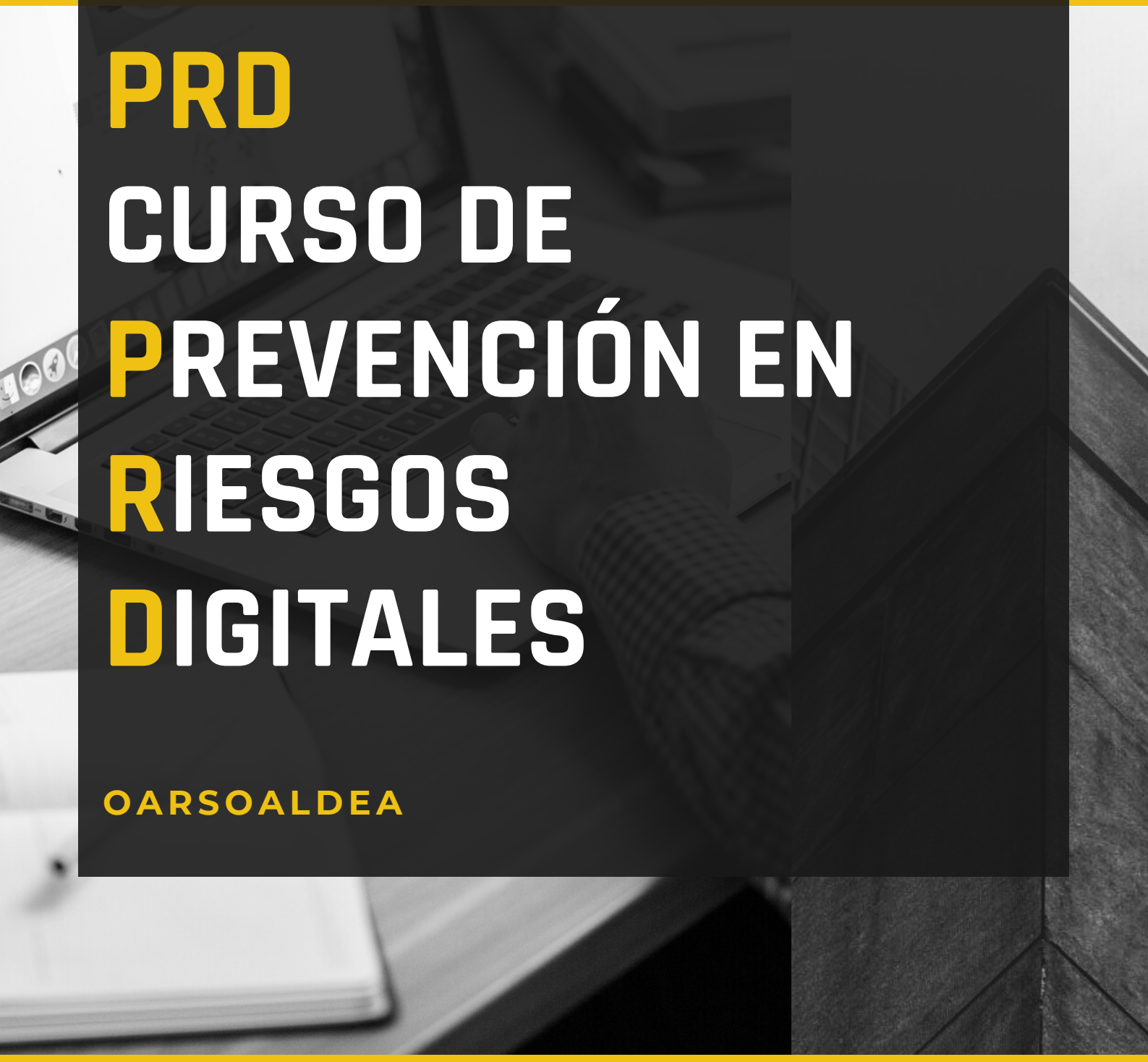
2023

PRD
CURSO DE PREVENCIÓN EN RIESGOS DIGITALES

OARSOALDEA



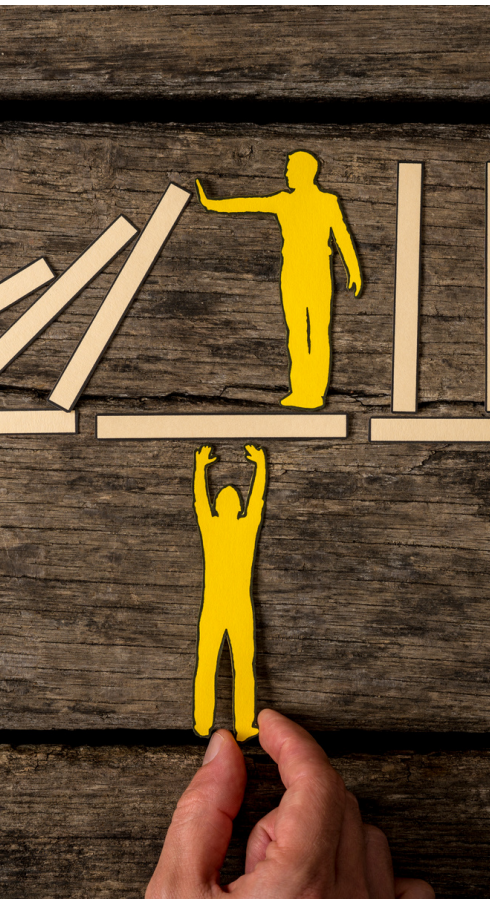
Oarsoaldea · berpiztu · Eusko Jaurlaritza Gobierno Vasco · OARSOALDEA · Z.A.P. Lehentasunezko Jarduera Zonaldea Zona De Actuación Prioritaria

INTRODUCCIÓN

Se considera que en una empresa el eslabón más débil en materia de ciberseguridad son las personas. Pero, al mismo tiempo, cuanto mayor conocimiento y concienciación tengan dichas personas pueden convertirse en el eslabón más fuerte. Porque la ciberseguridad no es solo cuestión de tecnología, también de personas.

El 85% de los ciber-incidentes comienzan por un error humano. Para reducir este porcentaje es necesaria formación para mejorar las habilidades digitales. Cuando las empresas forman a sus empleadxs en ciberseguridad, tienen un 93% de probabilidades de que estas personas pongan sus conocimientos en práctica.

La formación para la **P**revención en **R**iesgos **D**igitales funciona con sesiones de concienciación respecto a las amenazas y vulnerabilidades más comunes a las que están expuestos las empresas y los trabajadores que usan herramientas y procesos digitales. Se trata de poner las bases para que los empleados sean más conscientes y empiecen a desarrollar una cultura de prevención que les permita gestionar con autonomía los riesgos digitales que implica su labor.



FORMATO

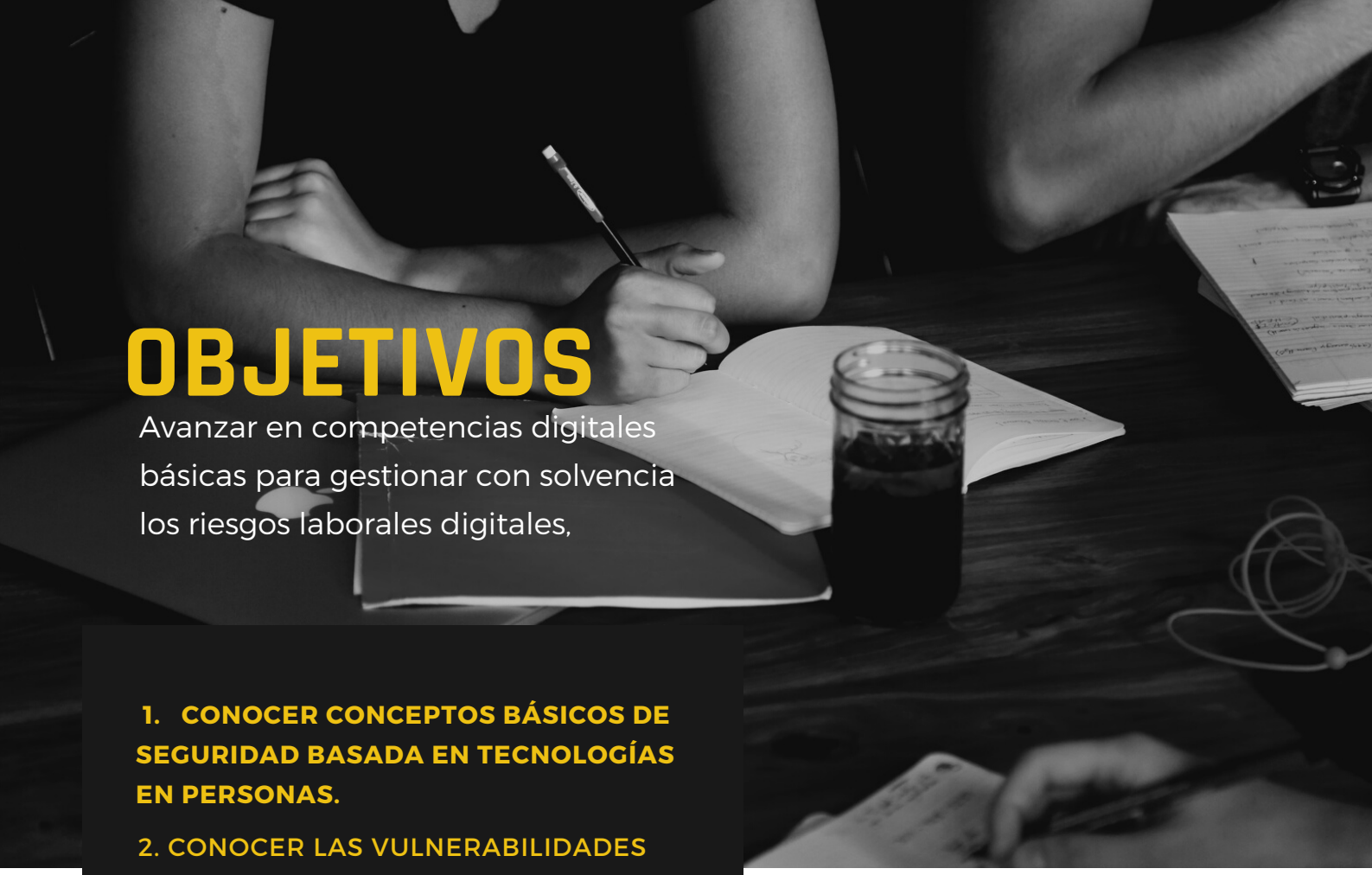
Curso presencial y GRATUITO de 1 jornada con una duración de 4 horas.

Para un mejor aprovechamiento de la sesión se plantea su realización en grupos de 10 – 15 personas.

¿A QUIÉN VA DIRIGIDO?

El curso **P**revención de **R**iesgos **D**igitales está dirigido a cualquier persona usuaria de herramientas ofimáticas o de sistemas de información de la empresa.

Personas autónomas, trabajadoras o desempleadas que quieran mejorar sus competencias en ciberseguridad.



OBJETIVOS

Avanzar en competencias digitales básicas para gestionar con solvencia los riesgos laborales digitales,

1. **CONOCER CONCEPTOS BÁSICOS DE SEGURIDAD BASADA EN TECNOLOGÍAS EN PERSONAS.**
2. CONOCER LAS VULNERABILIDADES QUE PUEDEN UTILIZAR LOS ATACANTES Y CÓMO PREVENIRLAS.
3. **HERRAMIENTAS Y CONCEPTOS DE SEGURIDAD.**
4. CONOCER LOS ATAQUES MÁS FRECUENTES Y COMO ESTABLECER MEDIDAS DE PROTECCIÓN.
5. **BUENA HIGIENE DIGITAL.**
6. CONOCER LA ARQUITECTURA DE LOS CORREOS FRAUDULENTOS.
7. **QUÉ HACER EN CASO DE SUFRIR O SOSPECHAR QUE HEMOS SIDO VÍCTIMAS DE UN ATAQUE.**
8. IMPLICACIONES DE NO GESTIONAR ADECUADAMENTE LA HUELLA DIGITAL PERSONAL.

CONTENIDOS

1. **AMENAZAS:** ATACANTES, RIESGOS POTENCIALES Y MÉTODOS USADOS.
2. **VULNERABILIDADES:** TECNOLOGÍA Y PERSONAS. EL ESLABÓN MÁS DÉBIL.
3. **PREVENCIÓN:** POLÍTICAS, HÁBITOS, HIGIENE DIGITAL Y BUENAS PRÁCTICAS DE SEGURIDAD.
4. **HERRAMIENTAS:** TECNOLOGÍAS QUE AYUDAN A TRABAJAR DE FORMA SEGURA.
5. **CIBERRESILENCIA:** ANTICIPAR, RESISTIR, RECUPERAR, AVANZAR.
6. **MÁS ALLÁ DE TU ESCRITORIO:** CONCEPTOS HOLÍSTICOS DE CIBERSEGURIDAD.

IMPARTIDO POR K35

Este taller ha sido diseñado y será impartido por especialistas del departamento de Ciberseguridad de K35 liderada por Jon Bengoetxea.

K35 es una empresa de la comarca pionera en el ámbito TIC, especializada en Ciberseguridad, infraestructuras TI y entornos de usuario modernos para ayudar a las empresas a evolucionar y mantener, de forma duradera, la seguridad, el rendimiento y la productividad que necesitan.

JON BENGOETXEA
K35 & KEVO IA technologies