PLAN DE ACTUACIÓN ZIUR 2023

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
- Coordinación de respuestas a incidentes
- Alertas y advertencias.

4. OBJETIVOS

El año 2022 ha sido el año del despliegue del Plan de Acción definido a finales del año 2021. El año 2022 se ha caracterizado por la **consolidación** de los servicios y su puesta a disposición del tejido industrial de Gipuzkoa y de los organismos educativos y universitarios del territorio y la puesta en marcha de nuevos **retos**.

- Asesoramiento de encaminamiento
- Observatorio de ciberseguridad (autodiagnóstico, estudios y proyectos con empresas industriales).
- Laboratorio de Ciberseguridad Industrial
- Talleres de capacitación
- Campañas de sensibilización

Las líneas principales de trabajo para el año 2023 se listan a continuación:

- Continuar el plan de inversiones anuales, basado principalmente en la ampliación de tecnologías en el laboratorio de ciberseguridad industrial. Para el año 2023 se prevé la adquisición de tecnología de análisis de ciberseguridad.

- 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.

- Identificar y explorar necesidades del tejido industrial gipuzkoano, con el objetivo de que ZIUR vaya evolucionando y adecuándose a las necesidades del mercado.

Las principales diferencias en la actividad con respecto al ejercicio 2022 serán:

- El despliegue de las siguientes iniciativas:

    - **Seguridad en la Cadena de Suministro:** Crear un buscador para ayudar a nuestras empresas industriales, a conocer los requerimientos de ciberseguridad en sus productos y servicios, que les van a exigir sus clientes, dependiendo del sector y del país del cliente.

- **Formación en Gestión de Incidentes de Ciberseguridad**: 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.

- **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.

- Puesta en marcha de un proyecto de colaboración entre CCTT, AFM y ZIUR para definir un ecosistema de análisis de producto industrial.

Se marca como objetivos cuantitativos para el ejercicio 2023:

- 10 actividades de utilización del Laboratorio por terceros o relacionadas con terceros.
- Participación de 100 empresas en iniciativas y actividades promovidas por el Observatorio de Ciberseguridad.

- Número de empresas atendidas (multipropósito) por el Centro de Ciberseguridad: 200

5. PRESUPUESTO DE INGRESOS Y GASTOS 2023

PRESUPUESTO DE GASTOS		GASTO TOTAL:	1.139.718,01 €
CLASIFICACIÓN ECONÓMICA			2023
Capítulo 1: Gasto de personal			326.180,39 €
Capítulo 2: Gastos corrientes en bienes y servicios			642.391,82 €
20. Arrendamientos			46.611,84 €
21. Reparaciones, mantenimiento y conservación			13.684,80 €
220. Material de oficina			2.000,00 €
221. Suministros			15.000,00 €
222. Comunicaciones			6.242,40 €
226. Gastos varios			6.242,40 €
227. Trabajos realizados por profesionales o empresas especializadas			539.085,18 €
23. Indemnizaciones por razón de servicio	Dietas, estancias, locomoción y traslados		13.525,20 €
Capítulo 6: Inversiones reales			171.145,80 €
622. Edificios y otras construcciones			- €
64. Mobiliario y enseres			4.681,80 €
65. Equipos para procesos de información			166.464,00 €

PRESUPUESTO DE INGRESOS	INGRESO TOTAL:	1.139.718,01 €
CLASIFICACIÓN ECONÓMICA		2022
Capítulo3: Tasas y otros ingresos		- €
34. Prestación de servicios (servicios a empresas+laboratorio)		- €
Capítulo 4: Transferencias y Subvenciones Corrientes		968.572,21 €
420. Transferencias de la Diputación Foral de Gipuzkoa		920.143,60 €
46. Transferencias de Ayuntamiento Donostia-San Sebastián		48.428,61 €
471. Transferencias de empresas privadas (patrocinadores)		- €
49. Transferencias del exterior (Proyectos europeos)		- €
Capítulo 7: Transferencias de Capital		171.145,80 €
72: Transferencias de Capital de Diputación Foral de Gipuzkoa		162.588,51 €
73: Transferencias de Capital deL Ayuntamiento Donostia-San Sebastián		8.557,29 €

6. MEMORIA EXPLICATIVA PRESUPUESTO 2023

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: **1.139.718**

6.1.1 Personal

Se contempla una plantilla total de 5 personas.

El gasto total de personal: **326.180€**

6.1.2 Gastos corrientes y bienes de servicios

El gasto total derivado de gastos corrientes y bienes de servicios es de **642.391€** 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: 46.611€

- **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: 13.683€

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

  El gasto total de Material de oficina: 2.000€

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

  El gasto total de suministros: 15.000€

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

  El gasto total de Comunicaciones: 6.242€

- **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: 6.242€

- **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 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: 539.085€

- **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: 13.525€

6.1.3 Inversiones reales

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

Inversiones reales por Mobiliario y enseres: 4.682€

- **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: 166.464€

6.2 Presupuesto de Ingresos

El modelo de negocio de ZIUR Fundazioa contempla 3 fuentes principales de ingresos. La primera y mayoritaria corresponde a la financiación de fuentes públicas. La segunda se corresponde por la provisión de servicios de la propia Fundación.

El presupuesto de Ingresos total: **1.139.718€**

- **Financiación pública.** mayoritariamente procedente de la Excelentísima Diputación Foral de Gipuzkoa y complementada por el Excelentísimo Ayuntamiento de Donostia San Sebastián.

  Ingresos por financiación pública: 1.139.718€

INFORME EXPLICATIVO 2023 ZIUR FUNDAZIOA Centro de Ciberseguridad Industrial de Gipuzkoa

El año 2022 ha sido el año del despliegue del Plan de Acción definido a finales del año 2021. El año 2022 se ha caracterizado por la **consolidación** de los servicios y su puesta a disposición del tejido industrial de Gipuzkoa y de los organismos educativos y universitarios del territorio y la puesta en marcha de nuevos **retos**.

- Asesoramiento de encaminamiento
- Observatorio de ciberseguridad (autodiagnóstico, estudios y proyectos con empresas industriales).
- Laboratorio de Ciberseguridad Industrial
- Talleres de capacitación
- Campañas de sensibilización

Las líneas principales de trabajo para el año 2023 se listan a continuación:

- Continuar el plan de inversiones anuales, basado principalmente en la ampliación de tecnologías en el laboratorio de ciberseguridad industrial. Para el año 2023 se prevé la adquisición de tecnología de análisis de ciberseguridad.

- 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.

- Identificar y explorar necesidades del tejido industrial gipuzkoano, con el objetivo de que ZIUR vaya evolucionando y adecuándose a las necesidades del mercado.

Las principales diferencias en la actividad con respecto al ejercicio 2022 serán:

- El despliegue de las siguientes iniciativas:
    - **Seguridad en la Cadena de Suministro:** Crear un buscador para ayudar a nuestras empresas industriales, a conocer los requerimientos de ciberseguridad en sus productos y servicios, que les van a exigir sus clientes, dependiendo del sector y del país del cliente.
    - **Formación en Gestión de Incidentes de Ciberseguridad**: 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.
    - **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.
- Puesta en marcha de un proyecto de colaboración entre CCTT, AFM y ZIUR para definir un ecosistema de análisis de producto industrial.