CERTIFIED CYBER SECURITY PROFESSIONAL

Certified Cyber Security Professional (CCSP)

Formulario de Acreditación de Experiencia Profesional

1. Introducción

Aquellos profesionales que hayan superado el examen de certificación, deben acreditar mediante este formulario contar con al menos **tres años** de experiencia profesional en el ámbito de la Seguridad de la Información.

Envíe su formulario completado, debidamente firmado y sellado, acompañado de una copia de su DNI a: **certificacion@ismsforum.es**

INFORMACIÓN PERSONAL

Apellidos		Nombre	
NIF o pasaporte		☐ Soy socio de ISMS Forum Spain	
Dirección		Nº	Pta.
Código postal	Ciudad	Provincia	
Teléfono	Móvil	Correo-e	

Recuerde que debe acompañar una copia de su D.N.I con la solicitud.

EXPERIENCIA PROFESIONAL

Indique cómo ha obtenido la experiencia profesional demostrable de al menos 3 años en el ámbito de la Privacidad, y/o Protección de Datos de carácter personal, y/o la Seguridad de la Información, marcando la(s) casilla(s) correspondiente(s).

.

		Desde (mm/aaaa)	Hasta (mm/aaaa)
CATEGORÍA A	Chief Security Officer (CSO)		
	Chief Information Security Officer (CISO)		
	IT Manager		
	Risk Manager		
	Responsable en departamento de Seguridad de la Información		
CATEGORÍA B	Abogado acreditando funciones en el ámbito de la Seguridad de la Información Auditor acreditando funciones en el ámbito de la Seguridad de la Información Consultor acreditando funciones en el ámbito de la Seguridad de la Información Asesor o técnico acreditando funciones en el ámbito de la Seguridad de la Información		
	Total de años de experiencia laboral acreditados (a completar por el Comité de Certificación):		

A continuación, indique, marcando la casilla correspondiente, en cuáles de las siguientes áreas ha obtenido su experiencia:

☐ Área 1: Gobierno de Seguridad

El candidato acredita experiencia como responsable de la dirección, gestión e implementación de los sistemas y recursos de seguridad de la información en organizaciones públicas o privadas.

En particular, el candidato ha intervenido significativamente en al menos, una de las siguientes actividades:

- Definición/ responsable de arquitectura de seguridad.
- Organización/ gestión/ estrategia de ciberseguridad.
- Aprobación de buenas prácticas de referencia (COBIT, ISO 27000).
- Organización de roles y responsabilidad.
- Auditoría, control y certificación.
- Terceras partes, Cloud y Movilidad.

☐ Área 2: Análisis y gestión de riesgos

El candidato acredita experiencia en la identificación, análisis y gestión de riesgos y amenazas, así como en riesgos tecnológicos.

☐ Área 3: Cumplimiento legal y normativo

El candidato acredita experiencia en la aplicación de la normativa de privacidad y protección de datos vigente dentro de organizaciones públicas y/o privadas.

El candidato acredita haber intervenido significativamente en al menos una de las siguientes actividades:

- Técnicas, metodologías y herramientas del compliance legal.
- Notificación, reporte, denuncia y presentación en juzgado.
- Cibercrimen y delito informativos.

En el marco de dicha experiencia, el candidatos ha aplicado los principios que rigen la protección de datos de carácter personal (información, consentimiento, calidad, entre otros) así como las distintas figuras existentes en el tratamiento de datos personales (responsable de fichero o de tratamiento, encargado del tratamiento, entre otras).

☐ Área 4: Operativa de Ciberseguridad

El candidato acredita experiencia en la aplicación de las técnicas necesarias para proteger los activos de información contenidos tanto en soportes automatizados, como en soportes no automatizados.

El candidato acredita la experiencia en el manejo de tecnologías, herramientas, servicios, capacidades, infraestructura de seguridad, SIEM, IDS, análisis de malware, BYOD, SOC, pentesting, gestión de vulnerabilidades y hacking ético.

☐ Área 5: Ciber-inteligencia, cooperación y capacidad

El candidato acredita experiencia en proyectos de gestión de resiliencia, gestión de ciber-crisis, ciber-ejercicios y/o proyectos de intercambio de indicadores de compromiso.

☐ Área 6: Gestión eficaz de incidentes

El candidato acredita experiencia en la aplicación de medidas para la gestión de incidentes de seguridad, desde la detección y gestión hasta los programas de continuidad y resiliencia, o experiencia en el análisis forense.

En línea con las áreas de experiencia seleccionadas, describa la experiencia, las responsabilidades y tareas realizadas en cada una de ellas, en los campos que se le proporcionan a continuación. Indique claramente las fechas de inicio y fin de cada tarea.

Área 1: Gobierno de Seguridad

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

Área 2: Análisis y gestión de riesgos

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

Área 3: Cumplimiento legal y normativo

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

Área 4: Operativa de Ciberseguridad

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

Área 5: Ciber-inteligencia, cooperación y capacidad

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

Área 6: Gestión eficaz de incidentes

Resumen de la experiencia, responsabilidades y tareas.

Firma de la persona que suscribe la Carta de Acreditación Profesional (p.9)

CARTA DE ACREDITACIÓN DE EXPERIENCIA PROFESIONAL

Quien suscribe, por medio de la presente MANIFIESTA que ha leído la experiencia profesional descrita en la presente solicitud por el candidato a la Certificación Certified Cyber Security Professional (CCSP), y en este sentido, DECLARA que el contenido reflejado en la misma, se alinea con las competencias que el candidato ha demostrado tener dentro de la organización a la que pertenece.

Datos de la persona que acredita

Nombre	
Cargo	
Empresa	
Teléfono profesional	Correo-e profesional
Experiencia vinculada: (número del área)	

Nombre	
Cargo	
Empresa	
Teléfono profesional	Correo-e profesional
Experiencia vinculada: (número del área)	

Cláusula de Protección de Datos

Con objeto de dar cumplimiento a las obligaciones derivadas de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la Asociación Española para el Fomento de la Seguridad de la Información ISMS FORUM (en adelante, ISMS FORUM), le informa de los siguientes extremos:

1. Sus datos pasarán a formar parte de un fichero de titularidad de ISMS FORUM cuya finalidad es gestionar los procesos de inscripción a la certificación Certified Cyber Security Professional (CCSP) del solicitante. Los datos aportados podrán ser utilizados para contactarle en relación con la declaración que realiza mediante el presente formulario.

2. El Responsable del fichero es ISMS FORUM y su dirección es Calle Segre, 29, 1ºB, 28002 Madrid - España, a la cual podrá remitir los escritos de ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, identificados con la referencia "Protección de datos" y con las siguientes indicaciones:

- Nombre, apellidos y número de Documento Nacional de Identidad.
- Petición en la que se concreta la solicitud.
- Domicilio a efectos de notificaciones.

Firma

Sello de la empresa

Firmado en		a		de	de

ACREDITACIÓN DE EXPERIENCIA PROFESIONAL

Datos de contacto de otras entidades a las que se vincule la experiencia. (Máximo 2)

Sólo se requieren datos en caso de que se quiera acreditar experiencia obtenida en diferentes entidades.

Nombre	
Cargo	
Empresa	
Teléfono profesional	Correo-e profesional
Experiencia vinculada: (número del área)	

Nombre	
Cargo	
Empresa	
Teléfono profesional	Correo-e profesional
Experiencia vinculada: (número del área)	

El solicitante declara que los datos aportados son exactos y veraces. Asimismo, declara que ha obtenido el consentimiento de las personas cuyos datos aporta, con el objeto de que ISMS Forum Spain pueda contactarles para comprobar la experiencia manifestada en la presente solicitud.

FIRMA DEL SOLICITANTE

Cláusula de Protección de Datos

Con objeto de dar cumplimiento a las obligaciones derivadas de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la Asociación Española para el Fomento de la Seguridad de la Información ISMS FORUM (en adelante, ISMS FORUM), le informa de los siguientes extremos:

1.Sus datos pasarán a formar parte de un fichero de titularidad de ISMS FORUM, cuya finalidad es gestionar los procesos de inscripción de la certificación Certified Cyber Security Professional (CCSP), así como para remitirle información sobre eventos y actividades relacionadas con ISMS Forum.

2. El Responsable del fichero es ISMS FORUM y su dirección es Calle Segre, 29, 1ºB 28002 Madrid - España, a la cual podrá remitir los escritos de ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, identificados con la referencia “Protección de datos” y con las siguientes indicaciones:

- Nombre, apellidos y número de Documento Nacional de Identidad.
- Petición en la que se concreta la solicitud.
- Domicilio a efectos de notificaciones.

☐ Quiero recibir información sobre eventos y actividades relacionados con ISMS Forum.

Firma del solicitante: _____

Firmado en _____ a ____ de _____ de