MASTER ONLINE EN SEGURIDAD DE LA INFORMACIÓN

CARACTERÍSTICAS DEL CURSO

El curso se realiza de forma íntegra en nuestro “campus virtual”, el cual está operativo 24x7x365.

El campus dispone de diferentes vías de comunicación con los tutores/as del curso, desde las que el alumno podrá plantear las dudas que le surjan durante la realización de su formación.

La duración del curso es de 350h. las cuales se pueden realizar durante todo el periodo de vigencia de las claves de acceso.

A la finalización del curso con éxito, tras superar los controles de evaluación y la revisión de los contenidos formativos, se expedirá la certificación y será enviado digitalmente al alumno finalizado.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS - RGPD

OBJETIVOS

- Conocer los principios fundamentales de la protección de datos, así como las novedades que introduce el **Reglamento General de Protección de Datos Europeo.**
- Asignar las responsabilidades de cada uno de los sujetos que participan en el tratamiento de datos personales en la empresa.
- Conocer qué es un Delegado de Protección de Datos y qué empresas están obligadas a nombrar un DPO.
- Describir las principales obligaciones en el tratamiento de datos personales, así como los derechos que asisten a las personas afectadas.
- Distinguir entre cesión de datos y prestación de servicios.
- Introducir en la seguridad en la protección de datos, y cómo notificar una violación de seguridad.
- Conocer las infracciones en materia de protección de datos y qué sanciones podrían conllevar.

ÍNDICE DE CONTENIDOS

4.2.1. Derecho de oposición.
4.2.2. Derecho de acceso.
4.2.3. Derecho a la portabilidad de datos.
4.2.4. Derecho de rectificación.
4.2.5. Derecho de limitación del tratamiento.
4.2.6. Derecho de supresión o derecho al olvido.
4.2.7. Derecho a Indemnización.
4.2.8. Derechos de los ciudadanos ante las AA.PP.

5. CESIÓN DE DATOS

5.1. Qué se considera cesión o comunicación.
5.2. Comunicación de datos entre Administraciones Públicas.
5.3. Prestaciones de servicios.

6. SEGURIDAD EN LA PROTECCIÓN DE DATOS

6.1. Introducción.
6.2. Evaluaciones de Impacto.
6.3. Aplicación de medidas técnicas y organizativas.
6.4. Notificación de una violación de la seguridad de los datos personales.

7. INFRACCIONES Y SANCIONES

7.1. Introducción.
7.2. Infracciones graves.
7.3. Infracciones leves.
7.4. Sanciones.

SEGURIDAD DE LA INFORMACIÓN

OBJETIVOS

- Definir el concepto y elementos fundamentales de la seguridad de la información.
- Establecer los principios de la gestión de la seguridad de la información.
- Conocer las fases del ciclo de mejora continua del Sistema de Gestión.
- Conocer los elementos que podrían incluirse en el documento de política de seguridad de cualquier organización.
- Conocer los elementos de seguridad: firewall, protocolos, encriptación, etc.
- Ver a qué ataques y amenazas se enfrentan las empresas conectadas a redes.
- Describir los principales delitos y riesgos en la seguridad de los datos de carácter personal.
- Incidir en la importancia de la política de uso y gestión de contraseñas.
- Conocer los niveles de seguridad a aplicar según los tipos de datos personales.
- Establecer las medidas de seguridad en tres niveles.
- Describir los elementos del documento de seguridad.
- Conocer los sistemas de control y evaluación del sistema de seguridad: auditorías. Así como los sistemas de autorregulación: códigos de conductas y certificación, que favorece el nuevo Reglamento Europeo de Protección de Datos Personales.

ÍNDICE DE CONTENIDOS

6.3. Medidas de seguridad de nivel básico.
6.4. Medidas de seguridad de nivel medio.
6.5. Medidas de seguridad de nivel alto.
6.6. Medidas de seguridad según el elemento de la organización.
6.7. Documento de seguridad.
6.8. Auditoría de seguridad.
6.9. Codigos de conducta.
6.10. Certificación.

APLICACIÓN PRÁCTICA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS - RGPD

OBJETIVOS

- Aplicar los principios fundamentales de la protección de datos en su organización, así como las novedades que introduce el **Reglamento General de Protección de Datos Europeo.**
- Asignar las responsabilidades de cada uno de los sujetos que participan en el tratamiento de datos personales en la empresa.
- Conocer cuáles son las empresas que deben nombrar un delegado de protección de datos y cuáles son sus obligaciones.
- Establecer las medidas necesarias para proteger los derechos de los titulares de los datos personales y permitirles ejercerlos.
- Aplicar la protección de datos en los contratos de servicios que firme la empresa con sus proveedores de servicios.
- Distinguir las operaciones de cesión de datos y aplicar los requisitos que la ley establece para realizarlas.
- Establecer los requisitos necesarios para proteger los datos personales en la gestión de los recursos humanos.
- Conocer cuestiones específicas como son el tratamiento de morosos o de la publicidad desde el respeto y la protección de los datos personales, además de las características de determinados sectores como son las cadenas hoteleras, las comunidades de vecinos, etc.
- Aplicar los principios de protección de datos a la videovigilancia.
- Conocer las infracciones en materia de protección de datos y qué sanciones podrían conllevar.

ÍNDICE DE CONTENIDOS

9.3. Autoridades competentes: Agencia Española de Protección de datos y Agencias Autonómicas.
9.4. Responsable del tratamiento.
9.5. Responsable de seguridad de la información.
9.6. Encargado del tratamiento.
9.7. Afectado o interesado.
9.8. Otros: usuario, tercero, representante.

10. DELEGADO DE PROTECCIÓN DE DATOS (DPO)
10.1. Delegado de protección de datos.
10.2. Entidades que deben nombrar un delegado de protección de datos.
10.3. Funciones.
10.4. Obligaciones.
10.5. Cualificación del delegado de protección de datos.
10.6. Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (esquema AEPD-DPD).
10.7. Información sobre personas certificadas.

11. OBLIGACIONES Y DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS
11.1. Obligaciones.
11.1.1. Información en la recogida de datos.
11.1.2. Consentimiento del afectado.
11.1.3. Registro de actividades de tratamiento.
11.2. Derechos de las personas.
11.2.1. Derecho de oposición.
11.2.2. Derecho de acceso.
11.2.3. Derecho a la portabilidad de datos.
11.2.4. Derecho de rectificación.
11.2.5. Derecho de limitación del tratamiento.
11.2.6. Derecho de supresión o derecho al olvido.
11.2.7. Derecho a Indemnización.
11.2.8. Derechos de los ciudadanos ante las AA.PP.

12. CESIÓN DE DATOS
12.1. Qué se considera cesión o comunicación.
12.2. Comunicación de datos entre Administraciones Públicas.
12.3. Prestaciones de servicios.

13. SEGURIDAD EN LA PROTECCIÓN DE DATOS
13.1. Introducción.
13.2. Evaluaciones de Impacto.
13.3. Aplicación de medidas técnicas y organizativas.
13.4. Notificación de una violación de la seguridad de los datos personales.

14. INFRACCIONES Y SANCIONES
14.1. Introducción.
14.2. Infracciones graves.
14.3. Infracciones leves.
14.4. Sanciones.

15. **PROTECCIÓN DE DATOS EN DIFERENTES SECTORES DE ACTIVIDAD**
15.1. Introducción.
15.2. Ficheros de Recursos Humanos.
15.3. Video vigilancia.
15.4. Comunidades de vecinos.
15.5. Telecomunicaciones.
15.6. Ficheros de solvencia patrimonial y ficheros de morosos.
15.7. Cadenas Hoteleras.

16. SUPUESTOS PRÁCTICOS

- Teléfonos de familiares y amigos
- Hoja de cálculo clientes
- Fichero manual
- Campo observaciones
- Fichero con fines promocionales
- Datos de menores
- Fichero de Curriculums
- Información sobre cuentas bancarias
- Prestación de servicios de Marketing
- Ficheros de solvencia patrimonial
- Derecho de Acceso
- Identificación por razones de seguridad
- Fiesta de inauguración
- Control de Recursos Humanos
- Usuario y contraseña
- Contraseñas
- Caducidad de contraseñas
- Acceso no autorizado a su ordenador

FIRMA Y FACTURACIÓN ELECTRÓNICA

OBJETIVOS

- Adquirir los conocimientos para la utilización de la firma y el certificado electrónico.
- Conocer los requisitos necesarios para la implantación de la facturación electrónica en la empresa.
- Informarse sobre los últimos avances en la normativa, a partir de la publicación de la Ley de impulso de la factura electrónica y la creación del registro contable de facturas en el Sector Público.
- Aplicar la normativa obligatoria relativa a la facturación electrónica en empresas agrupadas en la categoría de: «Empresas que presten servicios al público en general de especial trascendencia económica».
- Conocer las novedades relativas al registro de facturas en el sector público y a la creación del Punto General de Entrada de facturas electrónicas de la Administración General del Estado (FACe).

ÍNDICE DE CONTENIDOS

1.2.3. Aplicaciones: FACe (Punto General de Entrada de Facturas de la Administración General del Estado)

2. LA FIRMA ELECTRÓNICA

2.1. Concepto de firma electrónica
- 2.1.1. Aspectos básicos de la firma electrónica según la ley 59/2003
- 2.1.2. Proceso de firma reconocida
- 2.1.3. Utilidad de la firma electrónica
- 2.1.4. El documento electrónico

2.2. Elementos de la firma electrónica
- 2.2.1. Sistemas criptográficos asimétricos o de clave pública
- 2.2.2. Las funciones hash
- 2.2.3. Los sellos temporales
- 2.2.4. La confidencialidad de los mensajes

2.3. Tipos de firmas
- 2.3.1. Firma electrónica simple
- 2.3.2. Firma electrónica avanzada
- 2.3.3. Firma electrónica reconocida o cualificada

2.4. Dispositivos externos de firma electrónica
- 2.4.1. Ejemplo software: eCoFirma
- 2.4.2. El certificado electrónico

3. IMPLANTACIÓN DE LA FIRMA ELECTRÓNICA

3.1. Requisitos básicos
- 3.1.1. Formatos de firma
- 3.1.2. Formatos de firma avanzados

3.2. Costes y plazos
- 3.2.1. ECoFirma
- 3.2.2. Certificado de usuario e Instalación de certificado de raíz de la entidad de certificación
- 3.2.3. Soluciones de escritorio para firma simple de documentos para pymes

3.3. Procesos
- 3.3.1. Banco de España

4. CERTIFICADO ELECTRÓNICO

4.1. Certificado electrónico
- 4.1.1. Qué es la clave pública y la clave privada

4.2. Entidades emisoras de certificados
- 4.2.1. Concepto de prestador de servicios de certificación
- 4.2.2. Prestadores de servicios de certificación de España

4.3. Tipos de certificado electrónico

4.4. Clases de certificados electrónicos

4.5. Procedimiento de obtención de un certificado electrónico de persona física
- 4.5.1. Cómo solicitar un certificado software
- 4.5.2. Cómo descargarlo e instalarlo en el equipo
- 4.5.3. Ciclo de vida de un certificado

4.6. La confidencialidad del certificado electrónico

4.7. Extinción de la vigencia de los certificados electrónico

4.8. Certificados reconocidos
- 4.8.1. Obligaciones del prestador de servicios
- 4.8.2. Comprobación de la identidad
- 4.8.3. El certificado electrónico del prestador extraeuropeo

5. LA FACTURACIÓN ELECTRÓNICA

5.1. Qué es la facturación electrónica
- 5.1.1. ¿Cómo se garantiza la autenticidad del emisor y la integridad del contenido?

5.2. Elementos sobre la factura electrónica

5.2.1. Requisitos
5.2.2. Condicionantes para la realización de e-factura
5.2.3. Certificados adecuados para la facturación electrónica
5.3. Emisor y receptor
5.3.1. Obligaciones de la e-factura para el emisor ó expedidor
5.3.2. Obligaciones de la e-factura para el receptor ó destinatario
5.4. Ventajas e inconvenientes
5.5. Tipos de Facturas
5.5.1. Formatos de factura
5.5.2. Escenarios de emisión y recepción de facturas telemáticas
5.5.2.1. Redes de valor añadido (EDI)
5.5.2.2. Entornos web centralizados
5.5.2.3. ERP to ERP
5.5.3. Digitalización certificadas ó conservación por medios electrónicos de facturas recibidas en papel
5.6. Ejemplos de facturas electrónicas
5.6.1. Factura XML “factura-e”
5.6.2. Add-in en Office
5.6.3. Plataformas de facturación electrónica
5.7. Infracciones y sanciones relacionadas con la facturación electrónica
5.7.1. Infracción tributaria por incumplir obligaciones contables y registrales
5.7.2. Infracción tributaria por incumplir obligaciones de facturación o documentación.
5.7.3. Infracción tributaria por resistencia, obstrucción, excusa o negativa a las actuaciones de la administración tributaria.
5.7.4. Resumen de las infracciones y sanciones relativas a la facturación electrónica