cursos

extensión universitaria

2017

universidad de león

DELEGADO DE PROTECCIÓN DE DATOS (180 HORAS)

06/11/2017 - 05/11/2018

Información y matrícula

Universidad de León
Unidad de Extensión Universitaria y Relaciones Institucionales.
Av. Facultad de Veterinaria, 25. 24004 · LEÓN.
Tel. 987 291 961 y 987 293 372 · Fax 987 291 963.
e-mail:ulesci@unileon.es
http://www.unileon.es/extensionuniversitaria

CEI TRIANGULAR-E3 LOS HORIZONTES DEL HOMBRE

unileon.es

universidad de león ule

DELEGADO DE PROTECCIÓN DE DATOS (180 HORAS)

DIRECTOR:
Luis Panizo Alonso. Profesor titular. Escuela de Ingenierías Industrial, Informática y Aeronáutica. Universidad de León.

LUGAR:
Online

FECHAS:
06/11/2017 - 05/11/2018

HORARIO:
Formación ON LINE. Plataforma abierta 24 horas.

DURACIÓN:
180 horas. Período recomendado para completar la formación: 21 semanas.

NÚMERO DE ALUMNOS:
Mínimo: 0 y Máximo: 150

TASAS:
- Ordinaria: 995 €
- Alumnos ULE: 875 €
- Alumnos de otras universidades: 875 €
- Desempleados: 795 €

DESTINATARIOS:

Dirigido a profesionales de privacidad, responsables de seguridad, responsables de calidad, gerentes y a cualquier persona que desee asegurar el cumplimiento de la protección de datos. Está especialmente orientado a superar el examen para la obtención del certificado de Delegado de Protección de Datos. No hay requisitos previos.

CRÉDITOS DE LIBRE CONFIGURACIÓN:
18 créditos LEC - 9 créditos ECTS

OBJETIVOS:

Conocer las obligaciones establecidas para los responsables y los encargados del tratamiento de datos personales.

Elaborar las cláusulas legales necesarias para recoger datos personales cumpliendo la nueva normativa europea.

Realizar un Análisis de Impacto relativo a la Protección de Datos.

Realizar el registro de actividades de tratamiento de datos establecido por el RGPD.

Desarrollar la implantación de todos los requisitos establecidos por la nueva normativa.

Al finalizar este curso, el alumno estará capacitado para implantar y gestionar la nueva normativa de protección de datos en cualquier entidad, así como a superar el examen para obtener el certificado de Delegado de Protección de Datos.

PROGRAMA:

DOMINIO 1: NORMATIVA GENERAL DE PROTECCIÓN DE DATOS

1. Introducción al RGPD

1.1. Origen.
1.2. Antecedentes.
1.3. La necesidad de un reglamento europeo.
1.4. Novedades importantes

2. Disposiciones generales y ámbito de aplicación

2.1. Los considerandos.
2.2. Objeto.
2.3. Ámbito de aplicación material.
2.4. Ámbito de aplicación territorial.
2.5. Conceptos.

3. Principios

3.1. Principios relativos al tratamiento.
3.2. Licitud del tratamiento.
3.3. Consentimiento.
3.4. Consentimiento de los niños.
3.5. Tratamiento de categorías especiales de datos personales.

4. Derechos de los interesados

4.1. Transparencia y modalidades.
4.2. Información a facilitar a los interesados.
4.3. Derechos de los interesados.
4.4. Nuevos derechos de los interesados.
4.5. Limitaciones de los derechos.

5. Responsable y encargado del tratamiento

5.1. Obligaciones del responsable.
5.2. Protección de datos desde el diseño y por defecto.
5.3. Registro de actividades del tratamiento del responsable.
5.4. Obligaciones del encargado.
5.5. Registro de actividades del tratamiento del encargado.

6. Seguridad de los datos personales

6.1. Seguridad del tratamiento.
6.2. Notificaciones de violación de la seguridad a la autoridad de control.
6.3. Notificaciones de violación de la seguridad a los interesados.

7. Evaluación de impacto relativa a la protección de datos (EIPD).

7.1. ¿Qué es una EIPD y quién debe realizarla?
7.2. Elementos de una EIPD.
7.3. Fases de una EIPD.

8. El delegado de protección de datos (DPO)

8.1. Designación por la entidad.
8.2. Posición del DPO.
8.3. Funciones del DPO.

9. Códigos de conducta y certificación

9.1. Los códigos de conducta.
9.2. Certificación y mecanismos.

10. Transferencias de datos a terceros países u organizaciones internacionales

10.1. Principio de las transferencias.
10.2. Tipos de transferencias y requisitos.
10.3. Normas corporativas vinculantes.
10.4. Excepciones.

11. Autoridades de control, cooperación y coherencia

11.1. Autoridad de control e independencia.
11.2. Competencia, funciones y poderes.
11.4. Cooperación.
11.5. Asistencia mutua.
11.6. Operaciones conjuntas de las autoridades de control.
11.7. Mecanismo de coherencia.

12. El Comité Europeo de Protección de Datos

12.1. El Comité Europeo de Protección de Datos.
12.2. Funciones, informes y procedimiento.
12.3. Presidencia.

13. Recursos y sanciones

13.1. Reclamaciones.
13.2. Representación de los interesados.
13.3. Derecho a indemnización y responsabilidad.
13.4. Imposición de multas administrativas y sanciones.

14. Situaciones específicas de tratamiento.

14.1. Tratamiento y libertad de expresión y de información.
14.2. Tratamiento y acceso público a documentos oficiales.
14.3. Tratamiento del número nacional de identificación.
14.4. Tratamiento en el ámbito laboral.
14.5. Tratamiento con fines de archivo en interés público, investigación científica o histórica o fines estadísticos.
14.6. Obligaciones de secreto.
14.7. Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.

15. Diferencias entre la LOPD y el RGPD

15.1. Obtención del consentimiento.
15.2. Obligaciones del responsable.
15.3. Obligaciones del encargado.
15.4. La evaluación de impacto relativa a la protección de datos.

16. Implantación del RGPD

16.1. Análisis de los tratamientos.
16.2. Análisis de riesgos.
16.3. La evaluación de impacto relativa a la protección de datos.
16.4. Requisitos documentales.
16.5. Transferencias internacionales de datos.

17. Directrices de interpretación del RGPD

17.1. Guías del GT art. 29.
17.2. Opiniones del Comité Europeo de Protección de Datos.
17.3. Criterios de órganos jurisdiccionales.

18. Normativas sectoriales afectadas por la protección de datos

18.1. Sanitaria, farmacéutica, investigación.
18.2. Protección de los menores.
18.3. Solvencia patrimonial.
18.4. Telecomunicaciones.
18.5. Videovigilancia.
18.6. Seguros.
18.7. Publicidad.

19. Normativa española con implicaciones en protección de datos

19.1. LSSI. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
19.2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
19.3. Ley forma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica.

20. Normativa europea con implicaciones en protección de datos.

20.1. Directiva e-Privacy.
20.2. Directiva 2009/136/CE.
20.3. Directiva (UE) 2016/680.

DOMINIO 2: RESPONSABILIDAD ACTIVA

1. Análisis y gestión de riesgos de los tratamientos de datos personales

1.1. Introducción.
1.2. Inventario y valoración de activos.
1.3. Establecimiento de las dependencias entre activos.
1.4. Identificación de las amenazas y vulnerabilidades.
1.5. Análisis y evaluación de los riesgos.
1.6. Gestión de riesgos.
1.7. Selección de salvaguardas.
1.8. Valoración de la protección.
1.9. Riesgo residual, riesgo aceptable y riesgo inasumible.

2. Metodologías de análisis y gestión de riesgos

2.1. Metodologías de análisis de riesgos.

3. Programa de cumplimiento de Protección de Datos y Seguridad en una organización

3.1. Diseño e implantación del programa de protección de datos en la organización.
3.2. Objetivos del programa de cumplimiento.
3.3. Accountability: la trazabilidad del modelo de cumplimiento.

4. Seguridad de la información

4.1. Marco normativo. ENS y Directiva NIS.
4.2. Ciberseguridad y gobierno de la seguridad de la información.
4.3. Conceptos de la seguridad de la información.
4.4. Métricas del gobierno de la seguridad de la información.
4.5. Estrategia de la seguridad de la información.
4.6. Puesta en práctica de la seguridad de la información.
4.7. Seguridad desde el diseño y por defecto.
4.8. El ciclo de vida de los sistemas de información.
4.9. Integración de la ciberseguridad y la privacidad en el ciclo de vida.

5. Evaluación de Impacto relativa a la Protección de Datos (EIPD)

5.1. ¿Qué es una EIPD y quién debe realizarla?
5.2. Elementos de una EIPD.
5.3. Fases de una EIPD.
5.4. Descripción del proyecto.
5.5. Identificación y evaluación de riesgos.
5.6. Consulta con los afectados.
5.7. Gestión de los riesgos identificados.
5.8. Análisis del cumplimiento normativo.
5.9. Redacción, publicación e integración del informe final.
5.10. Implantación de recomendaciones.
5.11. Revisión y realimentación.

DOMINIO 3: TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

1. La auditoría de protección de datos

1.1. EL proceso de auditoría.
1.2. Perfil del auditor.
1.3. Fases de la auditoría.
1.4. Elementos a auditar.
1.5. La Pre-auditoría.
1.6. Fases en la ejecución de la auditoría.
1.7. Estrategias de verificación.
1.8. Ejecución de la auditoría.
1.9. Metodología de ejecución.
1.10. Documentación de evidencias.
1.11. Elaboración del informe de auditoría.
1.12. Ejecución y seguimiento de acciones correctoras.
1.13. Archivo del informe de auditoría.

2. Auditoría de Sistemas de Información

2.1. La función de la auditoría en los sistemas de información.
2.2. Estándares y directrices de la auditoría de SI.
2.3. Control interno y mejora continua.
2.2. Integración de la auditoría de protección de datos en la auditoría de SI.
2.3. Planificación, ejecución y seguimiento.

3. La gestión de la seguridad de los tratamientos

3.1. Esquema Nacional de Seguridad e ISO 27001.
3.2. Gestión de la seguridad de los Activos.
3.3. Seguridad lógica.
3.4. Seguridad en los procedimientos.
3.5. Recuperación de desastres y continuidad de negocio.
3.6. Protección de los activos técnicos y documentales.
3.7. Planificación y gestión de la recuperación de desastres.

4. Otros conocimientos

4.1. El cloud computing.
4.2. Los smartphones.
4.3. Internet de las cosas (IoT).
4.4. Big Data y elaboración de perfiles.
4.5. Redes sociales.
4.6. Tecnologías de seguimiento de usuario.
4.7. Blockchain y últimas tecnologías.

PROFESORADO:
Julio Cesár Miguel Pérez. Director General Grupo CFI. Experto en Seguridad de la Información por AENOR y con las certificaciones CND, CHFI, CEH, ECSA y APEP.

ENTIDADES COLABORADORAS:
AEI Ciberseguridad