# PLAN DE ACTUACIÓN ZIUR 2026

**FUNDACIÓN**
**CENTRO DE CIBERSEGURIDAD INDUSTRIAL-INDUSTRI ZIBERSEGURTASUNEKO ZENTRUA**

## 1. DATOS GENERALES

- **Razón Social**: ZIUR FUNDAZIOA
- **CIF**: G75203067
- **Dirección**: Zuatzu Edificio Urola 1
- **Población**: Donostia – San Sebastián
- **Código Postal**: 20018
- **Teléfono de contacto**:943240988
- **Dirección de correo electrónico**: ziur@ziur.eus

# 2. FINALIDAD

La finalidad de la Fundación ZIUR, de acuerdo con lo señalado en sus Estatutos fundacionales es la de “reforzar las capacidades del territorio en materia de Fabricación Avanzada, en particular en materia de Ciberseguridad Industrial, impulsando el desarrollo del sector tecnológico y reforzando la competitividad y posicionamiento internacional de las empresas de Gipuzkoa, especialmente las del sector industrial”.

La puesta en marcha del centro constituye una apuesta decidida de la Diputación Foral de Gipuzkoa. En el Territorio de Gipuzkoa se concentra un importante número de las empresas de referencia en Ciberseguridad. Así mismo cuenta con centros universitarios y centros pertenecientes a la Red de Ciencia y Tecnología con un papel destacado en el campo de la Ciberseguridad.

Gipuzkoa es, por tanto, un Territorio que aúna demanda potencial, en un tejido industrial que por sí solo no puede desarrollar ambiciosos sistemas de protección; un conjunto de empresas referentes en la prestación de servicios en materia de ciberseguridad y diversos agentes generadores de conocimiento que pueden facilitar el avance constante en la prevención de amenazas en un entorno de industria 4.0.

Ante este ecosistema favorable, la Diputación de Gipuzkoa, a través de ZIUR FUNDAZIOA debe jugar aquí un papel de liderazgo y tratar de canalizar iniciativas que redunden en el beneficio del sector industrial y del de las tecnologías del ámbito de la Ciberseguridad, en orden a articular al Territorio como uno de los referentes mundiales en materia de protección y de conocimiento en dicho ámbito

Como resumen, la finalidad de ZIUR FUNDAZIOA se basa en los siguientes cuatro aspectos:

a) Impulso de la generación de conocimiento en el ámbito de la Ciberseguridad
b) Sensibilización y Formación de los agentes, empresas e industrias.
c) Difundir y hacer accesibles a las empresas la implantación de prácticas relacionadas con la Ciberseguridad.
d) Ofrecer herramientas de prevención e intervención.

# 3. ACTIVIDADES

Para el cumplimiento de sus fines, la fundación desarrollará actividades de:

Generación de conocimiento:

- Dinamizar a los actores académicos y de la RVCT para el desarrollo de proyectos en colaboración con empresas
- Puesta a disposición de las empresas de un laboratorio de ciberseguridad industrial.
- Análisis de seguridad de productos industriales
- Investigación en materia de ciberseguridad industrial.

Sensibilización y formación:

- Campañas técnicas
- Seminarios, charlas, foros.
- Generación de materiales formativos específicos.
- Creación de foros académicos
- Creación de cursos en colaboración con los colaboradores académicos

Difusión de hábitos relacionados con la ciberseguridad

- Difusión de la información
- Observatorio de tecnología
- Definir y desarrollar metodologías y herramientas
- Generación de una Base de datos de activos de empresas asociadas.
- Participar en redes nacionales e internacionales.
- Observatorio de tecnología

Herramientas de Prevención y e intervención.

- Ofrecer servicios de autodiagnóstico y canalizar diagnósticos específicos mediante la red de colaboradores
- Formación en la gestión de respuestas a incidentes
- Alertas y advertencias.

# 4. OBJETIVOS

Durante el año 2025 se ha continuado con el despliegue del Plan de Acción definido a finales del año 2024. El año 2025 se ha caracterizado por el despliegue de las siguientes iniciativas, dirigidas a ayudar al tejido industrial de Gipuzkoa en la mejora de sus procesos en materia de ciberseguridad. Para ello se han llevado a cabo las siguientes iniciativas:

- **Seguridad en el diseño de productos industriales:** Se ha llevado a cabo un proyecto en el que se han evaluado la ciberseguridad en el diseño de 6 productos industriales, de tres sectores diferentes: IoT, Automoción y Dispositivos médicos. El objetivo del proyecto es ir concienciando a las empresas productoras de Gipuzkoa de la necesidad de llevar a cabo estas evaluaciones, con el objetivo de prepararse para este tipo de certificaciones, de carácter obligatorio, que en los próximos meses se publicarán desde Europa, tales como CRA, UNECE R-155 y R-156, MDR, etc.

- **Chat Bot sobre NIS2 –** En el 2025 se ha aprobado una nueva Directiva europea, NIS2, que aplica a muchas empresas industriales, a las que la versión anterior de esta normativa no aplicaba (NIS1). Y, dado que hay un montón de dudas al respecto, hemos puesto en marcha, en la WEB de ZIUR, una chat, basado en un bot, que responde a preguntas sobre la directiva; para que las empresas puedan ir preparándose de cara a su aplicación en el 2026.

- **Formación en Gestión de Incidentes de Ciberseguridad**: Como en años anteriores, seguimos ayudando a las empresas a concienciar y formar en la gestión de incidentes de ciberseguridad a los usuarios y equipos de intervención de las empresas industriales de nuestro territorio, ante posibles ataques, y en particular, ante incidentes de ransomware por su impacto. En este caso usando una herramienta de gaming, para simular ciberincidentes.

- **CiberEngaño**: Con este proyecto se ponen en marcha “HoneyPots”, que son copias de dispositivos reales de las empresas industriales, y se intenta atraer a los hackers a dichos HoneyPots. El objetivo es engañarlos, que piensen que están en un dispositivo real de la empresa y retenerlo ahí el mayor tiempo posible, para obtener datos sobre ellos: Origen, objetivo, técnicas utilizadas, etc. De esta manera aportamos a las empresas industriales, participantes en el proyecto, información valiosa sobre sus atacante, para ser capaces de defenderse de manera más eficiente.

- **Formación a usuarios en Ciberseguridad**: Hemos puesto en marcha una proyecto en el que las empresas participantes en el proyecto pueden acceder a una plataforma de formación online, con el objetivo de formar a todos sus usuarios en buenas prácticas, en materia de ciberseguridad.

- **Simulación campañas Phising:** Hemos puesto en marcha campañas de simulación de phishing, donde los usuarios de las 24 empresas que han participado, reciben simulaciones de phishing, con el objetivo de concienciar y sensibilizar a los usuarios.

- **Campaña de Inteligencia de Amenazas**: Durante el 2025 hemos llevado a cabo una campaña de inteligencia de amenazas en la que han participado 83 empresas, en la que, utilizando una herramienta somos capaces de buscar en la dark web información sobre las empresas, sus dominios y sus usuarios; que los cibercriminales suelen compartir como fase previa a un posible ataque a una empresa.

- **Generación de Talento**: Seguir colaborando con el mundo académico, acercando las necesidades del mercado en lo relativo al talento e impulsando nuevas iniciativas para su generación.

Las líneas principales de trabajo para el año 2026 se listan a continuación:

- Realizar inversiones, basado principalmente en la ampliación de tecnologías en el ámbito de la red de ZIUR. Para el año 2026 se prevé la renovación de parte de la infraestructura de servidores y almacenamiento de la red interna de ZIUR, ya que la mayoría de esta infraestructura se queda fuera de soporte en los próximos meses.

- Durante finales del 2025 se ha licitado un proyecto cuyo objetivo es poner en marcha una iniciativa enfocada a la evaluación y certificación de la ciberseguridad en el ámbito de productos industriales, dispositivos y/o componentes conectados, con la finalidad de dar respuestas a las normativas y estándares sectoriales que establecen dichos requisitos.

  Esta iniciativa tiene como objetivo ayudar a las empresas manufactureras guipuzcoanas, de diferentes verticales, a empezar a prepararse para la adecuación a diferentes normativas europeas.

  Para ello se creará un MarketPlace, bajo el que diferentes empresas y agentes del ecosistema de ciberseguridad, colaborarán para prestar los servicios asociados al mismo.

- Seguiremos durante el 2026, con el proyecto iniciado en el 2025 de evaluación de la ciberseguridad en el diseño de 6 productos industriales, de tres sectores diferentes: IoT, Automoción y Dispositivos médicos.

- Puesta en marcha del proyecto licitado, a finales del 2025, en el que evaluaremos la madurez de ciberseguridad de 15 empresas industriales, en base a una solución de una start up vasca (NNEAT).

- Ejecución de servicios y actividades propias del Centro de Ciberseguridad Industrial de Gipuzkoa, incluyendo aquellas relacionadas el laboratorio de ciberseguridad y el observatorio, buscando siempre el refuerzo de las capacidades en ciberseguridad del tejido industrial de Gipuzkoa.

- Soporte al emprendimiento en materia de ciberseguridad para situar a Gipuzkoa como un polo de emprendimiento especializado en ciberseguridad.

Se marca como objetivos cuantitativos para el ejercicio 2026:

- 10 actividades de utilización del Laboratorio por terceros o relacionadas con terceros.
- Participación de 120 empresas en iniciativas y actividades promovidas por el Observatorio de Ciberseguridad.
- Número de empresas atendidas (multipropósito) por el Centro de Ciberseguridad: 230

# 5. PRESUPUESTO DE INGRESOS Y GASTOS 2026

| PRESUPUESTO DE GASTOS | GASTO TOTAL: | 2.224.684,00 € |
|---|---|---|
| CLASIFICACIÓN ECONÓMICA | | 2026 |
| Capítulo 1: Gasto de personal | | 332.703,00 € |
| Capítulo 2: Gastos corrientes en bienes y servicios | | 1.718.297 € |
| 20. Arrendamientos | | 45.547 € |
| 21. Reparaciones, mantenimiento y conservación | | 14.657 € |
| 220. Material de oficina | | 1.954 € |
| 221. Suministros | | 14.953 € |
| 222. Comunicaciones | | 6.099 € |
| 226. Gastos varios | | 6.367 € |
| 227. Trabajos realizados por profesionales o empresas especializadas | | 1.615.504 € |
| 23. Indemnizaciones por razón de servicio | Dietas, estancias, locomoción y traslados | 13.216 € |
| Capítulo 6: Inversiones reales | | 173.684 € |
| 622. Edificios y otras construcciones | | - € |
| 64. Mobiliario y enseres | | 4.080 € |
| 65. Equipos para procesos de información | | 169.604 € |

| PRESUPUESTO DE INGRESOS | INGRESO TOTAL: | 2.224.684 € |
|---|---|---|
| CLASIFICACIÓN ECONÓMICA | | 2.026 € |
| Capítulo3: Tasas y otros ingresos | | - € |
| 34. Prestación de servicios (servicios a empresas+laboratorio) | | - € |
| Capítulo 4: Transferencias y Subvenciones Corrientes | | 2.051.000 € |
| 420. Transferencias de la Diputación Foral de Gipuzkoa | | 1.948.450 € |
| 46. Transferencias de Ayuntamiento Donostia-San Sebastián | | 102.550 € |
| 471. Transferencias de empresas privadas (patrocinadores) | | - € |
| 49. Transferencias del exterior (Proyectos europeos) | | - € |
| Capítulo 7: Transferencias de Capital | | 173.684 € |
| 72: Transferencias de Capital de Diputación Foral de Gipuzkoa | | 165.000 € |
| 73: Transferencias de Capital deL Ayuntamiento Donostia-San Sebastián | | 8.684 € |

# 6. MEMORIA EXPLICATIVA PRESUPUESTO 2026

## 6.1 Presupuesto de Gastos

Los importes principales de gastos del Centro se atribuyen a los siguientes conceptos: Gastos de personal, Arrendamientos, Conservación de Equipos, Trabajos realizados por profesionales externos y Equipamiento de procesos de Información.

El presupuesto de gasto total: **2.224.684 €**

### 6.1.1 Personal

Se contempla una plantilla total de 4 personas.

El gasto total de personal: **332.703 €**

### 6.1.2 Gastos corrientes y bienes de servicios

El gasto total derivado de gastos corrientes y bienes de servicios es de 1.718.297 **€** que se desglosa de acuerdo con los siguientes conceptos

- **Arrendamientos**. Se contempla un local de aproximadamente 250 m2 en el Parque Empresarial de Zuatzu, en Donostia-San Sebastián.

  El gasto total de arrendamientos: 45.547 €

- **Conservación de equipos**. Dentro de esta partida se contemplan los gastos destinados a la puesta en marcha de soportes tecnológicos y su mantenimiento:
  - **Mantenimiento local**: estimación de los gastos derivados del mantenimiento del local.
  - **Impresión**: gastos de servicios de impresión.

  El gasto total de Conservación de Equipos: 14.657 €

- **Material de oficina.** Costes de material de oficina diverso y fungibles**.**

  El gasto total de Material de oficina: 1.954 €

- **Suministros.** Incluye los suministros comunes, como agua o luz, combustible, productos básicos.

  El gasto total de suministros: 14.953 €

- **Comunicaciones.** Telefonía fija, móvil y conexión a Internet.

  El gasto total de Comunicaciones: 6.099 €

- **Gastos diversos:** destinados a desarrollar una red de colaboraciones internacionales de primer nivel. Las cuotas de suscripción y participación en ellas se incluyen en este apartado**.**

  El gasto total de Gastos Diversos: 6.367 €

- **Trabajos realizados por profesionales o empresas especializadas.** Además del personal propio con dedicación al desarrollo de actividades habituales, se contará con personal especializado en diversas áreas que colaborarán con el centro. Los ámbitos contemplados son**:**
  - **Consultoría/auditoría**: en este apartado se han considerado los gastos derivados de la contratación de equipos especializados externos para el desarrollo de procesos de certificación, redacción de memorias y/o informes de observatorio, realización de proyectos experimentales.
  - **Marketing y publicidad**: Desarrollo del plan de comunicación de la fundación mediante servicios especialistas externos incluyendo generación de contenidos y realización de eventos específicos.
  - **Servicios externos**:

- El fuerte componente tecnológico del centro requiere de un soporte externo en este campo. Destaca la subcontratación de personal especializado de ciberseguridad con dedicaciones de mantenimiento y soporte técnico de los equipos y redes internas, así como en materia de comunicaciones externas.
- En este apartado se contempla el proyecto, detallado en el apartado 4, de creación de un MarketPlace, en Gipzukoa, para la evaluación de ciberseguridad en el diseño de productos industriales.
- En el ámbito de formación, junto con el plan de formación del personal de la fundación, se contemplan gastos derivados de actividades de sensibilización y formación de empresas y agentes. Se contemplan las jornadas destinadas a formación en materia de ciberseguridad de centros de FP y Bachiller, así como la participación en financiación de postgrados y Másteres universitarios.
- Se contemplan los servicios de soporte externos necesarios para que la fundación sea operativa.

El gasto total de Trabajos Realizados por profesionales o empresas especializadas: 1.615.504 €

- **Indemnizaciones en razón de servicio:** este apartado contempla los gastos de desplazamientos, dietas y similares del personal propio del centro.

El gasto total de Indemnizaciones en razón de servicio: 13.216€

### 6.1.3 Inversiones reales

- **Mobiliario y enseres:** Mobiliario de uso habitual en instalaciones de este tipo.

Inversiones reales por Mobiliario y enseres: 4.080 €

- **Equipos para procesos de información.** Se contemplan las inversiones necesarias para el desarrollo y mantenimiento de la plataforma tecnológica (HW, SW y otros elementos que puedan ser requeridos) necesaria para desarrollar la operativa del centro.

  Inversiones reales por Equipos para procesos de información: 169.604 €

## 6.2 Presupuesto de Ingresos

El modelo de negocio de ZIUR Fundazioa contempla una fuente principal de ingresos, correspondiente a la financiación de fuentes públicas.

El presupuesto de Ingresos total**: 2.224.684 €**