Área Tenerife 2030: Innovación, Educación, Cultura y Deportes.
Consejería con Delegación Especial en TIC y Sociedad de la Información
Servicio Técnico de Informática y Comunicaciones

Fecha: 12/12/2017 **Fax:** 922 239 468
Ref.: CBP/NBF **Tfno.:** 922 843 426

Asunto: Pliego de prescripciones técnicas para la contratación del servicio de apoyo para el cumplimiento normativo en seguridad de la información.

Destinatario: Servicio Administrativo de Informática y Comunicaciones.

PLIEGO DE CLÁUSULAS TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE APOYO AL CUMPLIMIENTO NORMATIVO EN SEGURIDAD DE LA INFORMACIÓN

1. Objeto

El objeto del contrato es la prestación de un conjunto de servicios de consultoría y auditoría, de naturaleza tanto técnica como jurídica, necesarios para lograr, y mantener durante la vigencia de la contratación, la adecuación y cumplimiento de la normativa asociada a la Ley Orgánica de **Protección de Datos de Carácter Personal** (LOPD) y al **Esquema Nacional de Seguridad** (ENS) en el Excmo. Cabildo Insular de Tenerife (ECIT), y que tendrá las siguientes componentes:

- **Servicio base**: se trata de la prestación principal y permanente dentro del contrato, y que debe incluir como mínimo las siguientes actividades:
  - Resolución consultas.
  - Concienciación y formación.
  - Adecuación y mantenimiento.
  - Realización de auditorías.
  - Delegado de Protección de Datos (DPO).

- **Servicio ampliados**: se corresponderá con la ejecución bajo demanda de trabajos, empleando los perfiles establecidos en el contrato, para dar cobertura a las siguientes tareas no previstas en el servicio base:
  - Ejecución de tareas y/o proyectos derivados de las auditorías y/o planes de adecuación, que tengan un alcance superior a las 100 horas de ejecución.
  - Adecuación a cambios normativos no previstos expresamente en los servicios base y que tengan un alcance superior a las 100 horas de ejecución.
  - Auditorías de aplicaciones web de nuevos desarrollos o ya implantadas con el objetivo de asegurar las medidas de protección de aplicaciones informáticas (MP.SW), y en general, otras auditorías adicionales a las previstas en los pliegos.
  - Apoyo a Ayuntamientos de la isla de Tenerife en cualquiera de las prestaciones incluidas en el pliego, incluido el perfil de Delegado de Protección de Datos (DPO).

Se entenderá incluida en el objeto de la presente contratación **cualquier normativa** adicional que pueda afectar con carácter general o particular la **seguridad de la información tratada** por el ECIT en el ejercicio de sus competencias.

La presente contratación tendrá como **objetivo principal conseguir la adecuación a la normativa** indicada en el ECIT, como máximo en **un año desde la adjudicación** del mismo

(considerando exclusivamente las tareas que puedan y deban ser ejecutadas por la adjudicataria) y **gestionar el posterior mantenimiento** de la misma durante la vigencia del contrato.

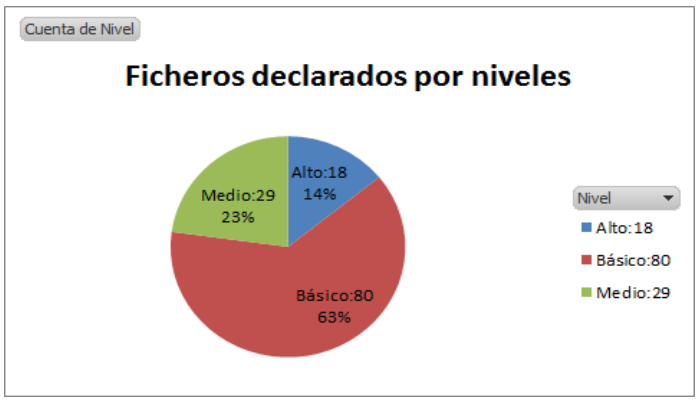
En concreto, y en el apartado de la LOPD, será objeto de la presente contratación la adaptación lo más inmediata posible al **Reglamento (UE) 2016/679** del Parlamento Europeo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos-RGPD-) y, en su caso, a la norma estatal de transposición del citado Reglamento europeo que en su momento se apruebe, de los tratamientos de datos de carácter personal (DCP) realizados en soporte automatizado y en el soporte papel de los que sea titular el ECIT.

En lo que respecta al ENS, será objeto del contrato la adaptación lo más inmediata posible al **Real Decreto 3/2010**, de 8 de enero, sobre el Esquema Nacional de Seguridad (ENS), y a su modificación, a través del **Real Decreto 951/2015**, de 23 de octubre, en respuesta a la evolución del entorno regulatorio de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

1.1. Situación actual LOPD

El ECIT cuenta actualmente con dos documentos de seguridad, uno para los tratamientos que se realicen a través de sistemas de información en soporte automatizado y otro para el tratamiento en soporte no automatizado o papel. Ambos documentos cuentan con una parte general, en donde se establecen las normas y los procedimientos necesarios para garantizar la seguridad de los datos de carácter personal, y una parte especial, donde se concreta para cada uno de los ficheros, las medidas de índole técnica y organizativa necesarias que garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Se muestran a continuación dos cuadros resumen de los 127 ficheros declarados por niveles y tratamiento:

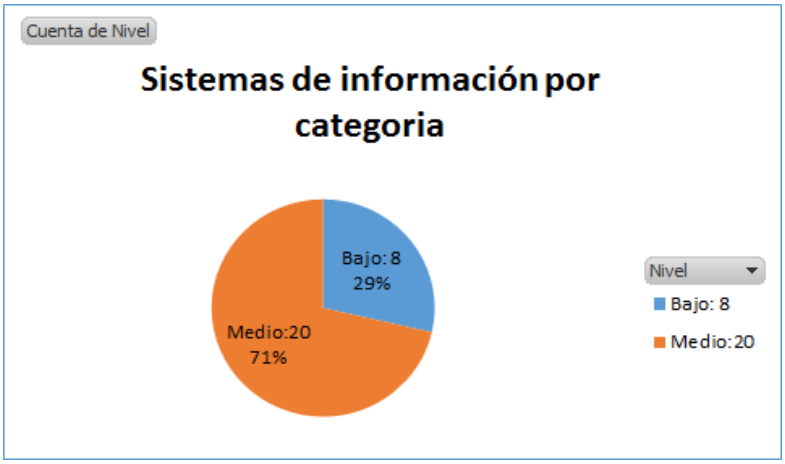


Nota: los datos aportados podrán ser susceptibles de variación al inicio (revisión inicial con actualización de la información) y durante la ejecución del contrato (de acuerdo a las necesidades del ECIT).

1.1. Situación actual ENS

En el año 2012 se realizó el plan de adecuación al ENS, en el cual se identificaron 27 sistemas de información para la prestación de de los servicios de Administración electrónica y el soporte del procedimiento administrativo general. La categoría máxima para cada uno de las dimensiones de seguridad se valoró como medio.

A día de hoy se dispone de 28 sistemas de información y en la siguiente tabla se clasifican por categoría:



Nota: los datos aportados podrán ser susceptibles de variación al inicio (revisión inicial con actualización de la información) y durante la ejecución del contrato (de acuerdo a las necesidades del ECIT).

En el plan de adecuación se identificaron una serie de actuaciones con el objetivo de subsanar las deficiencias encontradas. Concretamente se identificaron 15 acciones con objetivos claros y acciones a realizar. De esas 15 acciones se ha completado aproximadamente un 20% del trabajo.

Se detallan también los datos del cuadro de mandos del estado de la seguridad (INES) de 2016.

- Indicador de madurez del ENS: 48,82%
- Indicador de cumplimiento del ENS: 60,79%
- Organización de la seguridad: 38 (según métrica propia de INES).
- Gestión de incidentes: 180 (según métrica propia de INES).

2. Servicio base

Tendrán el siguiente alcance y dimensionamiento para cada una de las actividades previstas:

- **Resolución consultas**:
    - Alcance:
        - Atención de **consultas técnicas y/o jurídicas** referentes al cumplimiento ENS/LOPD.
            - La documentación y respuestas generadas, en base a las consultas planteadas, se deberá consolidar e incorporar a la herramienta de soporte a la gestión LOPD/ENS, indicada en los siguientes apartados, o en la herramienta que indique el ECIT (FAQ Intranet, herramienta de gestión del conocimiento, etc).
        - Redacción de **propuestas, estudios e informes** sencillos sobre la aplicación práctica de la normativa.

    - Dimensionamiento:
        - Bolsa de **120 horas/anuales**.

- **Concienciación y formación**:

    - Alcance:
        - Jornadas de **formación presencial**: **20 jornadas anuales** (de 8 horas), que se consumirá en sesiones de como mínimo 1 o 2 jornadas cada una.
            - Contenidos:
                - Cursos con diferentes niveles de profundidad sobre la normativa asociada a la seguridad de la información.
                - Cursos sobre buenas prácticas en el uso de servicios IT.
                - Cualquier otro curso que mejore las capacidades en cuanto al conocimiento de las normas internas, ciberseguridad, legislación, etc.. del personal del ECIT.
            - Colectivos: dirigida a:
                - Empleados en general.

        - Personal técnico y/o jurídico.
        - Mandos intermedios.
        - Altos cargos y responsables políticos.
    - Preparación de **cursos para teleformación** (Moodle):
        - Para cada sesión de formación del apartado anterior, se deberá hacer entrega de los contenidos del mismo en formato Moodle (SCORM).
    - Apoyo para la **preparación y ejecución de eventos:** de difusión y concienciación en materias asociadas a la seguridad de la información.
    - **Píldoras** formativas.
        - Una píldora audiovisual, de 1 minuto y 30 segundos como máximo, **cada mes**, sobre aspectos de concienciación y formación en seguridad, y en un formato audiovisual adecuado para captar la atención y transmitir las ideas de una forma sencilla y eficiente.
  - Dimensionamiento: el necesario para el desarrollo de las actividades previstas.

- **Adecuación y mantenimiento**: será la actividad principal del servicio base.
  - Alcance:
    - Deberá incluir en general las **tareas necesarias** para la gestión y ejecución de la **adecuación** normativa inicial y el **mantenimiento** posterior de la misma.
    - Puesta a disposición en modalidad software como servicio (**SaaS**) de una **herramienta informática para el soporte a la gestión normativa ENS/LOPD**:
        - Los requisitos mínimos son los indicados en el **Anexo II**.
        - La **responsabilidad en la carga y mantenimiento** de la información, necesaria para lograr una gestión adecuada para el cumplimiento normativo deseado, recaerá exclusivamente en la **empresa adjudicataria**, salvo en los aspectos en los que el ECIT indique expresamente lo contrario.
        - Posibilidad de **acceso y uso sin restricciones** para al menos **10 usuarios** asociados a los roles de consulta y gestión técnica y jurídica del ECIT (además de los necesarios por el personal de la adjudicataria).
        - Se deberá incluir **5 jornadas específicas** de **formación** de la herramienta al inicio del contrato (con independencia de las previstas en el apartado de Concienciación y formación).
        - **Implantación del Registro de Actividades** previsto en el RGPD, incluyendo la **carga inicial, con migración de datos existentes, y mantenimiento posterior**.
    - Ejecución de los siguientes **proyectos de análisis de situación y planificación de actuaciones al inicio del contrato**: en el **Anexo III** se

incluye el detalle asociado:

- **P1 Análisis de situación e impacto cambios ENS/RGPD**.
- **P2 Actualización plan de adecuación ENS/RGPD**.

- **Seguimiento y ejecución** de:
  - Acciones derivadas de los **planes de adecuación**.
  - **Resolución de aspectos no conformes** reflejados en las **auditorías**, aportando conocimiento para la obtención de la solución más adecuada, cuando la ejecución corresponda a terceros.
- **Propuesta, desarrollo, adaptación y/o mejora de la documentación** requerida para la adecuación y su mantenimiento:
  - Políticas de seguridad.
  - Normativas de seguridad específicas.
  - Procedimientos
  - Instrucciones Técnicas
  - Adaptación de la información y documentos a **cambios de estructura organizativa** en el ECIT.
- Revisión, propuesta y actualización de **documentación técnica de seguridad**.
  - Revisión, propuesta y seguimiento de **configuraciones seguras** sobre los sistemas.
  - Revisión, propuesta y seguimiento de **planes de contingencia y continuidad** de sistemas
- Definición, entrega, actualización y seguimiento de un **sistema de indicadores** que permita dar visibilidad a los técnicos y a la dirección del ECIT del estado de adecuación en todo momento:
  - Para el ENS, como mínimo la base del **CCN-STIC-824** empleada en **INES**.
  - Para la LOPD/RGPD es necesario que la adjudicataria defina un esquema equivalente.
  - Emisión de **informes mensuales** y distribución a los contactos que defina el ECIT.
- Realización y mantenimiento de los **análisis de riesgos** necesarios por ambas normativas.
  - Emplear una metodología basada en la gestión de riesgos, como por ejemplo la **ISO 31000:2010.**
  - Evaluación y determinación de los niveles de seguridad por actividad.
- **Gestión de cambios normativos**: seguimiento y alerta ante cambios normativos que se puedan producir en materia de ENS/LOPD:
  - Informando en cada momento de las implicaciones que estos cambios puedan producir. Realización de análisis, informe y

resumen de impacto.
                - Propuesta de plan de adecuación de información, documentos y procedimientos a los posibles cambios normativos, organizativos, etc.
                - Ejecución de acciones para la actualización de información y documentación.
            - Apoyo a la **comunicación**:
                - Preparar y distribuir informes, documentos, propuestas técnicas, organizativas y jurídicas para las distintas Áreas y Servicios del ECIT, así como para agentes externos .
            - Propuesta y soporte a la **gestión de crisis de seguridad**.
                - Definición de procedimiento de actuación.
                - Apoyo a la gestión de crisis de seguridad.
                - Intermediación en la comunicación a terceros.
            - Otras tareas de análisis, documentación y/o generación de informes técnicos/jurídicos necesarios para la adecuación normativa.
        - Dimensionamiento: Bolsa de **400 horas/anuales**.

- **Realización de auditorías**:
    - Alcance: ejecución de:
        - **Tareas** permanentes y rutinarias de **control, revisión y auditoría** de eventos asociados a la seguridad de la información:
            - Uso de otras aplicaciones o herramientas internas o de terceros que requiera una auditoría periódica sobre el acceso y uso de la misma. Por ejemplo: uso de la Plataforma de Intermediación de Datos / Sustitución de Certificados en papel (SCSP) para el cumplimiento de las obligaciones asociadas, etc.
        - **Proyectos de auditoría formales** indicados en el **Anexo III** (planificación y detalle). Estos proyectos se repetirán cíclicamente a lo largo de la ejecución del contrato, incluyendo sus posibles prórrogas.
            - Auditorías **año impar**:
                - P3 Auditoría ENS.
                - P4 Auditoría perimetral.
            - Auditoría **año par**:
                - P5 Auditoría RGPD.
                - P6 Auditoría interna.
    - Dimensionamiento: el necesario para el desarrollo de las actividades previstas.

- **Delegado de Protección de Datos (DPO)**:
    - Alcance:
        - Prestación con las funciones asociadas a la figura de Delegado de Protección de Datos, conforme a las **funciones** establecidas en **el RGPD**,

para el ámbito del ECIT:

- **Supervisar** el cumplimiento de lo dispuesto en el RGPD, normativa asociada aplicable, y de las políticas del responsable o del encargado del tratamiento en la materia.
- Ofrecer el **asesoramiento** que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- **Cooperar con la autoridad de control**. Actuar como punto de contacto para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.
- **Informar y asesorar** al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones aplicables.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

- Los datos de contacto del DPO serán publicados y comunicados a la autoridad de control.
- El ECIT facilitará los recursos necesarios para el desempeño de las funciones del DPO y el acceso a los datos personales y a las operaciones de tratamiento, para el mantenimiento de sus conocimientos especializados.
- Rendirá cuentas solamente al máximo responsable de la Consejería Delegada en TIC y Sociedad de la Información.
- Las **funciones genéricas** del DPD se pueden concretar en ejecutar tareas de **asesoramiento y supervisión** en, entre otras, las siguientes áreas:
  - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
  - Identificación de las bases jurídicas de los tratamientos.
  - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
  - Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
  - Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
  - Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-

encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos

  - Dimensionamiento: Bolsa de **400 horas/anuales**.

Los **perfiles mínimos** necesarios para la prestación del servicio base serán:

- Al menos un **Auditor** (según perfil indicado en **Anexo I**).
- Al menos un **Consultor** (según perfil indicado en **Anexo I**).
- Al menos un **DPO** (según perfil indicado en **Anexo I**).
- **Perfiles adicionales especializados**, según las necesidades del contrato, en:
  - Conocimientos jurídicos, expertos en Procedimiento Administrativo, expertos en Archivística, gestión documental y conservación a largo plazo, expertos con conocimientos relativos a la gestión de documentos y archivos electrónicos, y otros que se estimen pertinentes en función del sistema auditado.
  - Conocimientos técnicos, expertos en sistemas y comunicaciones.

A continuación se indican las **condiciones generales** del servicio base:

Horarios de escalado y del servicio:

- Telefónico y Correo electrónico: 9x5 (L a V de 8:00 a 17:00, horario canario).

Canales de escalado: debe contemplar al menos:

- **Telefónico**: deberá incluir exclusivamente numeración que no sea de tarificación especial y/o adicional (p.e.: numeración 900/800, nacional o local).
- **Correo electrónico**.
- **Herramienta gestión de tareas:** se podrá solicitar por parte del ECIT a la adjudicataria el acceso y uso de la herramienta que dispone el ECIT para la gestión de tiques y proyectos. En caso contrario la adjudicataria deberá poner a disposición una herramienta para el registro, consulta/seguimiento y generación de informes sobre el cumplimiento del ANS en lo que respecta a la ejecución de proyectos, consultas, tareas, etc.

3. Servicios ampliados

Se corresponderá con la ejecución, bajo demanda y empleando los perfiles del contrato, para dar cobertura a las siguientes tareas no previstas en el servicio base:

- Ejecución de tareas y/o proyectos derivados de las auditorías y/o planes de adecuación, que tengan un alcance superior a las 100 horas de ejecución.
- Adecuación a cambios normativos no expresamente en los servicios base y que tengan un alcance superior a las 100 horas de ejecución.
- Auditorías de aplicaciones web de nuevos desarrollos o ya implantadas con el objetivo de asegurar las medidas de protección de aplicaciones informáticas (MP.SW) definidas por el ENS, y en general, otras auditorías adicionales a las previstas en los pliegos.
- Apoyo a Ayuntamientos de la isla de Tenerife en cualquiera de las prestaciones incluidas en el pliego, incluido el perfil de Delegado de Protección de Datos (DPO).

Tendrán el presupuesto anual establecido en el apartado del precio del contrato.

Los recursos asignados a los servicios ampliados no podrán coincidir, por norma general, con los dispuestos para la prestación del servicio base. En el caso en el que el destinatario del servicio ampliado fuera un ayuntamiento podrían coincidir los recursos.

El **procedimiento de ejecución** será el siguiente:

- El Servicio Técnico de Informática y Comunicaciones (STIC) solicitará por correo electrónico al adjudicatario ofertas concretas ajustadas al precio unitario ofertado y al presupuesto anual máximo disponible.
- Los recursos asignados deberán cumplir los requisitos de perfiles establecidos en el PPT.
- La empresa a la vista de la petición formulada por el STIC a través de correo-e, deberá elaborar su oferta concreta en un plazo máximo de **2 semanas**, de acuerdo con las condiciones previstas en los pliegos de cláusulas administrativas y técnicas, así como al contenido de la oferta presentada, donde se incluirá los precios ofertados para esta clase de prestaciones, en base a la cual se le adjudicó el contrato y el acuerdo de adjudicación del órgano competente.
- Dicha oferta deberá ser remitida por correo electrónico al STIC para prestar su conformidad; una vez conformado el correspondiente presupuesto, se remitirá al Servicio

Administrativo de Informática y Comunicaciones (en adelante SAIC), junto con el informe técnico de justificación correspondiente, para su trámite administrativo, y a su finalización, el SAIC notificará al adjudicatario la aceptación del mismo por la Corporación Insular.
- El inicio de su ejecución deberá realizarse en un **plazo máximo de un mes** a partir de su notificación a la adjudicataria.
- Se dejará **constancia** por correo electrónico de la **fecha real de inicio** del servicio ampliado.

En el caso de servicios ampliados **cuyo destinatario sea un Ayuntamiento** la solicitud al adjudicatario se coordinará entre el STIC y la Unidad de Modernización y Asistencia Municipal. Una vez formalizado el servicio ampliado se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento para el seguimiento del servicio y visto bueno de las tareas ejecutadas. Las tareas más generales de gestión, control, lanzamiento de estos servicios las hará la Unidad de Modernización y Asistencia Municipal.

En el supuesto de que la adjudicataria haya **ofertado alguna bolsa de horas sin coste adicional para servicios ampliados**, dentro de los criterios de adjudicación:

- En las propuestas de servicios ampliados que se presenten, se debe tener en cuenta, y con carácter prioritario, que es necesario consumir primero estas horas sin coste, antes de poder facturar alguna hora del perfil asociado.
- Los límites de presupuesto anual indicados, no se verán afectados por las posibles bolsas de horas ofertadas como mejora, ya que las mismas son sin coste adicional para el ECIT.

4. Propiedad intelectual

Toda la documentación y entregables generados debe prepararse y entregarse en formatos editables (.doc, .docx u .odt) y empleando las plantillas e imagen corporativa del ECIT.

El ECIT podrá requerir al adjudicatario para que realice la carga de todo el conocimiento y documentación generada, además de la propia herramienta de gestión, en la herramienta de gestión de conocimiento del STIC.

El contratista acepta expresamente que los derechos de explotación de cualquier trabajo desarrollado y documentación generada al amparo del presente contrato corresponden únicamente al ECIT, con exclusividad y a todos los efectos.

La empresa adjudicataria NO PODRÁ HACER USO de los mismos, ya sea como referencia o como base de futuros trabajos, salvo que cuente con autorización expresa, escrita y registrada del ECIT.

5. Transferencia de conocimiento

Durante la ejecución del objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar al personal que determine el ECIT la información y documentación que se solicite para disponer de un pleno conocimiento de las circunstancias en que se desarrolla el mismo, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para resolverlos.

Una vez finalizado el contrato, el adjudicatario se compromete durante un periodo de tres meses y con un mínimo de 40 horas al mes, a realizar la transferencia de conocimiento a la nueva adjudicataria o al personal que determine el ECIT.

6. Acuerdo de Nivel de Servicios (ANS)

El ECIT podrá ponerse en contacto con la empresa adjudicataria siempre que lo considere necesario a fin de recabar información sobre la marcha general del Servicio. Asimismo podrá comprobar la materialización y calidad de los servicios prestados mediante los medios que considere oportunos.

La revisión del cumplimiento del ANS especificado en este apartado, se realizará coincidiendo con la facturación del contrato, para lo que se deberá aportar, de forma anexa a la factura, el informe detallado correspondiente.

La regularización por penalizaciones se aplicará en la facturación de alguno de los meses siguientes al de la revisión.

Los **indicadores, y sus valores objetivos,** que como mínimo se tratarán para el control de la calidad de los servicios serán los siguientes:

- **Servicios base:**
  - **Consultas**
    - **Tiempo de respuesta consultas**: tiempo entre el escalado de una consulta y el contacto inicial de un técnico para iniciar la resolución de la misma.
    - **Tiempo de solución consultas:** tiempo entre el escalado de una consulta y su resolución.
  - **Formación**
    - **Incumplimientos hitos concienciación y formación:** incumplimiento en la forma (requisitos del PPT) y/o plazo de los entregables asociados.
  - **Auditorías y otros proyectos previstos**
    - **Incumplimientos plazo de adecuación:** incumplimiento del plazo establecido para la adecuación normativa (un año, o un valor inferior ofertado como mejora).
    - **Incumplimientos en proyectos:** incumplimiento en la forma (requisitos del PPT) y/o plazo de los proyectos.
  - **Seguimiento y adecuación / DPO**
    - **Deficiencias en seguimiento, adecuación y DPO:** incumplimiento de los requisitos establecidos en los pliegos.

- **Servicios ampliados:**
  - **Tiempo de oferta servicios ampliados**: plazo entre la petición de un servicio ampliado y la recepción de la oferta correspondiente.
  - **Tiempo de inicio servicios ampliados**: plazo desde la aceptación de una oferta por el ECIT y el inicio efectivo de los trabajos.
  - **Incumplimientos servicios ampliados:** incumplimiento en la forma (requisitos del

PPT) y/o plazo de los servicios ampliados.

A continuación se indican los valores objetivos establecidos para estos indicadores. En el supuesto de que la adjudicataria no cumpla con alguno de los valores objetivos fijados para el contrato en el ANS establecido, por causas imputables a la misma, el ECIT tendrá derecho a exigir una compensación cuantificada según se indica en las siguientes tablas:

Indicador	**VALOR OBJETIVO**	**PENALIZACIÓN**
Tiempo de respuesta consultas	<= 2 horas laborales	5% del importe mensual del servicio base por cada incumplimiento.
Tiempo de solución consultas	<= 48 horas naturales	5% del importe mensual del servicio base por cada incumplimiento.
Incumplimiento hitos de concienciación y formación	<= 2 al mes	5% del importe mensual del servicio base por cada incumplimiento.
Incumplimiento plazo de adecuación	< 1 año (o reducción ofertada)	10% del importe mensual del servicio base, en cada mes de incumplimiento.
Incumplimiento en proyectos	< 1 al mes	10% del importe mensual del servicio base por cada incumplimiento.
Deficiencias en seguimiento, adecuación y DPO	<= 3 al mes	5% del importe mensual del servicio base por cada incumplimiento.

Tiempo oferta servicios ampliados	<= 2 semanas	5% del importe mensual del servicio base por cada incumplimiento.
Tiempo de inicio servicios ampliados	<= 1 mes	10% del importe del servicio ampliado.
Incumplimiento servicios ampliados	<= 2 incumplimientos al mes, en plazo y/o cumplimiento de requisitos del PPT, en todos los servicios ampliados en ejecución.	5% del importe de los servicios ampliados que tengan incumplimientos.

7. Confidencialidad

Protección general de la información

Con carácter general la empresa adjudicataria queda expresamente obligada a mantener absolutamente confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del presente contrato.

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención a la observancia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la anterior, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El adjudicatario estará obligado a la realización y al mantenimiento de los registros de evidencias del cumplimiento, durante al menos todo el periodo de ejecución del contrato, de las actividades relacionadas a continuación:

- Definir, implementar y mantener una política de seguridad de la información.
- Implementar los análisis, ingeniería y contramedidas de seguridad con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información, mediante la ejecución de los controles que den respuesta a los requisitos especificados en este clausulado; todo ello integrado en una gestión de análisis y gestión del riesgo.
- Extender lo especificado en el punto anterior a los posibles contratos o relaciones con terceros vinculados a sistemas de información, productos y servicios que estén

relacionados con la prestación del servicio objeto del contrato.

Protección en actividades de auditoría

Datos de carácter personal

Las tareas de auditoría a realizar no conllevan, necesariamente en sí mismas, el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios, es posible que se acceda a datos de carácter personal (por ejemplo, en alguna documentación revisada).

Por lo tanto, dado que en alguna circunstancia, se podría acceder a este tipo de datos, el equipo de auditoría de la adjudicataria se compromete, en cumplimiento de la legislación vigente en cuanto a tratamiento de datos de carácter personal, a tratar estos datos conforme a las instrucciones del responsable de los datos de carácter personal, a los que pudiera acceder, que no los aplicará o utilizará con fin distinto al que figure en este acuerdo y contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

La adjudicataria declara conocer la legislación vigente en materia de protección de datos, y el equipo de auditoría está instruido en estos requisitos. Por lo tanto, en caso de tener lugar este acceso, como consecuencia de los servicios a prestar, se compromete a observar los requisitos establecidos en esta legislación.

De igual forma el ECIT al cual pertenece el sistema auditado se compromete a no difundir ni utilizar para otros fines que los de la realización de la auditoría, cualquier dato de carácter personal del equipo de auditoría.

Información del sistema de información auditado por la adjudicataria se compromete a no difundir información alguna (procesos, sistemas, medidas de seguridad, y cualquier otra información relacionada o no con el sistema de información auditado, incluyendo el informe de auditoría) que se pueda conocer o a la que se tenga acceso durante la realización de la auditoría. En este sentido están instruidos todos los integrantes del equipo de auditoría, que han firmado sus respectivos acuerdos de confidencialidad.

Una copia de los documentos de trabajo que se elaboren para la realización de la presente auditoría será custodiada por la adjudicataria, como evidencia del trabajo realizado.

Será responsabilidad de la adjudicataria, además de su custodia, que todos y cada uno de los miembros del equipo auditor, firmen el presente acuerdo de confidencialidad, incluyendo a expertos, con independencia del momento en el que se incorporen al mismo.

Protección del acceso a los recursos TIC del ECIT

En los supuestos de prestación de un servicio que requiera o se estime conveniente el acceso local o remoto a los recursos TIC del ECIT, se establecen las siguientes limitaciones y responsabilidades específicas:

1. Condiciones técnicas:
    1. Acceso remoto:
        i. La comunicación se realizará punto a punto entre las dependencias del prestador del servicio y las del ECIT empleando un canal de datos seguro (cifrado).
        ii. Si existe la mediación de un tercero, la empresa adjudicataria será la única responsable de asegurar la confidencialidad del intercambio y de las consecuencias de su incumplimiento.
        iii. El medio técnico preferente de conexión para accesos puntuales será el establecimiento de una conexión VPN. Para ello, con independencia del presente clausulado se deberá cursar la petición expresa correspondiente ante el ECIT una vez iniciada la prestación.
1. Recursos TIC accesibles:
    1. Solamente se dará acceso remoto a los servidores de aplicaciones, bases de datos, etc., estrictamente necesarios para el cumplimiento del objeto contractual.
    2. No se permitirá con carácter general el acceso al escritorio o entorno gráfico de los servidores salvo por necesidades extraordinarias del servicio ante incidencias críticas y no exista otra alternativa viable (requerirá de forma obligatoria la validación expresa del ECIT).
2. Características del acceso local:
    1. El acceso local a recursos TIC de equipos de las empresas prestadoras de servicios se deberá integrar y cumplir con las medidas de seguridad de la red del ECIT (control de acceso a la red, disponibilidad de antivirus actualizado, parches seguridad, etc).
3. Potestad de control
    1. El personal autorizado del ECIT, teniendo como finalidad la protección, optimización y mejora de los servicios, monitorizará el tráfico cursado en este tipo de conexiones para la detección de actuaciones anómalas.
4. Deberes y obligaciones para la empresa adjudicataria:
    1. Solamente deberá tener acceso a los recursos del ECIT los usuarios de la prestadora de servicios autorizados y que sean estrictamente necesarios para los fines previamente autorizados por el ECIT.
    2. Los usuarios de la empresa prestadora de servicios deberán hacer un uso adecuado de la conexión, utilizándola eficientemente con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.
    3. Se deberá acceder desde equipos y/o redes protegidas que garanticen unas condiciones de seguridad adecuadas sobre todo en lo referente al control de accesos al personal autorizado y la protección de los activos del ECIT a los que se tenga acceso (lo que requiere el uso de soluciones actualizadas, antivirus, antispyware, etc…).
    4. La empresa adjudicataria será la responsable directa de todas las actividades realizadas bajo su nombre.
    5. Las incidencias de seguridad detectadas por el personal del ECIT o comunicadas por entidades externas serán trasladadas al usuario que pueda originarla para la aplicación de las medidas que se estimen oportunas.
    6. Los usuarios deberán reportar al ECIT aquellas incidencias de seguridad de las que

tuviesen conocimiento (p.ej.: pérdida o compromiso de las credenciales, etc.).

5. Uso no adecuado: el servicio de acceso remoto no debe ser usado para:
    1. Cualquier transmisión de información o acto que viole la legislación vigente que le sea de aplicación.
    2. Fines privados, personales o comerciales, no relacionados con las actividades propias y autorizadas por el ECIT.
    3. Transmisión de material que infrinja la legislación sobre propiedad intelectual (software, imágenes, video, audio, películas, etc.). En general el usuario se compromete a no hacer uso de los recursos informáticos y de comunicación para publicar o divulgar material obsceno, difamatorio u ofensivo que pueda suponer una violación de los derechos legales de terceros.
    4. Creación, utilización y transmisión de cualquier tipo de material que perjudique la dinámica habitual de los usuarios del ECIT o redes externas (virus, difusión de correo publicitario, cadenas de correo-e, etc.).
    5. Actividades deliberadas con alguna de las siguientes finalidades:
        i. Congestión de los enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
        ii. Escanear puertos de equipos sin autorización del titular/es del mismo.
        iii. Búsqueda de vulnerabilidades en equipos pertenecientes al ECIT o redes externas.
        iv. Denegación de servicios y desconexión de equipos.
        v. Destrucción o modificación de la información de otros usuarios o sistemas de información.
        vi. Violación de la privacidad e intimidad de otros usuarios.
        vii. Intentar o conseguir acceder de forma no autorizada a equipos.
    1. Bajo ningún concepto el usuario atentará contra la integridad, funcionamiento o disponibilidad de los recursos informáticos que componen la red del ECIT. Se considera un atentado contra la integridad de los recursos informáticos las acciones que no tomen las medidas pertinentes contra la inclusión y/o ejecución de software pernicioso (virus, sniffers, etc.) en los equipos a los que tienen acceso, así como el acceso a los recursos informáticos fuera de las condiciones autorizadas por el ECIT.

8. Anexo I – Descripción de perfiles

8.1. Delegado de Protección de Datos (DPO)

- Funciones: las indicadas en el PPT para el DPO.
- Formación básica:
  - Certificado de formación DPO de como mínimo 25 horas (LOPD), de una entidad oficial: Colegio Profesional, Asociación Profesional Española de Privacidad, AENOR, etc.
  - Al menos 100 horas en conocimientos especializados en el derecho de la protección de datos.
- Experiencia:
  - Experiencia verificable y evidenciada de al menos 3 años en materia de protección de datos.

8.2. Auditor

- Funciones: supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionados en el informe, así como preservar las evidencias de la auditoría.
- Formación básica: acreditar al menos 150 horas de formación en:
  - Auditoría de sistemas de información.
  - Seguridad y gestión de riesgos de seguridad.
  - Requisitos del ENS y LOPD.
- Experiencia:
  - Experiencia verificable y evidenciada de al menos 4 años, en auditoría de tecnologías de la información.
  - Experiencia probada de al menos 4 años en estos elementos en seguridad y gestión de riesgos de seguridad con alguna metodología reconocida.

8.3. Consultor

- Funciones: cualquier tarea técnica y/o jurídica especializada que sea necesaria para el cumplimiento del objeto del contrato.
- Formación básica: acreditar al menos:
  - 150 horas de formación en:
    - Conocimientos sistemas y comunicaciones.
  - 150 horas de formación en:
    - Normativa ENS y LOPD.
- Experiencia:
  - Experiencia verificable y evidenciada de al menos 3 años en consultoría de sistemas y comunicaciones.
  - Experiencia verificable y evidenciada de al menos 3 años en consultoría de normativa ENS y LOPD.

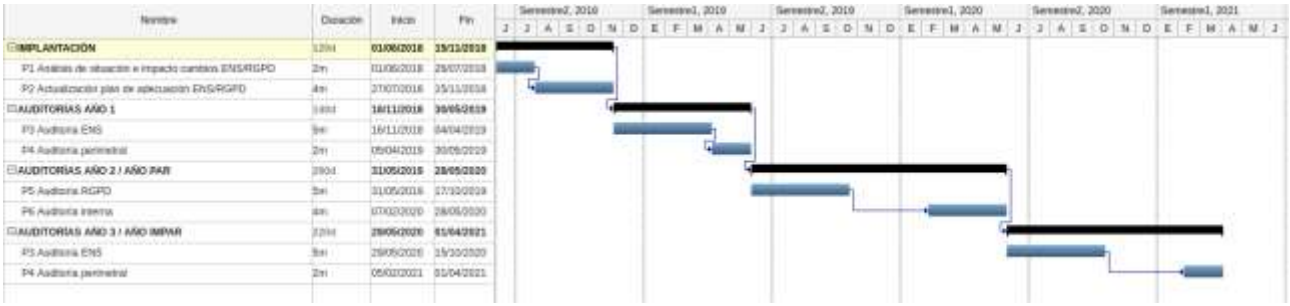
9. Anexo II – Requisitos software de gestión

- Aplicación de soporte a la gestión ENS/LOPD.
    - Se requiere la gestión del ciclo completo del ENS/LOPD.
    - Se debe suministrar:
        - Licencia de software de Gestión de ENS y carga de los datos en el mismo.
        - Licencia de software de Gestión de LOPD y carga de los datos en el mismo.
    - El adjudicatario será el encargado de incorporar al sistema las datos iniciales y realizar el completo mantenimiento de los mismos. La migración la deberá realizar el adjudicatario desde las fuentes actuales, asumiendo cualquier tarea de extracción, transformación y/o carga necesaria.
    - El software deberá permitir la exportación de absolutamente todos los datos cargados en la misma a formatos ofimáticos estándares cuando finalice el contrato.
    - El software en ENS deberá contar con:
        - Gestión completa del ciclo PDCA.
        - Gestor Documental.
        - Diseño de procesos / procedimientos.
        - Gestión de Métricas e Indicadores.
        - Módulo de Formación.
        - Gestión de Incidentes.
        - Gestor gráfico de activos y dependencias.
        - Motor de Análisis y Gestión de riesgos.
    - El software en LOPD deberá contar con:
        - Gestión de los datos de la organización
        - Gestión de ficheros.
        - Registro de actividades (RGPD).
            - Deberá contener, respecto de cada actividad, la información que establece el artículo 30 del RGPD y que habrá de organizarse, bien a partir de los ficheros actualmente inscritos en el Registro Estatal de Protección de Datos, bien en torno a las operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo, “gestión de clientes”, “gestión contable” o “gestión de recursos humanos y nóminas”) o con arreglo a otros criterios distintos debidamente motivados. La decisión a tomar le compete al ECIT, a propuesta motivada de la empresa que resulte adjudicataria.
            - Se debe incluir la migración al formato electrónico del Registro de Actividades del inventario final de ficheros titularidad del ECIT.
        - Gestión de los sistemas de tratamiento
        - Gestión de los procedimientos
        - Gestión de personal
        - Generación del documento de seguridad
        - Generación de manuales de usuarios y responsables
        - La gestión de los terceros y contratos de prestación de servicios asociados
        - Inscripción de ficheros e integración con NOTA.
    - De igual modo, se exigirá que las herramientas de gestión cumplan en todo momento con la normativa vigente, por lo que deberán ser adecuadas a los

cambios. Esta adecuación de las herramientas nunca será imputable al ECIT o a los servicios ampliados del contrato.

10. Anexo III – Detalle proyectos previstos

La planificación del plan de proyectos es la que se indica en la siguiente figura (suponiendo el inicio de ejecución del contrato para Junio de 2018, en el supuesto en el que la formalización del contrato se realice en una fecha diferente, se deberá ajustar el inicio del plan de proyectos a la misma):



El detalle de todos los proyectos es el indicado a continuación:

P1 Análisis de situación e impacto cambios ENS/RGPD (Máx: 2 meses)
Objetivos:
● Valorar situación implantación ENS/RGPD. ● Valorar impacto de cambios normativos (RD 951/2015, guías CCN, etc).
Alcance:
● ENS: aplicando las guías STIC-CCN correspondientes: ○ Revisión clasificación de los sistemas de información. ○ Revisión y elaboración de Informe de adecuación. ○ Revisión de estado plan de adecuación (año 2012) ■ (31 deficiencias detectadas, propuesta de 15 actuaciones de mejora para subsanarlas.). ○ Carga de información básica ENS en herramienta informática. ● LOPD-RGPD ○ Revisión de puntos para la adaptación al nuevo reglamento europeo (RGPD). ○ Con objetivo de adecuar al RGPD las medidas de seguridad actualmente aplicables a los tratamientos de DCP que conforman el inventario de ficheros titularidad de esta Corporación Insular, tanto en soporte automatizado como en soporte papel, forma parte del alcance de este contrato analizar las medidas de seguridad existentes, para determinar si las mismas cumplen con lo dispuesto en el Reglamento de referencia para todos los niveles de seguridad, Básico, Medio y Alto y proponer, en su caso, las modificaciones que se estimen oportunas para la adecuación al RGPD. ○ De igual forma, se actualizarán las reglas, normas y principios que inspiran la PDC (principio de responsabilidad proactiva y enfoque de riesgo) y los protocolos internos orientados a garantizar los

mismos contemplados en la parte general de los actuales Documentos de Seguridad.

- Actualizar el inventario de ficheros LOPD, abarcando tanto el tratamiento automatizado como el realizado en soporte papel. En tal sentido se identificarán:
  - Si se operan cambios con respecto a ficheros ya creados y registrados en la Agencia Española de Protección de Datos (AEPD) y en consecuencia procede su modificación.
  - Si hubiera que crear nuevos ficheros o suprimir alguno de los existentes (dar de alta o baja en el Registro de Actividades).
- En la línea de fortalecer los principios de "responsabilidad proactiva" y "enfoque de riesgos", como principios que propugna el RGPD para quienes tratan datos personales en los sectores público, se habrá de determinar las medidas técnicas y organizativas adecuadas al riesgo que conlleva el tratamiento a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. A tal efecto se analizarán los datos que son objeto de tratamiento, con qué finalidades lo hacemos y qué tipo de operaciones de tratamiento se llevan a cabo. A partir de este conocimiento se concretarán de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo.
- Esta labor implicará llevar a cabo un análisis de los riesgos asociados a todos los tratamientos de DCP titularidad del ECIT, para determinar si las medidas de seguridad técnicas y organizativas son las adecuadas para ofrecer un nivel de seguridad adecuado o por el contrario si fuere necesario completarlas con medidas adicionales o prescindir de alguna de las medidas. A tal efecto, se utilizará alguna de las metodologías de análisis de riesgo existentes. Las medidas técnicas y organizativas que se propongan tendrán en cuenta:
  - El coste de la técnica.
  - Los costes de aplicación.
  - La naturaleza, el ámbito, el contexto y los fines del tratamiento
  - Los riesgos para los derechos y libertades de las personas
- El Análisis de Riesgos concretará además:
  - Los tratamientos o situaciones en las que tratándose con DCP se entienda que procede la realización de una Evaluación de Impacto en materia de protección de datos (EIPD).
  - Los tratamientos o situaciones en las que tratándose con DCP se entienda que no procede la realización de una EIPD.
- Si del análisis de riesgo se concluye que existe un alto riesgo para los derechos y libertades de los interesados, se llevarán a cabo a cabo una Evaluación de impacto (EIPD), a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD. La EIPD recogerá, al menos, el contenido mínimo previsto en el RGPD. A tal efecto, se utilizará alguna de las metodologías de análisis de riesgo existentes y tomará como referencia la Guía para la Evaluación de Impacto en la Protección de Datos Personales elaborada por la Agencia Española de Protección de Datos (AEPD) y la Guía de evaluación de impacto en la protección de datos (DPIA) adoptada por el Grupo de Trabajo del Artículo 29 con fecha 4 de abril de 2017.
- En los casos en que las EIPD hayan identificado un alto riesgo que a juicio del responsable de tratamiento, esto es, el ECIT, previa motivación de la empresa contratista, no pueda mitigarse por medios razonables en términos de la tecnología disponible y costes de aplicación, la empresa formulará la consulta que el ECIT, en su caso, realizará a la autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto.

Entregables:

- Documento de análisis de situación e impacto de cambios normativos.

- Carga de información básica ENS en herramienta informática.
- Inventario de ficheros LOPD actualizado y actualización de cambios ante la AEPD.
- Evaluaciones de impacto (EIPD).
- Formación: herramienta de gestión ENS/LOPD.
- Formación: actualización normativa ENS/LOPD.
    - Personal técnico (6 horas).
    - Personal administrativo/jurídico (6 horas).

P2- Actualización plan de adecuación ENS/RGPD (Máx: 2 meses)

Objetivos:

- Definir un plan de adecuación para lograr un **pleno cumplimiento normativo en seis meses como máximo** (contando solamente con las tareas que sean responsabilidad de la adjudicataria).
- Ejecución de las tareas iniciales más importantes.

Alcance:

- ENS:
    - Seguimiento de todos los puntos de control definidos en la Guía CCN-STIC 806.
    - Identificación y valoración de información y sistemas:
        - Revisión y actualización inventario de activos.
        - Revisión y valoración de activos.
    - Categorías del sistema
        - Valoración de niveles.
        - Identificación de medidas.
        - Valoración de fragmentar sistemas.
    - Análisis de riesgos:
        - Identificación y asociación de amenazas.
        - Análisis de riesgos
        - Riesgo residual, frecuencia e impacto.
        - Establecer la metodología de análisis de riesgo y proceder a su implantación.
    - Declaración de aplicabilidad.
    - Análisis de las 75 medidas de seguridad exigidas en el anexo ii en base a la categorización de los sistemas.
    - Análisis diferencial.
    - Elaboración de plan de adecuación.
- LOPD:
    - Elaboración de plan de adecuación para conseguir una plena implantación.
    - Actualización y adaptación de la información y documentos específicos necesarios a raíz del RGPD y, en su caso, a la norma estatal de transposición, de los documentos que a continuación se indican (incluidos formularios) a través de los cuales el ECIT ha establecido directrices a seguir en el tratamiento de datos de carácter personal y confección de cualesquiera otros documentos que la empresa proponga elaborar de cara a informar, asesorar y sensibilizar a los usuarios del Cabildo que tratan DCP:
        - **Información y consentimiento**: adaptación del Manual de Buenas Prácticas para los usuarios con acceso a datos de carácter personal (automatizado y no automatizado) con

sus respectivas cláusulas y formularios, en donde se contemple los cambios operados a nivel de categorías de datos (según el RGPD "categorías especiales de datos"), en el deber de información, en el consentimiento, en las transferencias internacionales de datos, bases de legitimación para el tratamiento de datos, cesiones de datos o encargos de tratamientos, principios inspiradores de la protección de datos etc.

- **Derechos de los interesados**: adaptación a las nuevas exigencias del RGPD del actual Protocolo para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición incorporando los nuevos derechos: derecho al olvido, derecho a la limitación del tratamiento y derecho a la potabilidad.
- Así mismo entra en el alcance del contrato la actualización y /o confección de los formularios pertinentes.
- **Encargos de tratamientos y cesión de datos**: adecuación de las cláusulas de encargo de tratamiento que se recojan en los contratos, de forma que se reflejen los nuevos contenidos adicionales: el objeto y la duración del encargo; la naturaleza del tratamiento; el tipo de datos personales; las categorías de interesados; las obligaciones y los derechos del responsable; la previsión de que las personas que deberán tratar los datos se han comprometido a mantener la confidencialidad; la asistencia del encargado al responsable para que pueda atender las solicitudes de ejercicio de derechos; la supresión o la devolución de los datos al finalizar el encargo; la obligación de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones del encargado del tratamiento y para permitir y contribuir a la realización de auditorías e inspecciones por parte del responsable o de otro auditor autorizado por el responsable. A tal efecto se tendrán en cuenta la Directrices dadas por la AEPD para la redacción de estos contratos. De igual manera se hará expresa mención a las nuevas obligaciones expresamente dirigidas a los encargados del tratamiento, tales como la obligación mantener un registro de actividades de tratamiento, o el deber de determinar las medidas de seguridad aplicables a los tratamientos que realizan o el de designar a un Delegado de Protección de Datos en los casos que prevé el RGPD.

- Adecuación web y redes sociales: adecuación LOPD-LSSI y RGPD para todos los servicios que se prestan vía electrónica por medio de la web, correo electrónico, SMS, Fax, etc.
- En consonancia con los nuevos principios de responsabilidad proactiva y enfoque de riesgos y de cara a que en los futuros tratamientos el impacto se analice en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información (protección de datos desde el diseño), se concretarán, de la forma más exhaustiva posible, de entre los tratamientos de DCP que realice el Cabildo, la relación de situaciones en las que sería aconsejable llevar a cabo una evaluación de impacto y se propondrá un modelo de EIPD específica adaptada a la realidad organizativa y estructural de Cabildo Insular de Tenerife. A tal efecto se tendrán en cuenta las listas indicativas de tratamientos que requieran una EIPD que elaboren las autoridades de protección de datos y los dictámenes y recomendaciones que al efecto elaboren las autoridades nacionales y europeas de protección de datos así como el Grupo de Trabajo del art. 29 de la Directiva 95/46/CE sobre protección de datos.
- Para la delimitación de la noción de alto riesgo a los efectos de la obligatoriedad de llevar a cabo una evaluación de impacto y la delimitación de aquellos tratamientos o situaciones en las que tratándose con DCP se entienda que no procede la realización de una EIPD, se elaborará una relación de tratamientos en que no se precisa evaluación de impacto y se detallará qué aspectos en materia de protección de datos deben ser tenidos en cuenta en la fase inicial de cualquier proyecto en los que se traten DCP. A tal efecto se tendrán en cuenta las listas indicativas de tratamientos que no requieran una EIPD que elaboren las autoridades de protección de datos y los dictámenes y recomendaciones que al efecto elaboren las autoridades nacionales y europeas de protección de

datos así como el Grupo de Trabajo del art. 29 mencionado. Como resultado de este trabajo la empresa hará entrega de un Documento "Análisis del cumplimiento normativo de las regulaciones de protección de datos" que permita en un futuro para los nuevos tratamientos de DCP que se realicen después de la entrada en vigor del RGPD garantizar la materialización del principio de protección de datos desde el diseño.

Entregables:

- Actualización de información en herramienta de gestión.
- Informes de adecuación:
    - Por cada Sistema de Información afectado:
        - El resultado del análisis efectuado.
        - Las insuficiencias que – en su caso – se observen con ocasión del análisis y propuesta de medidas correctoras.
        - Las recomendaciones que – en su caso – se efectúen.
        - La opinión o conclusiones de los consultores acerca del grado de cumplimiento de la normativa legal contrastada.
- Análisis del cumplimiento normativo de las regulaciones de protección de datos

P3 Auditoría ENS (Máx: 5 meses):

Objetivos:

- Cumplimiento artículo 34 y Anexo III del Real Decreto 951/2015, y por lo tanto, verificar el cumplimiento de los requisitos establecidos por el Real Decreto 951/2015 en los capítulos II y III y en los Anexos I y II con el objeto de auditar el cumplimiento del Esquema Nacional de Seguridad.
- Emitir una opinión independiente y objetiva, basada en los principios de la integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia, sobre este cumplimiento de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera.

Alcance:

- Auditoría de cumplimiento ENS, que deberá usar una metodología basada en:
    - Auditoría de verificación de cumplimiento del ENS según las pautas establecidas en las guías **CCN-STIC 802 (Esquema Nacional de Seguridad. Guía de auditoría) Y 808 (Verificación del cumplimiento de las medidas en el ENS)**, siguiendo el itinerario, y los puntos de registro establecidos, con el objetivo de encauzar de una forma homogénea la realización de la auditoría con las premisas mínimas ya establecidas para su ejecución.
    - La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del RD 3/2010.
    - Seguimiento de estándares de calidad para auditorías definidos en la ISO 19011.
- Se emitirá un pre-informe de Auditoría, identificando incumplimientos detectados y posibles acciones correctivas a corto, medio y largo plazo.
- Se ejecutará una fase de adecuación para las acciones a corto plazo.
- Se emitirá un informe de Auditoría con las acciones a medio-largo plazo.
- Actualización de Plan de acción con mejoras con más impacto.

Entregables:

- Preinforme e informe con el siguiente contenido (cumplimiento de las guías CCN-STIC 802 y 808):
  - El resultado del análisis efectuado.
  - Las no conformidades que – en su caso – se observen con ocasión del análisis y propuesta de medidas correctoras (con indicación de prioridades).
  - Las recomendaciones que – en su caso – se efectúen.
  - La opinión o conclusiones de los auditores acerca del grado de cumplimiento de la normativa legal contrastada.
- Resumen ejecutivo por Áreas con las acciones que les correspondan.
- Resumen ejecutivo global para la presentación del resumen de la auditoría.
- Ejecución de las tareas necesarias para generar y publicar (en sede electrónica) la Declaración y Certificación de Conformidad con el ENS y distintivos de cumplimiento según la **CCN-STIC 809** sobre **Declaración y Certificación de Conformidad con el ENS y distintivos de cumplimiento**.

P4 Auditoría perimetral (Máx: 2 meses)

Objetivos:

- Consultorías de análisis sobre los niveles de seguridad en la red perimetral incluyendo las tareas de auditoría bajo una metodología de caja negra.

Alcance:

- Identificar vulnerabilidades y los riesgos potenciales: con a menos las siguientes actividades principales:
  - Recopilación de información.
  - Escaneo y pruebas automatizadas.
  - Pruebas manuales.
- Proponer medidas correctivas y preventivas, así como recomendaciones adicionales.
- Auditoría de revisión de las vulnerabilidades indicadas.
- El ámbito de aplicación sería:
  - 4 Aplicativos WEB (como mínimo www.tenerife.es, sede.tenerife.es, y extranet.tenerife.es): con las siguientes pruebas específicas mínimas:
    - Listado de directorios (directory traversal) y acceso a ficheros (file disclosure)
    - Manipulación de parámetros de formularios (parameter tampering)
    - Acceso no autorizado a bases de datos y repositorios. (SQL Injection, Blind SQL Injection, XPath Injection)
    - Robo de sesiones de usuario (XSS, Cross-site tracing, Cross-site Request Forgery)
    - Ejecución de exploits conocidos.
    - Análisis de parámetros ocultos (hidden fields)
    - Acceso a herramientas de administración y utilidades.
    - Desbordamiento (overflow) de cabeceras.
    - Errores en la segregación de privilegios.
  - 20 direcciones IP dentro del rango público de direccionamiento del ECIT: con las siguientes pruebas específicas mínimas (caja negra):
    - Detección de arquitectura del sistema.
    - Ejecución de exploits conocidos.
    - Desbordamiento (overflow) en parámetros del protocolo.
    - Explotación de relaciones de confianza entre servidores.
    - Acceso no autorizado a entornos de administración.
    - Evasión de listas de control de acceso (ACLs).

- Implementación de ataques man-in-the-middle.
- Identificación y versiones de productos software instalados.
- Open Relay Testing
- Enumeración de usuarios
- Ejecución de exploits conocidos
- Usuarios y contraseñas por defecto

Entregables:

- Informe detallado de la auditoría.
- Informe ejecutivo con cuadro de mandos sobre la ejecución y resultados de la auditoría.

P5 Auditoría RGPD (Máx: 5 meses)

Objetivos:

- Auditoría obligatoria en protección de datos de carácter personal (de conformidad con los artículos 96 y 110 RDLOPD) y Auditoría aspectos jurídicos.

Alcance:

- Auditoría de cumplimiento de la LOPD, que deberá usar una metodología basada en:
  - Los criterios establecidos en el marco normativo LOPD-RDLOPD
  - Los estándares de calidad para auditorías definidos en la ISO 19011
- Se emitirá un pre-informe de Auditoría, identificando incumplimientos detectados y posibles acciones correctivas a corto, medio y largo plazo.
- Se ejecutará una fase de adecuación para las acciones a corto plazo.
- Se emitirá un informe de Auditoría con las acciones a medio-largo plazo.

Entregables:

- Preinforme e informe de auditoría con el siguiente contenido mínimo:
  - Resultado del análisis efectuado. Se incluirán indicadores de cumplimiento en base a estándares de la ISO/IEC 27001.
  - Deficiencias que, en su caso, fueren encontradas y propuesta de medidas correctoras o complementarias.
  - Recomendaciones que, en su caso, se pudieren efectuar.
  - Opinión o conclusiones de los auditores acerca del grado de cumplimiento de la normativa legal.
- Resumen ejecutivo por Áreas con las acciones que les correspondan.
- Resumen ejecutivo global para la presentación del resumen de la auditoría.

P6 Auditoría interna (Máx: 4 meses)

Objetivos:
● Conocer cuál es la situación exacta de los activos de información en cuanto a protección, control y medidas de seguridad implantadas en cada organización. ● Emplear técnicas de hacking ético.
Alcance:
● Realización de un test de intrusión desde la red interna, con distintos perfiles: como usuario autenticado y sin autenticación. ● Obtener las vulnerabilidades de los sistemas. ● Sobre cada uno de los activos que se determinen (como máximo dos servicios en cada auditoría del tipo DNS, LDAP, SMB, DHCP, Telefonía IP, etc), se realizarán controles de seguridad específicos, a todos los niveles, detectando posibles vulnerabilidades y riesgos, analizando la confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles, etc. Tareas mínimas: ○ Análisis de vulnerabilidades: Se trata de una toma de datos sobre las vulnerabilidades (propias, tecnológicas y no tecnológicas) de los activos implicados en el proyecto (Hardware, Software, Configuración que tienen o utilizan los servicios). ○ Test de intrusión: Adicionalmente, se realizará una explotación profunda de las vulnerabilidades existentes mediante pruebas manuales de “Hacking” o intrusión en los activos, obteniendo datos de mayor profundidad que los obtenidos en el análisis de vulnerabilidades. ● Realizar auditoría de código (una aplicación seleccionada por el ECIT en cada ejecución del proyecto de auditoría interna) y que deberá incluir la realización de las siguientes tareas: ○ Análisis inicial: con el objetivo de conocer y analizar cada aplicación y sus usos, así como los flujos de información presentes. ○ Revisión automática de código fuente. Mediante herramientas automatizadas se comprobará el código fuente en busca de patrones que identifiquen vulnerabilidades típicas: Cross-site Scripting (XSS), Inyecciones SQL, Inclusiones locales o remotas, ejecución de comandos, fugas de información. ○ Revisión manual de código fuente.
Entregables:
● Elaboración del informe de auditoría: Como resultado de las anteriores actividades el adjudicatario deberá elaborar un informe detallado acerca del estado actual de la seguridad interna detallando las vulnerabilidades y debilidades identificadas, incluyendo un listado de recomendaciones y soluciones, además de un plan de acción asociado para su corrección. ● Acciones prioritarias a ejecutar para solventar situaciones de seguridad graves en caso de detectarse (se deberán entregar a medida que se detecten dichas situaciones). ● El informe no deberá consistir únicamente en una mera extracción de los resultados de las herramientas utilizadas sino que debe ser de aplicabilidad a las aplicaciones/sistemas del ECIT.

En Santa Cruz de Tenerife, a 12 de diciembre de 2017.

Técnico Superior de Sistemas de Información

Natalia Bello Figueroa

El Jefe de Servicio

Clemente Barreto Pestana