Fundación GOODJOB

GUÍA ALUMNOS

FORMACIÓN ITINERARIOS PREVIOS AL

#INCLUDE

2023-2024

/Rooted

QUIENES SOMOS

La **Fundación GoodJob** es una organización cuyo objetivo principal es mejorar la **inserción laboral** y fomentar la empleabilidad de personas con discapacidad.

Nuestra **misión** como institución no lucrativa es **contribuir activamente** a la **integración** en el mercado laboral de las personas con discapacidad, como uno de los factores más determinantes para garantizar su igualdad de oportunidades.

Desde la **Fundación GoodJob** consideramos que la inserción laboral favorece la autonomía económica de la persona con discapacidad y su entorno familiar, la mejora de su autoestima, el sentimiento de pertenencia a la comunidad y, por consiguiente, su plena integración en la sociedad.

Estamos **comprometidos** con la configuración de un mercado laboral inclusivo y solidario, que favorezca la contratación de las personas con necesidades especiales y sea respetuoso con la diversidad.

En **Fundación GoodJob** valoramos los avances logrados en los últimos años en materia de inserción promovidos por agentes políticos, sociales y empresariales, pero la realidad demuestra que muchas de las personas con discapacidad que pueden y quieren trabajar están desempleadas. En concreto, una de cada cuatro personas con discapacidad en edad activa no tiene trabajo y es el colectivo que tiene más dificultades para acceder al mercado laboral. Además, muchos de los que trabajan lo hacen en sectores nicho y en empleos de baja calidad y retribución.

Ante este escenario, la **Fundación GoodJob** propone un **cambio en la visión y en la forma de intervenir** por parte de cada uno de los grupos de interés, incluyendo a las organizaciones de economía social. Este nuevo modelo apuesta por la integración de las personas con discapacidad en la empresa ordinaria, mediante los enclaves laborales como fórmula de colaboración prioritaria.

Fundación GOODJOB

QUÉ ES EL PROYECTO #INCLUDE

Wikipedia: "*Include (incluir en inglés) es una palabra clave que hace referencia a una instrucción al preprocesador que está presente en la gran mayoría de lenguajes de alto y medio nivel, de forma genérica se usa para adicionar un archivo al código, como por ejemplo la llamada a una biblioteca de funciones en C/C++: #include <stdio.h>*".

"*Un #include es una llamada dentro del código de un programa, que permite incorporar nuevas capacidades que nuestro programa no tendría por sí mismo*" **~ Proyecto #include**

Fundación GOODJOB

Contenido

INTRODUCCIÓN

El presente documento describe una serie de contenidos formativos asociados con el Proyecto #include (programa de ciberseguridad de la Fundación) que esperamos que sean útiles para ti como alumno y ¡que te despierten interés!

Este programa ha sido realizado en colaboración con la **Fundación Goodjob**, **RootedCON** y distintos actores institucionales, así como con las diversas empresas #includeR que colaborarán en el proyecto.

Adicionalmente, colaboran instituciones de relevancia tal como la Consejería de Economía, Empleo y Competitividad de la Comunidad de Madrid, la Junta de Castilla y León, la Agencia de Ciberseguridad de la Generalitat (*CESICAT*), INCIBE o el Centro Criptológico Nacional (CCN-CERT).

Un esquema simplificado de esta propuesta de itinerario de capacidades en juego podría definirse de acuerdo con las siguientes premisas estratégicas:

- **Independencia y autonomía**: queremos que los ejercicios y pruebas que te planteamos te estimulen. Por ello, creemos en que la resolución de ellos sea autónoma y que no requiere de apoyo externo para lograrlo.
- **Enfoque escalonado**: para poder tener la sensación de que progresas, debes tener hitos concretos a corto plazo que, combinados, te aportarán logros a medio-largo plazo. Todos los ejercicios siguen esta premisa.
- Información accesible: toda la información necesaria para resolver estos ejercicios está disponible en Internet. Insiste en las búsquedas, que siempre aparece algo útil para resolver un ejercicio específico.

Fundación GOODJOB

INDEPENDENCIA Y AUTONOMÍA DE LOS PROFESIONALES

Es crítico que los profesionales seáis completamente autónomos a la hora de adquirir nuevos conocimientos o capacidades. Una de las habilidades más poderosas y a la vez más necesarias en un profesional de tecnología es la capacidad de operar de forma autónoma, siendo especialmente importante en situaciones de incertidumbre o de estrés.

Es un desafío en sí mismo el resolver problemas de cosas que no conoces y, uno de los añadidos a conseguir resolverlos es que, con toda probabilidad, vas a descubrir habilidades en ti mismo que puede que ni supieras que están ahí.

Dentro de los trabajos, en el mundo real, esta capacidad de ser autónomo e independiente buscando soluciones o informaciones que lleven a ellas es **MUY IMPORTANTE**.

ENFOQUE ESCALONADO

En el camino de desafíos propuesto, los alumnos vais a trabajar en las siguientes áreas de mejora, en mayor o menor profundidad, dependiendo del nivel de afinidad personal con una práctica determinada y, naturalmente, el nivel de asimilación de conceptos evaluado:

- **Conceptos de riesgo**: lo que permite la comprensión abstracta de la ciberseguridad, naturalmente, pero también de amenazas y problemas potenciales.
- **Búsqueda de información**: con distintos ejercicios con distintos niveles de dificultad, que refuercen las habilidades de búsqueda de información, siempre con la premisa esencial de "saber buscarse la vida".
- **Obtener y gestionar los recursos**: muy conectado con el punto anterior ("búscate la vida"), pero orientado esencialmente a ser capaz de determinar qué recursos vamos a necesitar y cómo debemos coreografiar nuestras acciones para lograr los mejores beneficios con el menor esfuerzo y coste.
- **Diseño y arquitectura de soluciones**: mediante ejercicios sencillos, que nos permitan esbozar cómo "modelar" servicios de ciberseguridad.

Fundación GOODJOB

CONOCIMIENTOS Y ACTIVIDADES TRANSVERSALES

Los conocimientos y actividades que enumeramos a continuación deben ser considerados como ESENCIALES por parte de los alumnos y profesionales.

Son conocimientos sobre herramientas, técnicas o habilidades “blandas” (no técnicas), que van a ser relevantes para cualesquiera que sean las opciones profesionales en puestos tecnológicos.

Conocimientos genéricos

Glosario de términos en materia de Ciberseguridad:

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

https://cybersecurityguide.org/resources/cybersecurity-101/

LECTURA Y ESCRITURA INGLÉS:

En tecnología el inglés **ESCRITO** es esencial. Así como la conversación tiene solamente relevancia en caso de prestar soporte o servicios a clientes en ese idioma, la **lectura** y **escritura** del inglés forma parte esencial de las actividades en materia de tecnología.

Es CRÍTICO mejorar el nivel leído y escrito de manera sistemática. Es por ello que los ejercicios contenidos en este documento asumen que buscaréis fuentes de información que podrían estar en inglés.

USO DE OFFICE:

El uso de herramientas de Office, sobre todo WORD, EXCEL y POWERPOINT es crítico en el día a día de la tecnología.

Hay que saber usar estas herramientas con un nivel de efectividad adecuado. En concreto:

- Uso básico de Excel, Word y Powerpoint.
- Uso de algunas funcionalidades más avanzadas: tales como tablas pivot, elementos incrustados, plantillas etc.

Para seguir este camino es importante:

- **Tener pensamiento creativo y lateral**: debes reflexionar contigo mismo y tu tutor para decidir si tu perfil de personalidad está alineado con este requisito.
- **La curiosidad**: debes reflexionar contigo mismo y tu tutor para decidir si tu perfil de personalidad está alineado con este requisito.
- **El tesón y disciplina**: debes reflexionar contigo mismo y tu tutor para decidir si tu perfil de personalidad está alineado con este requisito.
- **Tolerancia a la frustración**: distintos problemas en el mundo de la ciberseguridad solamente pueden resolverse cuando realizas intento tras intento, hasta que das con la solución. Pero, para llegar a una solución que funcione, debes fallar una y otra vez. Es muy importante saber gestionar estos fallos teniendo claro siempre el objetivo final.

Las actividades propuestas para evolucionar hacia este tipo de perfil están clasificadas en tres niveles de dificultad:

- **Inicial**: Punto de partida para comenzar a aprender el mundo de la ciberseguridad
- **Intermedio**: Conoce algunos conceptos y está preparado/a para empezar a profundizar
- **Avanzado**: Conoce algunos conceptos con cierta profundidad y está preparado/a para mejorar y avanzar en aspectos más complejos.

Para seguir el presente itinerario, es importante el ir escalando niveles, por eso es importante que el propio candidato gestiones el esfuerzo para ir avanzando a lo largo de estas semanas previas al programa #include.

Todas las recomendaciones en este documento se han pensado en un plan de un máximo de cuatro/cinco semanas de atención.

- Búsqueda y gestión de información y datos
  - Periodicidad: todas las semanas
  - Pista: podéis utilizar herramientas de comunicación como el grupo de Telegram o los que creáis necesarios para hablar entre vosotros:
  - **Inicial**: busca 5 noticas distintas relacionadas con la ciberseguridad. Para cada noticia, es habitual que esta se publique en diferentes medios. Por lo tanto, identifica los medios por cada noticia y contesta a la siguiente pregunta
    - ¿Qué información tienen en común cada una de las noticias?
    - Responde las 5W (*who, what, when, where, why*). Quién, qué, cuándo, dónde, por qué. Y, si es posible, el cómo (*How*).
  - **Intermedio**: busca e identifica la fuente original de la noticia, a ser posible la primera de todas
  - **Avanzado**: busca cómo ocurrió y explícalo.

- Comunicación y Colaboración
  - Periodicidad (todas las semanas): ponemos de acuerdo para crear una hoja de cálculo (Google Spreadsheets, por ejemplo) o cualquier otro recurso donde podáis incorporar cambios de manera colaborativa.
  - Todos los alumnos deben participar en este ejercicio siguiendo las instrucciones que detallamos a continuación (para cada nivel).
  - **Inicial**: Añade una nueva hoja con tu nombre partiendo de la plantilla, crea el recopilatorio de noticias del ejercicio fila a fila. Finalmente, bloquea la edición de la pestaña para que nadie pueda editar tu información, pero sí leerla, podrás crear dicha funcionalidad con la parte de "proteger".
  - **Intermedio**: **Crea la hoja o el recurso compartido**. Añade tu opinión y tendencias para cada una de las noticias que has agregado. Puedes utilizar herramientas como *Google Trends* entre otros…
  - **Avanzado**: A partir de la información de tus compañeros, lee y busca conceptos de vulnerabilidades y enuméralos. Ayuda: https://attack.mitre.org/

- Comunicación y Colaboración
  - Periodicidad: última semana del periodo.
  - **Inicial**: Busca y elabora un documento para identificar la siguiente cuestión: ¿Cuál es el proceso que debe seguir un ciudadano español si se le ha caducado el certificado del DNI electrónico? Pista: cada dos años caduca.
  - **Intermedio**: cita y compara otros mecanismos y autoridades de certificación existentes para firmar con certificado digital o tarjetas internacionales. Por ejemplo: FNMT, CAMERFIRMA, Tarjeta sanitaria europea o certificado COVID…
  - **Avanzado**: Explica cómo firmar un documento en PDF con un certificado. Firma uno como ejemplo y mándalo por email a tareasimpact@goodjob.es

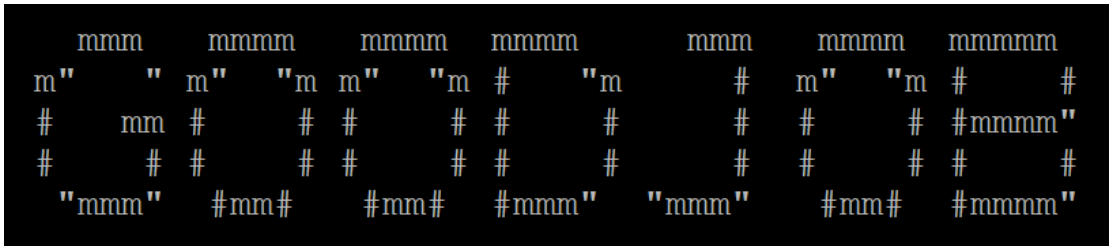
- Creación de contenidos digitales
  - Periodicidad: En las primeras dos semanas del periodo de cuatro/cinco.
  - **Inicial**: Crea un documento libre (Word, PowerPoint, HTML, Libreoffice, Google SUITE) donde incluyas las noticias del primer ejercicio, además incorpora contenido multimedia con licencias CC0 (Creative Commons cero)
  - **Intermedio y avanzado**: solicita la autorización al autor para la utilización de recursos bajo licencia, si lo consigues, inclúyelo en la presentación. Además, es necesario presentar las evidencias de la autorización y aceptación si lo consigues.
  - **TODOS**: publica el documento en un hosting de tu preferencia. Identifica la URL para acceder al recurso.

- Creación de contenidos digitales
  - Periodicidad: todo el periodo (sin importar en qué momento se complete).
  - **Inicial y Intermedio**: Completa los ejercicios adicionales del portal de Blockly
    - https://blockly.games/turtle?lang=en
  - **Avanzado**: programa en Python una aplicación que reciba como entrada una cadena de caracteres e imprime por consola el texto en formato banner ampliado.

Fundación GOODJOB

Ejemplo de entrada: GOODJOB

Ejemplo de salida:



Para simplificar el desarrollo, ten presente las siguientes características:

- No distinguir entre mayúsculas y minúsculas, todo en mayúsculas.
- No tengas presente los caracteres especiales como la ñ ç entre otros….
- El formato del banner es libre, pero se aconseja ser lo más práctico.

Puedes consultar el siguiente curso en Python: https://www.w3schools.com/python/default.asp

- Seguridad
  - **Inicial**: realiza un informe con las herramientas de protección que utilizas (antivirus, antimalware, cortafuegos…) además identifica herramientas que utilizas o puedes utilizar para cifrar los datos.
    - Crea un plan de desconexión digital para vosotros mismos (a lo largo de las dos primeras semanas del periodo).
  - **Intermedio y avanzado** (todas las semanas): Crear un informe sobre herramientas para la protección y escaneo de amenazas: crea 1escaneo por semana y presenta las evidencias. Explica cómo realizas un uso avanzado de la seguridad en referencia a la protección de datos y privacidad de la información.
    - Crea un plan de desconexión digital para un adolescente (a lo largo de las dos primeras semanas del periodo).

- Resolución de problemas
  - Periodicidad: en las dos últimas semanas del periodo.
  - **Inicial**: crea un árbol de decisión en base a la siguiente información: El ordenador no arranca.
  - **Intermedio y avanzado**: imagínese que desea llevar su ordenador al punto limpio, cree un plan donde ofrezcan garantías sobre la privacidad de los datos. Es decir, que nadie pueda acceder a la información del disco duro o medios de almacenamiento.

- Identificar lagunas en las competencias digitales:
  - **A5 (TODOS)**: Plan de autoevaluación
  - Periodicidad (primera semana del periodo y repetir la última): es importante que valores cómo de bien te ves en materias de ciberseguridad en la primera semana y en la última del periodo (para que tú mismo observes la evolución).

Identifícate del 1 al 5, siendo 1 el menor nivel de confianza que sientes que tienes sobre la materia y 5 el mayor, sobre los siguientes puntos de la ciberseguridad que veremos en el próximo IMPACT#include.

1.- Ciberinteligencia: La **ciberinteligencia** es la recopilación, análisis e interpretación de la información a través de técnicas rigurosas; para identificar, mitigar o prevenir posibles ciberataques.

2.- Seguridad perimetral: La seguridad perimetral corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles

3.- Operaciones de ciberseguridad: Las operaciones de seguridad (SecOps) mantienen y restauran las garantías de seguridad del sistema a medida que los adversarios directos lo atacan. Las tareas de SecOps se describen bien mediante las funciones del Marco de ciberseguridad de NIST de Detectar, Responder y Recuperar.

4.- Seguridad en nube: La seguridad de cómputo en la nube o simplemente seguridad en la nube es un subdominio de la seguridad informática, seguridad de redes y más ampliamente, seguridad de información

5.- Gobernanza y protección de datos: Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos

6.- Análisis de datos en ciberseguridad: El análisis de datos es el uso de procesos y tecnología, generalmente algún tipo de software de análisis, para extraer información valiosa de los conjuntos de datos. Luego, esta información se aplica de varias maneras según el negocio, su industria y otros requisitos únicos.

Fundación GOODJOB

WEBS ADICIONALES E INTERESANTES:

- Serie “El enemigo anónimo”: https://www.elenemigoanonimo.com/
- Guru99: “What is hacking?” https://www.guru99.com/what-is-hacking-an-introduction.html (y la secuencia de tutoriales, https://www.guru99.com/ethical-hacking-tutorials.html).
- Revisar el mapa de todos los dominios de Ciberseguridad: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang (https://app.box.com/s/sj5xaz8a1461e7u7si3ip1361r070fed)
- Ejercicios simples sobre Ciberseguridad: https://www.osi.es/sites/default/files/docs/senior/osi_ejercicios-actividades-practicas-primeros-pasos-ciberseguridad.pdf
- Completar el juego Hackend: https://hackend.incibe.es/
- Recursos documentales sobre ciberseguridad y hacking: https://derechodelared.com/documentales-de-ciberseguridad-hacking/
- Ejercicios avanzados en HackTheBox https://www.hackthebox.com/. Escoge los ejercicios que creas que son asequibles para ti si lo consideras.