Agencia Digital de Andalucía

SOC DE LA JUNTA DE ANDALUCÍA | CENTRO CIBERSEGURIDAD ANDALUCÍA

MOOC

Preparación a la certificación CISM

Ficha técnica

Acción formativa MOOC.
Del 22 de abril al 31 de mayo 2024

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: MOOC: Preparación a la certificación CISM

Modalidad: MOOC

Fecha de celebración: Del 22 de abril al 31 de mayo de 2024

Dirigido a:

Este curso de formación está dirigido a Profesionales TIC de la Junta de Andalucía y entidades vinculadas que tienen de 3 a 5 años de experiencia laboral reciente a tiempo completo en la gestión de la seguridad de la información.

- CISOs
- CIOs
- CSOs
- Profesionales de la seguridad de la información
- Responsable de la seguridad de la información
- Aquellos con responsabilidades de gestión
- Personal de seguridad de la información

Número máximo de personas participantes: 200.

2 DESCRIPCIÓN

El objetivo del MOOC de preparación a la certificación CISM, es brindar las herramientas necesarias para elaborar, administrar, diseñar, supervisar y evaluar programas de seguridad de la información de una organización, garantizando una gestión de eficaz y un asesoramiento continuo.

CISM (*Certified Information Security Manager*), es una certificación de ISACA que entró en validez en el año 2002. La misma es una certificación en Gestión de Seguridad de la Información dirigida a profesionales experimentados en el ámbito.

La CISM está directamente enfocada en la gestión de la Ciberseguridad. Promueve prácticas de seguridad avaladas a nivel internacional y acredita a personas que administran, supervisan, diseñan y evalúan la seguridad de una organización.

3 OBJETIVOS

- Establecer y/o mantener un marco de gobierno de la Seguridad de la Información y procesos de apoyo para asegurar que su estrategia esté alineada con las metas y objetivos de la organización.
- Gestionar el riesgo de la información a un nivel aceptable basado en el apetito de riesgo para cumplir las metas y objetivos de la organización.
- Desarrollar y mantener un programa de Seguridad de la Información que identifique, administre y proteja los activos de la organización al mismo tiempo que se alinea con los objetivos comerciales, apoyando así una postura de seguridad efectiva.
- Planificar, establecer y gestionar la capacidad de detectar, investigar, responder y recuperarse de los incidentes de Seguridad de la Información para minimizar el impacto comercial.
- Entenderá cómo establecer y mantener los marcos necesarios que aseguren que las estrategias de seguridad de la información están alineadas con los objetivos del negocio y son consistentes con las leyes y regulaciones aplicables.
- Identificar y gestionar con confianza los riesgos de seguridad de la información para alcanzar los objetivos del negocio
- Estar familiarizado con la terminología aceptada por la industria y las prácticas utilizadas por los profesionales de la seguridad de la información
- Obtener el conocimiento y las habilidades necesarias para el examen CISM de ISACA

4 CONTENIDOS

Módulo 0: Introducción a la certificación CISM:

- Introducción a CISM
- Conociendo los recursos disponibles para obtener la certificación
- Requisitos para obtener la certificación en CISM
- Los 4 dominios en los que se divide las áreas de conocimientos
- Beneficios de la certificación CISM

Módulo 1: Gobierno de la seguridad de la información:

- Estrategia de seguridad.
- Marco de referencia de gobierno para soportar el programa de seguridad.
- Involucramiento del Gobierno Corporativo en el Gobierno de la Seguridad para lograr los objetivos estratégicos.
- Definición y establecimiento de la Política de Seguridad.
- Desarrollo de casos de negocio para optimizar las inversiones de seguridad.

Identificación de los Factores Ambientales de la Organización (contexto interno y externo) y los Activos de los Procesos de la Organización) que influyen en la elaboración e implementación de la estrategia de seguridad.

- Definición de los roles y responsabilidades de seguridad.
- Aseguramiento del compromiso de la Alta Dirección y los interesados más importantes.
- Definición y obtención de los indicadores de efectividad del programa de seguridad.

Módulo 2: Gestión de riesgos de la información:

– Clasificación y aseguramiento de los activos de información.

– Identificar las obligaciones legales de cumplimiento por la organización.

– Aseguramiento periódico de la revisión de los riesgos, análisis de vulnerabilidades y la evaluación de las medidas de mitigación.

– Definición e implementación del plan de respuesta a los riesgos identificados.

– Integración de la gestión del riesgo con los procesos de negocio y la tecnología de la información.

– Monitorización de los riesgos para identificar y gestionar los cambios en los mismos.

Módulo 3: Desarrollo y gestión del programa de seguridad de la información:

– Aseguramiento de que el programa y los objetivos de negocio están alineados.

– Gestión de los recursos necesarios para la implementación y el cumplimiento del programa.

– Establecimiento y mantenimiento de la arquitectura de seguridad para la realización del programa.

– Definir, desarrollar, implantar, comunicar y revisar los procedimientos, guías, etc. que soportan la Política de Seguridad de la Información.

– Definición del Plan de Formación y Concienciación en Seguridad.

– Integración de los requisitos de seguridad en los procesos de la organización.

– Integración de los requisitos de seguridad con terceros que acceden a la información de la organización.

– Monitorización de la efectividad del programa.

Módulo 4: Gestión de incidentes de seguridad de la información:

– Definición de incidentes de seguridad de la información para su identificación, clasificación, comunicación y seguimiento.

– Desarrollo del Plan de Respuesta ante Incidentes de Seguridad.

– Desarrollo de procedimientos de identificación de incidentes.

– Desarrollo de procedimientos de investigación de incidentes para determinar sus causas, cumplir los requisitos legales, etc.

– Desarrollo del Plan de Concienciación ante Incidentes.

– Desarrollo del Plan de Comunicación ante Incidentes.

– Revisión de la efectividad de la gestión de los incidentes de seguridad sufridos por la organización.

Modulo 5: Simulacro de examen:

- Simulacro 1: Examen de 4 horas con 150 preguntas como simulacro de la certificación

- Simulacro 2: Examen de 4 horas con 150 preguntas como simulacro de la certificación

5 TEMPORALIZACIÓN

Fecha: Del 22 de abril al 31 de mayo de 2024

Carga lectiva: Se estima una carga lectiva de 2 horas diarias. Se entiende por carga lectiva el trabajo que dedica una persona participante al curso comprendiendo tareas de visionado de los elementos de la plataforma, trabajo y estudio autónomo

Modalidad: MOOC (online)

6 METODOLOGÍA

La metodología que vamos a seguir es la basada en los cursos masivos y abiertos en modalidad online (MOOCS):

Una de las características clave de los MOOC es su enfoque en la participación activa de las personas que participáis. Esto se logra a través de diversas actividades, como la realización de tareas por pares. Estas tareas fomentan la colaboración entre los participantes y les permiten aplicar los conceptos aprendidos en un entorno práctico.

También los foros de discusión son otro componente fundamental de la metodología MOOC. Estos foros proporcionan un espacio para que los participantes interactúen entre sí y con los tutores. Aquí, los participantes pueden plantear preguntas, debatir ideas y compartir experiencias relacionadas con el contenido del curso. Los foros de discusión no solo promueven un aprendizaje colaborativo, sino que también permiten a los estudiantes explorar diferentes perspectivas y enfoques.

Además de las actividades por pares y los foros de discusión, se ofrecen una variedad de recursos de aprendizaje, como videos, lecturas y cuestionarios. Estos contenidos están diseñados para ser accesibles y flexibles, lo que os permite aprender a vuestro propio ritmo.

Se ofrecerán una serie de tutorías en línea, donde los participantes pueden recibir orientación adicional y resolver dudas específicas sobre el material del curso. Se irán organizando y comunicando a lo largo del curso.

7 DOCENTE

IMPARTIDO POR: Adrián Ramírez

Asesor en ciberseguridad tanto en el sector público como privado, integrando varios comités de seguridad, director del departamento de Ciberseguridad de Dolbuck con más de 17 años de experiencia en el campo de la ciberseguridad. Perito informático especialista en análisis forense de entornos GNU/Linux y Windows. Investigador de seguridad durante más de 8 años. Ha sido ponente en varios eventos de seguridad a nivel nacional e internacional.

Consultor y auditor de certificación de sistemas de gestión de la seguridad como ENS, ISO 27001. Cuenta con varias certificaciones en el sector de la seguridad de la información y seguridad ofensiva. Docente en las formaciones de Seguridad de sistemas y redes, Sistemas operativos de Servidores, Esquema Nacional de Seguridad (ENS), Gestión del riesgo y Hacking ético. Para empresa del sector privado y público. Especializado en virtualización y en ingeniería de sistemas y redes.

8 EVALUACIÓN

Para aprobar este MOOC, deberá haber obtenido una nota media de 6 sobre 10 puntos de los siguientes módulos:

- Módulo 0: Introducción
- módulo 1 Gobierno de la seguridad de la información
- módulo 2 Gestión de riesgos de seguridad de la información y cumplimiento
- módulo 3 Desarrollo y gestión del programa de seguridad de la información
- Módulo 4 Gestión de incidentes de seguridad de la información
- Evaluación final del curso con 30 preguntas.

Las tareas por pares serán voluntarias, aunque muy recomendables para conocer cómo otros profesionales enfocan y resuelven el problema planteado.

En referencia al Módulo 5 Simulacro de examen, se recuerda que dicho módulo no se evalúa, ya que su finalidad es que sirva de entrenamiento para la preparación del certificado CISM. Contiene 2 simulacros con 150 preguntas cada uno, con un total de 4 horas para realizarlo.

Por lo que los resultados obtenidos servirán de referencia a cada alumno para valorar su nivel de preparación frente a una certificación de CISM y se podrá realizar tantas veces se quiera, sin que eso afecte la nota final del MOOC.