ESIBE
ESCUELA IBEROAMERICANA DE POSTGRADO

Titulación expedida por Escuela Iberoamericana de Postgrado

Maestría en Protección de Datos, Transparencia y Acceso a la Información

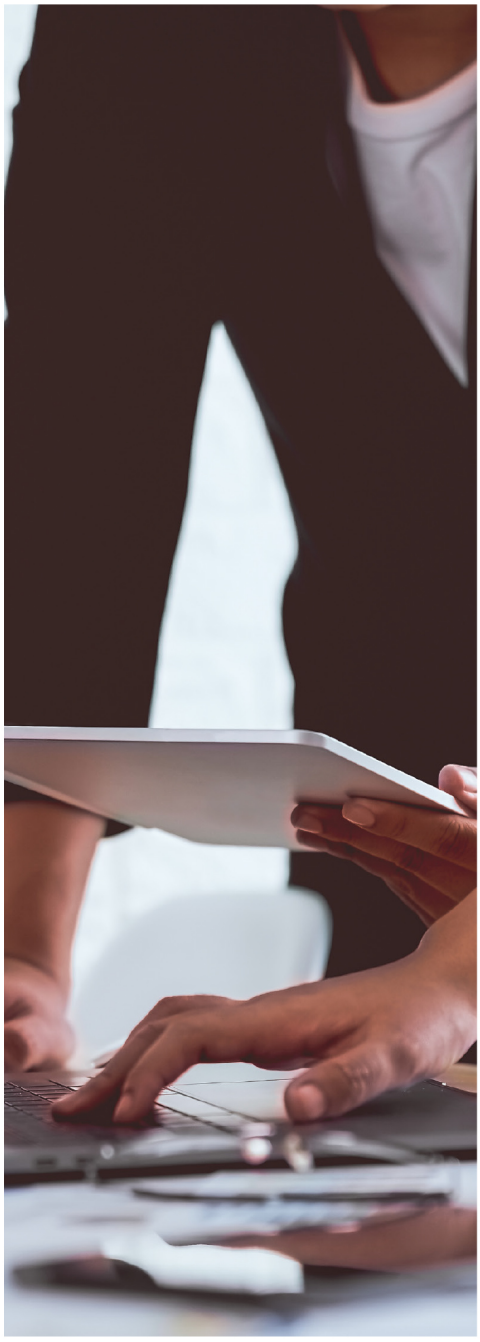
ALIANZA ESIBE Y UNIVERSIDAD DEL NORTE

ESIBE, Escuela Iberoamericana de Postgrado colabora estrechamente con la Universidad del Norte con el objetivo de **democratizar el acceso a la educación y apostar por la implementación de la tecnología en el sector educativo.** Para cumplir con esta misión, ambas entidades aúnan sus conocimientos y metodologías de enseñanza, logrando así una formación internacional y diferenciadora.

Esta suma de saberes hace que el proceso educativo se enriquezca y ofrezca al alumnado una oferta **variada, plural y de alta calidad.** La formación aborda materias desde un enfoque técnico y práctico, buscando contribuir al desarrollo de las capacidades y actitudes necesarias para el desempeño profesional.

ACREDITACIONES

Adobe Certified Associate · amadeus Your technology partner · Microsoft Office Specialist · sage software · hp ATA Accredited Technical Associate HP ExpertONE · Unión Europea · CECAP · Google for Education · Responsabilidad Social Corporativa RSC · Confianza Online · AENOR Gestión de la Calidad ISO 9001 · AENOR Seguridad Información ISO/IEC 27001 · AENOR Gestión Ambiental ISO 14001 · IQNet



Escuela Iberoamericana de Formación en línea.

ESIBE nace con la misión de crear un punto de encuentro entre Europa y América. Desde hace más de 18 años trabaja para cumplir con este reto, teniendo como finalidad potenciar el futuro empresarial de los profesionales de ambos continentes a través de programas de master, masters oficiales, master universitarios y maestrías.

ESIBE cuenta con Euroinnova e INESEM como entidades educativas de formación online colaboradoras, trabajando unidas para brindar nuevas oportunidades a sus estudiantes. Gracias al trabajo conjunto de estas instituciones, se ha conseguido llevar un modelo pedagógico único a miles de estudiantes y se han trazado alianzas estratégicas con diferentes universidades de prestigio.

ESIBE se sirve de la Metodología Active, una forma de adquirir conocimientos diferente que prima el aprendizaje personalizado atendiendo al contexto del estudiante, a sus objetivos y a su ritmo de aprendizaje. Para conseguir ofrecer esta forma particular de aprender, la entidad educativa se sirve de la Inteligencia Artificial y de los últimos avances tecnológicos.

ESIBE apuesta por ofrecer a su alumnado una formación de calidad sin barreras físicas, aprendiendo 100 % online, de forma flexible y adaptada a las necesidades e inquietudes del alumnado.

¡Aprende disfrutando de una experiencia que se adapta a ti!

VALORES

Los valores sobre los que se asienta Euroinnova son:

1

Accesibilidad
Somos cercanos y comprensivos, trabajamos para que todas las personas tengan oportunidad de seguir formándose.

2

Honestidad
Somos claros y transparentes, nuestras acciones tienen como último objetivo que el alumnado consiga sus objetivos, sin sorpresas.

3

Practicidad
Formación práctica que suponga un aprendizaje significativo. Nos esforzamos en ofrecer una metodología práctica.

4

Empatía
Somos inspiracionales y trabajamos para entender al alumno y brindarle así un servicio pensado por y para él.

A día de hoy, han pasado por nuestras aulas más de **300.000 alumnos** provenientes de los cinco continentes. Euroinnova es actualmente una de las empresas con mayor índice de crecimiento y proyección en el panorama internacional.

Nuestro portfolio se compone de cursos online, cursos homologados, baremables en oposiciones y formación superior de postgrado y máster.


Bolsa de empleo

METODOLOGÍA ACTIVE

Nuestra **Metodología Active** tiene en cuenta el perfil de cada estudiante y adapta el contenido a sus preferencias a través de la inteligencia artificial. Es una formación 100 % online, práctica y profesional.

1. Aprendizaje significativo y práctico

Los conocimientos se incorporan de forma sustantiva en la estructura cognitiva del alumnado. A través de sucesivas **prácticas** y de **ejercicios de reflexión**, se conduce al estudiante a relacionar los nuevos contenidos con los anteriormente adquiridos, conformando las bases de un aprendizaje sólido, útil y pragmático.

2. Flexibilidad

Aprendizaje a tu ritmo, a la hora que prefieras y desde cualquier lugar. **ESIBE se adapta a ti**, a tus circunstancias y a tu contexto. Tenemos en cuenta tus intereses y tu motivación y respondemos ofreciéndote un temario y un servicio acorde a tus preferencias y necesidades.

3. Acompañamiento docente

Contamos con **profesionales en activo**, con gran vocación y con dilatada experiencia para ofrecerte una formación de calidad y acorde a la realidad laboral. Además, contamos con un equipo de asesoramiento que te guiará durante todo el proceso de aprendizaje y te dará pautas para superar con éxito tu etapa educativa.

4. Innovación

Apostamos por la **implementación de la tecnología** y de los últimos **avances en e-learning.** Nos servimos de la IA para un aprendizaje inteligente, que tenga en cuenta tus metas y te permita desarrollarte profesionalmente en función de tus preferencias y potencial.

5. Desarrollo de competencias profesionales más demandadas

La metodología Active te prepara para el **desarrollo de las competencias más demandadas** del mercado. Conectamos el talento con la realidad laboral. Primamos el desarrollo de personas autónomas, críticas, con grandes dotes comunicativos y capaces de resolver casos reales.

6. ESIBE contigo

Te ofrecemos la oportunidad **de estar conectado** a distintos **temas de interés** gracias a nuestros **seminarios**. Profesionales de áreas especializadas nos cuentan de forma periódica los avances y novedades en los distintos campos, así como trucos y consejos.

7. Campus virtual

Aprende en un **entorno dinámico, avanzado e intuitivo.** Disfruta de un campus virtual diseñado por expertos y con múltiples funcionalidades para un aprendizaje óptimo.

8. Contenido de calidad

Temario actualizado, de calidad y acorde al contexto actual. Aprenderás con contenido elaborado específicamente para la formación en cuestión y con recursos didácticos que te permitirán una mejor comprensión. El temario está sometido a constantes cambios en función de la evolución del campo de especialización.

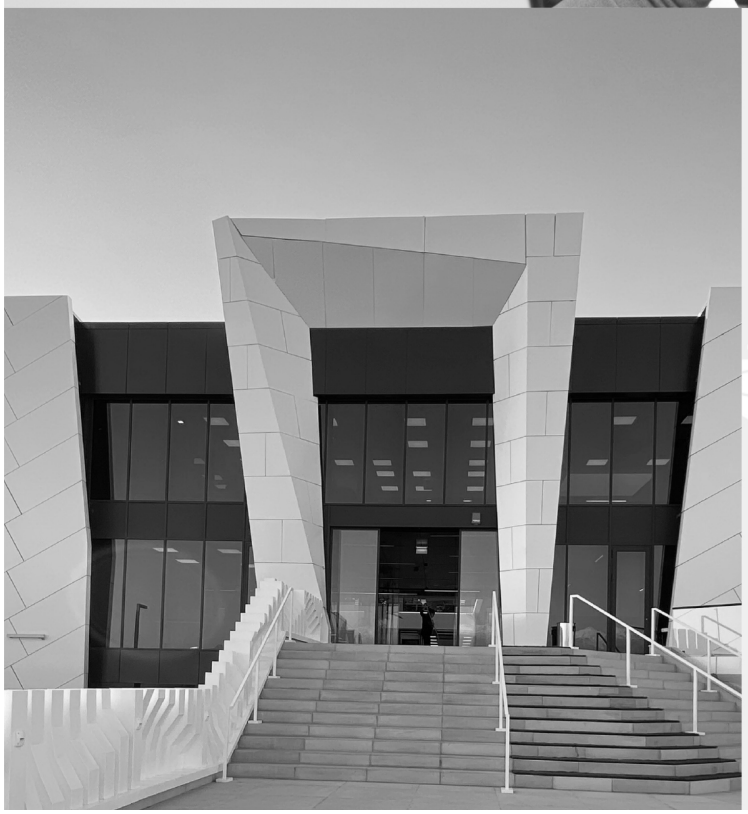
+200K Estudiantes formados

+18 Años de experiencia en el sector de la formación

5 Alumnado de los 5 continentes

98% de satisfacción

84% de los estudiantes repiten en ESIBE



Nuestras Sedes

España | Miami | México

ESIBE

Maestría en Protección de Datos, Transparencia y Acceso a la Información

DURACIÓN
1500 horas

MODALIDAD
Online

ACOMPAÑAMIENTO PERSONALIZADO

TITULACIÓN

Titulación de Maestría en Protección de Datos, Transparencia y Acceso a la Información con 1500 horas expedida por ESIBE (ESCUELA IBEROAMERICANA DE POSTGRADO).


ESIBE
Escuela Iberoamericana de Postgrado
NOMBRE DEL ALUMNO/A
Acción Formativa
Con un nivel de aprovechamiento [CALIFICACIÓN]

DESCRIPCIÓN

Gracias a esta Maestría en Protección de Datos, Transparencia y Acceso a la Información podrás conocer de primera mano cómo tratar los datos personales, tanto las entidades tanto públicas como privadas, en un contexto tan complicado como el actual, en el que las TIC están cada vez más implantadas en los diferentes ámbitos de la vida y en el que la circulación de grandes volúmenes de datos personales es muy frecuente. Cuando se haya finalizado, el alumno tendrá conocimientos para asesorar sobre contenidos relacionados con el tratamiento de datos personales como son la legitimación para el tratamiento de datos personales, el derecho de información del interesado, el ejercicio de derechos y la aplicación de medidas de responsabilidad proactiva, entre otros.

OBJETIVOS

- Identificar las bases que legitiman para llevar a cabo el tratamiento de datos personales.
- Conocer los derechos que el RGPD y la LOPD reconoce a los interesados.
- Realizar un análisis de riesgos y una evaluación de impacto relativas al tratamiento de datos de carácter personal.
- Llevar a cabo una auditoría relativa al tratamiento de datos personales.
- Analizar los sistemas comparados de acceso a la información.

A QUIÉN VA DIRIGIDO

Esta Maestría en Protección de Datos, Transparencia y Acceso a la Información está dirigido a profesionales interesados en ejercer como delegado de protección de datos en las organizaciones, tanto públicas como privadas, como a aquellos interesados en formarse en esta materia para ejercer labores de asesoría.

PARA QUÉ TE PREPARA

Con esta Maestría en Protección de Datos, Transparencia y Acceso a la Información o tendrás la posibilidad de conocer las obligaciones introducidas por el RGPD y la LOPD tanto a responsables como a encargados del tratamiento en el tratamiento de datos personales. Conocerás cómo llevar a cabo la labor del delegado de protección de datos en el seno de las organizaciones, adaptando los tratamientos de datos personales a la normativa vigente.

Programa Formativo

MÓDULO 1. FUNDAMENTOS LEGALES PARA EL TRATAMIENTO DE DATOS PERSONALES

UNIDAD DIDÁCTICA 1. Protección de Datos: Contexto normativo

1. Normativa General de Protección de Datos
2. Privacidad y protección de datos en el panorama internacional
3. La Protección de Datos en Europa
    1. - Antecedentes
    2. - Propuesta de reforma de la Directiva 95/46/CE
4. La Protección de Datos en España
5. Estándares y buenas prácticas

UNIDAD DIDÁCTICA 2. Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD). Fundamentos

1. El Reglamento UE 2016/679
2. Ámbito de aplicación del RGPD
3. Definiciones
    1. - Otras definiciones
4. Sujetos obligados
5. Ejercicio Resuelto. Ámbito de Aplicación

UNIDAD DIDÁCTICA 3. Principios de la Protección de Datos

1. El binomio derecho/deber en la protección de datos
2. Licitud del tratamiento de los datos
3. Lealtad y transparencia
4. Finalidad del tratamiento de los datos: la limitación
5. Minimización de datos
6. Exactitud y Conservación de los datos personales

UNIDAD DIDÁCTICA 4. Legitimación para el Tratamiento de los Datos Personales en el RGPD y la LOPDGDD

1. El consentimiento del interesado en la protección de datos personales
2. El consentimiento: otorgamiento y revocación
3. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado
4. Eliminación del Consentimiento tácito en el RGPD

5. Consentimiento de los niños
6. Categorías especiales de datos
7. Datos relativos a infracciones y condenas penales
8. Tratamiento que no requiere identificación
9. Bases jurídicas distintas del consentimiento

UNIDAD DIDÁCTICA 5. Derechos de los Ciudadanos en la Protección de sus Datos Personales

1. Derechos de las personas respecto a sus Datos Personales
    1. - Impugnación de valoraciones
    2. - Tutela de derechos
2. Transparencia e Información
3. Acceso, Rectificación, Supresión (Olvido)
4. Oposición
5. Decisiones individuales automatizadas
6. Portabilidad de los Datos
7. Limitación del tratamiento
8. Excepciones a los derechos
9. Casos específicos
10. Ejercicio resuelto. Ejercicio de Derechos por los Ciudadanos

UNIDAD DIDÁCTICA 6. Protección de datos de Carácter Personal: Medidas de cumplimiento en el RGPD y la LOPDGDD

1. Las políticas de Protección de Datos
2. Posición jurídica de los intervinientes. Responsables, corresponsables, Encargados, subencargado del Tratamiento y sus representantes. Relaciones entre ellos y formalización
    1. - Relaciones Responsable - Encargado
    2. - Encargados, sub-encargado, etc.
    3. - El contrato de Encargo
3. El Registro de Actividades de Tratamiento: identificación y clasificación del tratamiento de datos
    1. - Identificación y clasificación del tratamiento de datos

UNIDAD DIDÁCTICA 7. La Responsabilidad Proactiva

1. El Principio de Responsabilidad Proactiva
2. Privacidad desde el Diseño y por Defecto. Principios fundamentales
3. Evaluación de Impacto relativa a la Protección de Datos (EIPD) y consulta previa. Los Tratamientos de Alto Riesgo
4. Seguridad de los datos personales. Seguridad técnica y organizativa
5. Las Violaciones de la Seguridad. Notificación de Violaciones de Seguridad
6. El Delegado de Protección de Datos (DPD). Marco normativo
7. Códigos de conducta y certificaciones
    1. - La supervisión de los códigos de conducta
    2. - Certificaciones

UNIDAD DIDÁCTICA 8. El Delegado de Protección de Datos (DPD, DPO o Data Privacy Officer) en el RGPD y la LOPDGDD

1. El Delegado de Protección de Datos (DPD)
2. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses
3. Ejercicio de funciones: Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección
4. El DPD en el desarrollo de Sistemas de Información
5. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones
6. Comunicación con la Autoridad de Protección de Datos
7. Competencia profesional. Negociación. Comunicación. Presupuestos
8. Capacitación y Desempeño del DPO: Formación, Habilidades personales, Trabajo en equipo, Liderazgo, Gestión de equipos

UNIDAD DIDÁCTICA 9. Transferencias Internacionales de datos en el RGPD y la LOPDGDD

1. El Movimiento Internacional de Datos
2. El sistema de decisiones de adecuación
3. Transferencias mediante garantías adecuadas
4. Normas Corporativas Vinculantes
5. Excepciones
    1. - Supuestos sometidos a información previa
6. Autorización de la autoridad de control
    1. - Procedimiento de autorización a la AEPD
7. Suspensión temporal
8. Cláusulas contractuales
9. Ejercicio resuelto: Transferencias internacionales de datos

UNIDAD DIDÁCTICA 10. Las Autoridades de Control en el RGPD y la LOPDGDD

1. Autoridades de Control: Aproximación
    1. - Cooperación y Coherencia entre las distintas autoridades de Control
    2. - Instrumentos de Asistencia Mutua
    3. - El Mecanismo de Coherencia
    4. - El Procedimiento de Urgencia
2. Potestades
3. Régimen Sancionador
    1. - Sujetos responsables
    2. - Infracciones
    3. - Prescripción de las infracciones y sanciones
    4. - Procedimiento en caso de vulneración de la normativa de protección de datos
4. Comité Europeo de Protección de Datos (CEPD)
    1. - Supervisor Europeo de Protección de Datos (SEPD)
5. Procedimientos seguidos por la AEPD
6. La Tutela Jurisdiccional

7. El Derecho de Indemnización

UNIDAD DIDÁCTICA 11. Directrices de interpretación del RGPD

1. Grupo Europeo de Protección de Datos del Artículo 29 (WP 29)
2. Opiniones del Comité Europeo de Protección de Datos (CEPD)
3. Criterios de Órganos Jurisdiccionales

UNIDAD DIDÁCTICA 12. Normativas sectoriales afectadas por la Protección de Datos

1. Normativas sectoriales sobre Protección de Datos
2. Sanitaria, Farmacéutica, Investigación
3. Protección de los menores
4. Solvencia Patrimonial
5. Telecomunicaciones
6. Videovigilancia
7. Seguros, Publicidad y otros

UNIDAD DIDÁCTICA 13. Normativa española con implicaciones en Protección de Datos

1. Aproximación a la normativa estatal con implicaciones en Protección de Datos
2. LSSI, Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
3. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
4. Ley Firma-e, Ley 59/2003, de 19 de diciembre, de Firma Electrónica
5. Otras normas de interés

UNIDAD DIDÁCTICA 14. Normativa europea con implicaciones en Protección de Datos

1. Normas de Protección de Datos de la UE
2. Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002
3. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009
4. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016

MÓDULO 2. RESPONSABILIDAD PROACTIVA EN EL TRATAMIENTO DE DATOS

UNIDAD DIDÁCTICA 1. PROGRAMA DE CUMPLIMIENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD EN UNA ORGANIZACIÓN

1. El diseño y la Implantación del Programa de Protección de Datos en el contexto de la organización
    1. - Guía para implantar el programa de protección de datos
2. Objetivos del Programa de Cumplimiento
3. Accountability: La Trazabilidad del Modelo de Cumplimiento

UNIDAD DIDÁCTICA 2. SEGURIDAD DE LA INFORMACIÓN

1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos
    1. - Esquema Nacional de Seguridad
    2. - Directiva INS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de la SI
    1. - Diferencias entre Seguridad de la Información y Seguridad Informática
    2. - Conceptos de Seguridad de la Información
    3. - Alcance
    4. - Estrategia de SI. El modelo PDCA
3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI
    1. - Puesta en práctica de la seguridad de la información
    2. - Seguridad desde el diseño y por defecto
    3. - El ciclo de vida de los Sistemas de Información
    4. - Integración de la seguridad y la privacidad en el ciclo de vida
    5. - El control de calidad de los SI

UNIDAD DIDÁCTICA 3. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS TRATAMIENTOS DE DATOS PERSONALES

1. Introducción. Marco general de la Evaluación y Gestión de Riesgos. Conceptos generales
    1. - Impacto en la Protección de Datos
    2. - ¿Qué entendemos por “Riesgo”?
    3. - ¿Qué debemos entender por “aproximación basada en el riesgo”?
    4. - Otros conceptos
2. Evaluación de Riesgos. Inventario y valoración de activos. Inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante
    1. - Principales tipos de vulnerabilidades
    2. - Particularidades de los distintos tipos de código malicioso
    3. - Principales elementos del análisis de riesgos y sus modelos de relaciones
    4. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
    5. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
    6. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
    7. - Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

8. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
9. - Determinación de la probabilidad e impacto de materialización de los escenarios
10. - Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
11. - Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
12. - Relación de las distintas alternativas de gestión de riesgos
13. - Guía para la elaboración del plan de gestión de riesgos
14. - Ejercicio resuelto Análisis de Riesgo: FACILITA_RGPD

3. Gestión de Riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible
    1. - Etapas en la gestión de riesgos
    2. - Valoración del riesgo, valoración de probabilidad y valoración de gravedad
    3. - Implicaciones en la protección de datos de la gestión de riesgos
    4. - Gestión de riesgos por defecto
    5. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
    6. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
    7. - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

1. Metodologías de Análisis y Gestión de riesgos
    1. - Análisis de riesgos
    2. - Aproximación basada en riesgo del RGPD
    3. - Asignación de responsabilidades mediante RACI
    4. - Describir el ciclo de vida de los datos
    5. - Gestión de riesgos: Identificar, evaluar y tratar
2. Incidencias y recuperación
    1. - Notificación de brechas de seguridad
3. Principales metodologías
    1. - Octave
    2. - NIST SP 800-30
    3. - Magerit versión 3

UNIDAD DIDÁCTICA 5. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS “EIPD”

1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares
    1. - Origen, Concepto y Características de la EIPD
    2. - Alcance y necesidad
    3. - Estándares
2. Realización de una Evaluación de Impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas
    1. - Aspectos preparatorios de la ejecución de la EIPD

2. - Análisis de la necesidad de hacer una Evaluación de Impacto
3. - Descripción sistemática de las operaciones de tratamiento
4. - Objetivos y finalidades del tratamiento. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento
5. - Gestión de Riesgo. Informe de Evaluación
6. - La Consulta Previa
7. - Ejercicio resuelto EIPD: GESTIONA_RGPD

MÓDULO 3. AUDITORÍA EN LA NORMATIVA DE PROTECCIÓN DE DATOS

UNIDAD DIDÁCTICA 1. LA AUDITORÍA DE PROTECCIÓN DE DATOS

1. La Auditoría de Protección de Datos
2. El Proceso de Auditoría. Cuestiones generales y características básicas
3. Informe de Auditoría. Elaboración, aspectos básicos e importancia
4. Ejecución y seguimiento de Acciones Correctoras

UNIDAD DIDÁCTICA 2. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. La función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices
2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI
3. Planificación, ejecución y seguimiento

UNIDAD DIDÁCTICA 3. LA GESTIÓN DE LA SEGURIDAD DE LOS TRATAMIENTOS

1. Esquema Nacional de Seguridad, ISO/IEC 27001:2022
2. Gestión de la Seguridad de los Activos Seguridad lógica y en los procedimientos Seguridad aplicada a las TI y a la documentación
3. Recuperación de desastres y continuidad del Negocio Protección de activos técnicos y documentales Planificación y gestión de la Recuperación de Desastres

UNIDAD DIDÁCTICA 4. OTROS CONOCIMIENTOS

1. El Cloud Computing
2. Los Smartphones
3. Internet de las cosas (IoT)
4. Big Data y elaboración de perfiles
5. Redes sociales
6. Tecnologías de seguimiento de usuario
7. Blockchain y últimas tecnologías

UNIDAD DIDÁCTICA 5. MODELOS HABITUALES PARA EL CUMPLIMIENTO DEL RGPD

1. Modelo de contrato de encargo con cláusula informativa

2. Modelos para el uso y la navegación en páginas web
3. Modelo de acuerdo de encargo de tratamiento
4. Modelos para el ejercicio de derechos
5. Modelos de respuesta para el ejercicio de derechos
6. ANEXO. DOCUMENTOS DE SEGURIDAD RGPD-LOPDGDD
7. Anexo I: Plantilla de análisis de la necesidad de la realización de una EIPD
8. Anexo II: Plantilla de descripción de las actividades de tratamiento
9. Anexo III: Plantilla para documentar el análisis básico de riesgos
10. Anexo IV: Plantilla de registro de actividades de tratamiento (Responsable de tratamiento)
11. Anexo V: Plantilla de registro de actividades de tratamiento (Encargado de tratamiento)

MÓDULO 4. TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. FUNDAMENTO Y PRINCIPIOS DE LA TRANSPARENCIA Y EL ACCESO A LA INFORMACIÓN

1. Concepto de transparencia y su importancia en el sector público.
    1. - Importancia de la trasparencia en los sistemas democráticos.
    2. - Transparencia de los gobiernos.
    3. - Transparencia en la Administración Pública.
2. Normativa vigente en materia de transparencia.
    1. - Evaluación de los índices de transparencia.
3. Consejo de Transparencia y Buen Gobierno: infraestructuras para la aplicación de la ley de transparencia.
4. Gobierno Abierto.
    1. - Planes de acción para el cumplimiento de garantías.
    2. - Rendición de cuentas.
5. Portal de Transparencia de la Administración General del Estado.
    1. - Principios técnicos.
    2. - Publicidad activa y su función en el Portal.
6. “Open data”: conceptos, funciones y relación con el Gobierno Abierto.

UNIDAD DIDÁCTICA 2. ACCESO A LA INFORMACIÓN Y ACCESO A ARCHIVOS Y DOCUMENTOS

1. Acceso a la información pública: concepto y su aplicación a nivel internacional y europeo.
    1. - Principios básicos del derecho al acceso de la información.
2. Archivo: garantía de acceso y transparencia por parte del Gobierno Abierto.
    1. - Derecho de acceso a los archivos públicos.
3. Archivo: gestión en materia de transparencia y “Open Data”.
    1. - Gestión documental aplicada a las políticas de transparencia y datos abiertos.
    2. - Herramientas para la identificación de una buena transparencia.
4. Participación ciudadana y archivo 2.0.
    1. - Estándares para el fomento de la participación pública.
    2. - Diferentes tipologías de colaboración existentes.
    3. - Archivo 2.0.

5. Administración electrónica: conceptos fundamentales, digitalización y gestión de documentos.
    1. - Documento electrónico: concepto, estructura y formato.
    2. - Firma electrónica.

UNIDAD DIDÁCTICA 3. LÍMITES DEL DERECHO DE ACCESO A LA INFORMACIÓN

1. Normativa vigente y aspectos fundamentales del límite al derecho de acceso a la información pública.
    1. - Protección de datos como límite de acceso a la información.
2. Procedimiento para el acceso a la información.
3. Solicitud de acceso a la información: fase inicial y tramitación.
4. Solicitud de acceso a la información: resolución y tramitación.

UNIDAD DIDÁCTICA 4. PROTECCIÓN, GARANTÍA Y TUTELA DEL DERECHO DE ACCESO A LA INFORMACIÓN

1. Barreras y facilitadores de la accesibilidad.
2. Barrera y facilitadores de accesibilidad a la información: discapacidad visual y auditiva.
    1. - Ayudas técnicas.
3. Barreras y facilitadores de acceso a la información: discapacidad cognitiva.
    1. - Sistemas alternativos que facilitan el acceso a la información.
    2. - Estrategias de fácil lectura.

UNIDAD DIDÁCTICA 5. REUTILIZACIÓN DE LA INFORMACIÓN DEL SECTOR PÚBLICO

1. Identificación de fuentes de información.
    1. - Información interna y externa.
    2. - Algunas fuentes de información electrónica.
2. Recuperación de información.
    1. - Proceso interactivo.
    2. - Motores de búsqueda.
    3. - Otros recursos.
3. Metodología de búsqueda electrónica de información.
4. Selección, discriminación y valoración de la información.
    1. - Discriminación y selección de la información.
    2. - Criterios de calidad de las fuentes electrónicas.
5. Técnicas de protección de accesos públicos y privados, en archivos convencionales e informáticos.
    1. - Niveles de protección: determinación.
    2. - Disposición de contraseñas y atributos de acceso.
    3. - Autorizaciones de acceso o consulta, detección de errores en el procedimiento.
6. Aplicación de procedimientos de seguridad y confidencialidad de la información.
    1. - Normativa vigente de protección de datos y conservación de la documentación.
    2. - Copias de seguridad.

UNIDAD DIDÁCTICA 6. ACCESO A LA INFORMACIÓN AMBIENTAL

1. Introducción a la información ambiental.
    1. - Concepto de información ambiental.
    2. - Formato universal de la información ambiental.
2. Derechos de participación ciudadana impulsados por la Unión Europea.
3. Derecho de acceso a la información en materia ambiental.
4. Participación de los ciudadanos por la defensa del medio ambiente.
    1. - La iniciativa legislativa popular.

MÓDULO 5. AUDITORÍA DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

1. Código deontológico de la función de auditoría
2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información
3. Criterios a seguir para la composición del equipo auditor
4. Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
5. Tipos de muestreo a aplicar durante el proceso de auditoría
6. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
7. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
8. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
9. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

UNIDAD DIDÁCTICA 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Principios generales de protección de datos de carácter personal
2. Normativa europea recogida en la directiva 95/46/CE
3. Normativa nacional recogida en el código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
4. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
5. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
6. Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

UNIDAD DIDÁCTICA 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

1. Introducción al análisis de riesgos
2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su

actualización permanente, así como criterios de programación segura
3. Particularidades de los distintos tipos de código malicioso
4. Principales elementos del análisis de riesgos y sus modelos de relaciones
5. Metodologías cualitativas y cuantitativas de análisis de riesgos
6. Identificación de los activos involucrados en el análisis de riesgos y su valoración
7. Identificación de las amenazas que pueden afectar a los activos identificados previamente
8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
12. Determinación de la probabilidad e impacto de materialización de los escenarios
13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
15. Relación de las distintas alternativas de gestión de riesgos
16. Guía para la elaboración del plan de gestión de riesgos
17. Exposición de la metodología NIST SP 800-30
18. Exposición de la metodología Magerit versión 2

UNIDAD DIDÁCTICA 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

1. Herramientas del sistema operativo tipo Ping, Traceroute, etc
2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
3. Herramientas de análisis de vulnerabilidades tipo Nessus
4. Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.
6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

UNIDAD DIDÁCTICA 5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS.

1. Principios generales de cortafuegos
2. Componentes de un cortafuegos de red
3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
4. Arquitecturas de cortafuegos de red
5. Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la

organización auditada

2. Guía para la elaboración del plan de auditoría
3. Guía para las pruebas de auditoría
4. Guía para la elaboración del informe de auditoría