CURSO AVANZADO

Gestión de Riesgos y Evaluación de Impacto en la Protección de Datos

GRCx3 | Instituto Superior de Auditoría y Gobernanza Aplicada

Carga lectiva	Estructura	Modalidad
63 horas síncronas **Más de 120 horas académicas**	**18 clases** **4 dominios + 4 workshops**	**100% síncrono** **Enfoque internacional extrapolable**

Un programa diseñado para profesionales que necesitan entender, gobernar y ejecutar el análisis de riesgos y la evaluación de impacto con criterio técnico, profundidad metodológica y aplicabilidad real.

Versión	Fecha	Estado del documento	Autoría
1.0	2026	Versión final del brochure académico-comercial	GRCx3

Índice

Presentación del programa

La gestión de riesgos y la evaluación de impacto en la protección de datos exigen hoy una aproximación más madura que la mera revisión normativa o el uso mecánico de matrices y plantillas.

Este curso avanzado ha sido diseñado para profesionales que necesitan comprender con profundidad la arquitectura del dato, del riesgo y del daño; las metodologías que permiten analizar con criterio; la gobernanza real del sistema; y el momento y la forma en que deben activarse y ejecutarse la evaluación de impacto y, cuando proceda, una lectura ampliada sobre derechos fundamentales.

No se trata de un curso introductorio. Es un programa de alto nivel orientado a construir criterio técnico, solidez metodológica y capacidad real de ejecución.

Propuesta de valor

Razones por las que este programa es diferencial
• Parte de la taxonomía del dato, del riesgo y del daño, no de la plantilla. • No enseña una sola metodología: compara marcos, métodos estructurados, cualitativos y cuantitativos. • Integra la gobernanza del sistema: política, procedimiento, umbrales, disparadores y roles. • Une análisis de riesgos y evaluación de impacto en una secuencia lógica y defendible. • Cada dominio cierra con un workshop aplicado. • Incorpora FRIA en el bloque final para escenarios de afectación intensificada de derechos.

Requisito de acceso

Este es un curso avanzado. Está dirigido a profesionales ya formados en protección de datos personales. Se exigirá evidencia de formación previa y/o experiencia profesional en delegación o responsabilidad en privacidad, consultoría de cumplimiento, auditoría, análisis de riesgos, seguridad de la información, gobierno del dato o funciones jurídicas especializadas.

A quién va dirigido

- Delegados y responsables de protección de datos.
- Consultores de privacidad y cumplimiento.
- Auditores internos y externos.
- Analistas de riesgos.
- Profesionales de seguridad, gobernanza y cumplimiento.
- Juristas especializados en privacidad y riesgo.
- Responsables de proyectos con tratamientos complejos, intensivos o de especial sensibilidad.

Carga lectiva del programa

• 63 horas de formación síncrona.
• Más de 120 horas académicas totales.

- 18 clases de 3,5 horas.
- 4 workshops de cierre, uno por dominio.
- Examen final de 150 preguntas.

Estructura académica del curso

Módulo	Denominación	Propósito	Horas	Clases
1	**Taxonomía de datos y riesgos**	Construir la base conceptual del curso: taxonomía del dato, del riesgo y del daño, y su articulación metodológica.	**21 h**	**6**
2	**Metodologías de análisis de riesgos y evaluación de impacto**	Analizar comparativamente marcos, métodos estructurados, métodos cuantitativos, cualitativos y modelos de evaluación de impacto.	**14 h**	**4**
3	**Gobernanza y ejecución del análisis de riesgos**	Diseñar el sistema de gobernanza del análisis y ejecutar un análisis de riesgos completo y defendible.	**14 h**	**4**
4	**Ejecución de la evaluación de impacto y FRIA**	Determinar cuándo procede la evaluación de impacto, cómo ejecutarla y cómo integrar FRIA en escenarios de afectación intensificada de derechos.	**14 h**	**4**
	Total		**63 h**	**18**

Módulo 1 — Taxonomía de datos y riesgos (21 horas | 6 clases)

Módulo 1: núcleo estratégico del programa
Aquí se construye el modelo: dato → tratamiento → riesgo → evento → daño → impacto. Sin esta base, cualquier metodología corre el riesgo de convertirse en un ejercicio mecánico o superficial.

Contenidos

Este módulo constituye el núcleo conceptual del programa. Su función es construir el lenguaje y la arquitectura mental que permiten comprender correctamente el riesgo en protección de datos como riesgo sobre derechos y libertades.

- Naturaleza del dato como objeto jurídico, técnico y organizativo.
- Diferencia entre dato, información, metadato e inferencia.
- El tratamiento como unidad de análisis.
- Ciclo de vida del dato y transformaciones relevantes.
- Categorías de datos personales y categorías de especial exposición.
- Identificadores en línea, rastreo, datos derivados e inferidos.
- Perfilado, biometría, localización, salud, menores y datos persistentes.
- Taxonomía del riesgo en protección de datos.
- Riesgo sobre derechos y libertades.
- Riesgo jurídico, organizativo, tecnológico y operacional.
- Riesgo inherente y residual.
- Taxonomía del daño.
- Daño material, físico, moral, discriminatorio, social y pérdida de control.
- Relación estructural entre dato, tratamiento, amenaza, daño e impacto.
- Construcción del lenguaje común del curso.

Workshop de cierre

Workshop 1 — Taxonomía aplicada. Ejercicio individual orientado a modelar correctamente la relación entre dato, tratamiento, riesgo y daño sobre un caso de trabajo.

Módulo 2 — Metodologías de análisis de riesgos y evaluación de impacto (14 horas | 4 clases)

Clave del módulo 2
El alumno no sale “casado” con una metodología, sino con criterio para elegir, combinar y defender la más adecuada para cada escenario.

Contenidos

Este módulo estudia comparativamente los principales marcos y métodos aplicables a la gestión de riesgos y a la evaluación de impacto. Su objetivo no es enseñar una sola vía, sino desarrollar criterio para seleccionar, combinar y justificar metodologías.

- Diferencia entre marco, método y técnica.
- ISO 31000 como marco general de gestión del riesgo.
- ISO 31022 y la dimensión del riesgo legal.
- ISO/IEC 27005 y su conexión con seguridad de la información.
- MAGERIT como método estructurado.
- FAIR y FAIR-CAM.
- Cuantificación del riesgo y racionales cuantitativos.
- Valor en Riesgo, Valor en Riesgo cibernético y Valor en Riesgo de datos personales.
- Probabilidad condicional, Monte Carlo y enfoques bayesianos y frecuentistas.
- Delphi y calibración experta.
- Modelo Lens y reducción del ruido.
- Criterios cualitativos de severidad inspirados en ENISA.
- ISO/IEC 29134 como estándar de evaluación de impacto en privacidad.
- ISO/IEC 42005 como estándar especializado para evaluación de impacto en inteligencia artificial.
- Modelos regulatorios comparados y sus principios metodológicos comunes.

Workshop de cierre

Workshop 2 — Comparación y selección metodológica. Ejercicio grupal orientado a justificar qué marco o combinación metodológica sería más adecuada según contexto, tratamiento y nivel de madurez organizativa.

Módulo 3 — Gobernanza y ejecución del análisis de riesgos (14 horas | 4 clases)

Clave del módulo 3

La evaluación de impacto no se trata como un documento aislado, sino como la consecuencia lógica de un sistema de gobernanza y análisis bien diseñado.

Contenidos

Este módulo construye el sistema operativo del análisis de riesgos. Aquí el análisis deja de ser una idea metodológica y se convierte en una función gobernada, documentada y ejecutable.

- Política de gestión de riesgos en protección de datos.
- Política de evaluación de impacto.
- Requisitos de dirección y patrocinio.
- Umbrales, criterios de aceptación y tolerancia.
- Disparadores y escalado.
- Procedimiento de análisis de riesgos.
- Procedimiento de activación y tramitación de la evaluación de impacto.
- Roles y responsabilidades.
- Modelo RASCI.
- Comité, aprobaciones y control de cambios.
- Evidencias mínimas y trazabilidad.
- Establecimiento del contexto.
- Alcance, supuestos y dependencias.
- Identificación de actores, sistemas y terceros.
- Construcción de escenarios.
- Amenazas, vulnerabilidades y exposición.
- Criterios de impacto y probabilidad.
- Priorización y clasificación del riesgo.
- Medidas técnicas, organizativas, contractuales y operativas.
- Riesgo residual, aceptación y seguimiento.

Workshop de cierre

Workshop 3 — Análisis de riesgos aplicado. Construcción guiada de un análisis de riesgos completo y defendible, con criterios de impacto, probabilidad, medidas y riesgo residual.

Módulo 4 — Ejecución de la evaluación de impacto y FRIA (14 horas | 4 clases)

Clave del módulo 4

La evaluación de impacto se enseña como herramienta de decisión seria. FRIA amplía la perspectiva en contextos en los que el análisis debe ir más allá del riesgo estrictamente vinculado a protección de datos.

Contenidos

Este módulo aborda la lógica y el momento de la evaluación de impacto: cuándo procede, cómo se estructura y cómo se conecta con el análisis de riesgos previo. Además, incorpora FRIA como marco complementario para escenarios de afectación intensificada de derechos.

- Umbral de alto riesgo.
- Disparadores normativos.
- Listas de tratamientos o actividades publicadas por autoridades.
- Disparadores metodológicos y organizativos.
- Criterios derivados de estándares internacionales.
- Decisión de activación y su justificación.
- Lógica del informe de evaluación de impacto.
- Necesidad y proporcionalidad.
- Riesgos sobre derechos y libertades.
- Medidas, garantías y riesgo residual.
- Procedimiento de ejecución.
- Evidencias y fuentes de soporte.
- Participación de las funciones implicadas.
- Integración con política, procedimiento y gobierno del sistema.
- Documentación de la decisión final.
- Qué es FRIA y qué aporta.
- Diferencias y conexiones entre EIPD y FRIA.
- Escenarios de afectación intensificada de derechos.
- Casos especiales: inteligencia artificial y decisiones automatizadas; biometría; monitorización y geolocalización; rastreo intensivo e identificadores persistentes; tratamientos de alta complejidad, escala o sensibilidad.

Workshop de cierre

Workshop 4 — Evaluación de impacto y FRIA. Aplicación práctica sobre un caso que obligue a decidir el instrumento adecuado, estructurar la evaluación de impacto y valorar cuándo procede una lectura ampliada sobre derechos fundamentales.

Evaluación, recursos y calendario

El programa incorpora cuatro workshops de cierre, uno por dominio, y un examen final de 150 preguntas.

Recursos y soporte

- Campus virtual.
- Materiales de apoyo.
- Grabaciones disponibles durante 12 meses.
- Workshops y evaluación integrados en el programa.

Calendario base y usos horarios

Ubicación	Horario
Islas Canarias	16:30–20:00
España peninsular	17:30–21:00
Chile	11:30–15:00
Ecuador	10:30–14:00
México D. F.	09:30–13:00
Costa Rica	08:30–12:00

Cierre

Una formación para quienes no buscan una visión superficial del cumplimiento, sino una comprensión rigurosa de la taxonomía del dato, la selección metodológica, la gobernanza del análisis de riesgos, la lógica de la evaluación de impacto y la posible extensión del análisis hacia FRIA cuando el contexto lo exija.

Un curso único. Un contenido de alcance global.