CURSO DE PREPARACIÓN PARA EL EXAMEN INTERNACIONAL COMO GERENTE CERTIFICADO EN SEGURIDAD DE LA INFORMACIÓN C.I.S.M 2017

Certified Information Security Manager (C.I.S.M) es una certificación de prestigio internacional, que asegura a las organizaciones que el personal a cargo de la administración de seguridad de información posee el conocimiento y experiencia en mejores prácticas internacionales para gestión de seguridad de la información; facilitando el logro de los objetivos estratégicos de la empresa y el fortalecimiento del Buen Gobierno Corporativo.

C.I.S.M es una certificación creada por la Asociación de Control y Auditoría de Sistemas de Información (**ISACA**) (Information Systems Audit and Control Association) y acreditada por **ANSI**. Esta certificación es actualmente reconocida de forma global como credencial de excelencia.

OBJETIVO GENERAL

Adquirir o fortalecer los conocimientos y habilidades necesarias para realizar de manera práctica y efectiva, el diseño, realización y mejora continúa de un programa de seguridad de la información; teniendo en cuenta las mejores prácticas reconocidas internacionalmente en esta materia.

OBJETIVOS ESPECÍFICOS

- Adquirir los conocimientos y destrezas necesarias para incrementar la probabilidad de aprobar el examen de certificación internacional como Certified Information Security Manager - C.I.S.M
- Conocer de primera mano, lecciones aprendidas por el instructor en sus años de experiencia diseñando, implementando y liderando sistemas de seguridad de la información en reconocidas empresas internacionales, donde se desempeñó como Gerente de Riesgos en VISA, Director de Riesgos en IQ, Jefe de la Oficina de Control Interno (e) de la hoy Superintendencia Financiera de Colombia y Consultor ERS en Deloitte&Touche.
- Promover programas de capacitación y sensibilización al interior de la empresa, con el fin de lograr mayor grado de conciencia entre los principales involucrados en la gestión efectiva de seguridad de la información, como facilitadora para el logro de los objetivos organizacionales y fortalecimiento del Gobierno Corporativo.

DURACIÓN

Total 24 horas. Discriminadas en 20 horas teórico prácticas y 4 horas destinadas para simulacro del examen de certificación y discusión de las respuestas.

CONTENIDO

MÓDULO 1

Gobierno de la Seguridad de la Información

- Establecer y mantener una estrategia de seguridad de la información acorde con los objetivos de la organización.
- Establecer y mantener un marco de referencia para el Gobierno de Seguridad de la Información como guía que soporta el programa de seguridad de la información.
- Asegurar que el Gobierno de Seguridad de la Información hace parte del Gobierno Corporativo y ayuda al logro de los objetivos estratégicos.
- Establecer y mantener políticas de seguridad de la información, como guía al desarrollo de estándares, procedimientos y prácticas; así como medio de comunicación por parte de la Alta Dirección.
- Desarrollar casos de negocio que soporten las inversiones en seguridad de la información.
- Identificar y analizar el contexto interno y externo de la organización con influencia en la elaboración e implementación de la estrategia de seguridad de la información.
- Definir y comunicar los roles y responsabilidades de seguridad de la información, estableciendo líneas claras de autoridad.
- Obtener el compromiso de la Alta Dirección y las partes interesadas relacionadas.
- Establecer, monitorear, evaluar métricas sobre la efectividad del programa de seguridad de la información.

CONTENIDO

MÓDULO 2

Gestión de riesgos de la información y Cumplimiento

- Establecer y mantener un proceso de clasificación y aseguramiento de activos de información, acorde y proporcional a su valor para el negocio.
- Identificar obligaciones legales, regulatorios y organizacionales aplicables para la empresa y los requisitos para gestionar el riesgo de incumplimiento sobre niveles aceptables previamente definidos.
- Asegurar que la valoración del riesgo, evaluación de las vulnerabilidades, análisis de medidas de tratamiento sean realizadas periódicamente como parte de la gestión del riesgo de seguridad de la información.
- Determinar medidas apropiadas de tratamiento para gestionar el riesgo dentro de los niveles aceptables establecidos.
- Integrar la información de gestión de riesgo, con los procesos del negocio y tecnología de información T.I
- Monitorear riesgos identificados y asegurar que cualquier cambio es identificado y gestionado oportunamente.
- Reportar incumplimientos o cambios en los riesgos de seguridad de la información soportando una adecuada toma de decisión.

MÓDULO 3

Desarrollo y gestión de un programa de seguridad de la información

- Asegurar el alineamiento entre el programa de seguridad de la información y los objetivos del negocio.
- Identificar, adquirir, gestionar requerimientos de recursos internos y externos necesarios para la implementación y cumplimiento del programa de seguridad de la información.
- Establecer y mantener la arquitectura de seguridad de la información (personas, procesos, tecnología), para la realización del programa de seguridad de la información.
- Establecer, comunicar y mantener, procedimientos, estándares, prácticas y guías documentadas que soporten el cumplimiento de la política de seguridad de la información.
- Establecer e implementar programas de sensibilización y capacitación que fortalezcan la cultura en seguridad de la información.
- Integrar requerimientos de seguridad de la información a los procesos organizacionales (Control de cambios, planes de continuidad del negocio, desarrollo, mantenimiento y adquisición, etc)
- Integrar requisitos de seguridad de la información en la relación con terceros
- Establecer programas e informes periódicos de monitoreo y evaluación de la efectividad del programa de seguridad de la información.

CONTENIDO

MÓDULO 4

Gestión de incidentes de seguridad de la información

- Establecer y mantener una definición organizacional de incidente de seguridad de información, que permita su adecuada identificación, categorización, reporte y seguimiento.
- Establecer y mantener un plan de respuesta a incidentes de seguridad de la información que permita atenderlos oportunamente
- Desarrollar e implementar procedimientos que permitan la oportuna identificación de incidentes de seguridad de la información.
- Desarrollar e implementar procedimientos para investigar y documentar incidentes de seguridad de la información que permita determinar sus causas y dar cumplimiento a requisitos legales y contractuales vigentes a aplicables.
- Desarrollar programas de capacitación, sensibilización y entrenamiento en gestión de incidentes de seguridad de la información.
- Establecer y mantener planes de comunicación internos y externos ante incidentes de seguridad de la información.
- Establecer y mantener planes de revisión sobre la efectividad de la respuesta dada por la organización ante un incidente de seguridad de la información y recopilación de lecciones aprendidas, junto con la identificación de causa raíz y planes correctivos que eviten reincidencias.

MÓDULO 5

Simulacro examen de certificación "CISM "

- Simulacro individual por escrito de 100 preguntas.
- Solución y discusión de las respuestas al simulacro.

METODOLOGÍA DE APRENDIZAJE

La formación incluye presentaciones magistrales basadas en el material del curso elaborado por el instructor y entregado a cada estudiante para su uso individual; así como ejercicios prácticos y transferencia de lecciones aprendidas por el instructor en sus años de experiencia profesional.

MATERIAL DE APOYO Y ESTUDIO

Al final del curso, se hará entrega a cada asistente del material de estudio en medio electrónico, elaborado por el instructor con base en el último material oficial ofrecido por **ISACA** y material complementario utilizado como referencia dentro del desarrollo del curso. Igualmente se hará entrega de una constancia de asistencia al curso, para quienes hayan participado en el 85% del programa.

INSTRUCTOR

RESTREPORAMAS S.A.S.

CARLOS ALFONSO RESTREPO ORAMAS

(CISA, CISM, CGEIT, CRISC, CBCP, Lead Implementer ISO 22301, ISO 27001, ISO 20000 Lead Auditor ISO 22301, ISO 27001, ISO 20000, Risk Manager ISO 31000, ITIL V3, Cobit 5).

Formador certificado por el Instituto Tecnológico de Monterrey México, con 20 años de experiencia profesional en el sector financiero colombiano; capacitando, diseñando, auditando, implementando, operando y liderando sistemas de gestión integral de riesgo y continuidad del negocio para empresas de reconocido prestigio internacional.

Carlos A. Restrepo se ha desempeñado en los últimos 17 años como: Gerente General en Restrepo&Oramas SAS, Gerente de Procesos y Riesgo en Visa_Colombia, Experto de Seguridad TI y Continuidad del Negocio en Synapsis Colombia, Consultor E.R.S en Deloitte&Touche, Jefe (e) de la Oficina de Control Interno de la hoy Superintendencia Financiera de Colombia y Director de Riesgo Operativo en IQ Outsourcing S.A".

Su capacidad de combinar conocimiento y experiencia como catedrático, consultor, auditor, implementador de Sistemas de Gestión Integral de Riesgo y Continuidad; así como ejercer su rol de Gerente de Procesos y Riesgos en VISA, le han permitido obtener las máximas calificaciones en calidad y satisfacción para la totalidad de los seminarios impartidos en México, Costa Rica, Honduras, Nicaragua, Guatemala, Panamá, República Dominicana, Colombia, Venezuela, Perú, Bolivia, Chile, Ecuador, Paraguay y Argentina.

Para mayor información por favor contáctenos al correo: info@ro-sas.com