



isms forum

Desarrolla conocimiento. Impulsa seguridad. Mantente a la última.

Quiénes somos y por qué formamos

ISMS Forum es una organización sin ánimo de lucro fundada en 2007 y dedicada a promover la cultura de la seguridad de la información en España y Latinoamérica. Con más de 18 años de trayectoria, se ha consolidado como un referente en ciberseguridad, privacidad y gobierno de las tecnologías de la información. Como organización sin ánimo de lucro, nuestro compromiso es impulsar una cultura sólida de seguridad y privacidad en el tejido empresarial.



Nuestra misión

Empoderar a profesionales y empresas con conocimientos prácticos, actuales y alineados con las exigencias normativas y tecnológicas del presente.



Nuestra visión

Ser el ecosistema de referencia en la formación especializada en ciberseguridad, privacidad e inteligencia artificial en el ámbito hispanohablante.



Nuestros valores

Rigor técnico, actualización constante, experiencia práctica y compromiso con el desarrollo profesional continuo de nuestra comunidad.

FORMACIONES BASE

TELEFORMACIÓN

Curso de Concienciación en Ciberseguridad

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Iniciación a la Ciberseguridad en la Nube	Curso orientado a comprender la ciberseguridad desde una perspectiva de gestión y riesgo, proporcionando una visión estructurada sobre amenazas, protecciones, análisis de riesgos y colaboración con organismos y terceros. Incluye fundamentos de gestión de la ciberseguridad, identificación y tratamiento de riesgos tecnológicos, así como los mecanismos de cooperación e intercambio de información en el ámbito de la seguridad.	• Comprenderás los principios clave de la gestión de la ciberseguridad en las organizaciones. • Aprenderás a identificar, analizar y gestionar riesgos y amenazas tecnológicas. • Conocerás los principales tipos de amenazas, vulnerabilidades y medidas de protección. • Mejorarás tu capacidad para participar en la gestión de incidentes y riesgos de ciberseguridad. • Entenderás la importancia de la colaboración con organismos nacionales e internacionales y el intercambio de información (IOCs).	La ciberseguridad requiere una gestión coordinada y basada en riesgos, no solo soluciones técnicas. Las organizaciones necesitan profesionales capaces de identificar amenazas, evaluar su impacto y colaborar eficazmente con terceros y organismos especializados para dar respuesta a incidentes y cumplir con las exigencias actuales de seguridad.	Mayor exposición a riesgos tecnológicos que no son identificados o que se gestionan de forma inadecuada, lo que reduce la capacidad de respuesta ante incidentes de ciberseguridad. Además, dificulta la colaboración eficaz con terceros, organismos especializados y equipos de seguridad, incrementando significativamente el impacto operativo, económico y reputacional de las ciberamenazas para la organización.

6
horas lectivas


Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



**Cybersecurity Awareness
Training Certification**

Curso introductorio al marco normativo de Ciberseguridad: Cyber Compliance

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Introductorio al marco normativo de Ciberseguridad: Cyber Compliance	Visión clara del marco regulatorio de ciberseguridad, del ENS y de los elementos clave para implantar un sistema de CyberCompliance en la organización.	• Comprenderás las principales normas y obligaciones que regulan la ciberseguridad en el entorno empresarial. • Sabrás cómo estructurar un plan básico de CyberCompliance con controles, indicadores y procesos de evaluación. • Identificarás roles, responsabilidades y estructuras necesarias para un modelo de gobierno eficaz. • Entenderás el papel de autoridades como INCIBE, CCN, AEPD o ENISA y los regímenes de sanciones que aplican.	Porque las empresas deben cumplir un marco normativo cada vez más exigente y demostrar responsabilidad y diligencia en materia de ciberseguridad.	Aumenta el riesgo de sanciones, incumplimientos regulatorios, pérdida de confianza y exposición a incidentes o delitos que podrían haberse prevenido.

7
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



Cyber Compliance Basic
Training Certification

Primeros pasos para la Gestión de la Cadena de Suministro

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Gestión de la Cadena de Suministro	Esta formación ofrece una visión práctica sobre la gestión del riesgo y el gobierno IT en supply chain. Abarca desde la colaboración con proveedores hasta ciberseguridad y calidad del dato. Permite comprender y optimizar procesos críticos para garantizar operaciones más seguras y eficientes.	• Anticipación y gestión eficaz de riesgos, reforzando la ciberseguridad y reduciendo vulnerabilidades. • Mejora de la colaboración con proveedores, creando relaciones más sólidas y eficientes. • Optimización de la gobernanza IT y de la calidad del dato para decisiones estratégicas más fiables. • Mayor resiliencia operativa para responder mejor ante interrupciones o cambios en el entorno.	Las cadenas de suministro actuales son complejas y vulnerables a riesgos operativos y tecnológicos. Contar con conocimientos sólidos permite proteger procesos críticos y asegurar la continuidad del negocio. Además, facilita el cumplimiento de estándares y buenas prácticas.	Aumenta la exposición a riesgos, fallos operativos y brechas de ciberseguridad. Se debilita la gobernanza IT, afectando migraciones, supervisión y control del dato. Esto puede comprometer la resiliencia y continuidad de la cadena de suministro.

5
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



Supply Chain Basic
Training Certification

Curso Punto de Partida Directiva NIS2

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Punto de Partida Directiva NIS2	Esta formación ofrece una visión práctica sobre la gestión del riesgo y el gobierno IT en supply chain. Abarca desde la colaboración con proveedores hasta ciberseguridad y calidad del dato. Permite comprender y optimizar procesos críticos para garantizar operaciones más seguras y eficientes.	• Anticipación y gestión eficaz de riesgos, reforzando la ciberseguridad y reduciendo vulnerabilidades. • Mejora de la colaboración con proveedores, creando relaciones más sólidas y eficientes. • Optimización de la gobernanza IT y de la calidad del dato para decisiones estratégicas más fiables. • Mayor resiliencia operativa para responder mejor ante interrupciones o cambios en el entorno.	Las cadenas de suministro actuales son complejas y vulnerables a riesgos operativos y tecnológicos. Contar con conocimientos sólidos permite proteger procesos críticos y asegurar la continuidad del negocio. Además, facilita el cumplimiento de estándares y buenas prácticas.	Aumenta la exposición a riesgos, fallos operativos y brechas de ciberseguridad. Se debilita la gobernanza IT, afectando migraciones, supervisión y control del dato. Esto puede comprometer la resiliencia y continuidad de la cadena de suministro.

5
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



Supply Chain Basic
Training Certification

Curso Base de Protección de Datos

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Base de Protección de Datos	Curso introductorio que ofrece una visión clara y práctica de los conceptos fundamentales de la protección de datos y de las obligaciones que implica su correcta gestión en el ámbito sanitario.	• Comprenderás los conceptos esenciales del marco de protección de datos y su aplicación práctica. • Identificarás los roles, responsabilidades y obligaciones que regulan el tratamiento de datos personales. • Conocerás los principios legales que deben seguirse para garantizar un tratamiento adecuado y seguro. • Sabrás cómo actúan las autoridades de control y cuáles son sus competencias. • Mejorarás tu capacidad para detectar riesgos, evitar incumplimientos y actuar conforme a la normativa.	Porque todas las organizaciones manejan datos personales y es obligatorio garantizar un tratamiento adecuado conforme a la normativa vigente.	Se incrementa el riesgo de incumplimiento legal, sanciones económicas, pérdida de confianza de clientes y daños reputacionales.

3
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de privacidad



Data Privacy Basic
Training Certification

FORMACIONES INTERMEDIAS

TELEFORMACIÓN

Curso de conceptos básicos sobre Ciberseguridad

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Conceptos básicos sobre Ciberseguridad	Curso orientado a la proporcionar una visión sólida y práctica de los principios fundamentales de la ciberseguridad. Abarca los conceptos clave, amenazas más comunes, buenas prácticas y controles básicos necesarios para proteger la información y los sistemas en cualquier entorno organizativo.	• Adquirirás una base sólida en ciberseguridad aplicada a entornos reales. • Comprenderás las principales amenazas, vulnerabilidades y riesgos digitales. • Mejorarás la capacidad para identificar incidentes de seguridad básicos. • Aumentarás la concienciación en ciberseguridad a nivel profesional y organizativo. Obtendrás una certificación reconocida como base para itinerarios avanzados en ciberseguridad.	La ciberseguridad ya no es solo responsabilidad de los equipos técnicos. Las organizaciones exigen que todos los profesionales comprendan los riesgos digitales, adopten buenas prácticas y contribuyan activamente a la protección de la información frente a amenazas cada vez más frecuentes y sofisticadas. Este curso constituye el punto de partida imprescindible para desarrollar una cultura de seguridad eficaz.	Mayor exposición a incidentes de seguridad básicos (phishing, malware, accesos no autorizados). Falta de conocimientos mínimos exigidos en muchos entornos corporativos. Dificultad para avanzar hacia certificaciones y roles especializados en ciberseguridad. Riesgo de impacto reputacional y operativo por errores humanos evitables.

10
horas lectivas


Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



Cyber Security Basic
Training Certification



Curso de iniciación a la Ciberseguridad en la Nube

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Iniciación a la Ciberseguridad en la Nube	Curso introductorio para comprender los conceptos clave de la Nube y cómo impactan en la ciberseguridad de las organizaciones. Incluye fundamentos tecnológicos, modelos de servicios cloud, entornos híbridos y multicloud, así como el impacto organizativo y estratégico derivado de su adopción.	• Conocerás los modelos fundamentales de la Nube y su relación con la ciberseguridad. • Entenderás los riesgos y responsabilidades compartidas en entornos cloud. • Sabrás identificar arquitecturas, servicios y escenarios de uso adecuados para tu organización. • Tendrás una visión clara de cómo la adopción de la Nube transforma procesos, roles y operaciones. • Mejorarás tu capacidad para participar en proyectos de transformación digital con enfoque seguro.	Porque la Nube es ya un entorno crítico y una parte fundamental de los procesos y servicios de la mayoría de las empresas.	Mayor riesgo de configuraciones inseguras, dependencia de terceros mal gestionada y brechas derivadas de un uso inadecuado del cloud.

6
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de ciberseguridad



Cloud Cybersecurity
Governance Basic Training
Certification

Novedades en el Marco Regulatorio de Protección de Datos

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Novedades en el Marco Regulatorio de Protección de Datos	Curso orientado a comprender el marco regulatorio europeo aplicable a la Inteligencia Artificial, así como los requisitos de privacidad, cumplimiento y gestión de riesgos asociados al tratamiento de datos personales en sistemas de IA. La formación aborda la Data Governance Act, la Data Cyber Resilience Act, la regularización de tratamientos de datos en IA, el análisis de riesgos y la realización de evaluaciones de impacto, apoyándose en guías y herramientas de referencia.	- Comprenderás el marco normativo europeo que regula la gobernanza de datos y la resiliencia en entornos de IA. - Conocerás cómo se tratan y almacenan los datos personales en sistemas de Inteligencia Artificial. - Aprenderás a aplicar los principios de licitud, transparencia y privacy by design en proyectos de IA. - Mejorarás tu capacidad para realizar análisis de riesgos y evaluaciones de impacto en privacidad y derechos fundamentales. - Dispondrás de guías y herramientas prácticas para reforzar la seguridad de los datos personales.	El uso de sistemas de Inteligencia Artificial implica riesgos significativos en materia de privacidad, cumplimiento normativo y derechos fundamentales. Las organizaciones deben garantizar que sus tratamientos de datos en IA cumplen con la normativa europea, integran la privacidad desde el diseño y evalúan adecuadamente los riesgos para evitar impactos legales, económicos y reputacionales.	El uso de sistemas de Inteligencia Artificial implica riesgos significativos en materia de privacidad, cumplimiento normativo y derechos fundamentales. Las organizaciones deben garantizar que sus tratamientos de datos en IA cumplen con la normativa europea, integran la privacidad desde el diseño y evalúan adecuadamente los riesgos para evitar impactos legales, económicos y reputacionales.

3
horas lectivas


Tasa de satisfacción
Entre nuestros alumnos de privacidad



**Data Privacy Basic
Training Certification**

Curso de introducción a la Ciberseguridad de la IA

	Descripción	Beneficios	Por qué es esencial	Qué pasa si no lo haces
Introducción a la Ciberseguridad de la IA	Curso que introduce los fundamentos de los sistemas de IA y los principales riesgos, amenazas y medidas de ciberseguridad asociadas a su uso y operación.	- Comprenderás cómo funcionan los principales tipos de IA (Machine Learning, Deep Learning, sistemas generativos) y qué implicaciones tienen en la seguridad. - Identificarás las amenazas más comunes en sistemas de IA: manipulación de datos, ataques adversarios, extracción de modelos, suplantación de prompts, etc. - Conocerás buenas prácticas y controles para un uso seguro de herramientas de IA en la organización. - Sabrás cómo aplicar IA para mejorar la ciberdefensa, automatizar detecciones y reforzar la respuesta ante incidentes. - Obtendrás una visión clara del equilibrio entre innovación, riesgo y cumplimiento normativo relacionado con la IA. - Mejorarás tu capacidad para evaluar riesgos y apoyar decisiones técnicas o estratégicas sobre la adopción segura de IA.	Porque la IA se ha convertido en un componente crítico de muchos procesos y puede ser tanto un habilitador de seguridad como una fuente de nuevas amenazas si no se gestiona correctamente.	Aumenta la exposición a ataques dirigidos a modelos de IA, riesgos de manipulación, fugas de información y uso inseguro de herramientas generativas dentro de la organización.

10
horas lectivas



Tasa de satisfacción
Entre nuestros alumnos de IA



Artificial Intelligence Basic
Training Certification



 **INSCRÍBETE AQUÍ A NUESTRA OFERTA FORMATIVA**



formacion@ismsforum.es

www.ismsforum.es

