



COMM01 – CIBERSEGURIDAD Y REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) APLICADO AL COMERCIO ELECTRÓNICO

DURACIÓN: 40 HORAS

MODALIDAD: PRESENCIAL/AULA VIRTUAL

FECHA INICIO/FIN:

OBJETIVOS:

Identificar las tendencias, normativa vigente y herramientas en materia de ciberseguridad y protección de datos para su aplicación y su utilización en las transacciones que se realizan a través del comercio electrónico.

Identificar y aplicar las obligaciones que rigen a todo prestador de servicios de venta online, así como acercar los derechos de los clientes/usuarios de estas plataformas, atendiendo de forma especial al tratamiento de los datos de carácter personal.

Determinar los riesgos, amenazas y vulnerabilidades que, desde la perspectiva de la seguridad de la información, afectan a los proyectos de comercio electrónico y utilizar las herramientas de Ciberseguridad para hacer frente a los mismos.

PARTICIPANTES:

Personas trabajadoras OCUPADAS que han estado en ERTE

Personas trabajadoras DESEMPLEADAS inscritas en los servicios públicos de empleo.

Personas trabajadoras en situación de ERTE.

REQUISITOS DE ACCESO:

Cumplir como mínimo alguno de los siguientes requisitos:

- Título de Técnico Superior (FP Grado Superior) o equivalente
- Haber superado la prueba de acceso a Ciclos Formativos de Grado Superior
- Haber superado cualquier prueba oficial de acceso a la universidad
- Certificado de profesionalidad de nivel 3
- Título de Grado o equivalente
- Título de Postgrado (Máster) o equivalente

Experiencia profesional

Experiencia profesional como docente de Formación Profesional para el Empleo o como profesor de Formación Profesional en la familia profesional de Comunicación y Marketing, preferentemente en el área profesional de Marketing y Relaciones Públicas o Compraventa, durante al menos 6 meses en los últimos 2 años.

CONTENIDOS:

1. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN PROYECTOS DE COMERCIO ELECTRÓNICO

- 1.1 Determinación de los aspectos clave del comercio electrónico (e-commerce)
 - 1.1.1 Aproximación al nuevo paradigma del entorno digital
 - 1.1.2 Conceptos básicos del comercio electrónico
 - 1.1.3 Identificación de las posibilidades y aplicaciones prácticas del comercio electrónico
 - 1.1.4 Aplicación de las garantías legales en proyecto de e-commerce.
 - 1.1.5 Identificación de las principales plataformas tecnológicas para desarrollar un ecommerce
- 1.2 Identificación de los elementos necesarios para afrontar con garantías la adaptación al Reglamento General de Protección de Datos en proyectos de ecommerce.
 - 1.2.1 Marco jurídico aplicable: principales novedades en el ámbito legislativo.
 - 1.2.2 Conceptos teóricos básicos de la normativa protectora de datos de carácter personal aplicado al comercio electrónico: datos de carácter personal; tratamiento de datos; figuras del tratamiento de datos; tipos de tratamiento de datos; categoría de datos; transferencias de datos (internacionales/ transfronterizas).
 - 1.2.3 Tratamiento de los datos conforme a las bases de legitimación: el consentimiento como elemento clave.
 - 1.2.4 Obligaciones del responsable del tratamiento.
 - 1.2.5 Obligaciones del encargado del tratamiento.
- 1.3 Comprensión de los aspectos legales básicos que tienen que ser respetados por un servicio de venta online
 - 1.3.1 Ley de Servicios de la Sociedad de la Información (LSSI): ámbito de aplicación, principales obligaciones para plataformas de servicios online y régimen sancionador
 - 1.3.2 Régimen jurídico de las comunicaciones comerciales, ofertas y concursos por vía electrónica.
 - 1.3.3 Uso de cookies y tecnologías similares: tipología y obligaciones
 - 1.3.4 Contratos por vía electrónica: obligaciones previas e información posterior a la contratación.
 - 1.3.5 Terceros de confianza: servicios de confianza electrónica.
- 1.4 Exposición de las obligaciones en materia de consumidores y usuarios
 - 1.4.1 Información previa a la celebración del contrato
 - 1.4.2 Factura electrónica
 - 1.4.3 Entrega de los bienes
 - 1.4.4 Información post-contractual
 - 1.4.5 Derecho de desistimiento

2. CIBERSEGURIDAD EN EL COMERCIO ELECTRÓNICO

2.1 Identificación de las ciberamenazas y formas de fomentar la ciberseguridad en el comercio electrónico

2.1.1 Principales riesgos, amenazas y vulnerabilidades

2.1.2 Análisis de las Medidas de protección

2.1.3 Buenas prácticas para mejorar la confianza de los clientes

2.2 Determinación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.

2.2.1 Necesidad de llevar a cabo un análisis de amenazas y riesgos potenciales

2.2.2 Evaluaciones de impacto en materia de protección de datos

2.2.3 Plan de acción para tratar los riesgos detectados

2.3 Actuación ante un incidente de seguridad

2.3.1 Detección y comunicación en punto de notificación establecido

2.3.2 Fases para la gestión y tratamiento de incidentes de seguridad

2.3.3 Obligación de notificación a la autoridad de control y usuarios en caso de que el incidente afecte a datos personales

2.3.4 Ejemplos de incidentes de seguridad

PARA PODER TENER SUPERADO EL CURSO HAY QUE CUMPLIR LOS SIGUIENES REQUISITOS:

- TENER SUPERADAS TODAS LAS PRUEBAS DE EVALUACIÓN QUE SE REALICEN DURANTE EL PROCESO DE APRENDIZAJE Y LA PRUEBA FINAL DE LA ACCIÓN FORMATIVA.