

[Home](#) | [White Paper on Cybersecurity](#) | [Basque Digital Innovation Hub](#) | [About BCSC](#)



# Basque Digital Innovation Hub

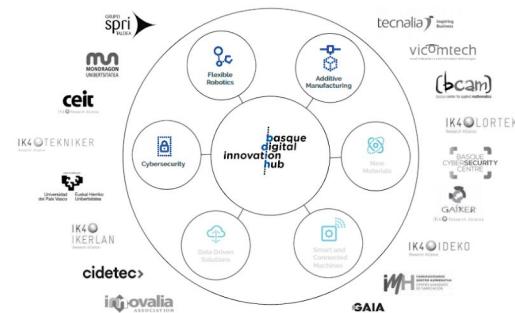
The Basque Digital Innovation Hub (BDIH) is a connected network of advanced manufacturing assets and services infrastructure for training, research, testing and validation available for companies, with the capacity to offer knowledge and concrete services in different areas such as Additive Manufacturing, Flexible Robotics and Cybersecurity.

The aim of this initiative is to provide industrial enterprises, especially SMEs, with the technological capabilities needed to meet the challenges of industry 4.0.

It consists of a digitally-linked network of R+D infrastructures, pilot plants and specialized know-how in different areas of advanced manufacturing. The network will be used for the development of R+D projects, scaling of industrial projects, exhibition of cutting-edge technologies and also as a resource for training and acceleration of start ups.

## Members

The network is owned by R&D Centers, vocational training centers and universities and it is supported by regional public institutions.



## Cybersecurity node

The cybersecurity node of the BDIH includes 5 interconnected laboratories distributed throughout the three territories of the Basque Country. They are used to foster entrepreneurship and innovation, highlighting projects such as smart-grid, automation, blockchain, product testing and certification, etc.



Vicomtech (San Sebastián)



Ikerlan (Arrasate)



Tecnalia (Gasteiz)



Tecnalia (Zamudio)



BCAM (Bilbao)

For further information visit this [link](#).



Zibersegurtasuna:  
Berrikuntza eta  
Lehiakortasuna  
industriarentzat

Ciberseguridad:  
Innovación y  
Competitividad  
para la Industria

BASQUE  
CYBERSECURITY  
CENTRE

ZIBERSEGURTASUNAREN EUSTALDEA  
CENTRO VASCO DE CIBERSEGURIDAD



GRUPO  
SPRI  
TALDEA







# El Cyber Range del nodo de ciberseguridad del BDIH, una infraestructura puntera para la capacitación de profesionales



01/04/2019 | [in](#) [t](#) [f](#) | [PDF](#) [DOCX](#) | [RSS](#)

El Gobierno Vasco puso en marcha el año pasado el nodo de ciberseguridad del Basque Digital Innovation Hub con el objetivo de promover el desarrollo de proyectos de I+D+i.

El nodo de ciberseguridad, puntero en su sector, está formado por 5 laboratorios distribuidos por todo Euskadi.

Conecta Empleo es un proyecto social de Fundación Telefónica para formar en habilidades digitales a personas para mejorar su inserción laboral en base a las tecnologías y competencias con más demanda laboral (Big data, desarrollo web y de aplicaciones móviles, programación de videojuegos, y ciberseguridad).

El pasado 28 de marzo, un grupo de alumnos pertenecientes a la formación en ciberseguridad que se está impartiendo en la actualidad en Vitoria-Gasteiz asistió al Cyber Range del nodo de ciberseguridad del **Basque Digital Innovation Hub** para realizar un ejercicio de entrenamiento.

El Cyber Range es una plataforma que permite simular entornos reales para la formación y el entrenamiento individual o colectivo de profesionales. Estos entornos permiten realizar ejercicios de secuorización de sistemas, poner en práctica técnicas y tácticas tanto de ataque como de defensa, etc. Para ello, se llevan a cabo escenarios de **Read Team vs Blue Team**, en el que un grupo de participantes ataca una infraestructura mientras otro la defiende, o **Capture The Flag (CTF)**, en el que hay que resolver una serie de pruebas.

En esta ocasión, los alumnos de la Fundación Telefónica participaron en un escenario de CTF en el que realizaron ejercicios de entrenamiento diseñados para identificar las vulnerabilidades más habituales en aplicaciones web, y aprendieron a implementar controles para protegerlas.

## Nodo de ciberseguridad

El Gobierno Vasco, a través del Basque Cybersecurity Centre, SPRy los agentes de la Red Vasca de Ciencia Tecnología e Innovación (Tecnalia, Ikerlan, Vicomtech y BCAM), puso en marcha el año pasado el **nodo de ciberseguridad del Basque Digital Innovation Hub**. En la actualidad, en el BDIH hay 3 nodos activos: Fabricación aditiva; Robótica flexible; y Ciberseguridad.

En lo que se refiere al nodo de ciberseguridad, hay **5 laboratorios distribuidos geográficamente por Euskadi y conectados entre sí** a través de la red de I2basque:

- **Vicomtech (Donostia)**: Enfocado en Industria 4.0 y Blockchain.
- **Ikerlan (Arrasate)**: Especializado en testeo y certificación de productos, Industria 4.0 y Blockchain.
- **BCAM (Bilbao)**: Enfocado a modelos matemáticos y simulación.
- **Tecnalia PTB (Zamudio)**: Orientado a Smart-grid, Automoción y Blockchain.
- **Tecnalia PTA (Miñano)**: También conocido como Cyber Range. Enfocado al entrenamiento y la capacitación.

Este nodo de ciberseguridad es puntero en su sector, y su objetivo es promover el desarrollo de proyectos de I+D+i. En la actualidad existe una gran demanda de perfiles relacionados con la ciberseguridad en ámbitos como el hacking ético, la ciberinteligencia, la gestión de incidentes, la ciberseguridad industrial, etc., de ahí la importancia de fomentar la capacitación de profesionales.

## La importancia de fomentar la capacitación en ciberseguridad

En la actualidad existe una gran demanda de perfiles de ciberseguridad. Es por ello, que en coordinación con el Departamento de Educación del Gobierno Vasco, representado a través de la Viceconsejería de Formación Profesional, desde el Basque Cybersecurity Centre llevamos a cabo distintas iniciativas para fomentar que los estudiantes identifiquen la ciberseguridad como una vía de desarrollo profesional y que en su salida al mercado laboral estén más capacitados.

Así mismo, colaboramos de manera activa con los centros de formación profesional que imparten materias de ciberseguridad para, de este modo, fomentar la relación con empresas proveedoras de este tipo de servicios y facilitar la incorporación de los alumnos al mercado laboral.

Es responsabilidad de todos intentar trasladar a los más jóvenes las oportunidades existentes en el ámbito de la ciberseguridad de cara a que lo contemplen como un ámbito en el que desarrollar sus competencias laborales.

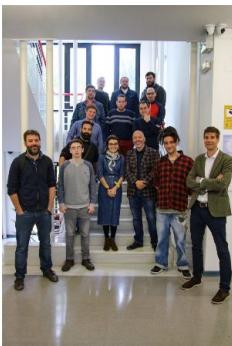


escuchar el artículo

## El Ayuntamiento y Fundación Telefónica clausuran el curso de ciberseguridad del programa "Conecta empleo" en Vitoria-Gasteiz

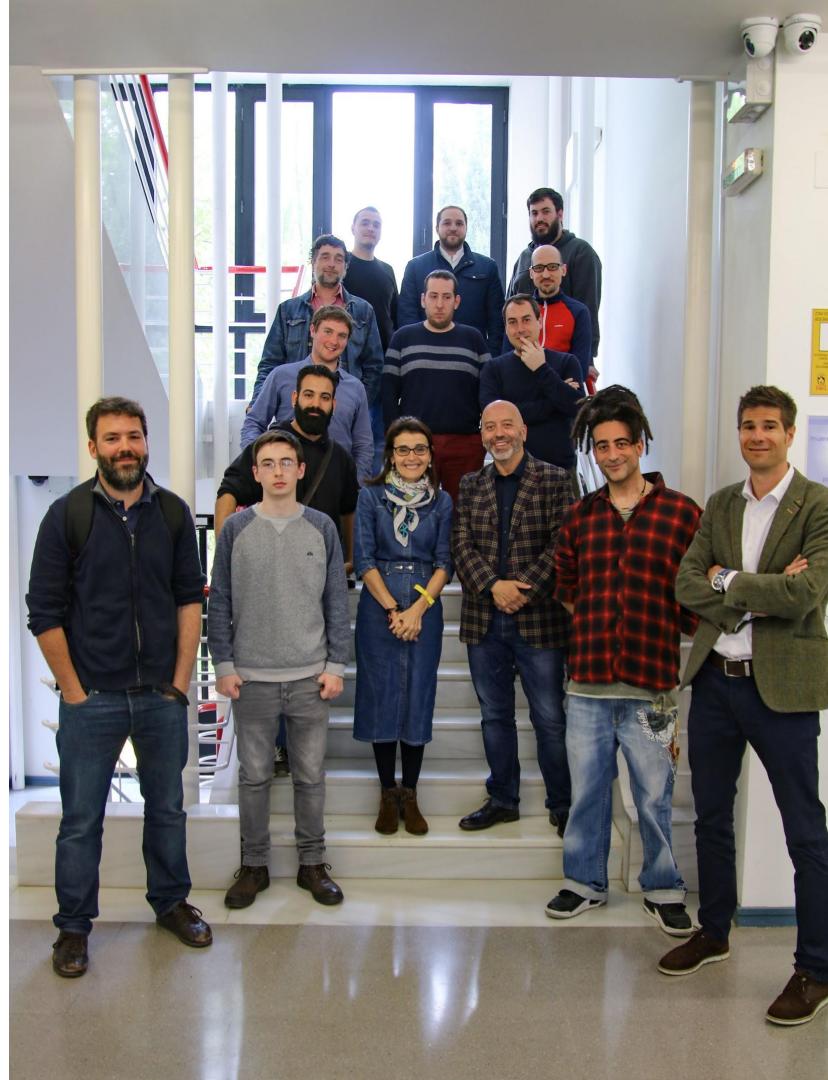
Categorías: [Notas de prensa](#) – Komunikazio Zerbitzua / Servicio de Comunicación – 3 mayo 2019 14:54

- El curso, de carácter gratuito, quiere servir de puente entre demandantes de empleo y empresas locales.
- Tras seis meses de formación, el alumnado, cuya media de edad ronda los 34 años y en su mayoría posee formación universitaria, ha presentado hoy 3 proyectos que ha realizado de la mano de empresas del sector.
- El curso ha sido fruto de la aplicación del Big Data a la demanda real de empleo digital en Vitoria-Gasteiz y su entorno



Once jóvenes vitorianos han presentado esta tarde en el salón de actos del CETIC sus proyectos como fin de curso del itinerario Ciberseguridad, en el marco del programa Conecta Empleo de Fundación Telefónica y el Ayuntamiento de Vitoria-Gasteiz están llevando a cabo para formar en competencias digitales, un perfil profesional en el ámbito de la industria 4.0 cuya demanda está creciendo en el mercado laboral.

Tras seis meses de formación en el CETIC, los alumnos han presentado hoy sus proyectos en un acto que ha contado con la presencia de **Nerea Melgosa**, concejala de Empleo y Desarrollo Económico Sostenible del Ayuntamiento de Vitoria-Gasteiz, y **Joan Cruz**, Director de Relaciones Institucionales de Fundación Telefónica, que han señalado que “queremos que estos itinerarios formativos sean un nexo de unión entre la demanda real de las empresas y la formación de quienes buscan empleo”.



## ES VITORIA CIBERSEGURIDAD ED 1

Inicio | [Actividades](#) | Doc. adicional | Mi progreso |

## INFORMACIÓN RELEVANTE PARA EL CURSO

## Carta de compromiso

## Calendario del curso

## Justificantes y ausencias

## Eventos relacionados

## MÓDULO HABILIDADES E+E

## M1. METODOLÓGIAS DE PROGRAMACIÓN

## M2. REDES Y SISTEMAS. PROGRAMACIÓN

## M3. SEGURIDAD WIRELESS

## M4. HACKING CON PYTHON

## M5. GOBIERNO Y RIESGOS (APT Y CIBERSEGURIDAD)

## M6. CRIPTOGRÁFIA Y ESTEGANOGRAFÍA

## M7. ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS

## M8. HACKING ÉTICO

## M9. METASPLOIT

## M10. VULNERACIÓN DE MECANISMOS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN

## M11. PROYECTO FINAL

## INFORMACIÓN RELEVANTE PARA EL CURSO



Si quieras ver más videos accede a [#ConectaEmpleo](#)  
En esta primera sección podrás encontrar información relevante del curso como:

- La carta de compromiso
- El calendario del curso
- Políticas de justificantes y ausencias
- Los eventos relacionados con el curso más destacados

### Módulos Técnicos (534h):

**Módulo 1**  
Metodología Programación -  
60 horas

**Módulo 2**  
Redes y Aplicaciones técnicas  
42 horas

**Módulo 3**  
Seguridad Wireless  
10 horas

**Módulo 4**  
Hacking con Python -  
90 horas

**Módulo 5**  
Gobierno y Risgos (APT  
y Ciberseguridad) - 24 horas

**Módulo 6**  
Criptografía y Esteganografía -  
70 horas

**Módulo 7**  
Análisis Forense de Sistemas  
Informáticos - 26 horas

**Módulo 8**  
Hacking Ético -  
90 horas

**Módulo 9**  
Metasploit-  
19 horas

**Módulo 10**  
Vulneración de Mecanismos de  
Identificación y autenticación -  
13 horas

**Módulo 11**  
Proyecto Transversal -  
90 horas

### Módulos Habilidades E + E (60h):

**Sesión 1**  
¿Emprender o Emplearme?

**Sesión 2**  
Mi yo Digital

**Sesión 3**  
Despertando el YO

**Sesión 4**  
Marca Personal

**Sesión 5**  
¿Qué hay ahí fuera?

**Sesión 6**  
¡Manos a la obra!

**Sesión 7**  
La prueba de fuego

**Sesión 8**  
La búsqueda de oportunidades

**Sesión 9**  
Presentaciones eficaces

**Sesión 10**  
El trabajo de buscar trabajo



escribe el texto a buscar

turismo  
& convention bureau !

Todas las redes sociales

**Personas**  
y colectivos**Actividades**  
y equipamientos**Transporte**  
y mapas**Empresas**  
y desarrollo sostenible**Trámites**  
y gobierno local**Participa**  
con tu propuesta

## CETIC (Centro de Tecnologías de la Información y Comunicación)



CETIC (Centro de Tecnologías de la Información y la Comunicación) ofrece un conjunto de recursos y actividades orientados a fomentar la capacitación profesional, el reciclaje y la inserción laboral a través de la realización de acciones de formación, orientación e información y el contacto con las empresas dentro del sector TIC.

### Contacto

- C/ Castro Urdiales, 10
- Tfno: 945 16 15 05 / Fax: 945 16 15 04
- [formacionempleo@vitoria-gasteiz.org](mailto:formacionempleo@vitoria-gasteiz.org)

### Destacamos



Ayudas al fomento del empleo estable y de calidad para personas mayores de 45 años



Coaching para la búsqueda de empleo (julio)



## CIBERSEGURIDAD

[Inicio](#) » [Nuestros servicios](#) » Ciberseguridad

En un entorno donde la seguridad es cada vez más importante, debemos disponer de los métodos más avanzados para detectar y prevenir los posibles ataques a nuestras organizaciones.

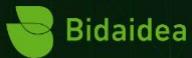
Los métodos de ataque han cambiado en los últimos años, pasando de ataques dirigidos a ataques indiscriminados, donde cualquiera puede ser objetivo de los ciberdelincuentes. Los métodos tradicionales de seguridad, por sí mismos, ya no son suficientes, y debemos complementarlos con otras medidas de seguridad más avanzadas.

Desde BeClever, le ayudaremos a complementar las medidas tradicionales con las medidas más avanzadas en ciberseguridad, de forma que pueda minimizar los riesgos y superficie de ataque.

El punto más vulnerable de todas nuestras organizaciones son los propios empleados y usuarios de las compañías, que, con el simple hecho de pulsar un link en un mail, pueden llegar a comprometer toda la información de la compañía.

Además, las nuevas normas, regulaciones, y leyes, como puede ser la nueva RGPD (Regulación General de Protección de Datos) o GDPR (General Data Protection Regulation) por sus siglas en inglés, de la Unión Europea, nos obligan a aumentar las medidas de seguridad de datos de carácter personal.





Consultoría · Auditoría · Ingeniería y Proyectos · Productos especializados · Centro de Servicios · Formación · I+D+i

Aumente su Seguridad Integral y visión  
360º a través de la Unificación de todas  
sus operaciones de:

**Seguridad  
Ciberseguridad  
Inteligencia**

## Bidaidea puede ayudarte

Contacta para que te podamos dar una solución personalizada.

Sin compromisos ni obligaciones.

Tu Nombre\*

Tu email\*

Compañía

Teléfono\*

Mensaje

Acepto la política de protección

**ENVIAR**

Keynetic focuses on developing cybersecurity solutions for Industry 4.0

We build on Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) to bring innovative products to the market

Contact us

## About BCSC

BCSC, which stands for "Basque Cybersecurity Centre", is the Organization appointed by the Basque Government (State of Spain) to promote cybersecurity in the Basque Country. Our mission is to promote and develop culture and awareness on cybersecurity in the Basque society, to streamline business activities concerning cybersecurity and to create a strong professional sector.

We are a cross-cutting initiative which represents the Basque Government's commitment to its citizens and companies in the field of cybersecurity.

The Basque Cybersecurity Centre (BCSC) is made up of the following stakeholders:

### BASQUE GOVERNMENT - DEPARTMENTS

- Economic Development and Infrastructures
- Security (regional police)
- Public Governance and Self-Government
- Education

### TECHNOLOGY CENTRES

- Basque Centre for Applied Mathematics
- Ik4-Ikerlan
- Vicomech
- Tecnalia

### THE IMPORTANCE OF DEVELOPING GREATER CYBERSECURITY

Ensuring cybersecurity boosts economic activity, thereby helping to **strengthen the professional sector**. This in turn contributes to **promoting and developing a culture of cybersecurity** in Basque society.

Our aim is to be recognised as a **meeting point** and to **spearhead collaborative initiatives**, thereby positioning the **Basque Country as an international benchmark** in the application of cybersecurity technologies to industry.

In order to rise to all these challenges, and with the aim of ensuring an effective response to any possible security-related incidents in the Basque Country, we are working side-by-side with different stakeholders from the **Basque science, technology and innovation network**, as well as with key public bodies within the Basque Government, such as the **EJE** (Basque Government IT Society), the **Ertzaintza** (Basque Regional Police Force) and the **Education Department**. We also work with other key stakeholders within the Basque Public Administration, including **Izenpe** (certification and service company), the **AVPD** (Basque Data Protection Agency) and public IT companies, along with a large number of different professional, business and citizen associations operating in our region.

- We are members of the **European Cyber Security Organisation (ECSO)** collaborating in several working groups.
- We are in partnership with the **Spanish National Cybersecurity Institute (INCIBE)** in Spanish) and with the **(INCIBE-CERT)**, mainly in the context of the cyber security incident response.
- We are in partnership with several non-profit organizations (basque, national and international) interested in promoting the cybersecurity in the Basque Country.

### OUR SERVICES: CSIRT

#### Incident handling.

Support and advice to Basque citizens and entities in the Basque Country. You can contact us either on our free helpline: **900 104 891** or via email at: [incidentes@bcc.eus](mailto:incidentes@bcc.eus) / [arazoiak@bcc.eus](mailto:arazoiak@bcc.eus)

#### Vulnerability handling.

We put those who discover vulnerabilities in touch with manufacturers, thus fostering responsible dissemination through fluid, honest communications.

#### Artifact handling.

We perform technical examination of artifacts and develop (or suggest) response strategies for detecting, removing and defending against these artifacts.

#### Alerts and warnings.

We provide practical and relevant information for mitigating and redressing security vulnerabilities in technological systems.

#### Announcements.

Information about particularly serious threats and risks.

#### Security-Related Information Dissemination.

We collect and disseminate computer and internet security-related information.

#### Threat Intelligence Sharing.

We share and exchange information on threats with other incident response teams, manufacturers, information service providers and various other collaborating entities.

#### Training for professionals.

We organise and run workshops and seminars to foster the knowledge level of cybersecurity, through [www.spt.eus/euskadiminva](http://www.spt.eus/euskadiminva)

#### Awareness Building.

For children and young people.  
We organise seminars to raise awareness among children and young people regarding the risks associated with the improper use of new technologies, and how to avoid them.

#### For companies and associations working in the Basque Country.

We organise seminars to help raise awareness in Basque industry regarding the need to implement the necessary cybersecurity measures in order to maintain current levels of competitiveness and innovation on different international markets.

### MEMBERSHIPS



### OUR SERVICES: Added value

#### Monitoring of the Basque public networks.

We identify and take measures to mitigate cyber-attacks which put the citizens and/or companies of the Basque Country at risk.

#### Collaboration with the Basque Police Force.

We work to improve our ability to prosecute cyber-criminals and to enhance the protection provided to Sensitive Facilities.

#### Fostering subsidies.

We foster the process of implementing cybersecurity measures in industrial environments. Promotion of Basque stakeholders. We actively seek the right partners to make contact with complementary stakeholders with the aim of enabling collaborative projects.

#### Aligning expertise.

We coordinate R&D+i initiatives.

#### Basque Digital Innovation Hub.

We work to create infrastructures and to place them at the service of the business community. Support for entrepreneurship in the field of cybersecurity. We work within the BIND 4.0 initiative to support Basque cybersecurity startups.

#### Support and identification of talent in relation to cybersecurity.

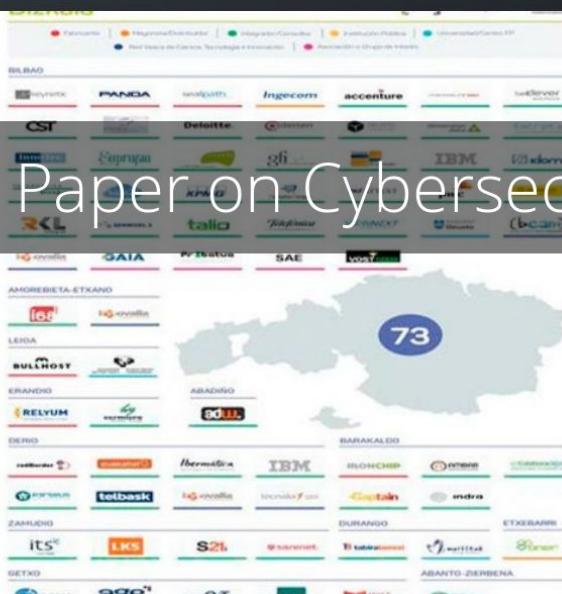
We collaborate in the development of initiatives which aim to encourage young people to see cybersecurity as a viable professional career.

Home | White Paper on Cybersecurity | Basque Digital Innovation Hub | About BCSC

Araba



卷之三



Gipuzkoan



White Paper on Cybersecurity

32



ZIBERSEGURTASUN EUSKAL ZENTROA  
CENTRO VASCO DE CIBERSEGURIDAD

[Home](#) | [White Paper on Cybersecurity](#) | [Basque Digital Innovation Hub](#) | [About BCSC](#)

## White Paper on Cybersecurity

By way of an introduction to the general situation of the Basque cybersecurity ecosystem, we have drawn up this study to show an analysis of the cybersecurity sector, including key aspects such as the prospects and opportunities facing the sector, and a detailed description of the current situation of organisations dedicated to cybersecurity existent in the Basque Country today.

The scope of this study has taken into account the different players offering cybersecurity services and solutions such as; companies, technology centres, universities, vocational training centres, relevant public bodies, clusters, associations, business accelerators and incubators whose collaboration and business support has been essential in the data validation process as well as at different points of the different study sections.

The document may be accessed via the following [link](#) and the infographics via the following [link](#).