularidad de la sociedad, a fin de constatar la existencia o no de los siguientes puntos:

- Que la titularidad de la URL corresponde efectivamente a al ayuntamiento.
- Que las imágenes utilizadas disponen de los consentimientos pertinentes hacia el derecho a la propia imagen.
- Revisión de la tipología de cookies que el dominio utiliza.
- Revisión y confección de los avisos legales y de privacidad por capas.
- Revisión de las condiciones de contratación.
- Revisión de los convenios de confidencialidad con los programadores web.

Análisis de las redes sociales y/o blogs de las que dispone la entidad:

- Revisar e inventariar todas las redes sociales que son responsabilidad del ayuntamiento.
- Revisar los contenidos, en especial, el uso de imágenes de personas físicas pero también cualquier tipo de contenidos sujetos a la Ley Orgánica (LO) 1/1982.
- Revisión y/o confección de los convenios de encargado de tratamiento y confidencialidad.

Una vez realizada la toma de datos presencial, se confeccionará toda la documentación necesaria para cumplir con la nueva normativa.
Con la aplicación efectiva del RGPD 2016/679, no se está obligado a comunicar ningún archivo a la Autoridad de Protección de Datos competente, pero se desean tener en disposición de esta autoridad, y permanentemente actualizados, los siguientes documentos:

- Registro de actividades: este será el documento que sustituirá el actual Documento de Seguridad y será la herramienta fundamental para documentar qué datos se tratan, con qué finalidad y las medidas técnicas y organizativas que se aplican.
- Redacción del Manual Interno: se redactarán los protocolos de las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento de datos se realiza conforme con el nuevo texto normativo, incluyendo entre otros:
  - Ámbito de aplicación, material, organizativo y humano.
  - Relación de tratamientos responsabilidad del ayuntamiento.
  - Análisis de impacto previo de los tratamientos identificados.
  - Evaluación de riesgos de los tratamientos identificados.
  - Relación de medidas de seguridad técnicas que se aplican efectivamente.
  - Relación de medidas de seguridad organizativas que se aplican efectivamente.
  - Relación de encargados de tratamiento y sus correspondientes convenios.
  - Registro de incidencias y fallos de seguridad, así como de violaciones de seguridad.
  - Identificación, funciones y propuesta de designar las figuras que el RD 3/2010 establece en su artículo 10:
    - Responsable de la información. Determinará los requisitos de la información tratada.
    - Responsable del servicio. Determinará los requisitos de los servicios prestados.
    - Responsable de seguridad. Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios

- Nombramiento del DPD/DPO si fuera necesario. (actualmente el ayuntamiento dispone de esa entidad asignada a una empresa externa mediante una adjudicación por procedimiento abierto)
- Funciones y obligaciones del personal.
- Compromiso de confidencialidad del personal.

- Análisis de riesgos: en esta fase se determinan los riesgos en función de los tratamientos y la tipología de los datos en relación con el número y tipo de finalidades a las que se destinan. En función del riesgo y del impacto se deberán adoptar unas medidas u otras a fin de mermar o extinguirlo en su caso.
- Evaluación de Impacto en la Protección de Datos Personales: se realizará un análisis de riesgos que un producto (una APP, un software, etc.…) o un servicio pueden implicar para la protección de la privacidad de los datos de los afectados y, como consecuencia de este análisis, la gestión de los riesgos identificados para que se eliminen o disminuyan.
- Evaluación de la necesidad de nombramiento de DPD/DPO: no todas las entidades tienen la obligación ni la necesidad de tener nombrado un DPD/DPO, por lo tanto, una vez auditado el ayuntamiento, se informará si es imprescindible o no su creación. En caso afirmativo, en el informe de auditoría se propondrá su creación y los motivos de la misma.
- Revisión y adecuación de la Web: según la LSSICE 34/2002 se revisarán los dominios web propiedad del ayuntamiento para que se cumpla con los avisos legales: el aviso general de privacidad, la política de cookies, los derechos de imagen y la captación directa de datos de los usuarios.
- Redacción de cláusulas y avisos: se revisarán todas las cláusulas existentes y si es necesario se harán nuevas.
- Redacción de los convenios de encargado de tratamiento y confidencialidad con terceros: se redactarán los acuerdos con todas aquellas empresas externas que al prestar sus servicios acceden a datos de su responsabilidad, y que por lo tanto, ostentan la condición de encargado de tratamiento. Estos acuerdos se realizan siguiendo las directrices de las autoridades de protección de datos para todas las empresas, tanto las que acceden a datos personales o estratégicos.
- Auditoría: realizar la correspondiente auditoría para poder revisar que todos los protocolos y procedimientos de seguridad establecidos son seguidos por los usuarios en el tratamiento de datos.
- Certificación: en la que consta el grado de cumplimiento.
- Asesoramiento y asistencia jurídica: en vía administrativa en materia de protección de datos.

b) Formación

Una vez confeccionada toda la documentación personalizada se hará la entrega de la misma. Es de suponer que el responsable del tratamiento y sus usuarios deben tener unas nociones básicas pero muy claras de qué tipo de datos e información están tratando y de qué manera deben hacerlo.

Se hace indispensable, por lo tanto, que tanto el Responsable del Tratamiento como los usuarios del sistema estén formados lo mejor posible y tengan claros los principios que informan la nueva legislación y cuáles son sus funciones y obligaciones.

Esta formación se dará, si la situación actual de pandemia lo permite si no de forma telemática, durante 4 sesiones de una hora cada una y se proporcionará el documento

del curso al ayuntamiento para que este esté lo ponga a disposición de todos los usuarios.

Como propuesta de temario a desarrollar sería el siguiente:

- Conceptos básicos de la privacidad.
- Regulación legal vigente.
- Obligaciones del Responsable del Tratamiento.
- Funciones y obligaciones de los usuarios.
- Atención de los derechos (Acceso, Rectificación, Cancelación, Oposición, Transparencia, Portabilidad, Limitación y Supresión).
- Protocolo de actuación en caso de violación de seguridad.

c) Asistencia técnica

La empresa adjudicataria dará apoyo continuado al ayuntamiento durante la vigencia del contrato, 1 año, ya sea en la resolución de dudas de simple complejidad como en la emisión de informes sobre temas relativos a la materia que impliquen una alta complejidad.

La aplicación que esta normativa implica y estos cambios a aplicar suponen que los responsables de los tratamientos requieran un plus de asesoramiento y formación en la nueva forma de cumplimiento de la normativa. Es por este motivo que se ofrecerá un servicio de asesoría y actualización normativa 24x365 o en horario laboral.

Este servicio consiste en dar apoyo jurídico a consultas planteadas por parte del ayuntamiento, informar puntualmente de los cambios legislativos, reglamentarios y/o resoluciones emitidas por las autoridades competentes en la materia, que puedan afectar al correcto cumplimiento de la normativa vigente, y a estar asistidos ante cualquier acción inspectora de la autoridad competente, en vía administrativa.

Los tiempos de resolución de consultas son los siguientes:

- Resolución de consultas simples: las consultas simples y habituales se contestarán antes de las 24 horas laborales en que sean formuladas, preferiblemente por correo electrónico, sin límite de consultas a realizar por parte del ayuntamiento.
- Resolución de consultas complejas: si estas no requieren de la emisión de informe específico y/o consulta vinculante o no a la autoridad, se resolverán antes de las 72 laborales en su formulación.
- Emisión de informes vinculantes: las realizaciones de informes vinculantes sobre temas relativos a la materia del objeto del presente contrato se entregarán al ayuntamiento antes de los 15 días hábiles, a contar desde el día siguiente a su formulación. Máximo 2 informes al año.

Consultas a la Autoridad: se redactará y se asesorará en su formulación con los plazos expresados en los puntos anteriores.

- Respuesta en función de la gravedad de la situación: si la causa que provoca la consulta no implica la paralización de ningún servicio se responderá en un máximo de 24 horas.
- Si la consulta implica el agotamiento de un plazo se resolverá dentro de la misma jornada laboral.
- Si la causa implica la paralización de un servicio o ya se ha sobrepasado un plazo, se pondrá en contacto con el responsable como máximo en una hora a contar desde la solicitud por parte de la persona autorizada.

Las consultas preferiblemente se formularán mediante correo electrónico, a fin de que quede constancia y control de las mismas.
El ayuntamiento podrá habilitar hasta 3 personas autorizadas a consultar a la empresa adjudicataria, bajo su responsabilidad, y con la supervisión del responsable de seguridad y/o DPD/DPO.

d) Forma de contacto entre ayuntamiento y empresa adjudicataria.

Tal y como se ha especificado en los apartados anteriores la comunicación entre el ayuntamiento y la empresa adjudicataria se realizará mediante correo electrónico y/o a través de alguna plataforma online en la que se facilite de forma bidireccional toda la documentación necesaria y se pueda consultar el estado de las tareas, proyecto, consultas, etc.

e) Calendario de trabajo

El calendario ordinario de ejecución de los trabajos de implantación y entrega de los informes de auditoría anuales será de tres meses a partir de la finalización de toma de datos.
Teniendo en cuenta que tanto la toma de datos inicial como la entrega de toda la documentación y formación el primer año se hacen de forma presencial, este calendario queda sujeto a la disponibilidad por ambas partes y a la situación de pandemia actual.

3.2) Esquema Nacional de Seguridad (ENS)

a) Plan de Adecuación al Esquema Nacional de Seguridad.

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar y aprobar la declaración de aplicabilidad de las medidas de seguridad del Anexo II del ENS (https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1071)
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución.
- Identificación de:
  - Responsable de la información. Determinará los requisitos de la información tratada.
  - Responsable del servicio. Determinará los requisitos de los servicios prestados.
  - Responsable de seguridad. Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios

b) Propuesta Técnica.

- **Planteamiento General**

  Las directrices generales del proyecto a presentar serán:
  - Implantación inicial del SGSI (Sistema de Gestión de Seguridad de la Información).
  - Proyecto "llave en mano": apoyo constante durante el primer año al ayuntamiento para la realización de un Plan de Adecuación al ENS.

- Consultoría y/o elaboración de la documentación de los controles del Anexo II del RD 3/2010.
- Formación y concienciación al equipo técnico del ayuntamiento.
- Compromiso de definir un sistema de trabajo sencillo, práctico y eficiente, adaptado a las necesidades reales de la organización.
- Consultoría, a ser posible, presencial.
- Incorporación de diagramas de flujo, para facilitar su comprensión.
- Plazo para alcanzar el Plan de Adecuación: 3 meses.

- **Fases del proyecto:**
  - **FASE 1:**
    - **Establecimiento del SGSI**
      - ✓ Establecimiento del Comité de Seguridad de Tecnologías de la Información y Comunicación (Comité STIC).
      - ✓ Definir Alcance del SGSI
      - ✓ Preparar y aprobar la política de Seguridad
      - ✓ Definir roles y Asignar personas:
        - Responsable de Seguridad
        - Responsable de la Información
        - Responsable del Sistema
    - **Valoración y Categorización del Sistema**
      - ✓ Inventario de la Información y los servicios (Implicaciones de Protección de datos)
      - ✓ Valorar (Alto, Medio, Bajo) la información y los servicios en cada una de las Dimensiones
        - Disponibilidad
        - Integridad
        - Confidencialidad
        - Autenticidad
        - Trazabilidad
      - ✓ Valoración de la categoría del sistema (Alto, Medio, Bajo).
    - **Análisis de Riesgos**
      - ✓ Identificación de Activos Esenciales
      - ✓ Valoración de las amenazas y salvaguardas
      - ✓ Analizar Impacto y Riesgo

      Herramientas de referencia: PILAR y metodología: MAGERIT v3
    - **Declaración de aplicabilidad**
      - ✓ Documento con las medidas de seguridad que son de aplicación al sistema de la Entidad
      - ✓ Adecuación de los controles

    - **Plan de Mejora**

      Elaboración del Documento final "Plan de Adecuación al ENS" en el que se definirá:
      - ✓ Hoja de ruta a seguir para el cumplimiento del ENS
      - ✓ Se plasmará en un documento llamado "Plan de Mejora de la Seguridad":
        - Definición de tareas necesarias para sanear las insuficiencias.
        - Indicando plazos

- Recursos asignados
- Responsabilidades
- Costes orientativos

✓ Tratamiento del Riesgo
- Transferir/Evitar/Asumir/Reducir

◆ **FASE 2:**

× **Kit de Concienciación**

El KIT de concienciación se compone por:

✓ Ataques simulados dirigidos y Evaluación Inicial
✓ Varias sesiones Formativas de 2 horas online para usuarios finales
✓ Test/Evaluación a los usuarios sobre los contenidos de la formación
✓ Distribución de material (posters y trípticos).
✓ Ataque simulado dirigido y evaluación final.

× **Consultoría en la adecuación al ENS**

✓ Elaboración de la documentación de los controles del ANEXO II RD/2010 según plan definido
✓ Sesiones online mensuales de seguimiento.

ANEXO I

Áreas dónde realizar el estudio y su ubicación.

1. Archivo Municipal (Plaza de España 8)
2. Cultura, Teatro Apolo (C/ La Cruz, alrededores de Plaza de España 8)
3. Conservatorio Municipal de Música (C/ Entrehuertas 10)
4. Instalaciones Deportivas Municipales (Camino Anduva s/n)
5. Gabinete Médico (Camino Anduva s/n)
6. Secretaría General (Plaza de España 8)
7. Gabinete de Alcaldía (Plaza de España 8)

8. Personal (Plaza de España 8)
9. Turismo, Comercio, etc (Plaza de Santa María, alrededores de Plaza de España 8)
10. Centro Joven (C/ Condado de Treviño)
11. Centro de Información Juvenil (Parque Antonio Machado)
12. OMIC (Oficina del Consumidor) (Plaza de España 8)
13. SAC (Servicio de Atención Ciudadana) (Plaza de España 8)
14. Aguas (Plaza de España 8)
15. Padrón Habitantes/Estadística/Centralita/Notificadores (Plaza de España 8)
16. Tesorería (Plaza de España 8)
17. Recaudación (Plaza de España 8)
18. Tributos (Plaza de España 8)
19. Contabilidad/Intervención (Plaza de España 8)
20. Informática (Plaza de España 8)
21. Contratación y Patrimonio (Plaza de España 8)
22. Obras y Servicios (C/ San Juan, alrededores de Plaza de España 8)
23. Escuela Taller (C/ San Juan, alrededores de Plaza de España 8)
24. Parque Móvil (C/ Eras de San Juan)
25. Urbanismo (C/ Condado de Treviño)
26. Industrial (C/ Condado de Treviño)
27. Medio Ambiente (C/ Condado de Treviño)
28. Servicios Sociales (C/ Condado de Treviño y Av República de Argentina)
29. Atención Temprana (C/ Comuneros de Castilla)
30. Casa de Cultura (C/ Río Ebro 31)
31. Igualdad (C/ La Charca)
32. Centro Socio Cultural de Mayores (C/ Los Almacenes)
33. Bomberos (C/ Californias)
34. Policía Local (Ctra. FuenteCaliente)

Puede darse el caso que algunas de las áreas el responsable coincida aunque la ubicación no sea la misma.

Esta estructura servirá a modo de referencia para la realización de la auditoría.