GUÍA DIDÁCTICA

CURSO DE CIBERSEGURIDAD

INTRODUCCIÓN

Bienvenido/a al curso online de Formación en CIBERSEGURIDAD.

Valoramos y reconocemos el esfuerzo que suponen los estudios a distancia, por lo que tratamos de hacer la experiencia on-line lo más intuitiva y sencilla posible.

La presente guía está diseñada para **acompañarte y orientarte sobre los contenidos** e instrucciones que deberás desarrollar durante el curso virtual.

Lee atentamente las **pautas y orientaciones** de la Guía y, para cualquier inquietud y/o orientación sobre el desarrollo del curso, **comunícate con el tutor o tutora** del campus, a través del sistema de mensajería interna.

CONTENIDOS DEL CURSO

EEl activo más importante de cualquier empresa so**n los datos y la información**, la ciberseguridad es clave para garantizar que están protegidos de **robos** o manipulación por terceros con **fines delictivos**. Las medidas técnicas son solo una parte de la solución para una política de protección de la información eficaz. La forma en que los empleados manejan la información de la empresa es, al menos, igual de importante ya que cada empleado puede ser el objetivo de los **ciberdelincuentes**.

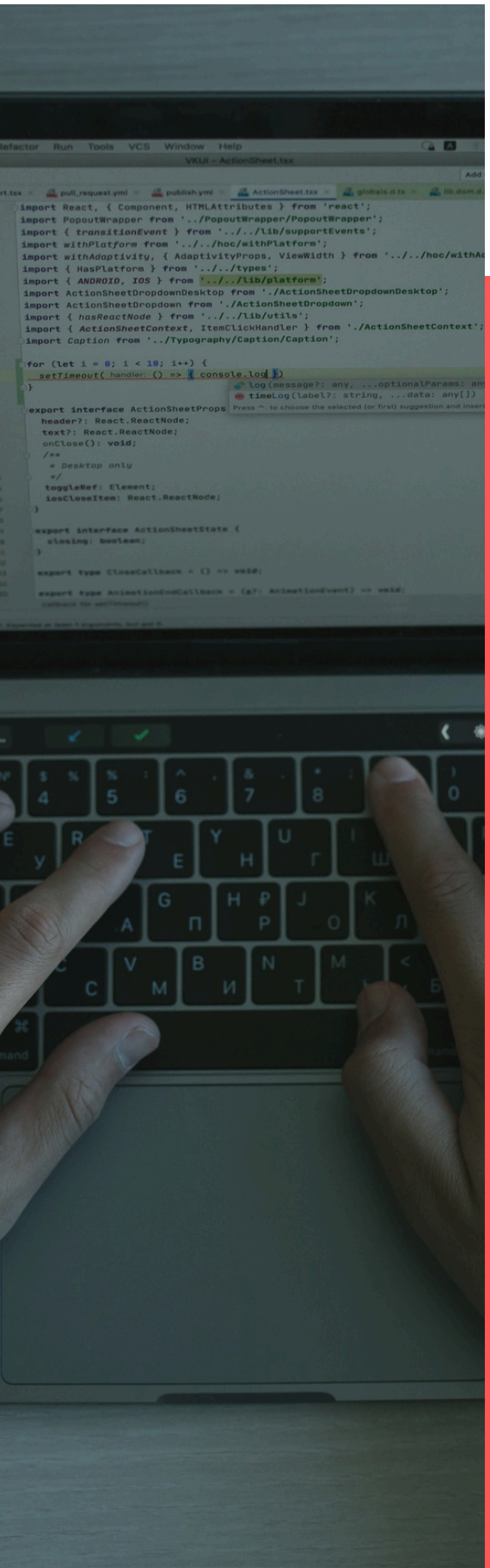
A lo largo de este curso online, sin necesidad de tener grandes conocimientos tecnológicos y a través de **píldoras formativas y microlearnings**, la plantilla aprenderá a identificar las principales amenazas y tipos de ataques a la seguridad de la información, los principios y buenas prácticas en materia de seguridad informática y conocerán la normativa esencial en materia de la protección de datos.

OBJETIVOS

Que todos el personal de tu organización sea **competente** para comportarse adecuadamente en el caso de que haya intentos de partes malintencionadas de obtener acceso a sistemas e información.

Al finalizar esta acción formativa podrán:

- Entender los principales retos de la **gestión y clasificación de la información**.
- Identificar las principales **herramientas de seguridad** y su aplicación en cada caso.
- Entender y manejar los **conceptos esenciales relacionados con ciberseguridad, la ingeniería social, la privacidad, las amenazas informáticas** y cómo defenderse de ellas.
- Estudiar cómo gestionar y responder a **incidentes de seguridad.**
- Analizar los problemas de **privacidad y de seguridad** en el uso de los dispositivos y en las acciones asociadas a una nueva forma de trabajar.



CONTENIDOS DEL CURSO

Curso de Ciberseguridad

- Ciberseguridad para ejecutivos

Los ejecutivos y managers desempeñan un papel crucial en la seguridad de la información. En este módulo formativo de introducción, no solo aprenderás por qué la ciberseguridad es importante y cómo manejar los riesgos cibernéticos, sino que también obtendrás consejos prácticos para proteger a la organización contra las amenazas cibernéticas. Después de completar esta formación, puedes crear un plan tú mismo para empezar a trabajar de inmediato.

- Gestión de riesgos

En esta formación, aprenderás qué es la gestión de riesgos, qué riesgos puedes encontrar y cuál es tu papel. Descubre cuál es el rol del administrador de riesgos dentro de la organización, aprende a mapear los riesgos mediante una autoauditoría y cuándo es importante solicitar el asesoramiento del administrador de riesgos.

- GDPR (Reglamento General de Protección de datos)

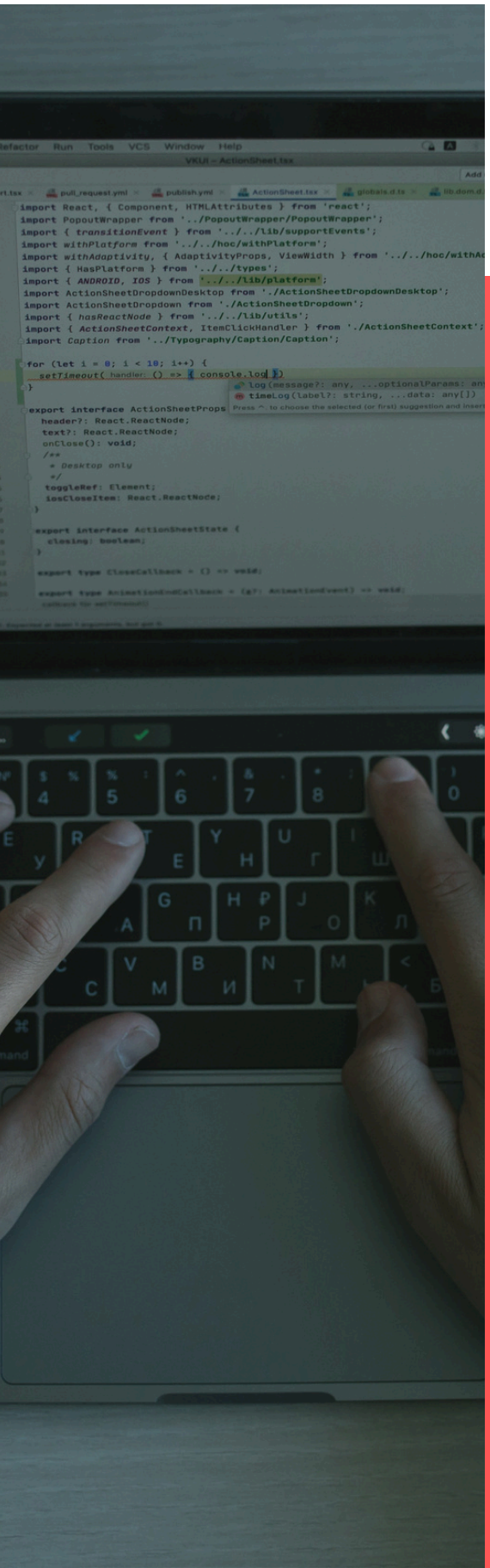
El Reglamento General de Protección de Datos, o GDPR, entró en vigor en 25 de mayo de 2018. Desde entonces, todas las organizaciones deben de garantizar el cumplimiento de esta nueva legislación europea de privacidad. En este módulo conocerás las principales pautas del GDPR y la forma correcta de proteger, procesar y almacenar datos personales.

- La nueva forma de trabajar.

La nueva forma de trabajar nos ha llevado a trabajar en cualquier momento y en cualquier lugar, pero esta forma de trabajo flexible no está exenta de riesgos para la seguridad de la información. Esta formación explica cómo aprovechar las ventajas de la nueva forma de trabajar de forma óptima y segura.

- Trabajar en la nube.

Gracias a la nube tienes acceso a la información en cualquier momento y en cualquier lugar. Ofrece enormes posibilidades, pero también conlleva riesgos. En esta formación, aprenderás todo lo que debes saber para trabajar de forma segura en la nube.



CONTENIDOS DEL CURSO

- Trabajar en espacios públicos.

El trabajo flexible es una oportunidad para empleados y organizaciones. Cada vez más empleados pueden trabajar donde y cuando quieran: desde casa, en la oficina, en el tren o en un espacio público, pero ello conlleva diferentes riesgos de seguridad. En menos de 2 minutos, a través de este vídeo, aprenderás a aprovechar de manera óptima el trabajo en lugares públicos sin correr el riesgo de perder información sensible o confidencial.

- Trabajar de forma segura fuera de la oficina.

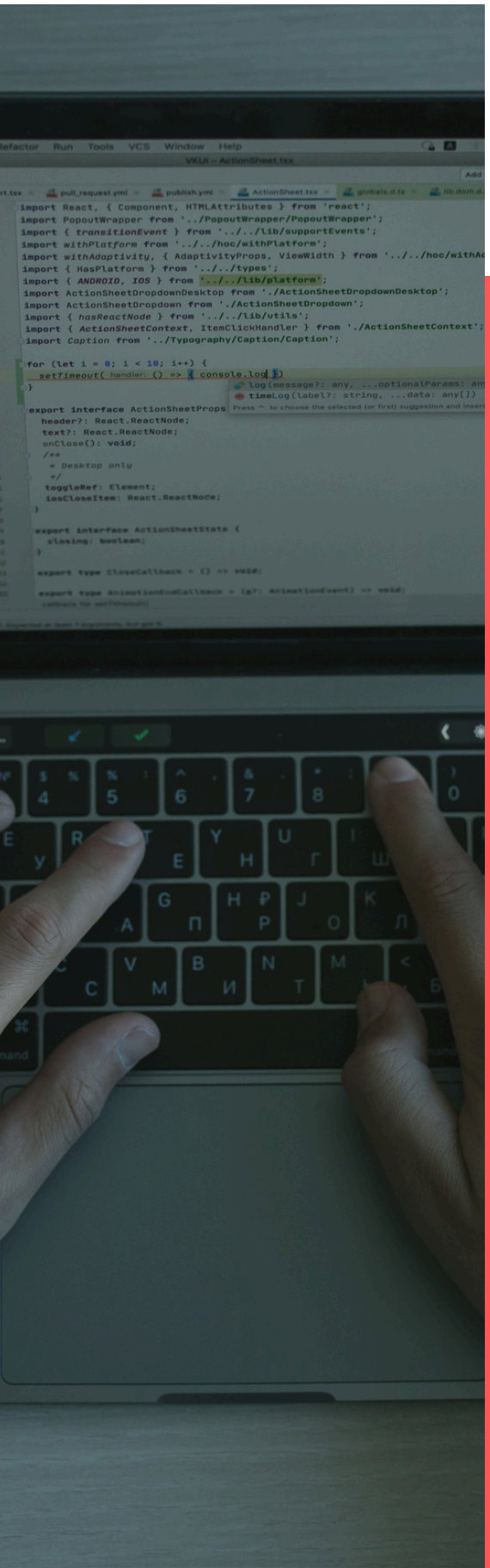
Trabajar fuera de la oficina es diferente a trabajar en la oficina. Fuera de la oficina, trabajas con dispositivos móviles y no dispones de una conexión a Internet segura de forma natural. En aproximadamente 3 minutos, este microlearning te enseña cómo puedes trabajar de manera óptima fuera de la oficina, sin riesgos de incidentes de seguridad de la información.

- Control de acceso.

Este video muestra por qué el control de acceso es importante para la protección de la información. El uso de un pase de acceso mejora la seguridad de un edificio porque solo las personas con pase tienen acceso directo. También proporciona información sobre quién está presente en el edificio. En caso de calamidades, es importante tener esa información. Por lo tanto, se debe de informar siempre de inmediato de la pérdida de un pase al departamento o al responsable.

- Clasificación de la información.

Trabajar con información es una parte esencial para una organización, por lo tanto, es importante que se clasifique de forma correcta. Así es como se indica qué niveles de protección son necesarios para que todos conozcan qué niveles de confidencialidad, integridad y disponibilidad se aplican al trabajar con dicha información y que no se pierda ni termine en manos equivocadas.



CONTENIDOS DEL CURSO

- ¿Cómo se clasifica la información? elemento práctico.

Trabajar con información es una parte importante de cualquier organización. Al clasificar correctamente la información se indica qué nivel de protección es necesario de forma que todos conozcan qué niveles de confidencialidad, integridad y disponibilidad deben aplicar al trabajar con ella. En este microlearning aprenderás por qué clasificar la información es importante para tu organización.

- Ingenería social.

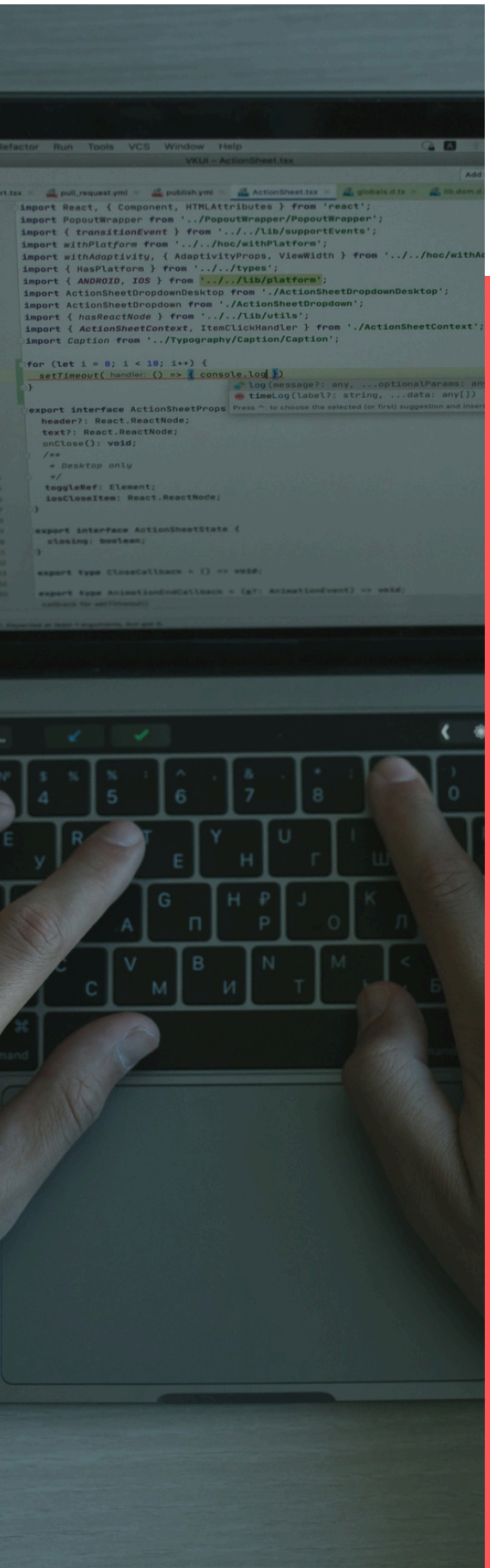
Un ingeniero social manipula el eslabón más débil de la seguridad de la información: las personas. Intenta acceder a la información de diversas formas, para poder modificarla o utilizarla con fines delictivos. En esta formación descubrirás cómo opera un ingeniero social y cómo puedes reconocer un ataque de ingeniería social.

- Seguridad física.

Las amenazas más importantes contra las que la seguridad física protege a una organización son las amenazas intencionadas de las personas, como pueden ser el robo o el acceso accidental. En este módulo conocerás las medidas puede tomar una organización para garantizar la seguridad física y cuál debe ser tu papel ante estas amenazas.

- Malware.

Malware es la abreviatura de "software malicioso". Es un nombre genérico para diferentes tipos de software malicioso y puede causar mucho daño a una organización. Por ejemplo, la información personal puede ser robada o la información sensible puede hacerse pública. Esta formación garantiza que conozcas los peligros de los diferentes tipos de malware y te prepares para prevenir infecciones.



CONTENIDOS DEL CURSO

- Phising.

Todos los días, los delincuentes intentan robar información confidencial mediante el uso de ingeniería social y otras formas de engaño. En esta formación, aprenderás a reconocer y denunciar un ataque de phishing.

- Phising - ejemplo práctico.

El phishing es una de las mayores amenazas de delitos informáticos en este momento. Hay muchas formas de ingeniería social, pero el phishing es, con mucho, la más conocida y exitosa. La idea es simple: después de hacer clic en un enlace o abrir un archivo adjunto, el ciberdelincuente tiene acceso a su información. Este video te muestra cómo puede reconocer correos electrónicos sospechosos, cuáles son los peligros y qué debes hacer si las cosas salen mal.

- Otros aspectos de seguridad:
  - Contraseñas fuertes
  - Cómo informar sobre los incidentes relacionados con la seguridad de la información.

LAS ACTIVIDADES

El curso es **totalmente virtual**. Todas las actividades se pueden desarrollan en cualquier horario, desde cualquier ordenador con acceso a Internet, desde cualquier lugar.

TIEMPO ASIGNADO

Las actividades y contenidos están diseñadas para que se desarrollen en aproximadamente 4 **horas**, por lo que sugerimos hacer una planificación personal para cumplir con los objetivos del curso.

MATERIALES DIDÁCTICOS

El desarrollo del temario se realizará mediante **vídeo-clases** de los/as profesores/as y presentaciones. Adicionalmente, el alumnado tendrá a su disposición **material complementario** y bibliografía por si quiere ampliar sus conocimientos.

LOS MEDIOS

El curso se desarrollará utilizando los módulos de la plataforma moodle, permitiéndo una comunicación virtual permanente a través de:

- **Foro General del Aula**, que permite el intercambio asincrónico del grupo sobre un tema compartido.
- **Novedades del Docente**, para las comunicaciones realizadas por el profesorado.

EVALUACIÓN DEL CURSO

Al final de cada uno de los módulos se realizarán **cuestionarios de autoevaluación** que serán de obligado cumplimiento para poder pasar al siguiente módulo.

El alumnado dispondrá de **intentos ilimitados para resolver cada cuestionario**, con tiempo **ilimitado.** Se escogerá el intento con mayor puntuación.

Al final del curso se realizará un **examen final**, de obligado cumplimiento, con los contenidos de todos los módulos.

Se requerirá de una **puntuación mínima** de al menos un 3.5 **en los cuestionarios** para poder hacer media. Se considerará **superado** el curso cuando se obtenga una nota global **media igual o superior a 5.**

La superación del curso supondrá la obtención de un **certificado acreditativo** de superación y aprovechamiento del curso.