Términos y Condiciones del programa CyberSkills. Formación en ciberseguridad para personas en situación de desempleo.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. OBJETIVOS 3
2. DESTINATARIOS 6
3. CARACTERISTICAS DEL PROGRAMA Y SUS PLAZAS DISPONIBLES 7
4. GESTIÓN 13
5. PROCESO DE SELECCIÓN Y ASIGNACION DE PLAZAS ENTRE CANDIDATOS 14
6. FISCALIDAD DEL PROGRAMA ..... ¡Error! Marcador no definido.
7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 15
8. MODIFICACIÓN DE LOS TÉRMINOS Y CONDICIONES DEL PROGRAMA. 17

1. OBJETIVOS

Fundación Universia con N.I.F. G-84545409 y domicilio social en Avda. de Cantabria s/n, Boadilla del Monte, Madrid (la "Fundación", en lo sucesivo), en colaboración con el S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A. (en adelante "INCIBE"), otorga el programa "CyberSkills. Formación en ciberseguridad para personas en situación de desempleo", Segunda Convocatoria, para la concesión de plazas gratuitas en cursos a personas que se encuentren en situación de demandante de empleo, la cual les permitirán mejorar sus competencias en ciberseguridad con el fin de aumentar su empleabilidad en el mercado laboral (el "**Programa**").

Este Programa ha sido diseñado y desarrollado por FUNDACIÓN UNIVERSIA en colaboración con INCIBE en el marco del «Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU».

El objetivo del programa "CyberSkills. Formación en ciberseguridad para personas en situación de desempleo", Segunda Convocatoria, es la concesión de plazas gratuitas en cursos, por parte de FUNDACIÓN UNIVERSIA, que permitirán a las personas demandantes de empleo mejorar sus competencias en ciberseguridad con el fin de aumentar su empleabilidad en el mercado laboral.

La financiación del Programa queda enmarcada en las siguientes líneas y componentes incluidos en el Plan de Recuperación Transformación y Resiliencia, concretamente:

- Línea directriz del plan: Transformación digital.
- Política (Palanca): VII - Educación y conocimiento, formación continua y desarrollo de capacidades.
- El Plan nacional de capacidades digitales se integra en la Agenda Digital España 2025, como línea estratégica para reforzar las competencias digitales de los trabajadores y del conjunto de la ciudadanía, reduciendo el porcentaje de la población española que carece de competencias digitales básicas. El plan se organiza en cuatro ejes que a su vez se dividen en siete líneas de actuación:
  - Competencias digitales transversales:
    - Capacitación digital para la ciudadanía (con énfasis en colectivos en riesgo de exclusión digital).
    - Lucha contra la brecha digital de género.
  - Transformación Digital de la Educación:
    - Digitalización de la Educación y desarrollo de las competencias digitales para el aprendizaje en la educación.
  - Competencias digitales para el empleo:
    - Formación en competencias digitales para personas desempleadas y ocupadas del sector privado, con especial énfasis en jóvenes desempleados.
    - Formación en competencias digitales para las personas al servicio de las administraciones públicas.

- Desarrollo de competencias digitales para las pequeñas y medianas empresas (pymes) para que afronten con garantías de éxito sus procesos de transformación digital adaptándose a la nueva economía digital.

- Profesionales digitales:
  - Fomento de especialistas TIC, Tecnologías de la Información y Comunicaciones (titulados de Formación Profesional).

- Inversión 4: "Profesionales digitales". Adaptar la oferta formativa de formación profesional existente y diseñar nuevas especialidades que permitan adquirir competencias digitales avanzadas e impulsar un programa de atracción y retención de talento en el ámbito digital. Creación de Recursos Educativos Abiertos para la enseñanza con medios digitales en inteligencia artificial, ciberseguridad... a distintos niveles, desde la ciudadanía en general hasta perfiles más específicos (y complejos).

Asimismo, la justificación presupuestaria se enmarca en las siguientes líneas y componentes incluidos en el Plan de Recuperación Transformación y Resiliencia, concretamente:

- Línea directriz del plan: Transformación digital.
- Componente 15: Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G.
- Inversión 7: Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMEs y profesionales; e Impulso del ecosistema del sector" como una de las actuaciones concretas orientadas a desarrollar las capacidades de ciberseguridad tanto de ciudadanos como empresas y al impulso del ecosistema de ciberseguridad español en el marco de la estrategia de soberanía digital europea.
- Eje 2: Impulso de la Industria.
- Pilar 3: Programas de Aceleración (por Comunidades Autónomas) para el crecimiento de startups con proyecto ciber.

De conformidad con el artículo 9 del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, los proyectos que se financien con cargo al Mecanismo de Recuperación y Resiliencia (actualmente PRTR) solo podrán recibir financiación de otros programas e instrumentos de la Unión siempre que dicha financiación no cubra el mismo coste.

Etiquetado digital: INCIBE, en sus indicadores asociados al C15.I07 debe cumplir, de acuerdo con el DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN: Análisis del plan de recuperación y resiliencia de España que acompaña a la Propuesta de Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España, un coeficiente concreto de contribución a la transición digital (021quinquiles), que se corresponde con una contribución del 100% a través de todas sus actuaciones. De acuerdo con el REGLAMENTO (UE) 2021/241 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, eso supone que todas las actuaciones deben explícitamente desarrollar y desplegar tecnologías, medidas e

instalaciones de apoyo en materia de ciberseguridad para los usuarios de los sectores público y privado a través de las actividades contempladas en este convenio.

Etiquetado verde: INCIBE no tiene obligaciones respecto a la contribución a los objetivos climáticos, tal y como indica el DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN: Análisis del plan de recuperación y resiliencia de España que acompaña a la Propuesta de Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España, concretamente en la página 126.

En el cálculo de los hitos y objetivos propuestos en este componente, no se computarán las inversiones realizadas con otros fondos de la Unión Europea.

Consecuentemente, para garantizar de forma efectiva la contribución al cumplimiento de los hitos CID 245 y CID 248, es necesario evitar del todo la cofinanciación europea en el ámbito de las presentes actuaciones.

2. DESTINATARIOS

Podrán ser beneficiarios de este Programa las personas demandantes de empleo que sean españolas o residentes en España que, además, satisfagan los criterios de selección previstos más adelante.

Este Programa ha sido diseñado y desarrollado por FUNDACIÓN UNIVERSIA, en colaboración con INCIBE en el marco del «Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU» con la finalidad de fomentar la inclusión socio-laboral de las personas pertenecientes a colectivos infrarrepresentados, en concreto, para aquellas personas demandantes de empleo.

La obtención de una plaza gratuita en los cursos de formación del Programa será compatible con la de otro tipo de financiación o beca de carácter asistencial de naturaleza distinta a la del objeto de este Programa, cualquiera que sea su origen público o privado, a las que pueda acceder el estudiante que realice la práctica al amparo del mismo.

3. CARACTERISTICAS DEL PROGRAMA Y SUS PLAZAS DISPONIBLES

El programa consistirá en la concesión de hasta 180 plazas para la realización de un curso online, de las cuales 90 plazas corresponden a la modalidad Red Team y 90 plazas a la modalidad Blue Team que se desarrollará de acuerdo con los detalles que se muestran a continuación:

CyberSkills. Formación en ciberseguridad para personas en situación de desempleo.

El Programa tendrá formato curso online y se impartirá en español en una plataforma de aprendizaje (Google Workspace (Classroom, y Meet), Slack u otras específicas para cada módulo) (la "Plataforma de Aprendizaje"). El curso se iniciará el día 19 de mayo de 2025 y tendrá una duración de 250 horas.

Requisitos de admisión:

Los requisitos que tendrán que cumplir los solicitantes, de forma cumulativa, para su admisión serán:

i. **Acreditar la situación como demandante de empleo o mejora de empleo, (tanto en el momento de inscripción como al inicio del curso)**

ii. Ser mayor de edad.

iii. Tener nacionalidad española o ser residente en España

iv. Aportar un currículum vitae actualizado.

v. Ser usuario en la plataforma Santander Open Academy (www.santanderopenacademy.com) y encontrarse inscrito en la convocatoria correspondiente del Programa.

.

vii. Superar un test sobre competencias, habilidades y conocimientos, a realizar por el gestor de la Plataforma de Aprendizaje, (la entidad "BRIDGE EDUCATION S.L."), a los efectos de seleccionar a los candidatos que podrán optar al Programa.

viii. Superar una entrevista con Fundación Universia en la que se evaluará la disponibilidad e interés del candidato para cursar la formación.

Para la asignación de las plazas, los candidatos deberán aportar la siguiente documentación telemáticamente, mediante la plataforma Santander Open Academy, en formato Word (.doc) o Adobe Acrobat (.pdf):

- **Currículum Vitae actualizado**, indicando datos personales y de contacto, formación, formación complementaria, experiencia profesional, actividades de

voluntariado y/o conocimientos de idiomas y digitales. Este documento debe estar en castellano.

- **Documento Nacional de Identidad** en vigor .
- **Certificado de situación de desempleo en vigor**.

Criterios de selección:

Para la asignación de las -plazas, Fundación Universia considerará y evaluará los siguientes criterios de selección:

i. Fase 1: Entrevista realizada con Fundación Universia, donde se valorará el interés y la disponibilidad del candidato para participar en el Programa.

ii. Fase 2: El resultado del test sobre competencias, habilidades y conocimientos, puesto a disposición en la Plataforma de Aprendizaje por el gestor de la misma (la entidad "BRIDGE EDUCATION S.L.").

Para la asignación de una modalidad u otra del curso, Fundación Universia considerará y tendrá en cuenta los siguientes factores:

I. Las preferencias mostradas por el candidato.

II. Las plazas disponibles en cada modalidad.

El contenido del curso será el siguiente:

Se proponen dos modalidades formativas a fin de formar a expertos en el ámbito de la ciberseguridad tanto en el ámbito defensivo como en el ofensivo.

- La modalidad **Red Team** (250 horas) consta de:

  Unidad 1: Ramp-up (45 horas): Esta primera unidad permitirá obtener los conocimientos básicos de hardware y virtualización de equipos además de la utilización de sistemas operativos GNU/Linux y Windows. Se realizarán instalaciones y configuraciones de máquinas virtuales además de profundizar en la arquitectura y utilización de sistemas operativos Windows 10 y Kali Linux: Estructuras de directorios, terminales, comandos fundamentales, edición de archivos, etc.

  - Módulo 1: Fundamentos de Hardware y sistemas operativos: hardware y virtualización, manejo básico de sistemas GNU/Linux y comparativa con sistemas Windows.
  - Módulo 2: Fundamentos de programación: programación interactiva: programación Shell, introducción a HTML e introducción a JavaScript.
  - Módulo 3: Fundamentos de redes y comunicaciones: conceptos básicos de redes, conceptos básicos de TCP/IP, paquete, socket, servicio y puerto. Modo monitor, captura de tráfico y hardware de red.
  - Módulo 4: Fundamentos de criptografía: bases teóricas de criptografía, CIA, diferencias entre cifrar y codificar, principios de Kerckhoffs, cifrado clásico y moderno, comparativa de tipos de cifra, codificación, función hash, PKI y CA, cifrado híbrido en HTTP's y TLS y SSL en detalle.

- Módulo 5: introducción a la seguridad informática: amenazas, ataques y vulnerabilidades. Red Team, Blue Team y Purple Team. Metodologías de ataque.

Unidad 2: Seguridad Ofensiva (205 horas): Este bloque se centra en obtener los conocimientos necesarios para recabar información de manera pasiva respecto al objetivo seleccionado (Fase 1 de un test de penetración). Para ello realizaremos una clasificación entre tipos de perfiles, utilizaremos herramientas y aplicaciones que nos permitan recopilar información de fuentes públicas de datos, infraestructura tecnológica utilizada y redes sociales. Una vez recopilada esta información crearemos un informe que nos ayudará a realizar la toma de decisiones respecto a sucesivas estrategias de ataque a seguir posteriormente.

- Módulo 1: Análisis del objetivo: ¿Qué es el análisis de objetivo? Localización dentro de las fases de un test de intrusión. Open Web vs Deep Web vs Dark Web. Fuentes deinformación básicas disponibles en Open Web ¿Qué es OSINT? Fases de un proyecto de OSINT Clasificación de objetivos. Tipos de perfiles. Herramientas Online, Herramientas Linux y Buscadores. Concepto de metadatos, creación de perfiles ficticios para investigación, aplicaciones para OSINT.
- Módulo 2: Ataques e infraestruturas de sistemas de redes: análisis de sistemas com NMap, análisis de vulnerabilidades y captura de tráfico.
- Módulo 3: ataques externos – aplicaciones web: Protocolo HTTP. Métodos GET y POST, principales Frameworks Web, herramientas propias de Seguridad Web, técnicas y ataques web y Webshells.
- Módulo 4: ataques a aplicaciones móviles: aplicaciones móviles (análisis estático, dinámico, certificate pinning y evasión de medidas antiroot).
- Módulo 5: ataques a redes wireless: Conceptos básicos Wifi: Protocolos, Tipos de redes y arquitectura Redes WiFi WEP, WPA y WPA2 Frecuencias y canales Canales WiFi y Frecuencias Ataques sobre redes WiFi: Redes abiertas: Análisis del tráfico de la red Guía de usuario de Wireshark DNS Tunelling. Tutorial DNS Tunelling Crackeando Redes WEP. Ataques estadísticos mediante aircrack. Crackeando redes WEP. Crackeando WPA. Captura de handshake. Crackeando redes WPA. Ataques de fuerza bruta mediante diccionario. Tutorial Aircrack y Hashcat. Creación de puntos de acceso falsos. Tutorial de Airbase. Tutorial de hostapd-wpe. Herramientas comerciales (Pineapple WiFi / FruityWiFi) WiFi Pineapple.
- Módulo 6: explotación y post-explotación: Iniciación a frameworks de explotación y bases de datos de exploits, conceptos interesantes de exploiting, Iniciación en la explotación de vulnerabilidades, vulnerabilidades comunes de Windows, ejemplos de vulnerabilidades, obtención de contraseñas en los servicios identificados con Hydra y Patator.
- Módulo 7: Evaluación de privilegios: iniciación de la escalada de privilegios, escalada de privilegios con Metasploit, Incorrecta gestión de permisos, escalada de privilegios atacando el fichero passwd, explotando ficheros con SETUID y SETGID, análisis de ficheros con información sensible en el sistema, escaladas de privilegios mediante ficheros con información

sensible, herramientas / Scripts para la enumeración de configuraciones vulnerables, checklist escalada de privilegios en Linux, checklist escalada de privilegios en Windows, Herramienta de enumeración para Linux, herramienta de enumeración para Windows, escalada de privilegios avanzada.

- Módulo 8: Evasión de defensas: Fundamentos genéricos del funcionamiento de medidas antivirus convencionales y sistemas de detección de intrusiones, enmascaramiento y packing de payloads para evasión de antivirus, ofuscación de información / payloads, borrado de huellas y persistencia.
- Módulo 9: Reconocimiento interno y movimientos laterales: Volcado de credenciales almacenadas del sistema, volcado de credenciales almacenadas de navegadores, ataques de red: MiTM (Responder), uso de Responder, responder cheatsheet, técnicas de reutilización de credenciales comprometidas, pass the hash, pass the ticket con Mimikatz, uso y manejo de CrackMapExec, movimientos laterales con CrackMapExec y pivoting.

- La modalidad **Blue Team** (250 horas) consta de:

  Unidad 1: Ramp-up (45 horas): Esta primera unidad permitirá obtener los conocimientos básicos de hardware y virtualización de equipos además de la utilización de sistemas operativos GNU/Linux y Windows. Se realizarán instalaciones y configuraciones de máquinas virtuales además de profundizar en la arquitectura y utilización de sistemas operativos Windows 10 y Kali Linux: Estructuras de directorios, terminales, comandos fundamentales, edición de archivos, etc…

  - Módulo 1: Fundamentos de Hardware y sistemas operativos: hardware y virtualización, manejo básico de sistemas GNU/Linux y comparativa con sistemas Windows.
  - Módulo 2: Fundamentos de programación: programación interactiva: programación Shell, introducción a HTML e introducción a JavaScript. Módulo 3: Fundamentos de redes y comunicaciones: conceptos básicos de redes, conceptos básicos de TCP/IP, paquete, socket, servicio y puerto. Modo monitor, captura de tráfico y hardware de red.
  - Módulo 4: Fundamentos de criptografía: bases teóricas de criptografía, CIA, diferencias entre cifrar y codificar, principios de Kerckhoffs, cifrado clásico y moderno, comparativa de tipos de cifra, codificación, función hash, PKI y CA, cifrado híbrido en HTTP's y TLS y SSL en detalle.
  - Módulo 5: introducción a la seguridad informática: amenazas, ataques y vulnerabilidades. Red Team, Blue Team y Purple Team. Metodologías de ataque.

Unidad 2: Seguridad Defensiva (205 horas): Con este módulo introduciremos los sistemas SIEM, sus características y ciclo de vida, y veremos algunas soluciones de mercado. Además, veremos las tareas fundamentales de los equipos Blue Team. Se preparará a los alumnos para saber responder ante posibles incidentes, así como para llevar a cabo el análisis forense en evidencias digitales.

- Módulo 1: Sistemas de información de seguridad y gestión de eventos (SIEM): explicación teórica genérica de los conceptos a desarrollar, ejercicios técnicos para comprender el funcionamiento básico de un SIEM, ejercicios relacionados con la carga de logs y montaje de un laboratorio.
- Módulo 2: Protección de activos: Protección de activos, protección en sistemas Windows, protección en sistemas Linux, protección para servicios críticos. Guias de bastionado CIS Firewalls Web Application Firewalls (WAF).
- Módulo 3: Detección y respuesta ante incidentes: Identificación de amenazas, monitorización en sistemas Windows y monitorización en sistemas Linux
- Módulo 4: Análisis forense: Fundamentos generales del procedimiento de análisis forense en una evidencia digital, estudio de los sistemas de ficheros más utilizados: NTFS, FAT32 y EXT4, fundamentos y metodología de adquisición de evidencias digitales: Cadena de custodia. Definición y análisis de los artefactos principales en sistemas Windows, definición y análisis de los artefactos principales en sistemas Linux, análisis forense del tráfico de red y principios y metodología para la redacción legal de informes.
- Módulo 5: Conceptos básicos de análisis de malware, introducción al lenguaje ensamblador, análisis estático y dinámico y técnicas AntiVM / AntiDebug. En cada módulo, el alumno deberá realizar un proyecto que le permita poner en prácticas los conocimientos adquiridos durante el desarrollo de los mismos.

Skills y/o aprendizajes obtenidos tras el Programa

- Red team: El bootcamp de Hacking Ético de The Bridge proporciona los conocimientos necesarios para convertirse en un miembro de un Red team (atacante)
- Blue team: El bootcamp de ciberseguridad Defensiva de The Bridge proporciona los conocimientos necesarios para convertirse en un miembro de Blue team (defensor)

Fundación Universia será el encargado de seleccionar a los admitidos en base al cumplimiento de los anteriores requisitos y conforme a sus habilidades y competencias técnicas.

Asimismo, en el supuesto de que existieran plazas asignadas que no hayan sido aceptadas por los participantes, Fundación Universia podría asignar las plazas a otros participantes que cumplan con los requisitos de admisión anteriormente señalados u otros adicionales

que Fundación Universia tenga a bien considerar con el objetivo de que las plazas no quedaran desiertas.

Para la obtención de una plaza en el Programa que permita realizar el curso, será condición ineludible:

Fase 1:

1. Inscribirse en la convocatoria del Programa a través de la plataforma Santander Open Academy habilitada a dichos efectos www.santanderopenacademy.com. La notificación de la concesión de la plaza será comunicada a través del sistema de gestión habilitado en la referida plataforma.

En su inscripción en la convocatoria, los solicitantes deberán aportar la documentación enumerada en el apartado ”3. Características del Programa y sus plazas disponibles", de las presentes bases.

4. GESTIÓN

Para la obtención de una plaza en el Programa que permita realizar el curso, será condición ineludible inscribirse en la convocatoria del Programa a través de la plataforma Santander Open Academy habilitada a dichos efectos www.santanderopenacademy.com. La notificación de la concesión de la plaza será comunicada a través del sistema de gestión habilitado en la referida plataforma.

La inscripción de los candidatos deberá realizarse entre el 10 de marzo de 2025 y el 30 de abril de 2025 a las 23:59 GMT+1 (zona horaria Madrid), sin perjuicio de que Fundación Universia pueda modificar los plazos.

En su inscripción en la convocatoria, los solicitantes deberán aportar la documentación enumerada en el apartado ”3. Características del Programa y sus plazas disponibles", de las presentes bases.

5. PROCESO DE SELECCIÓN Y ASIGNACION DE PLAZAS ENTRE CANDIDATOS

El proceso de selección se realizará entre el **01 de mayo y el 08 de mayo de 2025**, ambos inclusive.

Tal asignación se comunicará al participante **09 de mayo de 2025** quien dispondrá del plazo de **7 días naturales** desde la fecha y hora de la comunicación para cursar su aceptación, todo ello a través de la página web www.santanderopenacademy.com.

Terminado el plazo, en el supuesto de que existieran plazas asignadas que no hayan sido aceptadas por los participantes, Fundación Universia asignará las plazas a otros participantes que cumplan con los requisitos de admisión anteriormente señalados u otros adicionales que Fundación Universia tenga a bien considerar con el objetivo de que las plazas no quedaran desiertas. Todas las plazas deberán estar asignadas para el **19 de mayo de 2025**.

Para que una plaza se considere adjudicada, el seleccionado deberá aceptar el *check* correspondiente a la aceptación de la plaza en la plataforma Santander Open Academy.

6. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El Responsable del tratamiento de los datos de los usuarios (en adelante, el "Usuario" o los "Usuarios") para la concesión y la gestión del programa (en adelante, el "Programa") al cual te has inscrito a través de la plataforma de Santander Open Academy es Fundación Universia (en adelante, la "Institución") domiciliada en Avenida Cantabria s/n, Edificio Amazonia, Planta Baja Boadilla del Monte (Madrid) y con contacto del Delegado de Protección de Datos: dpo@universia.net, la cual solo será responsable del tratamiento de los datos personales de sus propios estudiantes.

Datos que tratamos y procedencia de los mismos.

La Institución obtiene los datos de los Usuarios que se inscriban en el presente Programa de la plataforma Santander Open Academy, cuyo responsable del tratamiento es Universia Holding, SL, en lo referido a la participación en este Programa. Estos datos son: nombre, apellidos, país de residencia, e-mail, fecha de nacimiento y datos relativos a la navegación y uso del Portal (éstos últimos únicamente en lo que pudiera aplicar puesto que el proceso se gestiona por la Institución a través de la plataforma Santander Open Academy).

Asimismo, la Institución incluirá en la convocatoria del presente Programa las preguntas y las solicitudes de información necesarias para acreditar, evaluar y gestionar la candidatura del Usuario. En este sentido, podrá tratar: datos identificativos, datos relativos características personales, datos académicos y profesionales, datos relativos al empleo, y datos relativos a la personalidad (estos últimos en relación con la evaluación que pudiera hacer la Institución de los Usuarios para el Programa).

Finalidades para las que se tratarán los datos personales.

Los datos de los Usuarios que se recaben a razón del presente Programa serán tratados para gestionar la presente convocatoria, evaluar a los candidatos y en su caso, conceder o denegar las plazas objeto del presente Programa. La base legitimadora que permite el referido tratamiento es la ejecución de las presentes Condiciones Particulares o Bases Legales.

Asimismo, la Institución podrá tratar adicionalmente los datos de los candidatos y beneficiarios para dar cumplimiento a las obligaciones legales que les exija la legislación vigente, siendo por tanto la base legitimadora de este tratamiento el cumplimiento de una obligación legal.

Destinatarios de los datos personales.

Los datos personales de los Usuarios únicamente se comunicarán a las autoridades y organismos públicos para el desarrollo de sus funciones cuando sean competentes para solicitarlos. En algunas ocasiones, la normativa aplicable exige compartir información con autoridades u organismos públicos para que puedan desarrollar sus funciones. Por ejemplo, autoridades fiscales o tribunales de justicia, que utilizarían los datos de los Usuarios para sus propios fines.

Asimismo, para el adecuado desarrollo del Programa los datos personales de los Usuarios serán compartidos con **S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P.,S.A.** (en adelante, el "Promotor") que lo ha patrocinado, promovido o

financiado con el fin de que el Programa pueda llevarse a cabo. Y, en último lugar con la Institución donde el Usuario cursa el programa con **BRIDGE EDUCATION S.L.**

Criterios de Conservación de los datos personales.

Los datos que se recojan a razón de esta convocatoria podrán ser conservados por la Institución de la siguiente manera:

- Respecto a los Usuarios postulantes que no se admitan en el Programa, los datos se conservarán durante el tiempo de gestión de la convocatoria y posteriormente durante el plazo para realizar los trámites necesarios hasta el cierre de la misma.
- Respecto a los Usuarios postulantes admitidos en el Programa, los datos se conservarán durante todo el periodo vinculado a la gestión de la convocatoria, se incorporarán si procede al expediente del estudiante en la Institución y se conservarán con finalidades de acreditación y certificación de la concesión y de cualquier otro mérito académico relacionado.

Los Usuarios tienen derecho a acceder a sus datos, así como a solicitar la rectificación de los datos inexactos, oponerse a su tratamiento, la limitación en su tratamiento, la portabilidad de sus datos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos, así como a no ser objeto de decisiones individuales automatizadas. Asimismo, los usuarios tienen el derecho a retirar su consentimiento para aquellas finalidades que lo otorgaron en cualquier momento.

Los usuarios podrán dirigirse a dpo@universia.net para el ejercicio de sus derechos o en su caso mediante correo postal en Avenida De Cantabria, S/n, Edificio Amazonia, Planta Baja. 28660, Boadilla Del Monte (Madrid), España.

No obstante, se recomienda la lectura de la Política de Privacidad disponible en la plataforma (www.santanderopenacademy.com/es/legal/privacy) para una mayor comprensión.

7. MODIFICACIÓN DE LOS TÉRMINOS Y CONDICIONES DEL PROGRAMA

El hecho de concurrir a la presente Convocatoria del Programa supone la aceptación por el participante de sus Términos y Condiciones y de su resolución, que será inapelable, así como la renuncia a cualquier tipo de reclamación sobre cualquier aspecto previsto en los mismos, sin ánimo de ser exhaustivos, aspectos tales como los criterios de asignación, selección y admisión.

Fundación Universia se reserva el derecho de modificar o rectificar cualesquiera de los Términos y Condiciones de la Convocatoria del Programa, parcial o totalmente en cualquier momento, pudiendo incluso suspender, posponer o cancelar la misma, atendiendo a una causa objetiva y debidamente justificada, y con la finalidad de preservar el impacto social que las Partes persiguen con la presente Convocatoria. En todo caso, se informará a los candidatos acerca de las modificaciones o rectificaciones introducidas a través de la página web www.santanderopenacademy.com