CONVENIO ENTRE EL CENTRO DOCENTE C.P.I.F.P. Alan Turing Y LA EMPRESA Agencia Digital de Andalucía PARA LA REALIZACIÓN DE LA FASE DE FORMACIÓN EN EMPRESAS U ORGANISMOS EQUIPARADOS DE LAS ENSEÑANZAS DE FORMACIÓN PROFESIONAL

Convenio de colaboración nº: 290202312024035.
En Campanillas (Málaga) a 17 de febrero de 2025, a la fecha de la firma digital.

REUNIDOS

D./Dña Miguel Ángel Domínguez Gómez, con DNI [redacted] como director/a del centro docente C.P.I.F.P. Alan Turing, con código 29020231, con sede en Campanillas, provincia de Málaga, de calle Frederick Terman, 3, CP 29590, Teléfono 951040449, e-mail del centro docente 29020231.edu@juntadeandalucia.es, 29020231@g.educaand.es, en adelante referido como "el centro docente".
En virtud de su nombramiento y de conformidad con lo recogido en la Orden de 29 de abril de 2024, por la que se aprueba el modelo de convenio tipo de colaboración para la realización de la fase de formación en empresas u organismos equiparados de las enseñanzas de formación profesional.

Y de otra parte, D./Dña. Raúl Jiménez Jiménez, con N.I.F. [redacted], en calidad de Representante legal, actuando como representante legal de Agencia Digital de Andalucía, con sede en Sevilla, provincia de Sevilla, Calle Juan Antonio de Vizarron, 41092, teléfono _____, e-mail _____, en adelante referida como "la entidad colaboradora".

Ambas partes se reconocen mutua y recíprocamente capacidad jurídica y de obrar suficiente para otorgar el presente convenio, actuando en el ejercicio de la representación que ostentan.

EXPONEN

Primero.- Que la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional, tiene por objeto la constitución y ordenación de un sistema único e integrado de formación profesional que se desarrollará mediante una distribución adecuada de los procesos formativos entre los centros de formación profesional y las empresas u organismos equiparados, contribuyendo ambos al logro de las competencias previstas en cada oferta de formación.

Segundo.- Que ambas partes manifiestan su interés en colaborar en la formación del alumnado de Formación Profesional, facilitando plazas formativas para la realización de la fase de formación en empresas u organismos equiparados de los ciclos formativos y cursos de especialización, que permita completar la adquisición de competencias profesionales y resultados de aprendizaje propios de cada oferta formativa, conocer la realidad del entorno laboral del sector productivo o de servicios de referencia, afianzar habilidades permanentes para la empleabilidad vinculadas a la profesión que requieren situaciones reales de trabajo y facilitar una experiencia de inserción y relacional en entorno de trabajo.

Tercero.- Que el objeto de este convenio es establecer la colaboración entre los centros de formación profesional y las empresas u organismos equiparados para el desarrollo de la fase de formación del alumnado que cursa enseñanzas oficiales de formación profesional en los ciclos formativos y cursos de especialización en la Comunidad Autónoma de Andalucía.

Cuarto.- Que la fase de formación en empresa u organismo equiparado está establecida por la Ley Orgánica 3/2022, de 31 de marzo, y regulada por el Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional, sin perjuicio de aplicar a todos los efectos, los contratos formativos en alternancia que viene desarrollándose en virtud de lo establecido en las Órdenes anuales de convocatoria de los proyectos de formación profesional dual para cada curso escolar y que contemplan la formalización de convenios entre los centros docentes y las empresas u organismos equiparados participantes en los proyectos seleccionados.

Quinto.- Que la disposición adicional quincuagésima segunda del texto refundido de la Ley General de la Seguridad Social aprobado por Real Decreto Legislativo 8/2015, de 30 de octubre, relativa a la inclusión en el Sistema de Seguridad Social de alumnos que realicen prácticas formativas o prácticas académicas externas

incluidas en programas de formación, establece que a partir de 1 de enero de 2024, la realización de prácticas formativas en empresas, instituciones o entidades incluidas en programas de formación y la realización de prácticas académicas externas al amparo de la respectiva regulación legal y reglamentaria, determinará la inclusión en el Sistema de la Seguridad Social de los alumnos de formación profesional, siempre que no se trate del régimen de Formación Profesional intensiva.

En el caso de las prácticas formativas remuneradas, el cumplimiento de las obligaciones de Seguridad Social corresponderá a la entidad u organismo que financie el programa de formación, que asumirá a estos efectos la condición de empresario. En el supuesto de que el programa esté cofinanciado por dos o más entidades u organismos, tendrá la condición de empresario aquel al que corresponda hacer efectiva la respectiva contraprestación económica.

En el caso de las prácticas formativas no remuneradas, el cumplimiento de las obligaciones de Seguridad Social corresponderá a la empresa, institución o entidad en la que se desarrollen aquellos, salvo que en el convenio o acuerdo de cooperación que, en su caso, se suscriba para su realización se disponga que tales obligaciones corresponderán al centro de formación responsable de la oferta formativa. Quien asuma la condición de empresario deberá comunicar los días efectivos de prácticas a partir de la información que facilite el centro donde se realice la práctica formativa (de acuerdo con lo establecido en la disposición quincuagésima segunda, 4.b).

Sexto.- Que por las razones expuestas y con el fin de llevar a cabo la fase de formación en empresas u organismos equiparados y garantizar asimismo su eficaz desarrollo, ambas partes

ACUERDAN

PRIMERO. Suscribir el presente convenio para el desarrollo de la fase de formación en empresa u organismo equiparado de las enseñanzas de formación profesional del sistema educativo, de acuerdo con la normativa emitida por la Consejería competente en materia de educación en ciclos formativos y cursos de especialización de formación profesional de la Comunidad Autónoma de Andalucía, que ambas partes conocen y acatan, y con lo dispuesto en las cláusulas que figuran en este documento.

Y, en prueba de conformidad, en el lugar y fecha del encabezamiento, firman los ejemplares correspondientes,

Por delegación de firma de la persona titular de la Consejería de Desarrollo Educativo y Formación Profesional Orden de 29 de abril de 2024 EL/LA DIRECTOR/A DEL CENTRO DOCENTE	EL/LA REPRESENTANTE DE LA ENTIDAD COLABORADORA
Fdo. Miguel Ángel Domínguez Gómez	Fdo. Raúl Jiménez Jiménez

CLÁUSULAS

PRIMERA.- Objeto del convenio.

El objeto del presente convenio es articular la colaboración entre el centro docente C.P.I.F.P. Alan Turing y la empresa Agencia Digital de Andalucía para el desarrollo de la fase de formación de las enseñanzas del G.E.C.E.G.S. (Ciberseguridad en Entornos de las Tecnologías de la Información), de acuerdo con las normas emitidas por la Consejería competente en materia de educación en los ciclos formativos y cursos de especialización del Sistema de Formación Profesional en la Comunidad Autónoma de Andalucía.

SEGUNDA.- Naturaleza jurídica de la relación alumnado-entidad colaboradora.

La fase de formación en empresa u organismo equiparado tendrá naturaleza académica y carácter formativo y de su realización no se derivarán en ningún caso obligaciones propias de una relación laboral o de prestación contractual de servicios, no siéndole de aplicación la legislación al respecto, ni su contenido podrá dar lugar a la sustitución de la prestación laboral propia de puestos de trabajo, salvo el alumnado acogido a la empresa u organismo equiparado a través del contrato de formación en alternancia cuya relación con la empresa estará establecida de conformidad al Real Decreto-ley 32/2021, de 28 de diciembre, de medidas urgentes para la reforma laboral, la garantía de la estabilidad en el empleo y la transformación del mercado de trabajo.

En ningún caso el alumnado podrá sustituir a personal de la plantilla en el momento de su inclusión en el convenio ni durante todo el período de duración de la fase de formación en empresa u organismo equiparado.

TERCERA.- Compromisos del centro docente.

El centro se compromete a:

a) Velar por la calidad de las actividades formativas en empresas u organismos equiparados a través de las oportunas acciones en las fases de programación, seguimiento y evaluación.
b) Elaborar un plan de formación para cada alumno/a. La programación de las actividades formativas a realizar en la entidad colaboradora y, recogida en el anexo I, se realizará en coordinación con el tutor o tutora dual de la empresa u organismo equiparado.
c) Designar al tutor o tutora dual del centro docente que será el responsable del seguimiento y de la comunicación con la empresa y cuyos datos figurarán en el plan de formación al que se refiere el apartado anterior.
d) Facilitar al tutor o tutora dual del centro docente la realización de las visitas, la celebración de reuniones y las comunicaciones periódicas con las empresas colaboradoras.
e) Proporcionar al alumnado participante la formación necesaria en el centro docente para que el plan de formación en la empresa se ejecute en condiciones de aprovechamiento y seguridad, tomando conciencia de la necesidad de adoptar medidas de prevención de riesgos laborales y cumpliendo las medidas de protección individual, colectiva y medioambiental.
f) Proporcionar asesoramiento y apoyo a la entidad colaboradora en cualquier aspecto relacionado con la planificación, gestión y desarrollo de la fase de formación en empresas u organismo equiparado, especialmente en su monitorización y valoración.
g) Comunicar a la entidad colaboradora, antes de la incorporación de las personas en formación, el protocolo de actuación en caso de accidentes y el procedimiento de reclamación patrimonial que debe seguirse en caso de producirse daños materiales atribuibles al alumnado durante el desarrollo de la fase de formación en empresas u organismos equiparados.
h) Informar, de forma previa a la realización de la fase de formación en empresa u organismo equiparado al alumnado de las condiciones y compromisos a asumir, al menos, con los siguientes puntos:

1. El alumno/a se identificará, durante la estancia en la entidad colaboradora, mediante DNI o documento acreditativo de la identidad y, en el caso de que sea necesaria, tarjeta de identificación del centro docente.
2. El alumno/a cumplirá las normas de carácter interno de la entidad colaboradora y seguirá las instrucciones que reciba de sus responsables.

3. El alumno/a cumplirá el calendario, horario y plan de formación acordado con la entidad colaboradora y se responsabilizará de remitir semanalmente al tutor dual del centro docente, la hoja semanal de seguimiento de actividades, debidamente cumplimentada y firmada, y cualquier otro requisito establecido para la evaluación de la fase de formación en empresas u organismos equiparados.
4. El alumno/a comunicará al centro y a la empresa, a la mayor brevedad posible, cualquier ausencia o retraso.
5. El alumno/a seguirá la normativa de organización, prevención de riesgos laborales, emergencias y protocolos ambientales establecidos por la entidad colaboradora, así como la política de confidencialidad aludida en este convenio.

i) Colaborar con el tutor o tutora dual en la valoración de la adquisición de los resultados de aprendizaje alcanzados, de acuerdo con los criterios de evaluación establecidos, recogida en los informes elaborados para su posterior calificación y registro en los documentos oficiales de evaluación.
j) Cumplir con la legislación vigente en materia de Seguridad Social durante la fase de formación en empresa u organismo equiparado (de conformidad con la cláusula quinta de este convenio).
k) Proporcionar la formación inicial del alumnado relativa a los riesgos específicos y las medidas de prevención de riesgos laborales correspondientes al perfil profesional y al uso de equipos de protección individual que se utilizan en el sector profesional en el que realiza la fase de formación en empresa u organismo equiparado.

CUARTA.- Compromisos de la entidad colaboradora.

La entidad colaboradora se compromete a:

a) Facilitar el uso compartido de las instalaciones y equipamientos garantizando que se cumplen los requisitos en las instalaciones y recursos definidos en la normativa reguladora para el desarrollo de las actividades formativas, con la finalidad de verificar la adquisición de los resultados de aprendizaje, de uno o varios módulos profesionales, de acuerdo con los criterios criterios de evaluación, de los ciclos formativos y/o cursos de especialización del Sistema de Formación Profesional.
b) Designar a un tutor o tutora dual de la empresa u organismo equiparado, cuyos datos figurarán en el anexo III, que tendrá entre sus funciones:

1. Tutorizar la realización en la empresa u organismo equiparado de las actividades formativas necesarias para la adquisición de los resultados de aprendizaje recogidos en el anexo I.
2. Procurar que se cumplan las normas de régimen interno establecidas por el centro de trabajo.
3. Asegurar que el alumnado porte los equipos de protección individual que se le proporcionen, así como el distintivo que les identifique como alumnado de formación profesional.
4. Colaborar con el profesorado del centro docente, mediante la elaboración de un informe de valoración, en el seguimiento del alumnado durante su estancia en la empresa y en la evaluación de los aprendizajes alcanzados.
5. Encomendar al alumnado, en base al plan de formación acordado, la realización de actividades formativas relacionadas con el perfil profesional del ciclo en el que se encuentra matriculado, orientadas a la adquisición de los resultados de aprendizaje establecidos en el currículo del título, y recogidas en el anexo I.

c) Poner a disposición del alumnado instrumentos y equipamientos necesarios para el cumplimiento de las actividades formativas, así como garantizar la adecuada orientación y asesoramiento para el correcto desempeño de las mismas.
d) Comunicar al tutor o tutora del centro docente, cualquier incidencia que pudiera atribuirse al alumnado respecto a sus compromisos con la empresa u organismo equiparado, a la mayor brevedad posible, para el correcto desarrollo de las actividades de formación, de acuerdo con el plan de formación y la programación establecida.
e) Informar, si procede, a los representantes de los trabajadores y trabajadoras de la empresa u organismo equiparado del plan de formación de la persona en formación sujeta al convenio.
f) No ocupar, ni siquiera con carácter interino, ningún puesto de trabajo en plantilla con el alumnado que realice las actividades formativas en la empresa u organismo equiparado.
g) Acreditar que el tutor o tutora dual de la empresa, en el caso de que el alumnado sea menor de edad, aporte un Certificado Negativo del Registro Central de Delincuentes Sexuales y Trata de Seres Humanos sexuales (de conformidad con el art. 57.1 de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia).

h) Cumplir con la legislación vigente en materia de Seguridad Social durante la fase de formación en empresa u organismo equiparado (de conformidad con la cláusula quinta de este convenio).
i) Cumplir las medidas de prevención de riesgos personales y colectivas, las medidas de seguridad e higiene, el protocolo de actuación ante emergencias, las medidas medioambientales y las medidas sobre equipos de protección individual que deberá utilizar el alumnado durante su estancia formativa.

QUINTA.- Obligaciones en materia de Seguridad Social y financiación.

[redacted]

1. Este acuerdo no implica la transferencia de recursos económicos entre las partes.

2. La colaboración tendrá la consideración de programas de prácticas formativas no remuneradas.
3. De conformidad con la disposición adicional quincuagésima segunda del Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, los costes y obligaciones derivados de la inclusión en el Sistema de la Seguridad Social del alumnado de enseñanzas de Formación Profesional de la Comunidad Autónoma de Andalucía sostenidas con fondos públicos durante la realización del período de formación en empresa u organismo equiparado serán asumidos por:

☒ La Consejería competente en materia de formación profesional. [redacted]
☐ La entidad colaboradora

SEXTA.- Calendario, jornada y horario.

El calendario, jornadas y horario de la fase de formación en la empresa u organismo equiparado de la persona en formación a la que afecta el presente convenio serán los especificados en el correspondiente anexo II. Este documento, será firmado para cada alumno o alumna y curso académico, entre el centro docente y entidad colaboradora.

SÉPTIMA.- Asignación del alumnado.

Cód.Centro: 29020231

El centro docente, en colaboración con la empresa u organismo equiparado, asignará los puestos formativos al alumnado que curse un ciclo formativo o curso de especialización para el que se desarrolla el convenio conforme a unos criterios objetivos (rendimiento académico, asistencia a las actividades lectivas, competencias personales, entre otros que se estimen oportunos) y acordes con la actividad de la entidad colaboradora, siempre que no supongan discriminación de acuerdo con la normativa en materia de Formación Profesional.

El tutor o tutora del centro detallará el alumnado participante en la fase de formación que quedará recogido en el anexo III, que será firmado en cada curso académico por el centro docente y la empresa u organismo equiparado participante.

OCTAVA.- Rescición del convenio.

Podrá rescindirse el convenio de una o varias personas en formación por decisión unilateral del centro docente, de la empresa u organismo equiparado, o conjunta de ambos, previa audiencia del interesado o interesada, en los siguientes casos:

a) Incumplimiento del plan de formación por parte de la persona en formación.
b) Faltas repetidas de asistencia o puntualidad no justificadas.
c) Actitud incorrecta.
d) Falta de aprovechamiento por parte de la persona en formación.

NOVENA.- Seguros.

1) Cualquier eventualidad de accidente que pudiera producirse será contemplada como contingencia profesional según lo establecido en el Real Decreto Legislativo 8/2015, de 30 de octubre.
2) Corresponde a la Consejería competente en materia de formación profesional de la Junta de Andalucía la cobertura de la responsabilidad civil del alumnado de centros docentes de titularidad pública y de enseñanzas sostenidas con fondos públicos.
En el caso de enseñanzas privadas, serán los centros educativos quienes se harán responsables de la cobertura de la responsabilidad civil del alumnado.

DÉCIMA.- Protección de datos y confidencialidad.

1. Las partes se comprometen a cumplir y respetar lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por la que se adapta el ordenamiento jurídico español a lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante RGPD), así como toda la normativa vigente en relación con el objeto del acuerdo, en especial aquella concerniente a la protección de los derechos fundamentales.

2. La Consejería competente en materia de formación profesional será, en el caso de centros docentes de titularidad pública, la responsable del tratamiento de los datos, y la otra parte actuará como encargado del tratamiento, conforme al artículo 28 del RGPD.
En el caso de centros docentes privados, serán estos los responsables del tratamiento de los datos, cuenten o no con enseñanzas sostenidas con fondos públicos.

3. El tratamiento por parte del encargado se hará con la única finalidad de realizar la fase de formación en la empresa u organismo equiparado. La duración del tratamiento será por el tiempo que dure la fase de formación en la empresa u organismo equiparado. Los datos personales que se podrán tratar son los datos identificativos y de contacto, los datos académicos (tipo y nombre de la enseñanza, curso) y, en su caso, los derivados de las pruebas que deba realizar el alumnado antes de su incorporación a las prácticas en la empresa. Las categorías de datos interesados son alumnado, profesorado encargado del seguimiento y personas que ejerzan la tutoría en la empresa u organismo equiparado. El tipo de operaciones que podrá contener el tratamiento de los datos serán la recogida, el registro, la modificación, la conservación, la extracción, la consulta, la difusión, el cotejo, la conservación en el sistema de información Séneca, la copia de seguridad, la destrucción de copias temporales, la supresión y la recuperación. Se estipula, en particular, que el encargado/a:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado/a; en tal caso, este/a informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
c) Tomará todas las medidas necesarias de conformidad con el artículo 32 del RGPD.
d) Respetará las condiciones indicadas en los apartados 2 y 4 del artículo 28 del RGPD para recurrir a otro encargado del tratamiento.
e) Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el Capítulo III del RGPD.
f) Ayudará al/ a la responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado/a.
g) Suprimirá o devolverá, a elección del/la responsable, todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.
h) Pondrá a disposición del/la responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del/la responsable o de otro auditor/a autorizado por dicho/a responsable.
i) En relación con lo dispuesto en la letra h), informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión Europea o de los Estados miembros.

4. En cumplimiento del artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, los/las responsables y encargados/as del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679, manteniéndose dicha obligación cuando hubiese finalizado la relación del obligado con el/la responsable o encargado/a del tratamiento.
De conformidad con el artículo 28.4 del RGPD, cuando un/a encargado/a del tratamiento recurra a otro/a

encargado/a para llevar a cabo determinadas actividades de tratamiento por cuenta del/la responsable, se impondrán a este otro encargado/a, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el/la responsable y el encargado/a a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro/a encargado/a incumple sus obligaciones de protección de datos, el/la encargado/a inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro/a encargado/a.

UNDÉCIMA.- Comisión de Seguimiento.

1. Se establecerá una Comisión de Seguimiento constituida, al menos, por dos representantes del centro docente, uno actuará como presidente y tendrá voto de calidad en caso de empate en las votaciones que se efectúen, y otros dos de la empresa u organismo equiparado, uno de los cuales actuará como secretario, con voz y voto, para realizar el seguimiento y control del cumplimiento del convenio, así como resolver posibles problemas de interpretación que pudieran plantearse.

2. La Comisión podrá reunirse cuantas veces lo solicite cualquiera de las partes y como mínimo una vez durante el curso académico, con una antelación mínima de diez días hábiles. Los acuerdos de la comisión se adoptarán por mayoría de sus miembros, todos ellos tienen derecho a voz y a voto, y de sus reuniones se levantará la correspondiente acta que será suscrita por el secretario o secretaria con el visto bueno del presidente o presidenta.

3. La Comisión podrá requerir la asistencia de cualquier persona, con voz, pero sin voto, que pueda aportar conocimientos o asesoramiento adecuados para un mejor desarrollo del objeto del presente convenio.

4. La Comisión de Seguimiento tendrá las siguientes funciones:

a) Coordinar los trabajos necesarios para la ejecución del presente convenio de colaboración.
b) Velar por el cumplimiento y seguimiento de lo establecido en el convenio de colaboración.
c) Estudiar el desarrollo y grado de ejecución de las actuaciones objeto del presente convenio de colaboración, evaluar y valorar los resultados y proponer las medidas correctoras ante las posibles dificultades y problemas que pudieran surgir.
d) Conocer y mediar en los conflictos derivados de la interpretación y aplicación del presente convenio de colaboración, con carácter previo a la intervención de la jurisdicción competente.

5. En caso de resolución anticipada del convenio, la Comisión de Seguimiento establecerá la forma de liquidación del mismo, emitiendo un informe de actuaciones realizadas hasta la citada fecha, garantizando la finalización de las actividades programadas y, en todo caso, la escolarización del alumnado.

6. El régimen de funcionamiento y organización de la Comisión de Seguimiento será el previsto para los órganos colegiados en la sección 3ª del capítulo ll del título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en la sección 1ª del capítulo ll del título IV de la Ley 9/2007, de 22 de octubre, de la Administración le la Junta de Andalucía.

DUODÉCIMA.- Vigencia.

Este convenio entrará en vigor el día siguiente de su firma hasta la finalización del curso académico, no estando prevista la prórroga del mismo.

DECIMOTERCERA.- Causas y efectos de extinción.

1. El Convenio se resolverá por alguna de las siguientes causas:

a) Transcurso del plazo de vigencia.
b) El mutuo acuerdo de las partes.
c) El incumplimiento del objeto o de cualquiera de sus estipulaciones, imputable a alguna de las partes del mismo.
d) Por cualquier otra causa de las previstas en el artículo 51.2 de la Ley 40/2015, de 1 de octubre.

En el supuesto establecido en la letra c), cualquiera de las partes podrá notificar a la parte incumplidora un requerimiento para que cumpla en un plazo de quince días. Del mismo modo, dicha información deberá ser comunicada a la Comisión de Seguimiento prevista en la cláusula undécima. Transcurrido dicho plazo y persistiendo el incumplimiento, la parte que lo dirigió notificará a la otra la concurrencia de causa de resolución y se entenderá resuelto el convenio. Dicha circunstancia deberá ser puesta en conocimiento de la Comisión de Seguimiento para la determinación, en su caso, de la indemnización de los perjuicios causados.

2. En lo que se refiere a los efectos de la resolución del convenio se estará a lo previsto en el artículo 52 de la Ley 40/2015, de 1 de octubre.

DECIMOCUARTA.- Naturaleza jurídica del convenio.

Este convenio tiene naturaleza administrativa y se regirá, además de por su clausulado, en lo no previsto en el mismo por lo dispuesto en el capítulo VI del título preliminar de la Ley 40/2015, de 1 de octubre, quedando excluido de la aplicación de la Ley 9/2017, de 8 de noviembre, de contratos de Sector Público, por la que se se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, al amparo de lo dispuesto en su artículo 6.2. Todo ello, sin perjuicio de que, conforme a su artículo 4, se apliquen los principios de esta ley para resolver las dudas y lagunas que pudieran presentarse.

Sin perjuicio de las funciones que se atribuyen a la Comisión de Seguimiento, cualquier cuestión litigiosa que pudiera surgir en cuanto a la interpretación y cumplimiento del mismo, que no haya podido ser dirimida por la misma, se resolverá por la jurisdicción competente.

Cód.Centro: 29020231

ANEXO I

ACTIVIDADES FORMATIVAS EN LA EMPRESA U ORGANISMO EQUIPARADO

Centro docente: C.P.I.F.P. Alan Turing	**Curso:** 2024/2025
Ciclo formativo: G.E.C.E.G.S. (Ciberseguridad en Entornos de las Tecnologías de la Información)	**Convenio nº:** 290202312024035
Empresa: Agencia Digital de Andalucía	**CIF:** [redacted]

Número de la actividad: 1 **Alumnos/as:** [redacted]

Descripción: En el marco de un proyecto o entorno de la empresa, realizar una auditoría de seguridad.

- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - a. Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.
- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - b. Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.
- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - c. Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.
- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - d. Se ha accedido a redes inalámbricas vulnerables
- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - e. Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.
- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a

ANEXO I

redes para demostrar sus vulnerabilidades. - f. Se han utilizado técnicas de "Equipo Rojo y Azul".

- Hacking Ético - R.A.2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. - g. Se han realizado informes sobre las vulnerabilidades detectadas

- Hacking Ético - R.A.5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas - a. Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.

- Hacking Ético - R.A.5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas - b. Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.

- Hacking Ético - R.A.5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas - c. Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.

- Hacking Ético - R.A.5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas - d. Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales. e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web. f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software

Número de la actividad: 2 **Alumnos/as:** [redacted]

Descripción: Actualizar el plan de revisiones normativas de la empresa en la que trabajan, considerando cambios recientes en la normativa o jurisprudencia aplicable a su actividad

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - a. Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - b. Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - c. Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - d. Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.

Número de la actividad: 3 **Alumnos/as:** [redacted]

Descripción: Implementar controles internos para garantizar el cumplimiento de una nueva normativa o cambio legislativo identificado en el plan de revisiones

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - c. Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - d. Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.

- Normativa de Ciberseguridad - R.A.5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia - e. Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones

Número de la actividad: 4 **Alumnos/as:** [redacted]

Descripción: Auditoría de seguridad en aplicaciones web y móviles: Evaluar la seguridad de aplicaciones web y móviles mediante la identificación de riesgos, validación de entradas, análisis de protocolos y configuraciones, y corrección de vulnerabilidades

- Puesta en Producción Segura - R.A.1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución - c. Se han reconocido los elementos básicos del código fuente, dándoles significado.

ANEXO I

- Puesta en Producción Segura - R.A.1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución - d. Se han ejecutado diferentes tipos de prueba de software.
- Puesta en Producción Segura - R.A.1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución - e. Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.
- Puesta en Producción Segura - R.A.2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados - a. Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, "Application Security Verification Standard").
- Puesta en Producción Segura - R.A.2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados - b. Se ha identificado el nivel de verificación de seguridad requerido porlas aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.
- Puesta en Producción Segura - R.A.2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados - c. Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.
- Puesta en Producción Segura - R.A.3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web - b. Se han detectado riesgos de inyección tanto en el servidor como en el cliente.
- Puesta en Producción Segura - R.A.3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web - d. Se ha hecho uso de roles para el control de acceso
- Puesta en Producción Segura - R.A.3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web - e. Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.
- Puesta en Producción Segura - R.A.4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. - 4. Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.
- Puesta en Producción Segura - R.A.4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. - 5. Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible

Número de la actividad: 5 **Alumnos/as:** [redacted]

Descripción: Automatización del despliegue seguro de aplicaciones web y móviles: Diseñar e implementar un sistema de despliegue automatizado seguro utilizando técnicas de integración continua y control de versiones, asegurando la recuperación ante fallos

- Puesta en Producción Segura - R.A.3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web - f. Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.
- Puesta en Producción Segura - R.A.3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web - g. Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).
- Puesta en Producción Segura - R.A.4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. - 2. Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.
- Puesta en Producción Segura - R.A.4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. - 3. Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - b. Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - c. Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - d. Se han planificado, implementado y automatizado planes de desplegado de software.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - e. Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - f. Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.
- Puesta en Producción Segura - R.A.5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos - g. Se han creado bucles de retroalimentación ágiles entre los

ANEXO I

miembros del equipo.
Número de la actividad: 6 **Alumnos/as:** [redacted] **Descripción:** Establecer y configurar controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de ciberincidentes, incidentes de seguridad física, y usando fuentes abiertas. Documentar todos los incidentes detectados
- Incidentes de Ciberseguridad - R.A.2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad - b. Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes - Incidentes de Ciberseguridad - R.A.2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad - c. Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física. - Incidentes de Ciberseguridad - R.A.2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad - d. Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT. Open Source Intelligence). - Incidentes de Ciberseguridad - R.A.2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad - e. Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización
Número de la actividad: 7 **Alumnos/as:** [redacted] **Descripción:** Definir a alto nivel el procedimiento de continuidad del negocio que permita restablecer los servicios afectados así como indicando las áreas involucradas en cada caso y los destinatarios de las notificaciones progresivas
- Incidentes de Ciberseguridad - R.A.4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas - b. Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros. - Incidentes de Ciberseguridad - R.A.4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas - c. Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados. - Incidentes de Ciberseguridad - R.A.4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas - d. Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad. - Incidentes de Ciberseguridad - R.A.4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas - e. Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".
Número de la actividad: 8 **Alumnos/as:** [redacted] **Descripción:** Configuración de dispositivos perimetrales: Los participantes configuran cortafuegos simulados basándose en requisitos de seguridad específicos.
- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - a. Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad. - Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - b. Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico. - Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - c. Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego. - Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - d. Se han implementado contramedidas frente a comportamientos no deseados en una red. - Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - e. Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
Número de la actividad: 9 **Alumnos/as:** [redacted] **Descripción:** Análisis de tráfico de red: Realización de pruebas prácticas para detectar errores de configuración mediante herramientas de monitoreo.
- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - a. Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

ANEXO I

- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - b. Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - c. Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - d. Se han implementado contramedidas frente a comportamientos no deseados en una red.
- Bastionado de Redes y Sistemas - R.A.5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. - e. Se han caracterizado, instalado y configurado diferentes herramientas de monitorización

Número de la actividad: 10 **Alumnos/as:** [redacted]

Descripción: Preparación inicial de sistemas informáticos: Configuración y particionado del sistema para mitigar riesgos y optimizar la instalación.

- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - a. Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - b. Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - c. Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - d. Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - e. Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

Número de la actividad: 11 **Alumnos/as:** [redacted]

Descripción: Instalación con cifrado y secuencia protegida: Implementación de un sistema con cifrado de archivos y protección frente a alteraciones del arranque.

- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - a. Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - b. Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - c. Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - d. Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
- Bastionado de Redes y Sistemas - R.A.6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques - e. Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

Número de la actividad: 12 **Alumnos/as:** [redacted]

Descripción: Optimización del sistema informático: Identificación y eliminación de servicios, programas y protocolos innecesarios.

- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - a. Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - b. Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - c. Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

[redacted]

Cód.Centro: 29020231

ANEXO I

- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - d. Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - e. Se han instalado y configurado sistemas de copias de seguridad.

Número de la actividad: 13 **Alumnos/as:** [redacted]

Descripción: Fortalecimiento de accesos remotos: Configuración segura de SSH y técnicas para prevenir explotación de procesos.

- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - a. Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - b. Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - c. Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - d. Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
- Bastionado de Redes y Sistemas - R.A.7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques - e. Se han instalado y configurado sistemas de copias de seguridad.

Número de la actividad: 14 **Alumnos/as:** [redacted]

Descripción: Análisis forense integral en sistemas digitales compuestos por distintos elementos como móviles, Cloud e IoT.

- Análisis Forense Informático - R.A.1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación - b. Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
- Análisis Forense Informático - R.A.2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas - b. Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.
- Análisis Forense Informático - R.A.3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas - c. Se han realizado las fases del análisis forense en Cloud.
- Análisis Forense Informático - R.A.3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas - d. Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).
- Análisis Forense Informático - R.A.4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas - b. Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias
- Análisis Forense Informático - R.A.4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas - c. Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.
- Análisis Forense Informático - R.A.4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas - d. Se han realizado análisis de evidencias de manera manual y mediante herramientas.

[redacted]

Cód.Centro: 29020231

En Campanillas (Málaga) a 17 de febrero de 2025, a la fecha de la firma digital.

Por delegación de firma de la persona titular de la Consejería de Desarrollo Educativo y Formación Profesional Orden de 29 de abril del 2024
EL/LA DIRECTOR/A DEL CENTRO DOCENTE

Fdo. Miguel Ángel Domínguez Gómez

EL/LA REPRESENTANTE LEGAL

Fdo. Raúl Jiménez Jiménez

Junta de Andalucía

Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"

Anexo II

CALENDARIO ANUAL CENTRO DOCENTE-EMPRESA U ORGANISMO EQUIPARADO

(A cumplimentar por el tutor o tutora dual de grupo correspondiente)

Empresa: Agencia Digital de Andalucía	CIF: [redacted]	Alumnado: [redacted]	
Sede: Centro de Ciberseguridad de Andalucía			
Centro docente: C.P.I.F.P. Alan Turing	Convenio nº: 290202312024035	Ciclo formativo: G.E.C.E.G.S. (Ciberseguridad en Entornos de las Tecnologías de la Información)	Curso: 2024/2025

Septiembre

L	M	MI	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Octubre

L	M	MI	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Noviembre

L	M	MI	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Diciembre

L	M	MI	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Enero

L	M	MI	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Febrero

L	M	MI	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

Marzo

L	M	MI	J	V	S	D
					1	2
3	4	5	6	7	8	9
(10)	(11)	(12)	(13)	(14)	15	16
(17)	(18)	(19)	(20)	(21)	22	23
(24)	(25)	(26)	(27)	(28)	29	30
(31)						

Abril

L	M	MI	J	V	S	D
(1)	(2)	(3)	(4)	5	6	
(7)	(8)	(9)	(10)	(11)	12	13
14	15	16	17	18	19	20
(21)	(22)	(23)	(24)	(25)	26	27
(28)	(29)	(30)				

Mayo

L	M	MI	J	V	S	D
			1	2	3	4
(5)	(6)	(7)	(8)	(9)	10	11
(12)	(13)	(14)	(15)	(16)	17	18
(19)	(20)	(21)	(22)	(23)	24	25
26	27	28	29	30	31	

Junio

L	M	MI	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Julio

L	M	MI	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Agosto

L	M	MI	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Cód.Centro: 29020231

Número de jornadas totales en las empresas:	48
Horas totales:	288:00

◯ Jornadas en la empresa (dual o FFOE).
□ FCT
▽ Ambos
□ Podrá desarrollarse total o parcialmente en teletrabajo

Jornadas en la empresa	
Periodo:	Calendario GE CE CiberSeguridad - Genérico 10_03 al 23_05 (10/03/25-23/05/25)
Horario:	9:00 - 15:00
Nº Horas por jornada:	6:00

Junta de Andalucía

Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"

Anexo II

CALENDARIO ANUAL CENTRO DOCENTE-EMPRESA U ORGANISMO EQUIPARADO

En Campanillas (Málaga) a 17 de febrero de 2025, a la fecha de la firma digital.

[redacted]

Por delegación de firma de la persona titular de la Consejería de Desarrollo Educativo y Formación Profesional Orden de 29 de abril de 2024
EL/LA DIRECTOR/A DEL CENTRO DOCENTE

Fdo. Miguel Ángel Domínguez Gómez

EL/LA REPRESENTANTE LEGAL

Fdo. Raúl Jiménez Jiménez

Cód.Centro: 29020231

Junta de Andalucía

Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"

ANEXO III

RELACIÓN DE ALUMNADO

Centro docente: C.P.I.F.P. Alan Turing	**Curso:** 2024/2025
Ciclo formativo: G.E.C.E.G.S. (Ciberseguridad en Entornos de las Tecnologías de la Información)	**Convenio nº:** 290202312024035
Empresa: Agencia Digital de Andalucía	**CIF:** [redacted]
Sede donde realiza la FFEOE: Centro de Ciberseguridad de Andalucía	

Alumno/a	Tutor/a dual de empresa	Tutor/a dual del centro/ Responsable del seguimiento	Período	Régimen	Contrato/beca	Cuantía total
[redacted]	[redacted]	[redacted]	10/03/25-23/05/25	Régimen intensivo		

En Campanillas (Málaga) a 17 de febrero de 2025, a la fecha de la firma digital.

Por delegación de firma de la persona titular de la Consejería de Desarrollo Educativo y Formación Profesional
Orden de 29 de abril de 2024
EL/LA DIRECTOR/A DEL CENTRO DOCENTE

Fdo. Miguel Ángel Domínguez Gómez

EL/LA REPRESENTANTE LEGAL

Fdo. Raúl Jiménez Jiménez

Cód.Centro: 29020231