



Área Formativa: **Seguridad de la Información**

Modalidad: **e-Learning**

Inicio/Convocatoria: **Consultar web**

Duración: **45+40+30 horas – 9 meses**

Precio: **Consultar web**

Idioma: **Español**



## **Pack de Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013, Protección de Datos: Reglamento Europeo de Protección de Datos y Actualización LOPD y Ciberseguridad esencial y ciberterrorismo**

### **Titulación:**

Una vez completado el programa formativo, el alumno recibirá los siguientes títulos:

Certificado del **Curso Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013, Protección de Datos: Reglamento Europeo de Protección de Datos y Actualización LOPD y Ciberseguridad esencial y ciberterrorismo**. Titulación expedida por Bureau Veritas Formación.

Certificado de **Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013** (con examen). Titulación expedida por Bureau Veritas.



**El certificado de este curso utiliza blockchain como tecnología de certificación digital.**

*Este sistema de verificación, mediante la inclusión de un código QR en el documento final, permite que puedas compartir con terceros, a través de un simple enlace, toda la información de tu certificado. Esta información es validada y confirmada en el sistema inmutable de la red evitando cualquier tipo de falsificación.*

### **Presentación:**

Todas las organizaciones deben tratar información en su gestión diaria, y pueden aparecer riesgos que afecten a su actividad empresarial. Y un aspecto clave para una empresa es la **seguridad de la información**, no solamente en relación a la tecnología y procesos de una organización, sino a las personas que forman parte de la misma, y que deben gestionar y utilizar los dispositivos tecnológicos precisos para gestionar el principal activo de las mismas, la información.

Asimismo, la formación y concienciación de las personas que intervienen en los procesos organizativos es fundamental, para impedir que una actuación incorrecta perjudique los activos de la organización.

Por ello, este curso permite a los participantes adquirir una formación y competencia en los tres ejes fundamentales en la seguridad de la información:

- Curso de **Auditor Interno de Sistemas de Gestión de Seguridad de la Información**, con el análisis de la Norma ISO 27001, clave para un diseño de un sistema de gestión de seguridad de la información que garantice la integridad, confidencialidad y disponibilidad de la misma.
- Curso de **Protección de Datos: Reglamento Europeo de Protección de Datos y Actualización LOPD**, donde los alumnos podrán adquirir los conocimientos precisos que la nueva normativa europea (RGPD) y española (Ley de Protección de Datos y Garantía de los Derechos Digitales) exige para garantizar el cumplimiento de la normativa actual en protección de datos.
- Curso de **Ciberseguridad esencial y ciberterrorismo**: donde los alumnos adquirirán las competencias precisas relacionadas con la evolución de las tecnologías de la información y de la comunicación, que hace que las redes y los sistemas de información desempeñen un papel crucial en nuestra sociedad, garantizando su fiabilidad y seguridad para el desarrollo eficaz de las actividades económicas y sociales.

## Destinatarios:

Los cursos de **Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001, Reglamento Protección de Datos: Europeo de Protección de Datos y Actualización LOPD, y Ciberseguridad esencial y ciberterrorismo** están destinados a todas aquellas personas que quieran enfocar su actividad laboral hacia una de las actividades con mayores expectativas y demanda de profesionales a corto plazo. El Curso **Auditor de Seguridad de la Información ISO 27001** está dirigido a todas aquellas personas interesadas en desarrollar eficazmente auditorías de seguridad de la información tanto internas como externas, dentro de una organización que tenga implantado el **Sistema de Gestión de Seguridad de la Información en base a las Normas ISO 27001 e ISO 19011 de auditoría**.

Los alumnos adquirirán también competencias actualizadas en el campo de la protección de datos y el tratamiento de datos personales en el curso **Reglamento Europeo de Protección de Datos**, y asimismo los profesionales que deseen iniciar o consolidar su carrera profesional en el ámbito de la seguridad de la información y la protección de datos, podrán diseñar e implantar estrategias de ciberseguridad en las organizaciones con las competencias adquiridas en el curso de **Ciberseguridad esencial y ciberterrorismo**.

En especial los cursos están dirigidos a:

- Profesionales que participan en el **área de recursos humanos** de una organización.
- **Consultores y asesores** especializados en Protección de Datos.
- **Directivos y cargos de responsabilidad** de empresas públicas y privadas con responsabilidad en el tratamiento de datos en áreas de RRHH, Compras, Comercial, etc.
- **Personal que gestiona sistemas de información y trata datos personales de las empresas**, para que puedan actualizar sus conocimientos.
- **Profesionales, universitarios y estudiantes** que deseen formarse y adquirir las competencias precisas en materia de protección de datos.
- **Ingenieros, licenciados y graduados en ingenierías**, ciencias experimentales u otras titulaciones universitarias, así como profesionales, expertos y consultores en el ámbito de la ingeniería TIC y de cualquier sector en el que se requiera el análisis de grandes volúmenes de datos.
- **Titulados Universitario con un Grado, Ingeniería o Licenciatura en Informática o Telecomunicaciones**, que desean consolidar su carrera profesional en el ámbito de la seguridad de la información y la protección de datos

- **Licenciados o graduados e Ingeniería Aeroespacial o Industrial, Matemáticas o Física** que cuenten con una experiencia previa en el campo de las TIC, al ser necesaria esta formación para el desarrollo de las estrategias de ciberseguridad.

## Objetivos:

Que los participantes adquieran las competencias, es decir, conocimientos, habilidades y actitudes relacionadas con la realización de **auditorías de seguridad de la información**, tanto internas como externas, **conocer las novedades que incorpora el Reglamento Europeo de Datos y que dan lugar a la actualización en España de la normativa de protección de datos**, tanto en el ámbito público como privado en la búsqueda de la mejora continua de las organizaciones.

Se formarán profesionales que puedan desempeñar con plena eficacia y eficiencia las tareas relacionadas con la implementación de las técnicas precisas frente a las amenazas a la seguridad de la información que pongan en riesgo a la organización.

Una vez finalizada la acción formativa y superado el preceptivo Examen, los alumnos serán capaces de:

- Ayudar a la organización con la **implantación de un SGSI en base a la norma ISO 27001**.
- **Realizar auditorías de Sistemas de Gestión de Seguridad de la Información** en empresas de cualquier sector, siguiendo para ello las pautas de la Norma de Auditoría **ISO 19011**.
- Interpretar y aplicar la **Norma de Sistema de Gestión de Seguridad de la Información ISO 27001 y la Norma de Auditoría ISO 19011**.
- Conocer el **Proceso de Certificación** de una organización.
- **Formarse como Auditor Interno de Seguridad de la Información**, en los nuevos requisitos planteados por el estándar internacional más reconocido en tecnología de la información y técnicas de seguridad cómo es la norma ISO 27001:2013.
- Conocer los **nuevos derechos** que amplía el Reglamento Europeo de Protección de Datos.
- Aplicar correctamente las **medidas técnicas y organizativas** precisas para **garantizar un nivel de seguridad adecuado en el tratamiento de datos**.
- Delimitar las **funciones y responsabilidades del Delegado de Protección de Datos**.
- Hacer un **análisis de riesgos del tratamiento para la protección de datos**.
- Analizar las **nuevas obligaciones exigidas al responsable y el encargado del tratamiento de datos**.
- Realizar el proceso de **verificación y evaluación de las medidas de seguridad** adoptadas.
- Identificar los **activos de la organización y definir las responsabilidades de protección** adecuadas.
- Garantizar la **integridad y disponibilidad de la información verificando que los datos sean verídicos** para el correcto funcionamiento de los sistemas de información
- **Diseñar las medidas precisas para garantizar el acceso de los usuarios autorizados**, evitando el acceso a los sistemas y servicios de personas sin la autenticación precisa.

# PROGRAMA:

## AUDITOR INTERNO DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO27001:2013

### Módulo 1: Sistemas de Gestión de Seguridad de la Información ISO 27001

- Importancia de la **Norma ISO 27001 en el SGSI** de una Empresa
- Análisis y Revisión de la Norma **ISO 27001**
- Necesidades y Expectativas de la Organización: Liderazgo y Compromiso de la Alta Dirección
- La Planificación y la Gestión de Recursos para el Sistema de Gestión de Seguridad de la Información
- Evaluación del Desempeño y los **Procesos de Mejora en un SGSI**
- Proceso de Implementación de la ISO 27001 en un SGSI

### Módulo 2: Auditoría y Certificación de los Sistemas de Gestión de Seguridad de la Información

- La Normalización Internacional y la Seguridad Industrial
- Principales Aspectos que Reúnen las **Auditorías de un SGSI**
- Planificación y Preparación de la Auditoría a un SGSI
- Proceso de Auditoría a un SGSI
- Análisis de la Elaboración del Informe de Auditoría de un SGSI
- Identificación del Perfil que Debe Reunir un Auditor de SGSI

## PROTECCIÓN DE DATOS: REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ACTUALIZACIÓN LOPD

- Marco Legal de la Protección de Datos
- **Fundamentos, Principios y Legitimación de la Protección de Datos**
- Derechos de los Usuarios: **Derechos ARCO**
- Nuevos Derechos del Reglamento Europeo: Derecho al Olvido, Portabilidad y Limitación del Tratamiento
- Seguridad de los Datos Personales: **Responsabilidad Proactiva**
- Medidas de Seguridad: Registro de las Actividades de Tratamiento
- Análisis y Gestión de Riesgos en los **Tratamientos de Datos Personales**
- Transferencias Internacionales de Datos

- El Delegado de Protección de Datos
- Autoridades de Control

## **CIBERSEGURIDAD ESENCIAL Y CIBERTERRORISMO**

- **Alcance, definiciones y principios** de la **seguridad en el entorno digital**
- Prevención, detección de patrones de ataque e inteligencia en ciberseguridad
- La ciencia de datos y el hacking ético
- **Legislación y normativa** en relación con la ciberseguridad
- **Ciberdelincuencia y economía sumergida**
- **Ciberataques, ciberterrorismo e infraestructuras críticas**



**e-Learning**



**Consultar web**



**45+40+30 horas – 9 meses**



**Consultar web**



**Español**



**Seguridad de la Información**

**CONSTRUYENDO UN  
MUNDO  
DE CONFIANZA**

**Bureau Veritas Formación**

 [formacion@bvbs.es](mailto:formacion@bvbs.es)

 **900921292**



© 2020 Aviso Legal | Condiciones de Uso | Política de Privacidad