



Área de Presidencia, Hacienda y Modernización  
Dirección Insular de Modernización

# Plan de Modernización Municipal 2021

---

<b>Introducción</b>	<b>1</b>
<b>Plan de Proyectos 2021</b>	<b>2</b>
<b>Fichas de proyectos</b>	<b>3</b>
<b>Términos y condiciones</b>	<b>21</b>
<b>Proyectos de planes anteriores</b>	<b>41</b>

## Introducción

En su condición de instituciones de las islas, como entes locales, los Cabildos Insulares tienen legalmente atribuida la asistencia a los municipios como competencia propia. Así resulta del artículo 36.1.b) de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, y de la Sección 2ª del Capítulo II del Título I de la Ley 8/2015, de 1 de abril, de Cabildos Insulares. El desarrollo efectivo por el Cabildo de Tenerife de esa competencia de asistencia a los municipios, es esencial para garantizar el ejercicio de la gestión pública municipal en la isla, constituyendo, asimismo, un instrumento vertebrador y equilibrador para que aquellos municipios que tienen una menor capacidad administrativa, puedan prestar a la ciudadanía unos servicios de calidad, que den respuesta a sus necesidades, y facilitar que el lugar donde se resida no sea un impedimento para el acceso a los mismos.

Por este motivo, el Cabildo de Tenerife se ha dotado de un reglamento específico que regula las condiciones y requisitos exigidos para los distintos tipos de asistencia a prestar a los municipios de la Isla de Tenerife, así como la forma de financiación que en cada caso corresponda.

En concreto, y en lo que se refiere a la prestación del servicio de asistencia técnica en materia de modernización administrativa, se establece la necesidad de la elaboración, participación y aprobación de un Plan de Proyectos con las actuaciones a realizar en cada anualidad.

En virtud de lo anterior, se emite el presente documento con la propuesta definitiva del Plan de Proyectos a ejecutar dentro del ejercicio 2021, una vez compartido su contenido con los municipios de la Isla a través del correspondiente proceso participativo.



---

## Plan de Proyectos 2021

De cara al inicio de la fase de solicitud de adhesión de los municipios, se indica a continuación la relación de los proyectos propuestos para ser ejecutados durante el ejercicio 2021 (**12 proyectos**):

- **Servicios cloud y conectividad desde el D-Alix**
  - **P21.1. Nube insular:**
    - **P21.1A. Piloto de virtualización de servidores y escritorios (PVI + VDI).**
    - **P21.1B. Mejoras portales web: soporte y accesibilidad.**
  - **P21.6. Red Insular:**
    - **P21.6A. Incorporación de la sede de los ayuntamientos a la red de fibra óptica.**
    - **P21.6B. Cesión de electrónica de red para conexión a la RTC-ALiX.**
- **Soporte a la administración electrónica municipal**
  - **P21.2. Apoyo para la implantación, evolución y/o mantenimiento de soluciones tecnológicas de la administración electrónica.**
- **Soporte a los procedimientos y backoffice municipal**
  - **P21.3. Seguridad y protección de datos**
    - **P21.3A. Apoyo y adecuación al ENS y al RGPD.**
    - **P21.3B. Marco de gobernanza insular de seguridad de la información**
  - **P21.4. Apoyo en modernización:**
    - **21.4A. Estudio unificación modelo y herramientas de gestión de personal y nóminas.**
    - **P21.4B. Análisis de situación en administración electrónica y estudio sobre archivo electrónico.**
- **Formación**
  - **P21.5. Formación.**
- **Fomento de la Sociedad de la Información**
  - **P21.7. Soporte básico al Servicio RICID.**
  - **P21.8. Impulso a la Ciudadanía Digital.**

Considerando que el presupuesto total estimado para la ejecución de estos proyectos es de **931.836,45 €** (impuestos incluidos), y que el presupuesto reservado para la anualidad 2021 de los proyectos aprobados en planes anteriores es de **350.000,00 €** (impuestos incluidos), el presupuesto total asociado de los proyectos a ejecutar en el ejercicio 2021 será de **1.281.836,45 €** (impuestos incluidos).



## Fichas de proyectos

<b><u>Servicios cloud y conectividad desde el D-Alix</u></b>
PROYECTO: <ul style="list-style-type: none"><li>● <b>P21.1. Alojamiento de infraestructuras y/o servicios municipales.</b><ul style="list-style-type: none"><li>○ <b>P21.1A. Piloto de virtualización de servidores y escritorios (PVI + VDI).</b></li></ul></li></ul>
FORMA DE EJECUCIÓN: Ejecución por el Cabildo.
OBJETO: Este proyecto tiene los siguientes objetivos: <ul style="list-style-type: none"><li>● Abstractar a los técnicos municipales de las tecnologías de la información y las comunicaciones (TIC) de la complejidad de la gestión de los dispositivos físicos, permitiéndoles centrarse en el despliegue de aplicaciones y servicios sobre una infraestructura de virtualización (IaaS).</li><li>● Mejorar las condiciones de seguridad física y lógica de las infraestructuras TIC.</li><li>● Reducir el coste total de operación de los sistemas informáticos insulares.</li></ul> <p>El alcance de este proyecto es la realización de un piloto con un subconjunto de los ayuntamientos de prioridad 1, lo que incluye la contratación y gestión de:</p> <ul style="list-style-type: none"><li>- Suministros de licencias y equipamiento necesario (100 puestos VDI / 10 servidores virtuales).</li><li>- Servicios de implantación, apoyo a la migración y soporte inicial.</li></ul> <p>El objetivo del piloto es realizar una implantación inicial que permita madurar y definir el modelo para su extensión de forma eficiente y progresiva al resto de municipios.</p>
VALOR ESTIMADO: 185.000 € (impuestos incluidos)
ANUALIDADES: - 2021: 185.000 €
PLAZO DE EJECUCIÓN: 1 AÑO (Año natural 2021)
DESTINATARIOS: Ayuntamientos de prioridad 1.  Se empezará a dar servicio a los ayuntamientos, en el orden de menor a mayor población, incorporando los que sea posible en función de los recursos disponibles.
COMPROMISOS: <u>Cabildo de Tenerife:</u> <ul style="list-style-type: none"><li>- Asumir el coste asociado al proyecto.</li><li>- Coordinar, gestionar y realizar la ejecución y seguimiento del proyecto.</li></ul>



- Cumplir las condiciones contenidas en el subapartado correspondiente a este proyecto, dentro del apartado “Términos y Condiciones” del presente documento.
- El Cabildo de Tenerife aporta:
  - o Espacio físico en el CPD D-Alix con todo lo que comporta: armarios, suministro eléctrico, climatización, seguridad física y lógica, etc.
  - o Recursos físicos de procesamiento y almacenamiento.
  - o Servicios de soporte para la implantación.

#### Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.
- Cumplir las condiciones contenidas en el subapartado correspondiente a este proyecto, dentro del apartado “Términos y Condiciones” del presente documento.
- Aceptar las pautas de mejora de seguridad y rendimiento indicadas por el Cabildo.
- Gestionar los recursos informáticos del ayuntamiento desplegados en la plataforma.
- Se compromete a recibir (asegurar disponibilidad) la formación necesaria para sus técnicos.
- Aceptar los protocolos de coordinación y actuación que se establezcan en el proyecto.

#### INDICADORES:

- FDCAN:
  - o General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 5.**
  - o Propios:
    - Inversión realizada en infraestructuras: **Objetivo: 185.000 €.**

### Servicios cloud y conectividad desde el D-Alix

#### PROYECTO:

- **P21.1. Alojamiento de infraestructuras y/o servicios municipales.**
  - o **P21.1B. Mejoras portales web: soporte y accesibilidad.**

#### FORMA DE EJECUCIÓN:

Ejecución por el Cabildo

#### OBJETO:

Mejoras en soporte y accesibilidad de los portales web municipales:

- Soporte: asegurar las actualizaciones de seguridad de los portales ya alojados en el Cabildo, así como abordar la migración de nuevos portales.
- Análisis y mejora de la Accesibilidad: análisis y ejecución de acciones para el cumplimiento del RD 1112/2018 en los portales web municipales.



VALOR ESTIMADO: 80.000 €

ANUALIDADES:

- 2021: 80.000€

PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1.

Se priorizará el servicio sobre los portales ya alojados en el Cabildo, incorporando los portales de otros ayuntamientos, en el orden de menor a mayor población, y en el número que sea posible en función de los recursos disponibles.

COMPROMISOS:

Cabildo de Tenerife:

- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar la ejecución y seguimiento del proyecto.

Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.
- Aceptar las pautas de mejora de seguridad y rendimiento indicadas por el Cabildo.

INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 10.**
  - Propios:
    - Inversión realizada en infraestructuras: **Objetivo: 80.000 €.**

### [Soporte a la administración electrónica municipal](#)

PROYECTO:

- **P21.2. Apoyo para la implantación, evolución y/o mantenimiento de soluciones tecnológicas de la administración electrónica.**

FORMA DE EJECUCIÓN:

Ejecución por los Ayuntamientos.

OBJETO:



El objetivo es proporcionar un apoyo para implantar, evolucionar, mantener, configurar y adaptar a las especificidades técnicas y funcionales de cada ayuntamiento, las herramientas tecnológicas que permitan la mejora de la Administración Electrónica municipal.

Se encuentran dentro del ámbito de este proyecto las siguientes actuaciones: implantación de nuevas herramientas, módulos, etc, evolución y mejora de las herramientas existentes, mantenimiento de licencias, soporte técnico, y/o servicios de consultoría para mejorar el uso y eficiencia de las soluciones tecnológicas.

VALOR ESTIMADO: 375.000 €

IMPORTE MÁXIMO DE LA APORTACIÓN:

El coste del proyecto dependerá de la dimensión del ayuntamiento:

-Ayuntamientos prioridad 1: 15.000 euros/año

-Ayuntamientos prioridad 2: 20.000 euros/año

TOTAL ESTIMADO: 375.000 € (impuestos incluidos)

ANUALIDADES:

- 2021: 375.000 €

PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1 y 2.

COMPROMISOS:

Cabildo de Tenerife:

- Asumir el coste asociado al proyecto, a través de la aportación económica correspondiente.

Ayuntamiento:

- Coordinar, gestionar y realizar la adjudicación y seguimiento de los trabajos asociados.
- Cumplir los plazos establecidos en el proyecto que le afecten directamente.
- Entrega de documentación de interés del proyecto para su difusión al resto de ayuntamientos.
- Una vez finalizado el proyecto, entrega de:
  - **Memoria de fin de proyecto ejecutado** (según **ANEXO III - Plantilla Memoria\_FinProyecto**).
  - Justificar la aportación económica (según **ANEXO II - Plantilla Certificado\_FinProyecto**) en un plazo de 3 meses una vez finalizado el proyecto.

INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 23.**
  - Propios:
    - Inversión realizada en infraestructuras: **Objetivo: 375.000 €.**



## Soporte a los procedimientos y backoffice municipal

### PROYECTO:

- **P21.3A. Apoyo y adecuación al ENS y al RGPD**

### FORMA DE EJECUCIÓN:

Ejecución por el Cabildo.

### OBJETO:

El objeto del proyecto propuesto es:

- Continuidad de la prestación de los servicios asociados al perfil de Delegado de Protección de Datos (DPO), de naturaleza tanto técnica como jurídica, necesarios para mejorar la adecuación y cumplimiento de la normativa asociada a la Protección de Datos de Carácter Personal.
- Incorporar el soporte a dudas, formación y ejecución de las primeras acciones necesarias para mejorar la adecuación al Esquema Nacional de Seguridad (ENS), es decir, la elaboración y aprobación de la Política de Seguridad, la definición de la Organización asociada, y la categorización de los sistemas de información municipales.

VALOR ESTIMADO: 15.735 €

### ANUALIDADES:

- 2021: 15.735 €

### PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1 y 2.

### COMPROMISOS:

#### Cabildo de Tenerife:

- Facilitar los recursos necesarios para la prestación de los servicios necesarios para el cumplimiento de los objetivos propuestos.
- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar el seguimiento del proyecto.

#### Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.

**INDICADORES:**

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 23.**
  - Propios:
    - Inversión realizada en la mejora de la capacitación: **Objetivo: 15.735 €.**

**Soporte a los procedimientos y backoffice municipal****PROYECTO:**

- **P21.3B. Marco de gobernanza insular de seguridad de la información**

**FORMA DE EJECUCIÓN:**

Ejecución por el Cabildo.

**OBJETO:**

Establecer un marco conjunto de gobernanza de la seguridad de la información a nivel insular que permita una adecuación lo más eficiente y eficaz posible con el Esquema Nacional de Seguridad y el resto de normativas aplicables en la materia.

Este marco se ha diseñado bajo los siguientes criterios:

- **Conjunto:** organización y documentación común con aplicación sobre todos los ayuntamientos: planes de adecuación, política de seguridad, normativas, procedimientos, medidas, instrucciones, etc.
- **Asistido:** con el soporte del Cabildo, designando incluso roles centralizados en el Cabildo para el apoyo a los ayuntamientos con menos recursos (ampliando al ENS la estrategia que ya está en marcha en el ámbito del RGPD, en el que ya existe la figura centralizada del DPO).
- **Insular:** se dirige principalmente a los ayuntamientos con menos recursos, ofreciéndoles una asistencia más extensa, sin embargo, también es posible la incorporación del resto de municipios, aunque con un apoyo más limitado.
- **Horizontal:** se contempla en el modelo tanto la adecuación normativa de los servicios comunes, que el Cabildo pueda poner a disposición de los ayuntamientos, como los servicios propios/específicos de cada ayuntamiento.
- **Integral:** incorpora todos los niveles de gestión de la seguridad necesarios: Gobierno (dirección y estrategia), Ejecutivo y supervisión (aprobación) y Operación, a través de la creación y apoyo en los órganos, grupos de trabajo y roles necesarios.

Las actividades principales previstas dentro de este proyecto son:

- Creación y/o nombramiento de Órganos, grupos y roles comunes:
  - Con soporte principal del Cabildo y con mayor apoyo para los ayuntamientos más pequeños.
  - Supone la delegación en estas figuras centralizadas de funciones sobre los ayuntamientos.
  - Se persigue reducir la necesidad de figuras en los Aytos a las mínimas necesarias.
- Desarrollo y uso de elementos comunes/reutilizables.





- Creación de documentación común o al menos reutilizable por cualquier ayuntamiento.
- Uso de herramientas y soluciones informáticas como soporte a la gestión de la adecuación, conformidad y seguimiento del estado de seguridad.
- Soporte a todo el ciclo de vida, es decir a la adecuación, y además:
  - Acreditación: certificación ENS.
  - Protección (vSOC): a través de servicios de seguridad comunes (de momento con apoyo sobre los ayuntamientos más pequeños).

VALOR ESTIMADO: 30.000 €

ANUALIDADES:

- 2021: 15.000 €
- 2022: 15.000 €

PLAZO DE EJECUCIÓN:

2 AÑOS (Año natural 2021 y 2022)

DESTINATARIOS: Todos los ayuntamientos.

COMPROMISOS:

Cabildo de Tenerife:

- Designar los roles y crear los órganos y/o grupos de trabajo necesarios.
- Dedicar los recursos necesarios para el funcionamiento del marco.
- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar el seguimiento del proyecto.

Ayuntamiento:

- En la aprobación de la solicitud de adhesión al proyecto:
  - Aceptar el cumplimiento de las condiciones contenidas en el subapartado correspondiente a este proyecto, dentro del apartado "Términos y Condiciones" del presente documento.
  - Designar e identificar los roles necesarios en cada ayuntamiento, de acuerdo a su dimensión. Remitir la información al Cabildo.
    - En todos los ayuntamientos:
      - Responsable de Información/Servicios/Tratamiento
      - Responsable de Sistemas del ayuntamiento.
    - Solamente en ayuntamientos de más de 20.000 habitantes:
      - Responsable de Seguridad del ayuntamiento.
- Asegurar la disponibilidad del personal designado para las funciones encomendadas.
- Seguimiento y ejecución de las funciones encomendadas.

INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 17.**



## Soporte a los procedimientos y backoffice municipal

### PROYECTO:

- **P21.4. Apoyo en modernización:**
  - **P21.4A. Estudio unificación modelo y herramientas de gestión de personal y nóminas.**

### FORMA DE EJECUCIÓN:

Ejecución por el Cabildo.

### OBJETO:

Se pretende analizar el modelo y las herramientas en uso para la gestión del personal y nóminas en los ayuntamientos, con el objetivo de determinar la viabilidad y acciones necesarias para la implantación de un modelo/herramienta común a nivel insular, lo que incluye entre otras actividades lo siguiente:

- Creación de un grupo de trabajo con los técnicos municipales.
- Formación a perfiles clave de los ayuntamientos.
- Análisis de la situación y modelo deseado.
- Plan de acciones.

VALOR ESTIMADO: 25.000€

### ANUALIDADES:

- 2021: 25.000€

### PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1

### COMPROMISOS:

#### Cabildo de Tenerife:

- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar la ejecución y seguimiento del proyecto.

#### Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.
- Entrega de documentación de interés del proyecto para su difusión al resto de ayuntamientos.

### INDICADORES:

- FDCAN:



- General
  - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 17.**
- Propios:
  - Inversión realizada en la mejora de la capacitación: **Objetivo: 25.000 €.**

### Soporte a los procedimientos y backoffice municipal

#### PROYECTO:

- **P21.4. Apoyo en modernización:**
  - **P21.4B. Análisis de situación en administración electrónica y estudio sobre archivo electrónico.**

#### FORMA DE EJECUCIÓN:

Ejecución por el Cabildo

#### OBJETO:

Se pretende analizar la situación de los ayuntamientos con respecto a la administración electrónica, prestando especial atención a la situación del archivo electrónico, con el objetivo de determinar la viabilidad y acciones necesarias para la implantación de un modelo/herramienta común a nivel insular, lo que incluye entre otras actividades lo siguiente:

- Creación de un grupo de trabajo con los técnicos municipales.
- Formación a perfiles clave de los ayuntamientos.
- Análisis de la situación y modelo deseado.
- Plan de acciones.

VALOR ESTIMADO: 30.000 €

#### ANUALIDADES:

- 2021: 30.000 €

#### PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1

#### COMPROMISOS:

##### Cabildo de Tenerife:

- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar la ejecución y seguimiento del proyecto.



#### Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.
- Entrega de documentación de interés del proyecto para su difusión al resto de ayuntamientos.

#### INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 17.**
  - Propios:
    - Inversión realizada en la mejora de la capacitación: **Objetivo: 30.000 €.**

#### Formación

##### PROYECTO:

- **P21.5. Formación y divulgación**

##### FORMA DE EJECUCIÓN:

1. Ejecución por el Cabildo.
2. Ejecución por el Cabildo, a través de una subvención a la Asociación Redeltic.

##### OBJETO:

1. Organizar, gestionar y llevar a cabo acciones formativas dirigidas a todo el personal de los ayuntamientos con el objetivo de mejorar la gestión administrativa y la prestación de servicios a la ciudadanía. Se plantean los siguientes contenidos en base a las necesidades obtenidas y derivadas de las propias reuniones con los ayuntamientos: dirigida a todo el personal municipal: Ciberseguridad, Ofimática (Office), Firma y documentos electrónicos, y dirigida a la dirección: modernización administrativa.
2. Subvención para cursos de formación organizados por la Red de Técnicos en Modernización y Tecnologías de la Información y las Comunicaciones de Entidades Locales de la isla de Tenerife (Redeltic).

Las acciones de formación se llevarán a cabo a través de la modalidad online o formación presencial, en función de las circunstancias marcadas por el COVID-19 y de los objetivos, destinatarios de las acciones concretas, presupuesto y disponibilidad.

El contenido específico final de las actividades de formación quedará definido en consenso con los ayuntamientos.

VALOR ESTIMADO: 15.000 €

##### ANUALIDADES:



1. 2021: 15.000 €, con el siguiente desglose.
  - a. 5.000 € (impuestos incluidos) ejecución directa por el Cabildo.
  - b. 10.000 € (impuestos incluidos) para una subvención nominativa a Redeltic.

PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1, 2 y 3.

COMPROMISOS:

Cabildo de Tenerife:

- Asumir la financiación de las acciones formativas.
- Coordinar, gestionar y apoyar la realización de la formación

Ayuntamiento:

- Designar y asegurar la disponibilidad del personal que estime más idóneo para recibir la formación organizada.

Redeltic:

- Coordinar, gestionar y realizar la formación.
- Justificar la actividad subvencionada en los términos que se establezcan.

INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 31.**
  - Propios:
    - Inversión realizada en la mejora de la capacitación: **Objetivo: 15.000 €.**

**Servicios cloud y conectividad desde el D-Alix**

PROYECTO:

- **P21.6. Mejoras de conectividad**
  - **P21.6A. Incorporación de la sede de los ayuntamientos a la red de fibra óptica.**

FORMA DE EJECUCIÓN:

Ejecución por los ayuntamientos

OBJETO:

Continuidad del proyecto 20.6, con el objetivo de adelantar la conexión por fibra óptica del Centro de Proceso de Datos (CPD)/Sala de servidores de cada Ayuntamiento con la arqueta más próxima de la



fase III del Anillo Insular de Telecomunicaciones de Tenerife (AITT), posibilitando así su conexión con la Red de Autoprestación del Cabildo Insular de Tenerife (RTC-ALiX), lo que permite:

- Adelantar temporalmente la conexión al AITT.
- Incrementar sustancialmente el caudal de la conexión de los Ayuntamientos con las infraestructuras del Cabildo (y la red SARA).
- Hacer viable el uso de servicios e infraestructuras alojadas en el Cabildo (como la PVI/VDI).

El proyecto consistiría en la ejecución por cada Ayuntamiento de su ramal de acceso o última milla (tramo de conexión entre su CPD y la arqueta del AITT), recibiendo por parte del Cabildo:

- La financiación parcial/total del coste de la ejecución del ramal.
- Una vez ejecutado el ramal, se procederá a la iluminación de la fibra óptica y a la activación y prestación del servicio de comunicaciones propio de la RTC-ALiX.

VALOR ESTIMADO: 100.000 €

#### IMPORTE MÁXIMO DE LA APORTACIÓN:

El proyecto dispone de un presupuesto total de 100.000 € (impuestos incluidos), que se repartirá entre los ayuntamientos que soliciten la adhesión al mismo, en función de los criterios de priorización definidos, y hasta atender todas las solicitudes o hasta agotar el crédito disponible.

Criterios para la determinación del orden de concesión (prelación):

- Las solicitudes recibirán financiación de acuerdo al criterio poblacional: primero los Ayuntamientos de prioridad 1 (los de menor dimensión), luego los de prioridad 2, y finalmente los de prioridad 3.
- También se tendrá en cuenta la viabilidad técnica de la conexión efectiva (extremo a extremo) de cada ayuntamiento al AITT, dentro del plazo previsto para el proyecto, promoviendo primero la financiación de los trabajos en aquellos ayuntamientos en los que solamente sea necesaria la ejecución de su ramal de acceso para hacer posible la conexión completa y efectiva con toda la RTC-ALiX.

El valor de la aportación a realizar a cada ayuntamiento se determinará a partir del reparto priorizado de los fondos disponibles, según los criterios de prelación indicados en el apartado anterior, así como a los costes indicados por cada Ayuntamiento para la ejecución de su ramal.

TOTAL ESTIMADO: 100.000 € (impuestos incluidos)

Se estima que con este presupuesto se podría abordar la ejecución de ramales de unos 12 ayuntamientos, considerando que el coste de la conexión actual de cada ayuntamiento es de unos 3.200 €/año, se estima que esta inversión se podría amortizar en un período inferior a 3 años.

#### ANUALIDADES:

- 2021: 100.000 €

#### PLAZO DE EJECUCIÓN:

1 AÑO (Año natural 2021)

DESTINATARIOS: Ayuntamientos de prioridad 1, 2 y 3

#### COMPROMISOS:



#### Cabildo de Tenerife:

- Realizar la financiación parcial de las solicitudes de proyecto aprobadas de acuerdo a las condiciones establecidas.
- Asumir la implantación y gestión del servicio de conexión con la red del Cabildo de Tenerife, a través de la Red de Autoprestación del Cabildo Insular de Tenerife (RTC-ALiX).

#### Ayuntamiento:

- Solicitar el proyecto adjuntando:
  - Para su valoración por el Cabildo, el **presupuesto** y la **memoria técnica**, elaborados por una empresa especializada, que incluirá el trazado del despliegue en formato KMZ, incluyendo fotos y descripción detallada del trazado (ver el epígrafe “Memoria técnica”, dentro del subapartado correspondiente a este proyecto, en el apartado “Términos y Condiciones” del presente documento).
  - El **plazo de adhesión** para este proyecto particular, dada la naturaleza particular de los trabajos a realizar, se establece en **30 días naturales**.
- Coordinar, gestionar y realizar la adjudicación de la contratación correspondiente y el seguimiento del proyecto, en coordinación con el Cabildo y bajo su supervisión cuando así lo requiera, y al menos en el replanteo inicial de la ejecución de los trabajos, y antes de la aceptación y entrega por el proveedor correspondiente al Ayuntamiento.
- Cumplir las condiciones establecidas por el Cabildo para la ejecución del ramal y el uso posterior de la red de autoprestación, contenidas en el subapartado correspondiente a este proyecto, dentro del apartado “Términos y Condiciones” del presente documento.
- Cumplir los plazos establecidos en el proyecto que le afecten directamente.
- Una vez finalizado el proyecto, entrega de:
  - **Memoria de fin de proyecto ejecutado** (según **ANEXO III - Plantilla Memoria\_FinProyecto**), y **memoria técnica** actualizada con cualquier cambio derivado de la propia ejecución del proyecto.
  - Justificar la aportación económica (según **ANEXO II - Plantilla Certificado\_FinProyecto**) en un plazo de 3 meses una vez finalizado el proyecto.

#### INDICADORES:

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 12.**
  - Propios:
    - Inversión realizada en infraestructuras: **Objetivo: 100.000 €.**

#### Servicios cloud y conectividad desde el D-Alix

#### PROYECTO:

- **P21.6. Mejoras de conectividad**
  - **P21.6B. Cesión de electrónica de red para conexión a la RTC-ALiX.**

#### FORMA DE EJECUCIÓN:



FONDO DE  
DESARROLLO  
DE CANARIAS



Ejecución por el Cabildo.

**OBJETO:**

Impulsar la conexión por fibra óptica del Centro de Proceso de Datos (CPD)/Sala de servidores de cada Ayuntamiento con la Red de Autoprestación del Cabildo Insular de Tenerife (RTC-ALiX) a través de:

- Compra y cesión de 2 equipos para cada ayuntamiento, con el objetivo de aprovechar la alta disponibilidad y el rendimiento de la conexión de la red del ayuntamiento con la RTC-ALiX (una vez ejecutado el ramal de acceso correspondiente), incluyendo su instalación básica en cada Ayuntamiento.

VALOR ESTIMADO: 30.000 €

**ANUALIDADES:**

- 2021: 30.000 €

**PLAZO DE EJECUCIÓN:**

1 AÑO (Año natural 2021)

**DESTINATARIOS:** Ayuntamientos de prioridad 1 y 2

Esta acción se priorizará sobre aquellos ayuntamientos que puedan tener cubiertos durante el 2021 el resto de aspectos necesarios para su conexión con la RTC-ALiX (por ejecución de sus ramales y finalización de los pendientes en el AITT por parte del Cabildo).

**COMPROMISOS:**

Cabildo de Tenerife:

- Asumir el coste asociado al proyecto.
- Coordinar, gestionar y realizar la ejecución y seguimiento del proyecto.

Ayuntamiento:

- Se nombrará un responsable/interlocutor del servicio por parte del Ayuntamiento.
- Conforme de las tareas que le correspondan.
- Seguimiento global del proyecto y comunicación interna en el ayuntamiento.
- Estudio y ejecución de las tareas que correspondan ejecutar al propio ayuntamiento.

**INDICADORES:**

- FDCAN:
  - General
    - Nº de Corporaciones Locales con implantación de servicios públicos digitales: **Objetivo: 15.**
  - Propios:
    - Inversión realizada en infraestructuras: **Objetivo: 30.000 €.**

**[Fomento de la Sociedad de la Información](#)**





**PROYECTO:**

- **P21.7. Soporte básico al Servicio RICID**

**FORMA DE EJECUCIÓN:**

Ejecución por el Cabildo

**OBJETO:**

El Cabildo de Tenerife ha venido gestionando durante los últimos años una red de Telecentros distribuida por toda la geografía insular, denominada la Red Insular de Centros de Inclusión Digital, RICID.

Cada uno de estos espacios está dotado de medios tecnológicos, opera con unos servicios de soporte y sirven para proporcionar determinados servicios orientados a facilitar a la población el proceso de integración en la Sociedad de la Información

El objeto del proyecto propuesto es la realización de un soporte mínimo a los centros con convenios RICID en vigor, mediante:

- Servicio de soporte y mantenimiento correctivo del equipamiento informático de los espacios asociados a RICID que incluye:
  - Soporte y mantenimiento correctivo del equipamiento TIC suministrado
  - Conectividad

**VALOR ESTIMADO:** 30.000 euros (impuestos incluidos)

**ANUALIDADES:**

- 2021: 30.000 euros

**PLAZO DE EJECUCIÓN:**

1 AÑOS

**DESTINATARIOS:** Ayuntamientos de prioridad 1, 2 y 3 (con convenio RICID en vigor)

**COMPROMISOS:**

Cabildo de Tenerife:

- Designar una persona "Responsable Insular" como responsable del Servicio, que actúe como canal de comunicación con la persona "Responsable Municipal" del Servicio.
- Asumir el coste asociado al mantenimiento correctivo del equipamiento informático software y hardware, a través de la aportación económica correspondiente, hasta el máximo de la aportación económica.
- Asumir el coste del Servicio de Atención a Usuarios para el mantenimiento remoto y presencial cuando resulte necesario y la gestión de incidencias, a través de la aportación económica correspondiente, hasta el máximo de la aportación económica.
- Asumir el coste asociado a la prestación de servicios de conectividad.



- Gestión de incidencias relacionadas con la conectividad de los espacios. (La conectividad de los centros se incluye en el contrato de Comunicaciones del Servicio Técnico de Informática y Comunicaciones).
- Suministro de equipamiento TIC a los nuevos municipios prioridad 1 adheridos al proyecto de impulso a la Ciudadanía Digital.

**Ayuntamiento:**

- Designar una persona “Responsable Municipal” como responsable de la operación del Servicio por parte del municipio, que actúe como canal de comunicación con el Cabildo.
- Garantizar los medios y condiciones de los espacios o locales para el funcionamiento correcto del equipamiento informático del Servicio, como locales con los metros cuadrados suficientes, el mobiliario o la instalación eléctrica adecuada a las necesidades de este equipamiento.
- Asumir el coste de los gastos corrientes, como suministro eléctrico, iluminación, limpieza del local o material fungible.
- Asumir el coste de los gastos para el aseguramiento del equipamiento informático ante riesgos ordinarios, y reemplazar los equipos en caso de hurto en no más de 60 días naturales.
- Designar una persona como “Responsable del Espacio” donde se ubica el equipamiento informático.
- Trasladar a la persona Responsable del espacio las políticas de uso del centro. En tanto no se desarrollen nuevas políticas se estará a lo recogido en el apartado 3 del Protocolo de Trabajo para la Gestión y Dinamización de los Telecentros del Cabildo de Tenerife.
- La persona responsable del espacio trasladará las normas de aplicación a los usuarios y velarán por su cumplimiento.

**INDICADORES:**

- FDCAN
  - Nº de equipos desplegados / Objetivo: 260
  - Nº de centros con fibra / Objetivo: 52

**Fomento de la Sociedad de la Información**

**PROYECTO:**

- **P21.8. Impulso a la Ciudadanía Digital**

**FORMA DE EJECUCIÓN:**

Ejecución por el Cabildo.

**OBJETO:**

El Cabildo de Tenerife ha venido gestionando durante los últimos años una red de Telecentros distribuida por toda la geografía insular, denominada la Red Insular de Centros de Inclusión Digital, RICID. Cada uno de estos espacios está dotado de medios tecnológicos, opera con unos servicios de soporte y sirven para proporcionar determinados servicios orientados a facilitar a la población el proceso de integración en la Sociedad de la Información.

El objeto del proyecto propuesto es reforzar la comunicación y dinamización de estos espacios para impulsar las competencias digitales de la ciudadanía en su vida cotidiana en un nuevo contexto social, educativo, de relación con las administraciones o en el ámbito laboral que se fundamenta cada vez más a través de medios digitales:

- Fortalecimiento de los servicios de dinamización y de asesoramiento adaptados a las nuevas necesidades de la ciudadanía para funcionar en un contexto digital, desde aspectos básicos de autoconfianza y autonomía en el uso de estos medios hasta el desarrollo de habilidades más complejas, como la configuración de dispositivos, la gestión de la ciberseguridad en diferentes medios, la tramitación de procesos de administración electrónica, la realización de transacciones de comercio o banca en línea o el fortalecimiento de competencias digitales para la empleabilidad.

**VALOR ESTIMADO:** 30.000 € (impuestos incluidos)

**ANUALIDADES:**

- 2021: 30.000 €

**PLAZO DE EJECUCIÓN:**

1 AÑO

**DESTINATARIOS:**

- 2021: Ayuntamientos prioridad 1, 2 y 3 (con convenio RICID en vigor)

**COMPROMISOS:****Cabildo de Tenerife:**

- Designar una persona "Responsable Insular" como responsable del Servicio, que actúe como canal de comunicación con la persona "Responsable Municipal" del Servicio.
- Proporcionar el Modelo de Gestión del Servicio.
- Asumir el coste asociado a la dinamización de los espacios RICID, a través de la aportación económica correspondiente, hasta el máximo de la aportación económica, y desde el momento de activación de esta capacidad.
- Apoyar, en su caso, a los "Dinamizadores Municipales" que, opcionalmente, algunos municipios directamente proporcionen con sus propios medios y costes.



- Asumir el coste del Servicio de Atención a Usuarios para el Servicio y la gestión de incidencias, a través de la aportación económica correspondiente, hasta el máximo de la aportación económica, y desde el momento de activación de esta capacidad.
- Asumir los costes de marca, sitio web y sistemas de información del Servicio, hasta el máximo de la aportación económica y desde el momento de activación de esta capacidad.
- Publicitar en la información del Servicio los datos asociados al municipio, como localizaciones, horarios, personas de contacto, agenda de actividades, etc., sujeto a la aportación económica disponible.

#### Ayuntamiento:

- Designar una persona “Responsable Municipal” como responsable de la operación del Servicio por parte del municipio, que actúe como canal de comunicación con la persona “Responsable Insular” del Servicio.
- Asumir el coste de los gastos del personal que el municipio adicionalmente pudiera aportar para la dinamización municipal, denominados “Dinamizadores Municipales”.
- Trasladar, en su caso, a la(s) persona(s) “Dinamizadora(s) Municipal(es)” las “Pautas de Operación” del Servicio y velar por su correcto seguimiento.
- Trasladar a las personas beneficiarias las pautas de uso del Servicio, recogidas en el Modelo de Gestión del Servicio, y velar por su correcto cumplimiento.
- Colaborar activamente con la entidad encargada de la operativa del Servicio, desde el momento de activación de esta entidad, para su mejora permanente.
- Seleccionar un único centro que se beneficie del presente proyecto ‘Impulso a la ciudadanía digital’. Este centro deberá estar entre los suscritos al proyecto de “Soporte Básico al Servicio RICID”.

#### INDICADORES:

- FDCAN
  - Nº de usuarios de los Centros de Inclusión Digital / Objetivo: 3.500 personas.
  - Nº de actuaciones de dinamización de los Centros de Inclusión Digital / Objetivo: 255 actuaciones.

## Términos y condiciones

### P21.1A. Piloto de virtualización de servidores y escritorios (PVI + VDI)

#### Acuerdo de servicio de servidores virtuales (PVI)

El Cabildo de Tenerife pondrá a disposición de los ayuntamientos una plataforma IaaS donde se podrá realizar el despliegue de servidores virtuales con el objetivo de liberar al personal técnico municipal de las complejidades asociadas a la infraestructuras necesarias.

Las responsabilidades del Cabildo y del ayuntamiento, representado por su Responsable Técnico, son las que se enumeran a continuación.

#### Cabildo de Tenerife



- Gestión del alta o modificación en el servicio.
- Evolución y mejora del servicio.
- Aprobar los recursos de cómputo, almacenamiento y/o conectividad (RAM, CPU, disco,...) solicitados por el **Responsable Técnico** del servidor.
- Mantenimiento de las comunicaciones y la infraestructura física (hardware) y lógica (software) de la plataforma IaaS.
- Soporte técnico y mantenimiento de la plataforma IaaS.
- Planificar tareas de reinicio a petición del Responsable Técnico del servidor virtual.

#### Seguridad

- Consensuar con el **Responsable Técnico** el **Plan de Copias** de las máquinas virtuales y/o almacenamiento.
- Planificar y revisar la correcta realización de estas copias de seguridad.
- Realizar la restauración de datos autorizados por el **Responsable Técnico**.

### **Responsable Técnico del Servidor virtual**

#### Sistema operativo

- Antivirus.
- Licencias y aplicar actualizaciones del sistema operativo.
- Realizar la administración local del servidor. Reinicio del servidor.

#### Aplicaciones

- Mantener actualización de software instalado
- No instalar software sin licencias. Las licencias que sean necesarias deberán ser suministradas por el ayuntamiento correspondiente.
- Soporte técnico a usuarios finales. Mantenimiento preventivo (operativas). Explotación.

#### Seguridad

- Realización de copias de seguridad dentro de las máquinas virtuales.
- Mantener la confidencialidad de las credenciales (cuentas de usuario, certificados,...)
- Mantener la seguridad del servidor
- 

#### Conectividad

- Gestionar la compra o mantenimiento de dominios DNS
- Consensuar con el Cabildo la publicación de aplicaciones o servicios TIC hacia Internet y la conectividad con los servicios municipales.

#### Observaciones

- El Cabildo no será responsable en ningún caso de los contenidos alojados en el servidor dedicado, ya sean los contenidos propiedad del ayuntamiento o propiedad de terceros
- En caso de problemas de seguridad originados en el servidor (p.e. virus) u otros problemas de funcionamiento que puedan afectar a otros servicios, el equipo se desconectará hasta que se solucione el incidente en cuestión, avisando lo antes posible al **Responsable Técnico** del servidor para que proceda a la solución del problema
- Canales:
  - o Consultas sobre alta/modificación/mejora de los servicios
    - Por correo electrónico: [tenerifelocal@tenerife.es](mailto:tenerifelocal@tenerife.es).
  - o Atención de incidencias y soporte técnico:
    - Por correo electrónico: [cau@tenerife.es](mailto:cau@tenerife.es).
    - Por teléfono: 922 239999.
    - Horario de servicio: Lunes a Viernes: 6.45 – 22.00 y Sábados: 9.00 – 15.00



---

## **Acuerdo de servicio de escritorios virtuales (VDI)**

Los términos y condiciones específicas de este servicio se determinarán durante su implantación.

### **Cláusulas de confidencialidad y protección de datos**

Como consecuencia de la prestación del presente servicio, el Cabildo puede acceder a datos de carácter personal que se encuentran bajo la responsabilidad, custodia y protección del Ayuntamiento (en adelante, el “Responsable del Tratamiento”); teniendo a estos efectos el Cabildo la condición legal de Encargado del Tratamiento con respecto a los mismos (en adelante, el “Encargado del Tratamiento”) y entendidos conjuntamente como las “Partes”.

En consecuencia y dando pleno cumplimiento a lo establecido en la normativa nacional y comunitaria que resulta de aplicación, las Partes desean recoger las condiciones del tratamiento de los datos por parte del Encargado del Tratamiento y, a tal efecto, suscriben las siguientes:

#### **Primera.- Tipología de datos personales y prestación del servicio.**

Como consecuencia de la prestación de los servicios de alojamiento y soporte técnico descritos en el presente Anexo, el Encargado del Tratamiento podrá acceder a los datos de carácter personal relativos a los ciudadanos del Responsable del Tratamiento.

Además, el Encargado del Tratamiento presta el Servicio de conexión a la red del Cabildo, infraestructuras y algunos servicios en Internet.

En concreto, los tipos de datos personales a los que el Encargado del Tratamiento podrá acceder son los correspondientes a los tratados por el Responsable de Tratamiento en los servicios alojados en las infraestructuras del Encargado del Tratamiento.

La naturaleza de los tratamientos que el Encargado del Tratamiento realizará por cuenta del Responsable será la recogida y almacenamiento de los datos de los interesados con la finalidad de alojar los servicios en las infraestructuras del Encargado y realizar el soporte técnico de los mismos.

#### **Segunda.- Deber de secreto**

Habida cuenta del carácter reservado de los datos, documentos e informaciones que obran en poder del Responsable del Tratamiento, en caso de que éstos pudieran ser conocidos por el Encargado del Tratamiento en virtud de la prestación del presente servicio, el Encargado del Tratamiento se compromete a que permanezcan en secreto.

Esta obligación de guardar secreto permanecerá incluso hasta después de cesar en su relación con el Responsable del Tratamiento, cualquiera que fuera la causa.

A estos efectos, el Encargado del Tratamiento se compromete a tomar, respecto de sus empleados, las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como Encargado del Tratamiento y que, en consecuencia, deben respetar.

#### **Tercera.- Instrucciones del Responsable del Tratamiento**

El Encargado del Tratamiento se compromete a tratar los datos personales a los que tenga acceso únicamente conforme a las instrucciones documentadas que, a tal efecto, le indique el Responsable



---

del Tratamiento. Este compromiso se extenderá asimismo con respecto a las Transferencias Internacionales de Datos de carácter personal a un tercer país o una Organización internacional.

En consecuencia, los datos que se conozcan u obtengan en virtud de la prestación del servicio, no podrán ser utilizados para ninguna otra finalidad distinta de la ejecución del mismo, tendrán carácter confidencial y no serán publicados o puestos en conocimiento de terceras partes sin la autorización previa y por escrito del Responsable del Tratamiento salvo en los casos expresamente autorizados por la Ley.

En este sentido, el Encargado del Tratamiento se compromete a informar inmediatamente al Responsable del Tratamiento en el caso en que una instrucción dirigida por este pudiera infringir las disposiciones que resultasen aplicables en materia de protección de datos recogidas en el ordenamiento comunitario o de los Estados miembros.

#### **Cuarta.- Subcontratación del objeto del Encargo**

El Cabildo podrá recurrir a subcontratistas para llevar a cabo determinadas actividades de tratamiento de datos personales por cuenta del Ayuntamiento (sub-encargado). Por medio de la presente el Ayuntamiento autoriza a los mismos. La documentación acreditativa sobre el cumplimiento de las garantías exigidas en materia de protección de datos por parte de dichas entidades se encuentra reflejado en los correspondientes contratos. El Ayuntamiento puede consultar y oponerse en cualquier momento al tratamiento por realizado por alguno de los sub-encargados.

El Cabildo impondrá por escrito al sub-encargado las mismas obligaciones de protección recogidas en la presente cláusula. Dichas obligaciones serán igualmente extensibles para el Cabildo en el supuesto de que el sub-encargado utilice otros terceros y en el caso de existir una cadena de subcontratistas, de tal modo que el Cabildo y cualquiera de los subcontratistas hasta llegar al último de la cadena queden sujetos a las mismas obligaciones.

El Cabildo será plenamente responsable ante el Ayuntamiento, y responderá del efectivo cumplimiento de las obligaciones en materia de protección de datos de los posibles subcontratistas que interviniesen en el tratamiento de los datos personales, ya sean designados directamente por el Cabildo o, bien, indirectamente a través de una cadena de subcontratación.

#### **Quinta.- Registro de actividades de tratamiento**

El Encargado del Tratamiento llevará un registro por escrito y en formato electrónico de todas las categorías de actividades de tratamiento efectuadas conforme al artículo 30 del Reglamento General de Protección de Datos.

#### **Sexta.- Medidas de seguridad**

El Encargado del Tratamiento se compromete a cumplir las medidas de seguridad, de carácter organizativo, técnico, físico y administrativo, que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo que pudiera derivarse del tratamiento, garantizar la seguridad, integridad, disponibilidad de los datos de carácter personal y evitar su alteración, pérdida, destrucción accidental o ilícita, tratamiento, revelación o acceso no autorizado en todo momento, habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza de los datos almacenados, el alcance del tratamiento, así como los riesgos a que estén expuestos y el impacto que esto pudiera tener sobre los derechos y libertades de las personas físicas, ya provengan de la acción humana o del medio físico o natural, dando así cumplimiento a lo exigido por la normativa vigente. Asimismo, el Encargado deberá implantar aquellos mecanismos para restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.



Asimismo, el Encargado del Tratamiento estará obligado a cumplir con sus deberes respecto a la realización de cualesquiera evaluaciones de impacto en materia de protección de datos (Data Protection Impact Assessment) que estuviera obligado a llevar a cabo y siempre que el Responsable del Tratamiento se lo requiera.

De acuerdo con la evaluación de riesgos realizada por el Responsable del Tratamiento y lo establecido en el artículo 28 del GDPR, el Encargado del Tratamiento adoptará como mínimo las siguientes medidas de seguridad técnicas y organizativas:

- Nombramiento de un responsable en materia de protección de datos, quien deberá asegurar el continuo cumplimiento de la normativa aplicable, que podrá tener la consideración de Delegado de Protección de Datos (DPO) en caso que sea necesario.
- Establecimiento de funciones y responsabilidades del personal que trate datos de carácter personal.
- Comunicación entre el personal de las funciones y responsabilidades definidas asociadas al cumplimiento de la normativa en materia de protección de datos.
- Definición de roles y perfiles para los usuarios de las aplicaciones y sistemas donde se traten dichos datos de acuerdo a las funciones y responsabilidades establecidas, de forma que se evite el acceso a datos o recursos distintos de los autorizados. Este sistema de control de acceso deberá garantizar adecuados mecanismos de identificación y autenticación de los usuarios, como por ejemplo a través del uso de contraseñas que han de ser renovadas de forma periódica, uso de datos biométricos, bloqueo automático de usuario ante intentos sucesivos fallidos de acceso, etc.
- Medidas automatizadas que limiten el acceso a la información para usuarios no autorizados o fuera del plazo de conservación determinado, como por ejemplo mediante técnicas de borrado o de seudonimización de datos.
- Procedimientos que limiten el acceso físico a las instalaciones donde se encuentren ubicados los sistemas de información o los soportes físicos.
- Registros de control y acceso sobre soportes que contengan datos de carácter personal, que además deberán contar con mecanismos de acceso limitado (p.e. cintas de backup, USBs, dossieres, CDs, etc.).
- Procedimientos de recuperación de datos de carácter personal ante su posible destrucción, pérdida o alteración, bajo la supervisión y aprobación del responsable en materia de protección de datos.
- Procedimientos de detección, evaluación y notificación, en caso de ser necesario, de incidentes de seguridad que puedan afectar a los derechos y libertades de los interesados.
- Ejecución de revisiones periódicas de cumplimiento y de definición y ejecución de los planes de acción para la mitigación de los riesgos detectados.

El Encargado del Tratamiento realizará su evaluación de riesgos, de cuyo resultado se podrá derivar la necesidad de adoptar otras medidas de seguridad técnicas y organizativas adicionales a las indicadas con anterioridad.

#### **Séptima.- Notificación de brechas de seguridad**

El Encargado del Tratamiento se compromete a notificar al Ayuntamiento en su calidad de Responsable del Tratamiento, de forma inmediata cualquier incidente de seguridad de los datos personales, en cualquier caso antes del plazo máximo de 48 horas, de conformidad con la naturaleza de los datos tratados, los riesgos asociados a la pérdida, destrucción o alteración de dichos datos de carácter personal y la información de que disponga el Encargado del Tratamiento a fin de que el





---

Responsable tome las decisiones oportunas con respecto al incidente de seguridad producido, las cuales serán trasladadas al Encargado del Tratamiento.

En dicha notificación, si fuera posible, el Encargado del Tratamiento informará de lo descrito a continuación:

- De la naturaleza de la violación de la seguridad de los datos, así como, si fuera posible, las categorías y el número aproximado de los interesados afectados, y las categorías y el número aproximado de registros de datos personales afectado.
- El nivel de riesgo estimado para los derechos y libertades de las personas físicas.
- De los datos de contacto de la persona que puede facilitar más información sobre el incidente de seguridad.
- De las posibles consecuencias del mismo.
- De las medidas adoptadas o propuestas para remediar la brecha de la seguridad y/o para mitigar los posibles efectos negativos.

Si en un primer momento el Encargado del Tratamiento no fuera capaz de informar de todas las cuestiones indicadas con anterioridad, las comunicará tan pronto tenga conocimiento de las mismas.

#### **Octava.- Derechos de los Interesados**

En relación a las personas físicas cuyos datos constan en la prestación del servicio (en adelante, “Firmantes”) así como los correos que intercambien en relación a la prestación de servicio, serán tratados en base al interés legítimo de las partes, con la finalidad de gestionar el mantenimiento, cumplimiento, desarrollo, control y ejecución de la prestación del servicio.

Tales datos se conservarán mientras que se mantenga en vigor la prestación del servicio entre las partes y, posteriormente, se conservarán bloqueados hasta un plazo máximo de 5 años en virtud de lo dispuesto en la legislación vigente.

Los firmantes podrán ejercitar sus derechos de acceso, rectificación, cancelación, en aquellos supuestos en que sea posible, y oposición, mediante un escrito dirigido a las direcciones que constan en el apartado postal situado al encabezamiento de este documento, adjuntando una copia de un documento acreditativo de su identidad. En su caso, el interesado también podrá plantear una reclamación ante la Agencia Española de Protección de Datos.

#### **Novena.- Devolución o destrucción de los datos**

Una vez cumplida la prestación del servicio por cualquier otra causa y a elección del Responsable del Tratamiento, el Encargado del Tratamiento se compromete a devolver y/o destruir en los plazos y formas que el Responsable del Tratamiento le indique todos los datos personales a los que tenga acceso para la prestación del servicio, al igual que cualquier soporte o documento en el que consten y se obliga a no tratar, bajo ninguna forma o concepto, dichos datos personales; obligándose también a mantener indemne al Responsable del Tratamiento por cualquier violación a la obligación contenida dentro de la presente cláusula.

En caso de que, transcurrido un plazo de 30 días naturales a contar desde la finalización del Convenio por cualquier causa, sin que el Cabildo haya recibido instrucciones al respecto, el Cabildo procederá a la destrucción de los datos y presentará en el plazo de una semana máximo certificado de dicha destrucción.

#### **Décima.- Deber de diligencia**



El Encargado del Tratamiento se compromete a facilitar al Responsable del Tratamiento toda aquella información que resulte necesaria para demostrar el cumplimiento de sus obligaciones, y, en su caso, informará al Responsable del Tratamiento en relación con su adhesión a un código de conducta aprobado, o su adscripción a cualquier mecanismo de certificación que pueda garantizar el cumplimiento de sus obligaciones en relación con el tratamiento de datos de carácter personal. En caso de que el Encargado del Tratamiento esté adscrito a un código de conducta o mecanismo de certificación, el Responsable del Tratamiento podrá requerirle en cualquier momento de la vigencia del Convenio para que lo justifique documentalmente.

En el caso de que el Responsable del Tratamiento así lo solicitara, el Encargado del Tratamiento permitirá la realización auditorías e inspecciones en relación con el tratamiento efectuado por éste, bien por parte del Responsable del Tratamiento o de otro auditor autorizado por el Responsable del Tratamiento.

El Encargado del Tratamiento facilitará el apoyo que, en su caso, le pudiera solicitar el Responsable del Tratamiento en la realización de los análisis de impacto y en las consultas previas que se pudieran realizar a la Agencia.

#### **DecimoTercera.- Obligaciones del Responsable del Tratamiento.**

Corresponden al Ayuntamiento las siguientes obligaciones:

- Entregar al Cabildo los datos objeto de tratamiento de conformidad con lo establecido en el presente convenio.
- Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el Cabildo, en el caso de que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas.
- Realizar las consultas previas que corresponda.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del Cabildo.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

#### **DecimoCuarta.- Confidencialidad de la información.**

En el marco de la prestación de los servicios indicados en el presente Anexo, las partes podrán revelarse determinada información relativa a sus actividades así como de desarrollo y materiales siempre que todo ello sea necesario para la prestación del servicio. Las partes acuerdan que la información que se revelen mutuamente (salvo que sean de dominio público, que ya se conociera por otra parte o que revele a un tercero por requerimiento legal con obligación de ser atendido) tendrá la consideración de confidencial por lo que se comprometen a guardar el más absoluto secreto sobre la información de la otra parte a que tengan acceso.

Los deberes de confidencialidad derivados de la prestación del servicio, permanecerán durante su periodo de vigencia y subsistirán con posterioridad a la extinción del mismo, por tres años. Asimismo, ambas partes se comprometen a devolverse o destruir la información confidencial en el momento de extinción del servicio sin que sea necesario requerimiento previo para ello.

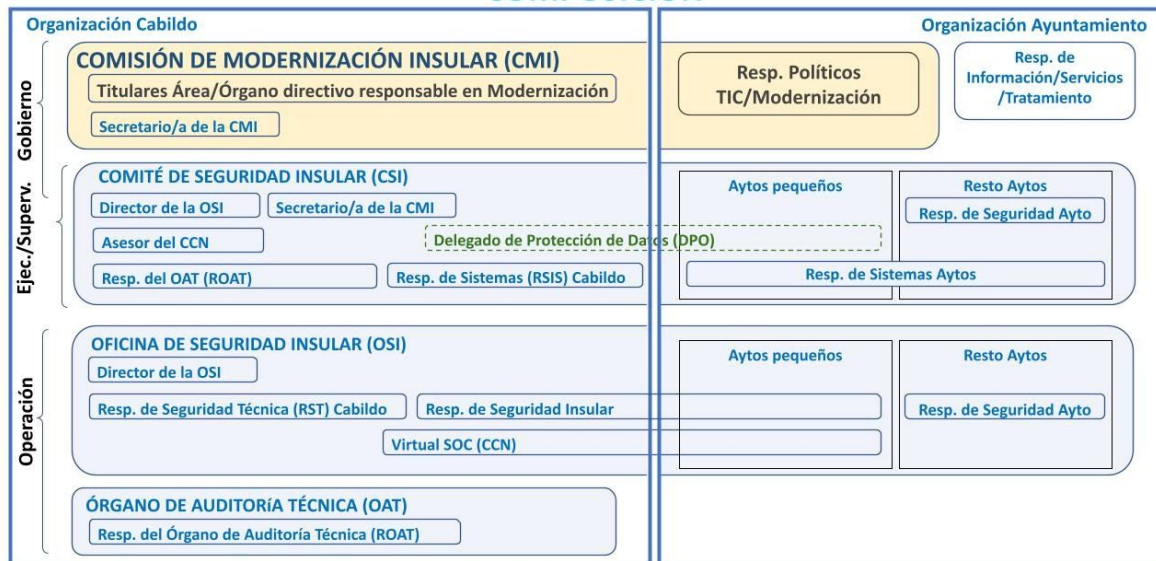
Las partes se comprometen a no copiar, reproducir, ceder información o material facilitado por la otra parte, así como a no permitir a ninguna otra persona física o jurídica la copia o reproducción o divulgación, sea total, parcial o de cualquier forma, de la información o materiales facilitados en cualquier momento, sin la autorización previa de la otra parte manifestada expresamente y por escrito.

### **P21.3B. Marco de gobernanza insular de seguridad de la información**

A continuación se describe la organización y funciones asociadas al marco:

## MARCO DE GOBERNANZA INSULAR DE SEGURIDAD

### COMPOSICIÓN



#### Nivel de gobierno - Comisión de Modernización Insular (CMI)

Es el **Órgano colegiado** regulado en el artículo 25 del Reglamento de Asistencia Integral a los Municipios (en fase de aprobación) y que asumirá las **competencias directivas y estratégicas** de la seguridad de la información.

Miembros:

- Los indicados en el artículo 25 del Reglamento de Asistencia Integral a los Municipios.

Funciones

- Proponer la estrategia de evolución de las entidades en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Conocer e informar regularmente del estado de la Seguridad de la Información a los máximos responsables institucionales de cada entidad.
- Resolver los conflictos de responsabilidad que puedan aparecer en todo el marco.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos. En particular deberá velar por la creación y utilización de servicios comunes que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Promover la realización de auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de las entidades en materia de seguridad de la Información, conociendo los resultados y definiendo la estrategia necesaria para su mejora.



- Liderar, coordinar y velar por el correcto desarrollo de los proyectos de adecuación al ENS que se impulsen en los Ayuntamientos adheridos al marco de gobernanza insular, adoptando las medidas que correspondan, de acuerdo a los fines establecidos en el mismo.
- Alentar los procesos de Certificación de la Conformidad con el ENS para tanto los servicios comunes prestados a los ayuntamientos, como los propios.
- Conocer y reorientar si se estimase necesario, la aprobación por el CSI de los niveles de seguridad de la información y/o servicios y de la Política de Seguridad común.

### Nivel Ejecutivo/Supervisión - Comité de Seguridad Insular (CSI)

Se trata del **órgano / grupo de trabajo** que dará respuesta desde el punto de vista ejecutivo y de supervisión a las exigencias de seguridad de la información derivadas de la Adecuación al ENS.

Miembros:

- Vocales:
  - **Director de la Oficina de Seguridad Insular (OSI)**, también asumirá el cargo de Secretario del CSI.
  - **Secretario/a** de la CMI.
  - **Resp. de Seguridad de Ayto (RSA)**: un máximo de 3 representantes (rotario en cada sesión según orden de población, empezando por los de menor población).
  - **Resp. de Sistemas (RSIS) del Cabildo**.
  - **Resp. de Sistemas de los Ayuntamientos**: un máximo de 3 representantes (rotario en cada sesión según orden de población, empezando por los de menor población).
  - **Resp. del Órgano de Auditoría Técnica (ROAT)**.
- Asesores: con voz pero sin voto
  - **Asesor del Centro Criptológico Nacional (CCN)**.

Miembros no permanentes:

- **Delegado de Protección de Datos**: cuando se traten temas asociados a la protección de datos de carácter personal.
- **Especialistas externos**: de los sectores público, privado y/o académico, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Funciones:

- Aprobar, y mantener actualizada, la Política común de Seguridad de la Información.
- Proponer para su análisis o revisión y, en su caso, aprobar y publicar Normas, Procedimientos, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de su Conformidad.
- Asesorar a los ayuntamientos en materia de seguridad de la información y en la adecuación normativa al ENS, respecto de los métodos, procedimientos, herramientas y criterios en materia de Certificación de su Conformidad y, en general, con su implantación, orientando su gestión al mejor servicio del sector público.
- Informar a la CMI de la aprobación y/o modificación de los niveles de seguridad de la información, niveles de seguridad de los servicios y de la Política de Seguridad conjunta.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección, remitiendo para ello la información a la CMI. También se encargará de la remisión de



información a las organizaciones públicas y privadas que corresponda sobre el grado de implantación de la Certificación de Conformidad con el ENS.

- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, para que sean elevadas a la CMI.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información.
- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Identificar y diseñar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información en todas las entidades.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre sus miembros, elevando si fuese necesario el asunto al la CMI.
- Velar por la coordinación de las diferentes áreas de seguridad.
- Delegadas de los responsables de Información de los ayuntamientos:
  - Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
  - Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
  - Aprobación formal de los niveles de seguridad de la información.
- Delegadas de los responsables de Servicios de los ayuntamientos:
  - Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
  - Aprobación formal de los requisitos de los servicios en materia de seguridad.
  - Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).

### **Nivel Operativo - Oficina de Seguridad Insular (OSI)**

**Grupo de trabajo** de naturaleza técnica y carácter permanente, que se establece como elemento operativo de la seguridad de la información.

Miembros:

- **Director de la OSI:** Resp. del Cabildo del proyecto de asistencia técnica en seguridad informática para los ayuntamientos.
- **Resp. de Seguridad Técnica (RST) del Cabildo.**
- **Resp. de Seguridad Insular (RSIN).**



- 
- **Resp. de Seguridad de Ayto (RSA).**
  - **Equipo vSOC (CCN):** Jefe de Proyecto y técnicos del Virtual SOC designados por el CCN.

Funciones:

- Redactar o actualizar Normas, Procedimientos, Criterios o Buenas Prácticas en materia de Seguridad y Adecuación al ENS y Certificación de su Conformidad, proponiendo su aprobación al CSI.
- Realización de análisis de riesgos.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar al CSI posibles actuaciones respecto de ellos
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos al CSI.
- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.
- Análisis y debate de las cuestiones relacionadas con la seguridad de los sistemas de información de los ayuntamientos que hubieren sido presentadas por los Responsables de los ayuntamientos.
- Mantener informado al CSI del resumen del estado, así como actuaciones e incidentes relevantes.
- Redacción y presentación de propuestas al CSI.
- Para los ayuntamientos de menos de 20.000 habitantes adheridos al marco, y a través del vSOC:
  - La gestión operativa de los servicios comunes de seguridad de las entidades adheridas al marco, su explotación y mantenimiento.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

### **Nivel Operativo - Órgano de Auditoría Técnica**

Es el **elemento de verificación y conformidad** de las entidades adheridas al marco que se establecerá en el Cabildo para prestar apoyo a los ayuntamientos de prioridad 1 adheridos al marco.

Miembros:

- **Resp. del Órgano de Auditoría Técnica (ROAT).**
- **Equipo de auditores técnicos.**

Funciones:

- Su actividad se dirigirá principalmente a los ayuntamientos de población inferior a 20.000 habitantes, aunque en la medida de las posibilidades atenderá también al resto de ayuntamientos en orden de población.
- Verificación de las medidas técnicas de seguridad adoptadas en las entidades.
- La gestión de la emisión de la certificación de conformidad correspondiente.



- La inspección documental del marco normativo y otras tareas relacionadas con la conformidad al marco normativo.
- Realización de auditorías de seguridad y de conformidad con el ENS de los sistemas de información tanto comunes del Cabildo como propios en los ayuntamientos.

## Roles

### Responsables de la Información/Servicio/Tratamiento

- Una o varias figuras nombradas en cada ayuntamiento (se recomienda que sea única en los ayuntamientos con menos recursos).
- Las funciones más técnicas y específicas previstas en el ENS para este rol se han trasladado al CSI, quedando en esta figura solamente aquellas funciones que por ámbito competencial se entiende indelegables.

### Funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- En cuanto a lo dispuesto en el RGPD, por delegación del Responsable del Fichero se le encomienda el desarrollo de las tareas relacionadas con la gestión de los ficheros y tratamientos de datos personales que se realizan en su área en concreto, lo cual deberá realizar en coordinación con el Delegado de Protección de Datos.

### Responsables de Seguridad

#### Ámbitos:

- **Resp. de Seguridad Técnica (RST) del Cabildo:** ejercerá las funciones de responsable de seguridad sobre los servicios comunes que presta el Cabildo a los ayuntamientos.
- **Resp. de Seguridad Insular (RSIN):** ejercerá las funciones de responsable de seguridad sobre los servicios propios de los ayuntamientos de menos de 30.000 habitantes.
- **Resp. de Seguridad de Ayto (RSA):** ejercerá las funciones de responsable de seguridad sobre los servicios propios en los ayuntamientos de 30.000 o más habitantes y será designado por el propio ayuntamiento.

#### Funciones:

Dentro de su ámbito de actuación:

- Política, Normativa y Procedimientos



- Participará en la elaboración de la Política y Normativa de Seguridad de la Información, para su aprobación por el CSI.
- Elaborará los Procedimientos Operativos de Seguridad de la Información para su aprobación por el CSI.
- Formación y concienciación
  - Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el CSI.
- Gestión de la Seguridad
  - Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
  - Proporcionar asesoramiento para la determinación de la categoría del sistema contando con la colaboración de la OSI. Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
  - Participar dentro de la OSI en la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación.
  - Facilitará a los Responsable de Información y a los Responsables de Servicio información, así como al propio CSI, sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
  - Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
  - Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el CSI.
  - Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el CSI y probados periódicamente por el Responsable de Sistemas.
  - Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
  - Participar en el análisis, diseño y toma de decisiones y propuesta de mejoras en los servicios comunes.
  - Gestionar las revisiones externas o internas del sistema.
  - Apoyar la gestión de incidentes de seguridad y la actividad de la OSI
  - Coordinar y apoyar los procesos de certificación con el soporte de la OAT.
- CSI.
  - Facilitará periódicamente al CSI un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema). Responsables de Sistemas

## Responsable de Sistemas

Ámbitos:





- **Resp. de Sistemas (RSIS) del Cabildo:** con responsabilidad sobre los servicios comunes que presta el Cabildo a los ayuntamientos.
- **Resp. de Sistemas de los Ayuntamientos:** con responsabilidad sobre los sistemas propios de cada ayuntamiento.

Funciones:

En los sistemas bajo su responsabilidad:

- Prestar al Responsable de Seguridad y/o el CSI asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado, salvo los que sean realizados de forma centralidad desde la OSI.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Gestionar el Sistema
  - Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
  - Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Establecer directrices y medidas
  - Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
  - Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
  - Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
  - Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Elaborar y aplicar
  - Elaborar procedimientos operativos de seguridad.
  - Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.



- 
- Aprobar
    - Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
    - Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
  - Monitorizar
    - Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

### Administrador de la Seguridad

#### Ámbitos:

- **Oficina de Seguridad Insular (virtual SOC):** asumirá las funciones de este rol, a través del virtual SOC, sobre los servicios comunes que presta el Cabildo a los ayuntamientos.
- **Resp. de Sistemas de los Ayuntamientos:** tendrán la responsabilidad de este rol sobre los sistemas propios de cada ayuntamiento.

#### Funciones:

- Implementar, gestionar y mantener la seguridad
  - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
  - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
  - Informar a los Responsables de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
  - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Gestión, configuración y actualización
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
  - Aprobar los cambios en la configuración vigente del Sistema de Información.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Gestión de las autorizaciones
  - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Monitorizar la seguridad
  - Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

## P21.6A. Incorporación de la sede de los ayuntamientos a la red de fibra óptica

### Acuerdo de servicio de conectividad



---

El diseño y dimensionado de la red troncal y de la red de distribución, así como su ejecución, será responsabilidad del titular del Anillo Insular de Telecomunicaciones de Tenerife (AITT, Cabildo de Tenerife, en adelante CIT).

El diseño y ejecución de la red de dispersión, ramal de acceso, desde las infraestructuras del AITT, será responsabilidad de la propiedad de la edificación (Ayuntamiento).

La conexión entre la red de dispersión y las infraestructuras del AITT será responsabilidad del titular del AITT (Cabildo de Tenerife).

La conexión entre la red de dispersión y el CPD del Ayuntamiento será responsabilidad del titular del CPD (Ayuntamiento). Esta conexión se deberá de realizar de forma coordinada con el Cabildo de Tenerife.

No obstante, para acelerar la conexión por fibra del CPD de cada ayuntamiento con la arqueta más próxima de la fase III del AITT y de la Red de Autoprestación del Cabildo (RTC-ALiX), el Ayuntamiento podrá ejecutar, con financiación parcial por parte del Cabildo, su ramal de acceso o última milla (ver el apartado “Requisitos técnicos del ramal de acceso”).

### **Limitaciones del servicio de conectividad**

Una vez ejecutado el ramal de acceso por cada Ayuntamiento y conectado a las infraestructuras del AITT, se procederá a la iluminación de la fibra óptica, y la activación y certificación de los enlaces correspondientes para la conexión de su red con:

- La del Cabildo: para el acceso a los servicios prestados a los ayuntamientos:
  - Alojamiento de portales Web y sedes electrónicas.
  - Alojamiento de infraestructuras municipales en el D-ALiX.
  - Otros que se determinen de forma expresa a través de los Planes de Proyecto anuales vinculados al Reglamento del Servicio de Asistencia Técnica específica en materia de implantación de tecnología de la información, de las comunicaciones y en administración electrónica a los municipios de la Isla.
- La red SARA: para el acceso a los sistemas y plataformas de uso compartido para las administraciones públicas.

La finalidad última del servicio es proveer una conectividad de alta capacidad y disponibilidad que posibilite el traslado de los CPDs de los ayuntamientos al D-ALiX. El D-ALiX es un CPD que cumple el nivel de exigencia del mercado internacional de centros de procesamiento de datos, con unas instalaciones de categoría TIER III+, obteniendo la configuración TIER IV en el sistema eléctrico. Esto le convierte en el CPD con mayor garantía para alojar servicios y aplicaciones críticas de toda la Isla..

Estratégicamente, se pretende, por tanto, la centralización de Servicios TI para mejorar la seguridad, la gestión, el mantenimiento, simplificar y homogeneizar la configuración, minimizar esfuerzos, reducir gastos (suministro eléctrico, climatización, energía, etc.) además de generar sinergias.

### **Delimitación de responsabilidades**



Los Puntos de interconexión (Puntos de terminación de red) realizan la unión entre la red de autoprestación del CIT y la red de área local del Ayuntamiento y delimitan las responsabilidades en cuanto a mantenimiento entre el CIT y el Ayuntamiento. Dado que la entrega de los servicios se realiza en dos emplazamientos claramente diferenciados (CPD del Ayuntamiento y D-ALiX) existen dos puntos de interconexión:

1. Ayuntamiento: El punto de interconexión se encontrará en el panel de parcheo del Ayuntamiento en su CPD, entregándose en dicho panel de parcheo los servicios de la RTC-ALiX mediante cuatro latiguillos LC multimodo. El CIT será quien proporcione y conecte dichos latiguillos una vez se certifique el enlace. Cualquier incidencia que ocurra desde el extremo de esos latiguillos hacia la electrónica del Ayuntamiento será responsabilidad del Ayuntamiento. Del mismo modo cualquier incidencia que ocurra desde el extremo del latiguillo hacia la RTC-ALiX, será responsabilidad del Cabildo.
2. D-ALiX: El punto de interconexión se encontrará en el panel de parcheo del Rack del Ayuntamiento en la sala de administraciones públicas de D-ALiX, entregándose en dicho panel de parcheo los servicios de la RTC-ALiX mediante cuatro latiguillos LC multimodo. El CIT será quién proporcione y conecte dichos latiguillos una vez se certifique el enlace. Cualquier incidencia que ocurra desde el extremo de esos latiguillos hacia la electrónica del Ayuntamiento será responsabilidad del Ayuntamiento. Del mismo modo cualquier incidencia que ocurra desde el extremo del latiguillo hacia la RTC-ALiX, será responsabilidad del Cabildo. Cuando el Ayuntamiento no disponga de rack y/o equipamiento propio en el D-ALiX, al no disponer de los recursos e infraestructuras necesarias, la entrega será realizada directamente a la electrónica de red dispuesta por el Cabildo, para hacer posible la conexión, a su red y la red SARA, de los Ayuntamientos que se encuentren en esta situación.

La interconexión de las redes de las entidades municipales y del Cabildo se realizará mediante el enlace proporcionado por la RTC-ALiX, añadiendo las capacidades necesarias de enrutamiento de la Red Corporativa Multiservicios (RCM), y será necesario el establecimiento de los correspondientes Sistemas de Protección de Perímetro (SPP 1), tal y como se recomienda en la GUÍA DE SEGURIDAD (CCN-STIC-811) INTERCONEXIÓN EN EL ENS del Centro Criptológico Nacional (CCN). El cambio de direccionamiento y demás operaciones para dar de alta y poner en producción el enlace, se realizará de forma coordinada entre todas las partes.

En el caso que nos ocupa, las responsabilidades del suministrador y operador del servicio (Cabildo de Tenerife, empleando el AITT, la RTC-ALiX y la RCM), son las que se enumeran a continuación:

## **Cabildo de Tenerife**

### Procedimientos

- Financiar el ramal de acceso o última milla del Ayuntamiento.
- Gestión del alta o modificación del servicio de conectividad.
- Coordinación de los distintos Servicios Técnicos del Cabildo y con el usuario final (Ayuntamiento).

### Interconexión

- Configuración firewall del Cabildo, direccionamiento IP, reglas de enrutamiento a través de la Red Corporativa Multiservicios (RCM).



FONDO DE  
DESARROLLO  
DE CANARIAS

Gobierno  
de Canarias



- 
- Acceso a la Red SARA.
  - Conexión y configuración de la electrónica de red del Cabildo en el D-ALiX.

#### Soporte y Mantenimiento

- Soporte y mantenimiento de la red de autoprestación (RTC-ALiX).
- Interlocución para la gestión y soporte de la red física de soporte a la autoprestación (AITT).
- Estimación y reparto de caudales.
- Monitorización de enlaces de comunicaciones en producción.
- Respuesta y resolución de incidencias relacionadas con el enlace de comunicaciones.
- Actualización de firmware de dispositivos de red del RTC-ALiX.
- Renovación de dispositivos de red del RTC-ALiX.
- Coordinar y notificar cortes por mantenimiento.

#### **Ayuntamiento**

- Gestionar la contratación de la ejecución de su ramal de acceso o última milla, previa adhesión al Plan de Proyectos anual, con el objeto de obtener ayuda para su financiación. Se deberá entregar el **presupuesto** y la **memoria técnica** (ver apartado “Requisitos técnicos del ramal de acceso”), elaborada por la empresa encargada de la ejecución.
- Realizar la administración y configuración local de su electrónica de red y Firewall.
- Tomar las medidas necesarias para evitar el acceso no autorizado y la manipulación incorrecta de la infraestructura ubicada en el interior de la edificación del ayuntamiento.
- Notificar incidencias que afecten al servicio, haciendo uso de los canales establecidos. Si se produjera cualquier incidencia, el usuario, antes de notificarla, comprobará la conectividad hasta el Punto de interconexión para verificar que, efectivamente, se trata de un problema en la red del CIT.
- Facilitar el acceso a sus instalaciones a los técnicos de soporte de RTC-ALiX.
- **Canales:**
  - o Consultas sobre alta/modificación/mejora de los servicios.
    - Por correo electrónico: [tenerifelocal@tenerife.es](mailto:tenerifelocal@tenerife.es).
  - o Atención de incidencias y soporte técnico:
    - Por correo electrónico: [cau@tenerife.es](mailto:cau@tenerife.es).
    - Por teléfono: 922 239999.
    - Horario de servicio: Lunes a Viernes: 6.45 – 22.00 y Sábados: 9.00 – 15.00
  - o El Centro de Atención al Usuario (CAU) del Cabildo de Tenerife será el punto de contacto para los ayuntamientos, y será el encargado de escalar las incidencias con los enlaces.

#### **Requisitos técnicos del ramal de acceso**

Para la conexión de diversos puntos de interés (PDI) tales como las sedes principales de los ayuntamientos de la isla, así como otras sedes municipales o insulares de interés, a las infraestructuras del AITT y RTC-ALiX, se precisa la ejecución de una serie de ramales en los que se instalará un cable de fibras ópticas desde las arquetas origen, en las infraestructuras del AITT, hasta las salas de telecomunicaciones de los PDI.

#### **Memoria técnica**



Los trabajos consistirán en la ejecución de la instalación de cableado sobre canalizaciones de alumbrado público, red semafórica o telecomunicaciones existentes en la vía pública; la ejecución de obra civil, tanto para el enlace entre canalizaciones, nuevas canalizaciones, como para instalar arquetas de reparto o derivación; instalaciones en fachada; así como la instalación en planta interna a través de las canalizaciones y patinillos propios de los edificios.

Al tratarse de contratos menores de obra, no se precisa proyecto, pero sí es necesario realizar una **memoria técnica**, que se adjuntará al presupuesto, describiendo pormenorizadamente el trazado, añadiendo las fotos que se consideren oportunas, tanto a pie de calle como aéreas. Será imprescindible generar y entregar un archivo KMZ con el recorrido.

La memoria técnica, para su aprobación, será entregada en la solicitud de adhesión al proyecto correspondiente y será revisada por el Cabildo, y éste podría añadir cambios si los considerase necesarios con el objetivo de asegurar la máxima reutilización y eficiencia de la inversión realizada para dar cobertura a medio o largo plazo a otras sedes públicas en el municipio.

La memoria técnica se volverá a entregar actualizada al finalizar la ejecución de los trabajos, contemplando cualquier cambio derivado de la propia ejecución del proyecto.

### **Punto de interconexión**

En todas las salas de telecomunicaciones de los PDI, el Punto de interconexión (Punto de terminación de red) consiste en una bandeja de parcheo de fibras ópticas en las que se terminarán los cables mediante la conectorización de al menos 8 fibras, usando conectores tipo SC/APC, independientemente del número de fibras que conformen el cable. Esta bandeja ya se encuentra instalada dentro del armario de RTC en los CPD de los Ayuntamientos y es en ella donde se deberá de terminar, mediante fusiones, el despliegue del ramal. Este trabajo, las fusiones del cable en la bandeja, deberán de ser coordinados con el Cabildo de Tenerife.

### **Cables de fibras ópticas**

Los cables de fibras ópticas deberán de:

- Disponer de 16 o 72 fibras ópticas dependiendo del ramal:
  - Ramal de acceso: desde el AITT hasta arqueta en el exterior del Ayuntamiento, cable de 72 fibras ópticas.
  - Ramal de planta interna: desde arqueta exterior del Ayuntamiento hasta el CPD del ayuntamiento, cable de al menos 16 fibra ópticas.
- Cables conformados por tubos de 8 ó 12 fibras ópticas.
- Fibras del tipo ITU T G-652d.
- Todos los cables utilizados, en cualquiera de los ramales, deben de disponer de protección dieléctrica anti roedores.
- Los cables utilizados en los ramales de planta interna deben de ser LSZH.
- Los cables deben tener la cubierta exterior de color amarillo.
- Los cables deberán de estar serigrafiados con la siguiente leyenda: "AITT – Cabildo Insular de Tenerife – 922.747.800".
- Los cables deberán estar etiquetados en cada una de las arquetas o tramos de patinillos por los que discurren, la etiqueta deberá de ser impresa mediante equipo de etiquetado, no se



admitirán etiquetas realizadas mediante rotuladores, deberán de ser de material plástico y en ella se deberá de recoger como mínimo la siguiente información:

AITT - Cabildo Insular de Tenerife
Nombre del cable
Arqueta origen
Arqueta destino

- Desde Cabildo se indicará el nombre de las arquetas y el nombre de los cables con el objeto de homogeneizar nomenclaturas.
- Los cables se deberán dejar debidamente anclados tanto en bandejas, patinillos o arquetas, respetando en todo momento los radios de curvatura del cable.

### Arquetas

Todas las arquetas que se ejecuten:

- Dispondrán de tapa D400.
- Dimensiones 800x800x800.
- Serán preferiblemente prefabricadas.
- Las tapas tendrán apertura mediante sectores triangulares.
- Las tapas estarán serigrafiadas con el logo del Cabildo y el acrónimo "AITT".
- Dispondrán de cierre mediante llave.
- El suelo de la arqueta estará cubierto de una capa no inferior a 10 cm de picón.
- En aquellas arquetas que sean de reparto se deberá de dejar una coca de, al menos, 10 metros.
- En aquellas arquetas de nueva ejecución que sean de paso se deberá de dejar una coca de, al menos, 5 metros.
- Todos los conductos que accedan a la misma estarán obturados mediante bolsas o tapones de goma (en ningún caso se utilizará espuma de poliuretano).

El número de arquetas a ejecutar a lo largo de los ramales dependerá de la sinuosidad del mismo, así como de la existencia o no de arquetas existentes sobre dicha canalización. La máxima distancia entre arquetas, existentes o nuevas, no será superior a los 50-75 metros, dependiendo de la sinuosidad del recorrido.

En la fachada del Ayuntamiento se deberá de ejecutar una arqueta de reparto en la que se finalice la instalación en planta externa y se realice el cambio de cableado, de cableado de planta externa a cableado de planta interna.

### Fusiones de fibras



Los trabajos incluirán las fusiones de fibras en planta interna y en aquellos que se indique o sean necesarios, en planta externa. En cualquier caso, las fusiones deberán de tener una pérdidas de inserción inferiores a 0,15dB, y en cada uno de los tramos la media de pérdidas deberá de ser inferior a 0,10dB. Aquellas fusiones que presenten, a la hora de su ejecución, unas pérdidas superiores a la indicada, deberán romperse y volver a ejecutarse. No se permitirá la re-fusión de aquellas que presentan pérdidas superiores sin haberlas roto previamente. Se deberá hacer reflectometría de al menos las fibras que se fusionen en el CPD municipal (el resto no).

En los extremos del cable que finalicen en una arqueta de reparto se deberá de proveer una caja de empalme igual o similar a la BPEO 2 de la marca 3M, en caso de que se ofrezcan cajas de empalmes diferentes a la indicada, deberán de tener la aprobación de uso por parte del Cabildo.

En caso de que haya una sede o punto de interés (PDI) entre el AITT y el Ayuntamiento, se deberá ejecutar una arqueta de reparto. Posteriormente se instalará un nuevo cable, sangrando el primero y fusionando las fibras.

### **Obra civil**

En trabajos de nueva obra civil, se utilizará idealmente un tritubo de 63mm con pared lisa. Si no se dispone de tritubo o no hay espacio para él, con 2x63mm será suficiente. El tamaño de la zanja será el que la empresa considere oportuno, porque dependerá de los servicios que tengan alrededor, lo mismo con la profundidad. Todos los tubos se deben dejar enhebrados con hilo guía.

### **Electrónica de red necesaria en los Ayuntamientos**

El ayuntamiento deberá contemplar la disponibilidad de la electrónica de red necesaria para la conexión de su red, con el equipamiento de terminación de red de la RTC-ALiX, desplegado en el CPD municipal, y con el objetivo de poder aprovechar todas sus capacidades de alta disponibilidad:

- La conexión de la electrónica de RTC-ALiX, dispuesta en las sedes municipales, con el equipamiento/infraestructuras de red municipales, se podrá realizar a través de hasta 4 latiguillos de fibra óptica multimodo con una capacidad cada uno de 1Gbps, lo que permite dar alta disponibilidad/protección simultánea ante errores de ruta y de equipos. Lo mínimo recomendado es la conexión de 2 de estos latiguillos (lo que daría protección de ruta y de equipo, pero de forma alternativa).
- Se requiere, por tanto, en el ayuntamiento, un mínimo de dos (2) Switch/Conmutadores, cada uno con 1 (deseable 2) puerto/s 1 Gbps SFP multimodo. Además, este equipo, con el objetivo de configurar adecuadamente la alta disponibilidad, debe tener soporte a través de configuración a: la creación de enlaces agregados con el protocolo LACP Dinámico y posibilidad de realizar VLAN tagging sobre los puertos agregados. La conexión de estos equipos se realizará siempre a través de paneles de parcheo y no mediante la conexión directa del equipo del Ayuntamiento con el de la Red de Autoprestación.
- Este equipo se deberá conectar con el resto de la red municipal a través del correspondiente Cortafuegos perimetral empleado en cada ayuntamiento.





---

## Proyectos de planes anteriores

A continuación se relacionan los proyectos, aprobados en planes correspondientes a anualidades anteriores, cuya ejecución se prevé abordar también durante el ejercicio 2021:

- **P20.1 Alojamiento de sedes electrónicas y portales web**
  - **Objetivo:** dar continuidad al alojamiento de las sedes electrónicas y portales webs municipales en las infraestructuras del Cabildo.
  - **Presupuesto:** ejecución con medios ya existentes y sin reserva presupuestaria específica.
  
- **P20.6 Incorporación de la sede de los ayuntamientos a la red de fibra óptica**
  - **Objetivo:** Impulsar la conexión por fibra óptica del Centro de Proceso de Datos (CPD)/Sala de servidores de cada Ayuntamiento con la arqueta más próxima de la fase III del Anillo Insular de Telecomunicaciones de Tenerife (AITT)
  - **Presupuesto:** se ejecutará con cargo a presupuestos del 2020: 100.000 € (aportación económica a realizar en el 2020).
  
- **P20.7 Apoyar la implantación del Teletrabajo en los ayuntamientos**
  - **Objetivo:** Apoyar la adaptación e implantación del modelo de teletrabajo que se defina en el Cabildo de Tenerife en los ayuntamientos.
  - **Presupuesto:** se ejecutará con cargo a presupuestos del 2021: 50.000 €
  
- **P20.8 Ciberseguridad. Centro de operaciones de seguridad virtual (vSOC)**
  - **Objetivo:** Mejora de la ciberseguridad del Cabildo y ayuntamientos a través del impulso de la adecuación con el ENS y la implantación de un Centro de Operaciones en Ciberseguridad (vSOC).
  - **Presupuesto:** se ejecutará la anualidad 2021-22 con cargo a presupuestos del 2021: 300.000 €.