

## Datos generales programa

<b>Departamento:</b>	93 - ZIUR
<b>Sección:</b>	9301 - ZIUR
<b>Programa:</b>	010 - Fundación Centro de Ciberseguridad Industrial
<b>Funcional:</b>	433 - Desarrollo empresarial

### Tipo de programa:

Finalista

### Misión:

El Centro busca 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.

### Evolución del diagnóstico de situación:

El proceso de digitalización en el que se encuentra envuelto el sector industrial, ha provocado un aumento en las exigencias del mercado en materia de ciberseguridad debido al aumento de la superficie de ataque empresarial a medida que aumenta la interconexión entre los sistemas instalados y la compartición de información con terceros, entre otros factores.

En esta línea, los ciberdelincuentes utilizan cada vez mecanismos más sofisticados y herramientas más complejas durante los ataques por lo que las organizaciones deben mantener actualizadas las medidas implementadas en todos sus sistemas para estar preparadas ante nuevos posibles ataques.

Dentro del sector industrial guipuzcoano, se destaca la madurez que han adquirido las diferentes empresas del sector durante 2022, aumentando el grado de concienciación entre sus empleados así como la inclusión de nuevos mecanismos de defensa. Sin embargo, esta madurez no es suficiente y deben seguir trabajando en mantenerse actualizados frente a las nuevas amenazas y normativas que surgirán durante los próximos años.

### Evolución de la necesidad:

Durante los últimos años, el proceso de transformación digital en el que está envuelto el sector industrial está provocando que muchas de las organizaciones estén adoptando nuevas tecnologías en conjunto con sus sistemas tradicionales, aumentando así la conectividad de estos.

Así mismo, los ciberataques cada vez son más frecuentes y dirigidos, especialmente dentro del sector industrial debido a la criticidad de muchas de sus operaciones, por lo que la implementación de medidas genéricas para las organizaciones ha dejado de ser un mecanismo eficaz.

Este proceso de digitalización va a continuar durante los próximos años, aumentando el número de organizaciones partícipes y aumentando las tecnologías que se incluyen dentro del alcance. Las principales necesidades sobre las que hacer foco son:

- Dispositivos conectados: Durante los próximos años, varias iniciativas entrarán en vigor con el objetivo de aumentar la seguridad en los sistemas conectados y los entornos cloud. Dentro de estas iniciativas se destaca un etiquetado de estos.
- Ciberseguridad en el teletrabajo: Desde el inicio de la pandemia, la cultura del teletrabajo se ha implementado en la mayoría de las organizaciones. La mayoría de las organizaciones industriales no estaban preparadas para hacer frente a la conexión de dispositivos no seguros en su red, y se encuentran aún en el proceso de identificar y mitigar los riesgos asociados al teletrabajo.
- Inteligencia Artificial: Debido al aumento en la sofisticación de los ataques así como los métodos utilizados, el uso de mecanismos de Inteligencia Artificial para la identificación y actuación frente a un intento de intrusión se vuelve necesario para protegerse ante estos ataques.
- Fomento de la cultura de ciberseguridad: Realización de campañas de formación y concienciación en materia de ciberseguridad, asegurando que los empleados conocen los riesgos asociados al uso de los sistemas y sean capaces de actuar.

### Población objetivo:

Empresas (gran empresa, pequeña empresa, PYMEs, Instituciones sin fines de lucro,...)

## Estrategia del programa.

### 1. Recursos (inputs):

Presupuestos: Personal, gastos corrientes, inversiones, contrataciones externas, colaboraciones e ingresos por actividades con terceros.

### 2. Actividades/procesos a

Impulso de la generación de conocimiento en el ámbito de la Ciberseguridad.

Sensibilización y Formación de los agentes, empresas e industrias.

Difundir y hacer accesibles a las empresas la implantación de prácticas relacionadas con la Ciberseguridad.

Ofrecer herramientas de prevención

### 3. Bienes y Servicios (outputs):

Asesoría de encaminamiento a todas aquellas empresas que decidan emprender su estrategia de ciberseguridad.

Vigilancia tecnológica en ciberseguridad como las normas, estándares y buenas prácticas o formas de hacer que se desarrollan en el sector.

Observatorio e identificación de las amenazas que son relevantes en materia de ciberseguridad industrial, que pueden afectar a las empresas de Gipuzkoa.

Posibilidad de probar, testear y analizar tecnologías de ciberseguridad y otros productos que interactúen con ellas.

Plataforma de interrelación con agentes especialistas en ciberseguridad nacionales e internacionales.

Grupos de trabajo específicos para empresas orientados a desarrollar y/o compartir conocimiento en materias específicas de ciberseguridad aplicadas a la industria.

Empresas sensibilizadas en Ciberseguridad y capacitadas para desarrollar proyectos orientados a mejorar el nivel de ciberseguridad de sus empresas.

Profesionales formados/as en materia de Ciberseguridad.

Base de conocimiento de ciberseguridad industrial aplicada a la realidad de las empresas del Territorio.

Herramientas y recursos orientados a la prevención de incidentes puestos a disposición de la población objetivo.

Proyectos experimentales cuyos resultados permitan conciencia y reforzar la ciberseguridad de la población objetivo.

### Marco regulador del Programa:

LEY 9/2016, de 2 de junio, de Fundaciones del País Vasco.

Norma Foral 4/2007 de 27 de marzo, de Régimen Financiero y Presupuestario del Territorio Histórico de Gipuzkoa.

## ACTUACIÓN ENTIDAD VINCULADA AL PLAN ESTRATÉGICO 2020-2023

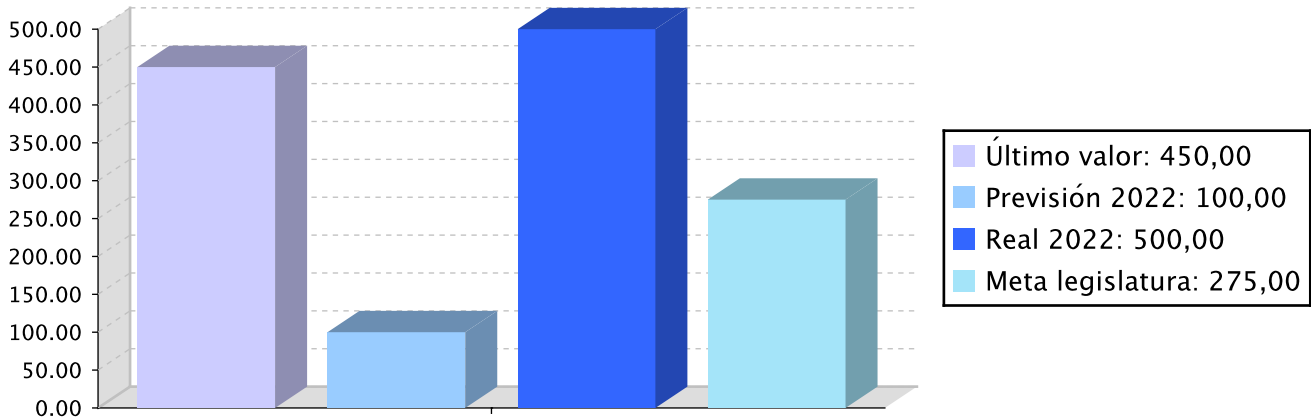
**Objetivo anual:** Impulsar ZIUR, nuevo Centro Avanzado de Ciberseguridad Industrial de Gipuzkoa para la incorporación de recursos de ciberseguridad industrial en la empresa guipuzcoana.

Indicador	Unidad de medida	Ultimo valor	Previsión 2022	Real 2022	Meta legislatura
Número de empresas atendidas	Número	450,00	100,00	500,00	275,00

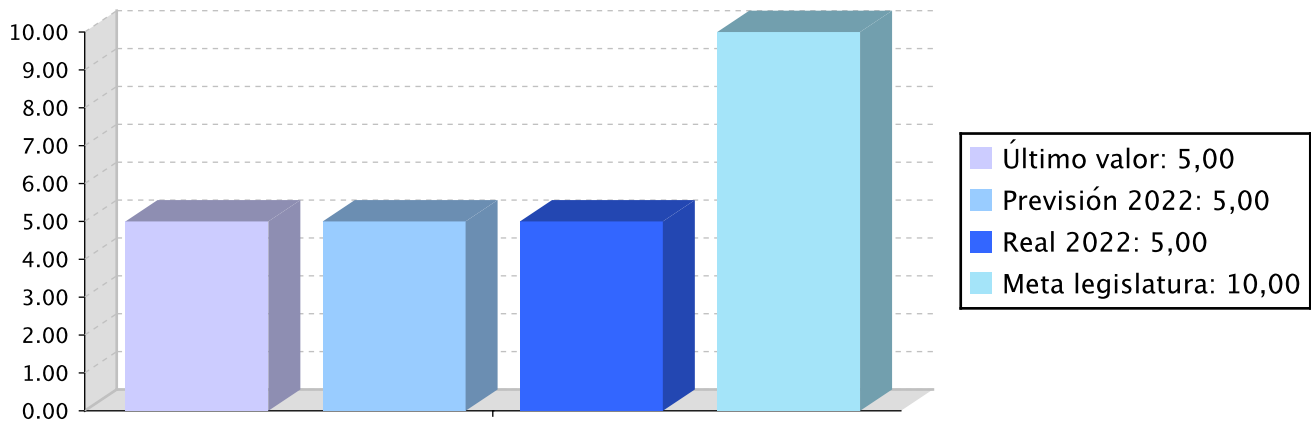
Indicador	Unidad de medida	Ultimo valor	Previsión 2022	Real 2022	Meta legislatura
Financiación no foral de al menos el 10% del presupuesto operativo en 2023	Porcentaje	5,00	5,00	5,00	10,00

**Tendencia**

Número de empresas atendidas – Número



Financiación no foral de al menos el 10% del presupuesto operativo en 2023 – Porcentaje



**Memoria**

La Fundación ZIUR - Centro de Ciberseguridad Industrial de Gipuzkoa, cuyo principal objetivo es reforzar y desarrollar las capacidades en ciberseguridad de las empresas industriales de nuestro territorio y reforzar su competitividad, cumple tres años desde su puesta en marcha oficial, el pasado 15 de noviembre 2019. El año 2022, una vez consolidada la Fundación, ha sido el año de donde se han puesto en marcha diferentes iniciativas puestas a disposición del tejido industrial de Gipuzkoa y de los organismos educativos y universitarios del territorio. Las líneas principales de trabajo para el año 2022 se listan a continuación:

Continuar el plan de inversiones, definido en el Plan Estratégico de ZIUR 2019-2022, basado principalmente en la ampliación de tecnologías en el laboratorio de ciberseguridad industrial.

Ejecución de servicios y actividades propias del Centro de Ciberseguridad Industrial de Gipuzkoa,

## Memoria

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.

Puesta en marcha del nuevo Plan Estratégico

A continuación, se presenta el cumplimiento de los compromisos adquiridos en el plan de actuación de 2022 tomando como base la memoria de actividades presentada:

Compromiso 1: Continuar el plan de inversiones, definido en el Plan Estratégico de ZIUR 2019-2022, basado principalmente en la ampliación de tecnologías en el laboratorio de ciberseguridad industrial.

Ejecución: Se han ejecutado las inversiones previstas relacionadas con la dotación de equipamiento informático y sistemas de información, incluyendo las inversiones previstas para ampliar las tecnologías del Laboratorio de Ciberseguridad Industrial, con el objetivo de ampliar los casos de uso de este. Se ha adquirido un robot, así como una tecnología de pentesting automática, dirigido a evaluar la ciberseguridad de productos industriales.

Compromiso 2: 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

Ejecución: Se han puesto en marcha proyectos dirigidos a ayudar a las empresas industriales de Gipuzkoa a mejorar en sus procesos de ciberseguridad, como por ejemplo: Proyecto de Breach and Attack Simulation (BAS), Spear Phishing, Cyber Deception, formación en gestionar ciber-incidentes, así como diferentes sesiones de sensibilización y formación a lo largo de todo el año y diversos talleres de capacitación.

Junto con los compromisos se incluía el siguiente objetivo: Se marca como objetivos cuantitativos para el ejercicio 2022:

8 actividades de utilización del Laboratorio por terceros o relacionadas con terceros.

Objetivo 8 - Ejecutado 13

Participación de 60 empresas en iniciativas y actividades promovidas por el Observatorio de Ciberseguridad.

Objetivo 60 - Ejecutado 150

Número de empresas atendidas (multipropósito) por el Centro de Ciberseguridad: 100

Objetivo 100 - Ejecutado 300

Compromiso 3: Soporte al emprendimiento en materia de ciberseguridad para situar a Gipuzkoa como un polo de emprendimiento especializado en ciberseguridad.

Ejecución: Se ha llevado a cabo relaciones y formalizado acuerdos con entidades y organismos con la finalidad de dar soporte al emprendimiento en Gipuzkoa en materia de Ciberseguridad, como por ejemplo (BIC Gipuzkoa, EHU/UPV, Mondragon Unibertsitatea). Se han impartido sesiones con StartUps junto con BIC Gipuzkoa.

Compromiso 4: Identificar y explorar necesidades del tejido industrial gipuzkoano, con el objetivo de que ZIUR vaya evolucionando y adecuándose a las necesidades del mercado.

Ejecución: Se ha llevado a cabo diferentes proyectos con empresas industriales de Gipuzkoa (Deception, BAS, Spear Phishing, Sesiones de formación ciber incidentes, etc.), a través de las cuales ZIUR extrae información acerca de los riesgos y amenazas a las cuales están expuestas las empresas industriales de Gipuzkoa.

Asimismo se han creado grupo de trabajo sectoriales, con los cuales ZIUR se reúne asiduamente con el objetivo de ir conociendo las necesidades del sector industrial:

AFM: donde además se ha desarrollado un Grupo de trabajo específico de Ciberseguridad.

MCC

Womes4Cyber Spain

Iraurgi Berritzen

Urola Kosta

**Memoria**

Colegio de Ingenieros  
ADEGI  
ASPEGI

**Líneas de actuación y acciones asociadas al objetivo**

**1. Línea de Actuación:**

Despliegue, consolidación y garantía de la sostenibilidad de ZIUR como Centro Avanzado de Ciberseguridad Industrial.



**Créditos de Pago**

	Presupuesto inicial	Ejecución	Ingresos afectados	Grado avance
<b>Total línea actuación</b>	<b>352.868,65</b>	<b>390.511,21</b>		
<b>1.1 Acción</b> Establecer canales de comunicación físicos y virtuales que faciliten a las empresas estar en contacto con la fundación y sus actividades	113.551,50	95.522,84		100,00
<b>1.2 Acción</b> Crear, mantener y evolucionar un mapa de relación y colaboración con agentes especialistas en la ciberseguridad aplicada a la industria tanto en el ámbito nacional como internacional.	239.317,15	294.988,37		100,00

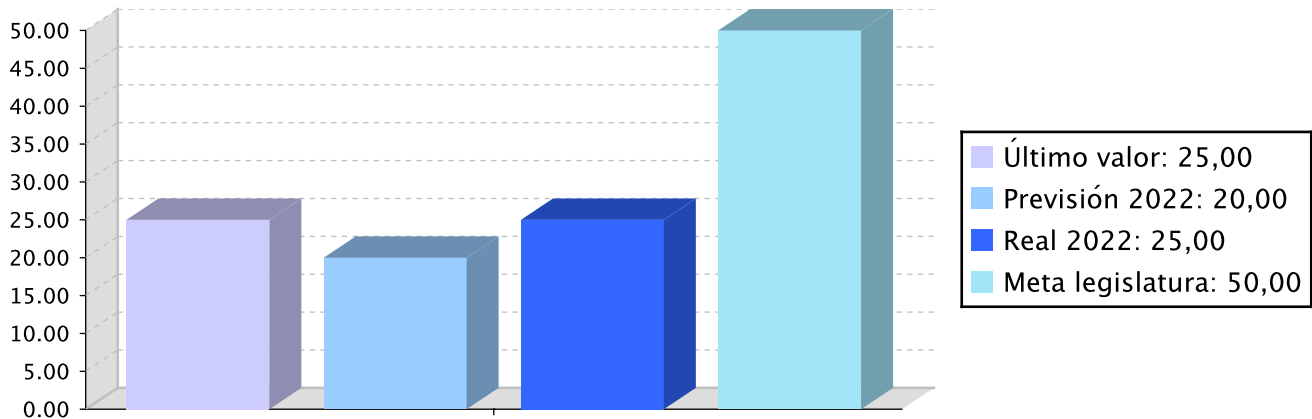
**Actuación operativa de la Entidad**

**Objetivo anual:** Realizar las actividades operativas ordinarias para la prestación de servicios de calidad en el ámbito de la ciberseguridad industrial

Indicador	Unidad de medida	Ultimo valor	Previsión 2022	Real 2022	Meta legislatura
Utilización del Laboratorio y Observatorio de Ciberseguridad	Porcentaje	25,00	20,00	25,00	50,00

**Tendencia**

Utilización del Laboratorio y Observatorio de Ciberseguridad – Porcentaje



## Memoria

Teniendo en cuenta el carácter estratégico del proyecto ZIUR, consideramos importante añadir a la información anterior aquella relacionada con hitos clave y actividades de alta relevancia que son críticas para la evolución del proyecto.

Despliegue de la actividad del Laboratorio de Ciberseguridad:

o Analizados 13 productos industriales de diferentes empresas (GH, ABC Compressors, Lazpiur, Enigmedia).

o Realización de actividades de formación

Master Ciberseguridad MU

Master de Inteligencia Artificial - Tecnum

Zubiri Manteo

Easo Poltekinkoa

Colegio de Ingenieros

Izarraitz LH

Talleres técnicos donde han participado 40 empresas

Despliegue de los servicios del Observatorio de Ciberseguridad:

o Publicación del informe sobre el proyecto de Rating de ciberseguridad

o Publicación de informes de inteligencia de ciberseguridad:

Informe de amenazas

Informe de Vigilancia Tecnológica y Tendencias

Asimismo, dentro de los servicios del Observatorio se han desarrollado las siguientes actividades, en colaboración con los agentes con los que se han formalizados acuerdos de colaboración:

o Campañas de análisis del grado de madurez de las defensas desplegadas en las empresas gipuzkoanas, a través de una tecnología de Breach & Attack Simulation (BAS).

o Campañas de sensibilización y concienciación en ataques de Phishing para PYMEs a través de un proyecto de Spear Phishing.

o Ciber ejercicios para la gestión de crisis.

Apoyo a la GFA-DFG en el desarrollo de la Estrategia de Ciberseguridad

o Apoyo al Departamento de Promoción Económica, Medio Rural y Equilibrio Territorial en la selección de los proyectos presentados en el Programa para promover la ciberseguridad en las empresas industriales de Gipuzkoa en los ámbitos de Ciberseguridad: Teletrabajo seguro y Ciberseguridad: I+D.

o Desde ZIUR se ha creado un Grupo de Colaboración de CIOs y CISOs de empresas industriales de Gipuzkoa (27 empresas representadas).

Desarrollo de actividades de formación y sensibilización

o Jornada de sensibilización (participación 100 empresas):

o Realización de diferentes jornadas de sensibilización con los siguientes organismos:

Iraurgi Berritzen

AFM

Tolosako Udala

Oarsoaldea

## Memoria

Urola Kosta  
ASPEGI  
Women4Cyber  
BIC Gipuzkoa  
EuskalHack  
APD

Cámara de Comercio de Gipuzkoa  
o Talleres de capacitación (participación 90 personas):  
Análisis de un ciber ataque en un entorno Industrial  
Medidas de seguridad a implantar en una planta industrial  
Ciberseguridad en Robotica  
Contratación de servicios para el correcto desarrollo de la actividad  
o 47 expedientes de contratación

Actividades enfocadas a integrar la Fundación en el ecosistema de agentes actual

Incorporación del convenio de colaboración como herramienta de trabajo, teniendo como evidencias, la firma de un convenio de colaboración con EHU-UPV, Mondragon Unibertsitatea, Women4Cyber Spain, ASPEGI, y en proceso de ampliar los convenios con más agentes.

Definición de los modelos de colaboración con los siguientes agentes:

Asociaciones empresariales (Elkargi, AFM, Cámara de comercio de Gipuzkoa, MCC, BIC Gipuzkoa, Colegio de Ingenieros)

Agencias de Desarrollo (UGGASA, Iraurgi Berritzen, Oarsoaldea, Urola Kosta, Debegesa, Tolosako Udala)

En materia de Educación (EHU/UPV, Mondragon Unibertsitatea, Tecnum, Zubiri Manteo, Easo Politeknikoa, Izarraitz LH)

Zentro Teknologikoak (Ikerlan, Tecnalía, Vicomtech, Ceit)

Agentes sectoriales (Incibe, ECSO.)

Colaboración de ZIUR como herramienta en el ecosistema de emprendizaje de Gipuzkoa, junto con BIC Gipuzkoa

Contacto con empresas de ciberseguridad, incluyendo startups, para conocer sus portfolio de servicios y productos, tecnologías y novedades, con objeto de poder asesorar a las empresas industriales acerca de las novedades del mercado, los potenciales proveedores especialistas, etc.

Actividades enfocadas a potenciar la promoción y posicionamiento de la Fundación

Publicación del Portal Web de la Fundación ZIUR y activación de la comunicación a través de redes sociales.

El desarrollo de diversas actividades de concienciación y sensibilización, con un alcance estimado superior a 100 empresas, a través de eventos organizados por terceros.

Exposición y difusión en medios de prensa (Diario Vasco, Noticias de Gipuzkoa y Berria), radiofónicos (Onda Vasca, Cadena SER-Radio San Sebastián, Radio Euskadi y Onda Cero) y Televisivos (ETB, TVE), así como en eventos especializados como ponentes.

Actividades enfocadas a dar servicios al tejido empresarial de Gipuzkoa

Desarrollo del servicio de asesoramiento de encaminamiento con actividad directa en 60 empresas de Gipuzkoa.

Servicio de autodiagnóstico de ciberseguridad, en el que se han autoevaluado 163 empresas.

Puesta en marcha del Laboratorio de ciberseguridad, donde se ha analizado la seguridad de 13 productos de empresas industriales de Gipuzkoa.

Una de las tareas más importantes del Observatorio es la de observar e identificar las amenazas más importantes en materia de ciberseguridad industrial que puedan afectar a las empresas guipuzcoanas. En 2022 hemos publicado siete (7) informes que han sido descargados por 185 personas.

Proyectos con más de 150 empresas industriales de Gipuzkoa.

Sesiones de concienciación y sensibilización (indicadas en el apartado anterior)

Despliegue de diversas acciones con agentes de educación (EHU UPV, Mondragon Unibertsitatea, Zubiri Manteo, Easo Politeknikoa) para contribuir al desarrollo de talento profesional en materia de ciberseguridad.

Se ha creado con UPV-EHU un Aula empresa de Ciberseguridad. Aula ZIUR.

## Líneas de actuación y acciones asociadas al objetivo

**1. Línea de Actuación:**

Desarrollo de actuaciones de sensibilización, formación, desarrollo de herramientas y servicios de Ciberseguridad



9,85 %



56,56 %



33,59 %

**Créditos de Pago**

	Presupuesto inicial	Ejecución	Ingresos afectados	Grado avance
<b>Total línea actuación</b>	<b>779.731,35</b>	<b>1.072.265,10</b>		
<b>1.1 Acción</b>				
Desarrollo de la actividad prevista por el centro como pueden ser sesiones de formación, capacitación, talleres, vigilancia tecnológica, grupos de trabajo, ...	493.904,60	720.311,29		100,00
<b>1.2 Acción</b>				
Equipar el centro de ciberseguridad con los recursos tecnológicos y humanos necesarios para llevar a cabo las actividades previstas.	285.826,75	351.953,81		100,00



**PLAN DE IGUALDAD DE GÉNERO**

**Relevancia de género del programa:** Media

**Colectivo afectado por el programa :**

Personas adultas

**Capacidad(es) afectada(s) por el programa:**

Acceso ingresos económicos

**Evolución de la necesidad:**

El empleo es una de las vías más importantes para promover la igualdad en nuestra sociedad. En ZIUR existe una paridad del 100% entre el número de trabajadoras y trabajadores. Asimismo en las licitaciones se ha incluido la obligación de incorporar perfiles femeninos en los equipos de trabajo.

**Cuantificación:** 53.613,02 ( 3,67 % )

Categoría	% Categoría	Cómo	Grado avance	Indicador asociado
Em.OO.9.3. Incrementar la presencia de mujeres en puestos públicos de representación y/o decisión social y política.	( 100,00 % )	Em.9.3.3. Apoyo a la visibilización de las organizaciones que cuenten - o estén promoviendo de modo activo- con una presencia equilibrada de mujeres y hombres en los puestos de dirección.	100,00	

**PLAN DE IGUALDAD LINGÜÍSTICA**

**Evolución de la necesidad:**

En el año 2022, ZIUR ha conseguido el certificado oro de BIKAIN.

**Cuantificación:**                    73.138,45    ( 5,00 % )

Categoría	% Categoría	Cómo	Grado avance
1.1. Rotulación y audiovisuales	( 6,25 % )	1.1.1. Rotulación y audiovisuales	100,00
1.2. Márquetin, publicidad y actos público	( 68,75 % )	1.2.1. Publicaciones, anuncios, campañas publicitarias, notas de prensa y papelería	100,00
		1.2.2. Actos públicos	100,00
		Se garantizar un uso equilibrado entre euskara y castellano en las convocatorias y actos públicos.	100,00
		Se garantizar un uso equilibrado entre euskara y castellano en las convocatorias y actos públicos. Se definirá el tratamiento lingüístico del acto en su fase de planificación, incluyendo la traducción.	100,00
		Garantizar el uso equilibrado entre euskera y castellano en el Plan de Comunicación	100,00
		Los anuncios en prensa y resto de actos publicitarios se realizarán en las 2 lenguas oficiales.	100,00
		Los anuncios en prensa y demás actos publicitarios se realizarán en las 2 lenguas oficiales.	100,00
2.2. Comunicación oral con las y los clientes (personas físicas) y la ciudadanía al ofrecer un servicio y/o un producto	( 25,00 % )	2.2.3. Respuestas en euskera a la demanda en euskera	100,00

**ODS**

**Cuantificación:** 1.462.776,31 ( 100,00 % )

**Relación de ODS asociados al programa**

ODS, Metas y Líneas de Actuación		Créditos de pago	Gastos futuros
	<p><b>8-TRABAJO DECENTE Y CRECIMIENTO ECONOMICO</b></p> <p>Fomentar el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo, y el trabajo decente para todos.</p>	<b>105.586,14</b>	
<b>Meta</b>	8.02 - Lograr niveles más elevados de productividad económica mediante la diversificación, la modernización tecnológica y la innovación, entre otras cosas centrándose en los sectores con gran valor añadido.	105.586,14	
	<b>Líneas de actuación</b>		
	Desarrollo de actuaciones de sensibilización, formación, desarrollo de herramientas y servicios de Ciberseguridad	105.586,14	
	<p><b>9-INDUSTRIA, INNOVACION E INFRAESTRUCTURA</b></p> <p>Desarrollar infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación.</p>	<b>820.883,48</b>	
<b>Meta</b>	9.1 - Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todas las personas	820.883,48	
	<b>Líneas de actuación</b>		
	Desarrollo de actuaciones de sensibilización, formación, desarrollo de herramientas y servicios de Ciberseguridad	606.523,31	
	Despliegue, consolidación y garantía de la sostenibilidad de ZIUR como Centro Avanzado de Ciberseguridad Industrial.	214.360,17	
	<p><b>16-PAZ, JUSTICIA E INSTITUCIONES SÓLIDAS</b></p> <p>Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles.</p>	<b>388.812,50</b>	
<b>Meta</b>	16.06 - Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas	388.812,50	
	<b>Líneas de actuación</b>		
	Desarrollo de actuaciones de sensibilización, formación, desarrollo de herramientas y servicios de Ciberseguridad	360.155,65	
	Despliegue, consolidación y garantía de la sostenibilidad de ZIUR como Centro Avanzado de Ciberseguridad Industrial.	28.656,85	
	<p><b>17-ALIANZAS PARA LOGRAR LOS OBJETIVOS</b></p> <p>Fortalecer los medios de ejecución y reavivar la alianza mundial para el desarrollo sostenible.</p>	<b>147.494,18</b>	



ODS, Metas y Líneas de Actuación		Créditos de pago	Gastos futuros
<b>Meta</b>	17.17 - Fomentar y promover la constitución de alianzas eficaces en las esferas pública, público-privada y de la sociedad civil, aprovechando la experiencia y las estrategias de obtención de recursos de las alianzas	147.494,18	
	<b>Líneas de actuación</b>		
	Despliegue, consolidación y garantía de la sostenibilidad de ZIUR como Centro Avanzado de Ciberseguridad Industrial.	147.494,18	
<b>Total</b>		<b>1.462.776,31</b>	

PROGRAMAREN AURREKONTUAREN LABURPENA / RESUMEN DEL PRESUPUESTO DEL PROGRAMA			
Gastuen kapituluak Capítulos gastos	Hasierako aurrekontua Ppto Inicial	Gauzatzea Ejecución	Gauzatze % % Ejecución
1. LANGILERIA GASTUAK/ GASTOS DE PERSONAL	322.473,00	278.944,10	86,50
2. ONDASUN ETA ZERBITZUEN GASTU ARRUNTAK/ GASTOS CORRIENTES EN BIENES Y SERVICIOS	642.337,00	920.032,02	143,23
3. FINANTZA GASTUAK/ GASTOS FINANCIEROS			
4. TRANSFERENTZIA ARRUNTAK/ TRANSFERENCIAS CORRIENTES			
<b>Eragiketa arruntak, guztira Total operaciones corrientes</b>	<b>964.810,00</b>	<b>1.198.976,12</b>	<b>124,27</b>
5. KONTINGENTZIETARAKO ETA BESTE EZUSTEKO BATZUETARAKO FUNTSA FONDO DE CONTINGENCIA Y OTROS IMPREVISTOS			
6. INBERTSIO ERREALAK/ INVERSIONES REALES	167.790,00	263.800,21	157,22
7. KAPITAL TRANSFERENTZIAK/ TRANSFERENCIAS DE CAPITAL			
<b>Kapitaleko eragiketak, guztira Total operaciones de capital</b>	<b>167.790,00</b>	<b>263.800,21</b>	<b>157,22</b>
8. AKTIBO FINANTZARIOAK/ ACTIVOS FINANCIEROS			
9. PASIBO FINANTZARIOAK/ PASIVOS FINANCIEROS			
<b>Finantza eragiketak, guztira Total operaciones financieras</b>			
<b>Guztira / Total</b>	<b>1.132.600,00</b>	<b>1.462.776,33</b>	<b>129,15</b>

**PROGRAMAREN GAUZATZEAREN LABURPENA / RESUMEN DE LA EJECUCIÓN DEL PROGRAMA**

Planen zenbateko osoa, kapituluka Total planes/capítulos	Ordainketa kredituak Créditos de pago		Konpromiso kredituak Créditos compromiso	
	Estrategikoa Estratégico	Operatiboa Operativo	Estrategikoa Estratégico	Operatiboa Operativo
1. LANGILERIA GASTUAK/ GASTOS DE PERSONAL	125.524,84	153.419,25		
2. ONDASUN ETA ZERBITZUEN GASTU ARRUNTAK/ GASTOS CORRIENTES EN BIENES Y SERVICIOS	264.986,37	655.045,64		
3. FINANTZA GASTUAK/ GASTOS FINANCIEROS				
4. TRANSFERENTZIA ARRUNTAK/ TRANSFERENCIAS CORRIENTES				
<b>Eragiketa arruntak, guztira Total operaciones corrientes</b>	<b>390.511,21</b>	<b>808.464,89</b>		
5. KONTINGENTZIETARAKO ETA BESTE EZUSTEKO BATZUETARAKO FUNTSA FONDO DE CONTINGENCIA Y OTROS IMPREVISTOS				
6. INBERTSIO ERREALAK/ INVERSIONES REALES		263.800,21		
7. KAPITAL TRANSFERENTZIAK/ TRANSFERENCIAS DE CAPITAL				
<b>Kapitaleko eragiketak, guztira Total operaciones de capital</b>		<b>263.800,21</b>		
8. AKTIBO FINANTZARIOAK/ ACTIVOS FINANCIEROS				
9. PASIBO FINANTZARIOAK/ PASIVOS FINANCIEROS				
<b>Finantza eragiketak, guztira Total operaciones financieras</b>				
<b>Guztira / Total</b>	<b>390.511,21</b>	<b>1.072.265,10</b>		
<b>Gauzatze gradua / Grado de ejecución: %</b>	<b>34,48</b>	<b>94,67</b>		

**PROGRAMAREN AURREKONTUAREN LABURPENA / RESUMEN DEL PRESUPUESTO DEL PROGRAMA**

Sarreraren kapituluak Capítulos de ingresos	Hasierako aurrekontua Ppto Inicial	Gauzatze Ejecución	Gauzatze % % Ejecución	Gastuari lotutakoak Afectados a gasto
1. ZUZENEKO ZERGAK/ IMPUESTOS DIRECTOS				
2. ZEHARKAKO ZERGAK/ IMPUESTOS INDIRECTOS				
3. TASAK ETA BESTELAKO SARRERAK/ TASAS Y OTROS INGRESOS				
4. TRANSFERENTZIA ARRUNTAK/ TRANSFERENCIAS CORRIENTES	964.810,00	964.810,50	100,00	
5. ONDARE SARRERAK/ INGRESOS PATRIMONIALES				
<b>Eragiketa arruntak, guztira Total operaciones corrientes</b>	<b>964.810,00</b>	<b>964.810,50</b>	<b>100,00</b>	
6. INBERTSIO ERREALAK BESTERENTZEA/ ENAJENACION DE INVERSIONES REALES				
7. KAPITAL TRANSFERENTZIAK/ TRANSFERENCIAS DE CAPITAL	167.790,00	167.790,50	100,00	
<b>Kapitaleko eragiketak, guztira Total operaciones de capital</b>	<b>167.790,00</b>	<b>167.790,50</b>	<b>100,00</b>	
8. AKTIKO FINANTZARIOAK/ ACTIVOS FINANCIEROS				
9. PASIBO FINANTZARIOAK/ PASIVOS FINANCIEROS				
<b>Finantza eragiketak, guztira Total operaciones financieras</b>				
<b>Guztira / Total</b>	<b>1.132.600,00</b>	<b>1.132.601,00</b>	<b>100,00</b>	