

## COMPETENCIA DIGITAL: 4.1 PROTECCIÓN DE DISPOSITIVOS. NIVEL AVANZADO

### 1 INFORMAZIO OROKORRA

- Prestakuntza arloa** IKT (Informazioaren eta komunikazioaren teknologiak)
- Modalitatea** Lineakoa
- Hizkuntza** Gaztelania
- Iraupena** 10 ordu

#### Hartzaileak

Euskal Autonomia Erkidegoko administrazio publikoetan lan egiten duten enplegatu publikoak.

#### Egutegia

- 1** Matrikulazioaren azken eguna  
**Urriaren 4a:** administrazio orokorra (\*)  
**Urriaren 11:** beste administrazio batzuk  
(\* **Oniritzi epea urriaren 7tik 11ra**)
- 2** Bajen jakinarazpenak  
**Urriaren 31ra arte**
- 3** Ikastaroaren aldia  
**Azaroaren 4a:** hasiera eguna  
**Azaroaren 15a:** amaiera eguna (\*)  
(\* Ikastaroa irekita egongo da azterken azken egunera arte)
- 4** Aprobetxamendu-probak  
**Azaroaren 18tik 22ra**





### **Ikastarorako sarbidea**

<https://autoprestakuntza.euskadi.eus>. Ikastaroa hasi baino bi egun lehenago, mezu elektroniko bat jasoko duzu, erabiltzaile-izenarekin eta pasahitzarekin. Gogoratu ikastaroa hasten den egunera arte ez dela sarrera gaituko.

### **Prezioa**

○ 88,20€

AGINDUA, 2022ko ekainaren 20koa, Gobernantza Publiko eta Autogobernuko sailburuarena, Herri Arduralaritzaren Euskal Erakundeak ematen dituen jarduera eta zerbitzuen prezio publikoen diru-zenbatekoa ezartzen duena.(uztailaren 8ko EHAA, 132. zk.)

## 2

### **IBILBIDEA**

Hau da ikastaroaren gaiari buruzko prestakuntza-ibilbidea.



Maila aurreratuan matrikulatzeko, ezinbestekoa da bitarteko maila gainditu izana.



Oinarrizko ikastaroa

Competencia digital: 4.1 Protección de dispositivos. Nivel básico

Bitarteko maila

Competencia digital: 4.1 Protección de dispositivos. Nivel intermedio

Maila aurreratua

Fitxa honen xede den ikastaroa

## 3

### **HELBURUAK**

#### **Helburu orokorrak**

Tresna eta aplikazio digitalak erabiltzea birus, malware eta bestelako gorabeheren aurrean gailuen segurtasuna kudeatzeko, pasahitzen kudeatzaileen bidez, eta egoera bakoitzerako tresna egokiak hautatzea.

#### **Gaitasunak**

Prestakuntza-ekintza amaitzean, ikaslea gai izango da:

- Aplikazio eta webguneetan erabiltzen dituen pasahitzen segurtasuna kudeatzeko.
- Gailuen segurtasuna kudeatzeko eta jarraipena egiteko, hackeetatik eta bestelako gorabehera maltzurretatik babesteko.
- Infektatutako fitxategien gailuak garbitzeko.
- Ingurune digitalean gailuak babesteko beharrezkoak diren prebentzio-neurriak aplikatzeko.
- Arriskuak identifikatzeko eta tresna egokia hautatzeko

# 4

## PROGRAMA

### 1. MODULUA

#### Pasahitzen kudeatzaileak

1. Zer diren pasahitz seguruen kudeatzaileak eta nola funtzionatzen duten
2. Pasahitzak kudeatzeko 5 tresna onenak
  - LastPass, Dashlane, Keeper, RoboForm, RememBear
3. LastPass pasahitzen kudeatzailea eta bere funtzionaltasuna
4. Dashlane pasahitzen kudeatzailea

### 2. MODULUA

#### Babeserako eta segurtasunerako web-tresnak

1. Antibirusa, Firewalls, Antimalware eta Cleaners
2. Gailuen segurtasuna indartzeko online tresnak
  - Avast Online Security & privacy
  - Avira Web fitxategi eta URL susmagarriak aztertzeko
  - Avira Browser Safety
5. Beste tresna batzuk

#### Metodologia:

Autoprestakuntza ikastaroa, online, eta tutoretza gabekoa. Ikastaroak hainbat unitate didaktiko ditu, baita ariketa praktikoa eta hausnarketa-ariketa batzuk ere.

# 5

## EBALUAZIOA

#### Ebaluazioa

Ebaluazioaren helburua izango da ikastaroaren helburu orokorrak betetzen direla bermatzea.

Aprobetxamendu-proba 15 galderako online test bat izango da; trebetasun galderez osatua, erantzun mota desberdinak dituztenak (erantzun bakarrekoak eta praktika-simulazio itxurakoak). Proba egiteko gehienezko denbora 30 minutukoa izango da.

- Proba egiteko, hurrengo helbidean eskatu berau egiteko data, ordua eta lekua 5 eguneko epean:  
<http://www.bait.eus>
- Azterketa egiteko deialdi bakarra duzu.

#### Aprobetxamendua

Aprobetxamendu-egiaztagiria lortzeko bete beharreko baldintzak:

- Aprobetxamendu-proba gainditzea: gutxienez, 11 erantzun zuzen.

#### Ziurtagiriak

Webgunetik <http://www.bait.eus> eta edozein momentutan probaren ziurtagiria deskargatzeko aukera duzu “Erabiltzailearen historia, matrikula eta erreklamazioen kudeaketa” atalean.



Ikastaroaren aprobetxamendu-ziurtagiria eskuragarri izango duzu posta elektronikoa jakinarazpena jasotakoan. Sartu “IVAPekiko izapideak”, “Ziurtatzeak” atalean.

## 6

### OHARRAK

#### **Baldintzak**

Posta elektronikoko kontu korporatibo bat, ikastarora joango den pertsona modu unibokoan identifikatzeko. Ez dugu onartuko postu bati esleitutako edo partekatutako posta-konturik.

Datuak Babesteko Erregelamendu Orokorraren (DBEO) 5.1 d) artikuluan xedatutakoaren arabera, datu pertsonalak zehatzak izango dira, eta, behar izanez gero, eguneratuak. Hori guztia zehaztasun-printzipioa betetzeko.

#### **Eskakizun teknikoak**

- Nabigatzaileak: Microsoft Edge, Mozilla Firefox edo Chrome eguneratuak
- Interneterako konexioa, eta YouTube zerbitzuko atzipena zabalik

#### **KKDD Europako esparrua**

Konpetentzia Digitalen Europako Esparrua Euskadiko administrazio publikoetan zabaldu dadin bultzatzea, eta ikasteko modu berriak eta ziurtapen-sistemak sustatzea.

Enplegatu publiko modernoaren curriculumean funtsezkoak diren konpetentziak Europako Batzordeak ezarrita ditu; eta konpetentzia horietako bat konpetentzia digitalei lotutakoa da.

Konpetentzia Digitalen Esparruan identifikatzen eta baliozkotzen dira konpetentzia digitalaren osagai nagusiak, digitalki gai izateko ezagutza, ahalmen eta jarrera gisa ulertuta.

DIGCOMP, (Digital Competence: Identification and European-wide validation of its key components for all levels of learners) proiektua da esparru horren oinarria, eta helburua, aldiz, 21 konpetentzia digital (5 arlotan bereizita) identifikatzea da. Jakite-maila bat, bi jakite-maila edo hiru jakite-maila aurreikusi dira konpetentzia bakoitzerako.



## Eskumenen esparrua

### 1. arloa: Datuen informazioa eta datu-alfabetatzea

Konpetentziak:

- 1.1 Nabigatzea eta datuak, informazioa eta eduki digitala bilatu eta filtratzea.
- 1.2 Datuak, informazioa eta eduki digitala ebaluatzea.
- 1.3 Datuak, informazioa eta eduki digitala kudeatzea.

### 2. arloa: Komunikazioa eta lankidetzak

Konpetentziak:

- 2.1 Teknologia digitalen bidezko interakzioa.
- 2.2 Teknologia digitalak erabiliz partekatzea.
- 2.3 Teknologia digitalak erabiliz herritarrek parte hartzea.
- 2.4 Teknologia digitalen bidezko lankidetzak.
- 2.5 Netiketa: sareko portaera.
- 2.6 Identitate digitala kudeatzea.

### 3. arloa: Eduki digitala sortzea

Konpetentziak:

- 3.1 Eduki digitala garatzea.
- 3.2 Eduki digitala integratzea eta berriz lantzea.
- 3.3 Egile-eskubideak eta jabetza intelektualeko lizentziak.
- 3.4 Programazioa.

### 4. arloa: Segurtasuna

Konpetentziak:

- 4.1 Gailuen babesa.
- 4.2 Datu pertsonalen babesa eta pribatasuna.
- 4.3 Osasuna eta ongizatea babestea.
- 4.4 Ingurumena babestea.

### 5. arloa: Segurtasuna

Konpetentziak:

- 5.1 Arazo teknikoak konpontzea.
- 5.2 Beharrianak identifikatzea eta konponbide teknologikoak ematea.
- 5.3 Teknologia digitalaren erabilera sortzea.
- 5.4 Konpetentzia digitaleko gabeziak identifikatzea.

## Azalpen bideoa

[Konpetentzia digitalak](#)

## Laguntza

Laguntza teknikoa behar izanez gero:

- Deitu CAUko telefono zenbakira (945016) 440
- Astelehenetik ostiralera 08:00etatik 20:00etara

Probaren funtzionamenduari buruz laguntza behar izanez gero:

- Deitu hurrengo telefono-zenbaki honetara 664110557 / 664101155
- Astelehenetik ostegunera 09:00etatik 18:30era. Ostiraletan 09:00etatik 16:00etara.

Aministrazio-gaiekin lotutako kontsultak egiteko: [prestakuntza@ivap.eus](mailto:prestakuntza@ivap.eus)

## COMPETENCA DIGITAL 4.1 PROTECCIÓN DE DISPOSITIVOS. NIVEL AVANZADO

### 1 INFORMACIÓN GENERAL

- Área formativa TIC (Tecnología de la Información y Comunicación)
- Modalidad Online
- Idioma Castellano
- Duración 10 horas

#### Dirigido a

Personas empleadas en las diferentes Administraciones Públicas de la Comunidad Autónoma de Euskadi.

#### Calendario

- 1** Último día de solicitud  
**4 de octubre:** Administración General (\*)  
**11 de octubre:** otras administraciones  
(\*) Período de VºBº del 7 al 11 de octubre
- 2** Aviso de bajas  
**Hasta el 31 de octubre**
- 3** Fechas curso  
**4 de noviembre:** inicio  
**15 de noviembre:** fin (\*)  
(\*) El curso permanecerá abierto hasta el último día del plazo de exámenes
- 4** Pruebas de aprovechamiento  
**Desde el 18 al 22 de noviembre**





### **Acceso curso**

<https://autoprestakuntza.euskadi.eus>. Dos días antes del inicio del curso recibirás un correo electrónico con el nombre de usuario/a y la contraseña. Recuerda que el acceso no se habilitará hasta el primer día de inicio del curso.

### **Precio**

○ 88,20€

ORDEN de 20 de junio de 2022, del Consejera de Gobernanza Pública y Autogobierno, por la que se fija la cuantía de los precios públicos de las actividades y servicios que presta el Instituto Vasco de Administración Pública.(BOPV nº 132, de 8 de julio)

## 2

### **ITINERARIO**

Este es el itinerario formativo sobre la temática del curso.



Para matricularse en el nivel avanzado es imprescindible haber superado el nivel intermedio

- Nivel básico Competencia digital: 4.1 Protección de dispositivos. Nivel básico.
- Nivel intermedio Competencia digital: 4.1 Protección de dispositivos. Nivel intermedio
- Nivel avanzado Curso objeto de esta ficha.

## 3

### **OBJETIVOS**

#### **Objetivos generales**

Proteger los dispositivos y el contenido digital y comprender los riesgos y las amenazas en entornos digitales. Saber acerca de medidas de protección y seguridad y tener debidamente en cuenta la fiabilidad y la privacidad.

#### **Competencias**

Al finalizar la acción formativa el alumnado será capaz de:

- conocer maneras sencillas de proteger los dispositivos y el contenido digital
- diferenciar riesgos y amenazas simples en entornos digitales
- aplicar medidas de seguridad sencillas configurando políticas de seguridad y privacidad

# 4

## PROGRAMA

### MÓDULO I

#### Gestores de contraseñas

1. Qué son los gestores de contraseñas seguras y cómo funcionan.
2. El top de los 5 gestores de contraseñas.
  - LastPass, Dashlane, Keeper, RoboForm, RememBear
3. Gestor de contraseñas LastPass y sus funcionalidades
4. Qué es Dashlane

### MÓDULO II

#### Herramientas Web de protección y seguridad

1. Antivirus, Firewalls, Antimalware y Cleaners
2. Herramientas on line para reforzar la seguridad de los dispositivos
  - Avast Online Security & privacy
  - Avira Web para analizar archivos y URL sospechosas
  - Avira Browser Safety
3. Otras herramientas

#### Metodología:

Curso de autoformación online sin tutoría. El curso consta de varias unidades didácticas así como ejercicios prácticos y de reflexión.

# 5

## EVALUACIÓN

#### Evaluación

El Objetivo de la evaluación será garantizar el cumplimiento de los objetivos generales del curso.

La prueba de aprovechamiento será un test online de 15 preguntas de habilidad, con distintos tipos de respuesta (única opción y de simulación práctica). El tiempo máximo para realizar la prueba será de 30 minutos.

- Para realizar la prueba tiene que solicitar fecha, lugar y hora dentro del plazo de 5 días, en la siguiente dirección: <http://www.bait.eus>
- Solo existe una única convocatoria de examen.

#### Aprovechamiento

Requisitos a cumplir para lograr el Certificado de aprovechamiento:

- Superar la prueba de aprovechamiento; al menos 11 respuestas correctas





### **Certificados**

El certificado de la prueba se lo podrá descargar en cualquier momento desde el “Historial de usuario, gestión de matrículas y reclamaciones” de la página de <http://www.bait.eus>

El certificado de aprovechamiento del curso, estará a su disposición una vez que reciba la notificación en su correo electrónico. Acceda a “Trámites con el IVAP” apartado “Certificaciones”.

## **6**

## **OBSERVACIONES**

### **Requisitos**

Una cuenta de correo electrónico corporativo que identifique unívocamente a la persona asistente al curso. No admitiremos cuentas de correo compartidas o asignadas a un puesto.

Conforme a lo dispuesto en el artículo 5.1 apartado d) del Reglamento General de Protección de Datos (RGPD), los datos personales serán exactos y, si fuera necesario, actualizados. Todo ello en cumplimiento del principio de exactitud.

### **Requisitos técnicos**

- Navegador: Microsoft Edge, Mozilla Firefox ó Chrome actualizados
- Conexión a Internet y acceso a YouTube

### **Marco Europeo de competencias digitales**

Promover la difusión en las administraciones públicas de Euskadi el Marco Europeo de Competencias Digitales, e impulsar nuevas formas de aprendizaje y sistemas de certificación.

La Comisión Europea establece las competencias clave en el curriculum del trabajador empleado público moderno, entre las que se encuentran las competencias digitales.

El Marco de Competencias Digitales identifica y valida los componentes clave de la competencia digital en términos de los conocimientos, habilidades y actitudes necesarias para ser digitalmente competente.

Este marco, desarrollado sobre la base del proyecto DIGCOMP, (Digital Competence: Identification and European-wide validation of its key components for all levels of learners) es un proyecto dirigido a identificar las 21 competencias digitales divididas en 5 áreas. Para cada competencia, hay uno, dos o tres niveles de dominio previstos.





## Marco competencial

### Área 1: Información y alfabetización de datos

#### Competencias:

- 1.1 Navegar, buscar y filtrar datos, información y contenido digital.
- 1.2 Evaluar datos, información y contenido digital.
- 1.3 Gestionar datos, información y contenido digital.

### Área 2: Comunicación y colaboración

#### Competencias:

- 2.1 Interactuar a través de tecnologías digitales.
- 2.2 Compartir a través de tecnologías digitales.
- 2.3 Participación ciudadana a través de tecnologías .
- 2.4 Colaborar a través de tecnologías digital.
- 2.5 Netiqueta: comportamiento en la red.
- 2.6 Gestionar la identidad digital.

### Área 3: Creación de contenido digital

#### Competencias:

- 3.1 Desarrollo de contenido digital.
- 3.2 Integración y reelaboración de contenido digital.
- 3.3 Derechos de autor y licencias de propiedad intelectual.
- 3.4 Programación.

### Área 4: Seguridad

#### Competencias:

- 4.1 Protección de dispositivos.
- 4.2 Protección de datos personales y privacidad.
- 4.3 Protección de salud y bienestar.
- 4.4 Protección del entorno.

### Área 5: Resolución de problemas

#### Competencias:

- 5.1 resolución de problemas técnicos.
- 5.2 Identificación de necesidades y respuestas tecnológicas.
- 5.3 Uso creativo de la tecnología digital.
- 5.4 Identificación de brechas en la competencia digital.

## Vídeo explicativo

### Competencias digitales

## Ayuda

En caso de necesitar asistencia técnica:

- póngase en contacto con el CAU en el (945016) 440
- de lunes a viernes de 08:00 a 20:00

En caso de necesitar asistencia sobre el funcionamiento de la prueba:

- póngase en contacto en el 664110557 ó 664101155
- de lunes a jueves de 09:00 a 18:30. Viernes de 09:00 a 16:00

Contacto: [prestakuntza@ivap.eus](mailto:prestakuntza@ivap.eus)