COMM01. Ciberseguridad y Reglamento General de Protección de Datos (RGPD) aplicado al comercio electrónico.

Sku: PS_COMM01

Horas: 40

Formato: HTML

OBJETIVOS

- 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.

CONTENIDOS

- **Unidad 1. Reglamento general de protección de datos (RGPD) en proyectos de comercio electrónico**
  - Conocimiento / Capacidades cognitivas y prácticas
    - Determinación de los aspectos clave del comercio electrónico (e-commerce)
    - Aproximación al nuevo paradigma del entorno digital
    - Conceptos básicos del comercio electrónico
    - Identificación de las posibilidades y aplicaciones prácticas del comercio electrónico
    - Aplicación de las garantías legales en proyecto de ecommerce.
    - Identificación de las principales plataformas tecnológicas para desarrollar un ecommerce
    - Identificación de los elementos necesarios para afrontar con garantías la adaptación al Reglamento General de Protección de Datos en proyectos de ecommerce.
    - Marco jurídico aplicable: principales novedades en el ámbito legislativo.
    - 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).
        - Tratamiento de los datos conforme a las bases de legitimación: el consentimiento como elemento clave.
        - Obligaciones del responsable del tratamiento.
        - Obligaciones del encargado del tratamiento.
        - Comprensión de los aspectos legales básicos que tienen que ser respetados por un servicio de venta online
        - Ley de Servicios de la Sociedad de la Información (LSSI): ámbito de aplicación, principales obligaciones para plataformas de servicios online y régimen sancionador.
        - Régimen jurídico de las comunicaciones comerciales, ofertas y concursos por vía electrónica.
        - Uso de cookies y tecnologías similares: tipología y obligaciones
        - Contratos por vía electrónica: obligaciones previas e información posterior a la contratación.
        - Terceros de confianza: servicios de confianza electrónica.
        - Exposición de las obligaciones en materia de consumidores y usuarios.
        - Información previa a la celebración del contrato
        - Factura electrónica
        - Entrega de los bienes
        - Información post-contractual
        - Derecho de desistimiento
    - Habilidades de gestión, personales y sociales.
        - Concienciación de la importancia de aplicar correctamente la normativa de protección de datos para proteger y asegurar el derecho fundamental a la protección de datos y privacidad de los usuarios del comercio electrónico.
        - Interés por la utilización de las herramientas y plataformas de e-commerce como base de la realización de transacciones seguras.
        - Responsabilidad a la hora de implementar las garantías legales en los proyectos de e-commerce.

- **Unidad 2. Ciberseguridad en el comercio electrónico.**
    - Conocimiento / Capacidades cognitivas y prácticas
        - Identificación de las ciberamenazas y formas de fomentar la ciberseguridad en el comercio electrónico.
        - Principales riesgos, amenazas y vulnerabilidades
        - Análisis de las Medidas de protección.
        - Buenas prácticas para mejorar la confianza de los clientes .
        - Determinación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.
        - Necesidad de llevar a cabo un análisis de amenazas y riesgos potenciales
        - Evaluaciones de impacto en materia de protección de datos

        - Plan de acción para tratar los riesgos detectados
        - Actuación ante un incidente de seguridad.
        - Detección y comunicación en punto de notificación establecido
        - Fases para la gestión y tratamiento de incidentes de seguridad
        - Obligación de notificación a la autoridad de control y usuarios en caso de que el incidente afecte a datos personales
        - Ejemplos de incidentes de seguridad
    - Habilidades de gestión, personales y sociales
        - Concienciación de los riesgos para los derechos y libertades de los usuarios y de la importancia de aplicar políticas y medidas técnicas y organizativas a fin de prevenir las ciberamenazas.
        - Interés por la seguridad de la información y la tecnología.