CURSO DE ANALISIS DE RIESGOS DE CIBERSEGURIDAD DE AUDIDAT

Online

Escuela DPO audidat

1 Información general

Escuela DPO reúne la experiencia necesaria y una extensa trayectoria en el campo de la Protección de Datos que transmite en cada uno de sus cursos para fomentar la seguridad confianza de todos los alumnos y convertirlos en auténticos DPO.

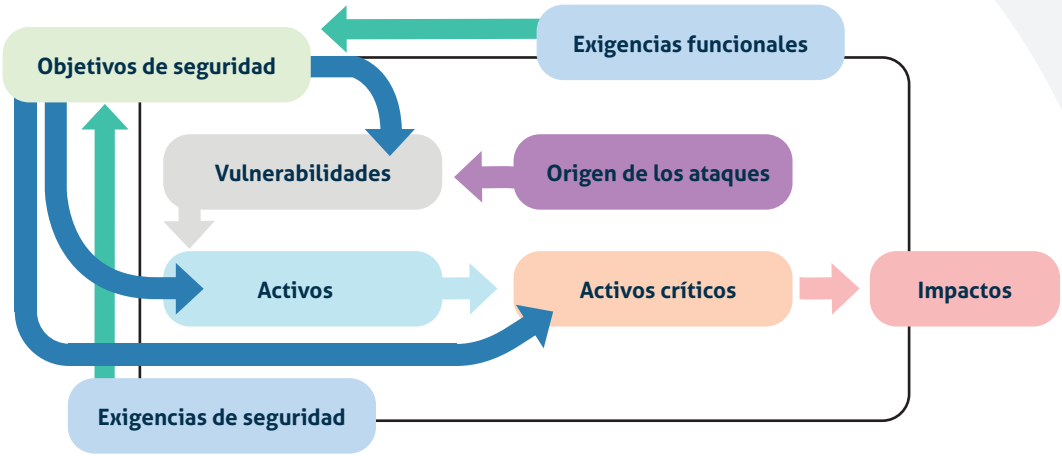
Escuela DPO audidat

2 Objetivo

Capacitar en el uso de la técnica y la práctica de la Herramienta AUDIDAT de Análisis de riesgos, para generar confianza ya sea en la propia organización o en los clientes a quienes se les prestan servicios de privacidad, conociendo cómo establecer el nivel de riesgo y dar recomendaciones de control hasta niveles aceptables, con lo que mejorar la gestión evitando debilidades y vulnerabilidades expuestas, así como también previniendo errores y aprovechando oportunidades para fortalecer la seguridad de la información.

Este curso supone una gran oportunidad al obtener un Diploma de Aptitud que supone un conocimiento básico en un área fundamental y fuertemente requerida por las organizaciones, para impulsar el perfil profesional de gran demanda actualmente e impulsar las habilidades propias en el empleo de la Herramienta AUDIDAT de Análisis de riesgos, haciendo de la necesidad virtud.

Exposición / Impacto	Bajo	Relativo	Significativo	Crítico
Crítico		6	10	14
Significativo		5	9	13
Relativo	2	4	8	12
Bajo	1	3	7	11



3 Programa académico

Unidades Didácticas

Duración = 10 horas

1. Objeto y alcance de la Evaluación de Ciberseguridad.
   1 hora.

2. Conceptos de análisis de riesgos de ciberseguridad.
   2 horas.

3. Calificación de la exposición: negocio, amenazas y vulnerabilidades.
   2 horas.

4. Calificación del impacto: requisitos legales, pérdida de información y sistemas.
   2 horas.

5. Evaluación y análisis de resultados.
   2 horas.

6. Resumen ejecutivo y realización de informes.
   1 hora.

3 Programa académico

1. Objeto y alcance de la Evaluación de Ciberseguridad.

- Ciberespacio y ciberseguridad
- Sistemas ciberfísicos y ciberespacio.
- Activos de información.
- Naturaleza de la ciberseguridad.
- Modelos de tecnología de la información y técnicas de seguridad.
- Amenazas en el ciberespacio. Contexto y enfoque.
- El rol de las partes interesadas.
- Áreas a considerar: Exposición e Impacto.

2. Conceptos de análisis de riesgos de ciberseguridad.

- Gestión de riesgos.
- Dimensiones de seguridad.
- Términos y definiciones de redes y análisis de riesgos.
- Glosario del Esquema Nacional de Seguridad.
- Niveles de Exposición e Impacto en el Modelo AUDIDAT.
- Nivel Bajo.
- Nivel Relativo.
- Nivel Significativo.
- Nivel Crítico.
- Perfiles del riesgo.

3. Calificación de la exposición: negocio, amenazas y vulnerabilidades.

- Principios de la Herramienta AUDIDAT.
- Estudio del contexto.
- Expresión de las necesidades de seguridad.
- Estudio de las amenazas.
- Expresión de los objetivos de seguridad.
- Determinación de los requisitos de seguridad.
- Exposición y modelo de negocio de la organización.
- Inventario de activos.

4. Calificación del impacto: requisitos legales, pérdida de información y sistemas.

- Aceptación de riesgos.
- Naturaleza del impacto.
- Impacto de una amenaza, impacto acumulado y repercutido.
- Dimensión de valoración y aceptación de riesgos.
- Identificación de medidas de protección.
- Impacto de los problemas legales y reglamentarios.
- Impacto de la pérdida de información.
- Impacto de los sistemas de información de la organización.

5. Evaluación y análisis de resultados.

- Evaluación y análisis con la Herramienta AUDIDAT.
- Vinculación de la exposición y el impacto con los requisitos de AR/GR.
- Representación de la Calificación del Perfil de Riesgo de AUDIDAT.
- Segmentos de Calificación del Perfil de Riesgo de AUDIDAT.
- Resultados de la Calificación del Perfil de Riesgo de AUDIDAT.
- Análisis de los resultados.
- Ejemplos de análisis de resultados desde el Perfil nº 1 hasta el nº 14.

6. Resumen ejecutivo y realización de informes.

- Presentación de los resultados.
- Proceso de preparación del evaluador y entrega de la evaluación.
- Preparación de Informes.
- Contenido de los informes.
- Resumen y evaluación.
- Análisis de los resultados y recomendaciones.

4 Estructura y metodología

Profesorado

Formado por profesionales en activo y actualizados.

Alumnos

Parte fundamental además de fuente de inspiración y superación.

Plataforma online

Facilita el aprendizaje y el contacto con los tutores.

5 ¿Por qué formarte con nosotros?

¿En qué nos diferenciamos?

+ de 16 años de dedicación
En 2003 Audidat se inició en la consultoría de Protección de Datos.

Acceso a 2 certificaciones
Certificación Audidat y ADOK.

Financiación personalizada
En función de las características del perfil de cada alumno interesado.

Grupos reducidos
Convocatorias con aforo mínimo que garantiza la atención personalizada.

Tutorías semanales
Profesores comprometidos con la resolución de las dudas y cuestiones.

6 A tener en cuenta

Este curso capacita para ser evaluador provisional de Análisis de Riesgos mediante la herramienta de ARC AUDIDAT, superando el examen de Aptitud de AUDIDAT Online.

Tras cinco trabajos de evaluación, se otorga el diploma de Evaluador.

• El ciberespacio es un ambiente complejo resultado de la interacción entre las personas, los programas informáticos y los servicios en Internet, soportado por información, tecnologías de la comunicación, dispositivos y redes.

• El mundo digital promueve la expansión de la innovación y genera nuevas oportunidades de negocio, pero no se puede dirigir la atención hacia los beneficios y otros resultados únicamente.

• Se ofrece un enorme potencial mediante la creación de nuevos mercados y productos, a través de la comprensión de las personas y los clientes, así como de encontrar diversas formas de conectarse a distancia, teletrabajo, formación online, etc.

• Debido a los cambios rápidos y constantes del entorno, muchas precauciones son omitidas y, como resultado, se subestiman los riesgos.

• Las amenazas en ciberseguridad han aumentado en número y en nivel de sofisticación, convirtiéndose en uno de los temas más relevantes relacionados con el riesgo.

• Como resultado de esto, los ciberatacantes han de ser considerados como una preocupación inminente, pues afecta desde a los gobiernos, hasta las pequeñas, medianas y grandes empresas, internacionales o locales.

• Los ciberataques están motivados por factores complejos, entre ellos, la ideología que poseen los atacantes, o bien por cuestiones financieras e incluso, existen programas que atacan según la capacidad de respuesta de la seguridad nacional.

• El impacto de los ataques varía: ya sea en la interrupción de los servicios (de cara al cliente), en fugas de información de activos sensibles (a través del espionaje industrial y dañando a los competidores) así como en la destrucción de los datos y sistemas que soportan los negocios y las administraciones (interrumpiendo los servicios y dañando los derechos de privacidad).

• Para que una organización ocupe un lugar más seguro y sostenible en el mundo digital, es necesario aplicar la óptica de riesgo en ciberseguridad a todo lo que hace.

• El punto de vista de gestión del riesgo tendrá un sentido diferente para los mandos directivos, así como para los socios, aliados, proveedores, comerciales, jurídico y otras partes de la organización.

• Se debe priorizar, racionalizar y trazar una ruta para la ciberseguridad con un enfoque personalizado, integral y eficaz para cada organización.

6 A tener en cuenta

• A fin de orientarla de manera eficiente a través de las capas de los riesgos de exposición y los impactos potenciales, los líderes deben tener la confianza para establecer el nivel de riesgo y estar preparados para entrar en acción para la gestión de cualquier incidente.

- La ciberseguridad comprende:
  - – Software (SW), tales como bases de datos, metadatos y archivos.
  - – Hardware (HW), tales como ordenadores, tablets y teléfonos.
  - – Redes de ordenadores.
  - – Activos de información.
- Los activos de información se gestionan a través de diferentes dispositivos conectados a Internet, por lo cual la ciberseguridad se ha convertido en uno de los mayores retos que afrontan las organizaciones, sea cual sea su tamaño.
- Una mala gestión de la seguridad puede tener tanto impacto económico, como afectar a la reputación y la confianza de socios, aliados, clientes y grupos de interés.

7 Tarifas

Fechas
Comienzo según convocatoria

Duración del curso
10 horas de formación online.

PRECIO
75 € + IVA

8 Anexo

Base jurídica

• **El análisis de riesgos** da cumplimiento a los preceptos recogidos en el RGPD 679/2016 UE:

Artículo 28 . Encargado del tratamiento.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la UE, (...), que estipulará: (...)

c) tomará todas las medidas necesarias de conformidad con el artículo 32; (**exposición del tratamiento= evaluar riesgos**). (...)

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

Artículo 32 . Seguridad del tratamiento.

1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un **nivel de seguridad adecuado al riesgo**,(...).

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los **riesgos que presente el tratamiento de datos**, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Artículo 35. Evaluación de impacto relativa a la protección de datos.

1. Cuando sea probable que un tipo de tratamiento, en particular **si utiliza nuevas tecnologías**, por su naturaleza, alcance, contexto o fines, **entrañe un alto riesgo** para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, **antes del tratamiento, una evaluación del impacto** de las operaciones de tratamiento en la protección de datos personales.

7. La evaluación deberá incluir como mínimo (extracto):

a) una descripción sistemática de las operaciones de tratamiento (...)

b) una evaluación de la necesidad y la proporcionalidad (...)

c) **una evaluación de los riesgos** para los derechos y libertades de los interesados a que se refiere el **apartado 1 (probabilidad de riesgo)**, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD (...).

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1 (probabilidad de riesgo), y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD (...).

Según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,

Artículo 28. Obligaciones generales del responsable y encargado.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que **el tratamiento es conforme** (...).

En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos (...).

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse (...).

Artículo 73. Infracciones consideradas graves.

f) **La falta de adopción de aquellas medidas técnicas y organizativas** que resulten apropiadas para garantizar **un nivel de seguridad adecuado al riesgo** del tratamiento, en los términos exigidos por el **artículo 32.1** del Reglamento (UE) 2016/679.

g) **El quebrantamiento**, como consecuencia **de la falta de la debida diligencia, de las medidas técnicas y organizativas** que se hubiesen implantado conforme a lo exigido por **el artículo 32.1** del Reglamento (UE) 2016/679 (..).

p) El tratamiento de datos personales sin llevar a cabo una **previa valoración** de los elementos mencionados en el **artículo 28** de esta ley orgánica (..) (**medidas técnicas y org./ eval. impacto / análisis de riesgos**).

t) El tratamiento de datos personales sin haber llevado a cabo la **evaluación del impacto** de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

Contacto

Teléfono 910353366

Email info@escueladpo.com

Facebook @EscuelaDPO

Instagram @EscuelaDPO

Linkedin @EscuelaDPO

AUDIDAT CENTRAL
Telf. **902106766** • Fax **967523369**
Antiguo Edificio de "La Unión y el Fénix Español"
C/ Martínez Villena n.º 14 - 3ª Planta
02001 • Albacete
www.audidat.com
coordinaciondpo@audidat.com
bgarcia@audidat.com

Escuela DPO audidat

www.escueladpo.com