Curso de Preparación para la Certificación CISM (Certified Information Security Management)

Código: CISM-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas

El curso de preparación para la certificación CISM (Certified Information Security Management) está dirigido a profesionales que desean profundizar sus conocimientos en Seguridad de la Información, dicha certificación está enfocada en la gestión, promueve prácticas internacionales de seguridad y acredita personas que administran, diseñan, supervisan y evalúan la seguridad de la información de una empresa, diseñada para los profesionales responsables de administrar el riesgo de la empresa a través de eficaces controles de Seguridad de la Información, es decir los profesionales de gestión y auditoría de TI, de riesgos, de control, de seguridad, de análisis de negocio, de proyectos y de cumplimiento regulatorio.

Los profesionales que acepten el reto encontrarán en esta certificación, una herramienta de gran valor para las empresas. A la fecha, CISM está entre las certificaciones mejor retribuidas, y ha sido obtenida por más de 32,000 profesionales en todo el mundo.

AUDIENCIA

- Este curso está dirigido a Profesionales del Área de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores y Responsables de Seguridad de la Información que deseen prepararse para una certificación reconocida internacionalmente.

PRE REQUISITOS

- Conocimientos básicos de Seguridad de la Información
- Experiencia en el ramo de la Seguridad de la Información
- Conocimientos básicos de Auditoria de Sistemas

OBJETIVOS

- El curso ha sido diseñado para fortalecer los conocimientos y ayudar a los participantes en los temas clave de los contenidos del examen y que éstos asimilen el enfoque y filosofía de ISACA.

CERTIFICACIÓN DISPONIBLE

- Certficado oficial de **COGNOS**.
- Este curso lo prepara para la certificación: **CISM - Certified Information Security Manager.**

CONTENIDO

1. GOBIERNO DE SEGURIDAD DE LA INFORMACION

1.1. ESTABLECER Y MANTENER UNA ESTRATEGIA DE SEGURIDAD .
1.2. ESTABLECER Y MANTENER UN MARCO DE GOBERNANZA DE LA SEGURIDAD
1.3. INTEGRAR LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACION
1.4. ESTABLECER Y MANTENER POLITICAS DE SEGURIDAD DE LA INFORMACION
1.5. DESARROLLAR CASOS DE NEGOCIOS
1.6. IDENTIFICAR LAS INFLUENCIAS INTERNAS Y EXTERNAS
1.7. IMPLEMENTACION EXITOSA DE LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACION.
1.8. DEFINIR Y COMUNICAR LAS FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACION
1.9. ESTABLECER, MONITOREAR, EVALUAR E INFORMAR METRICAS

2. GESTION DE RIESGOS DE LA INFORMACION

2.1. ESTABLECER Y MANTENER UN PROCESO DE CLASIFICACION
2.2. IDENTIFICAR REQUISITOS LEGALES, REGLAMENTARIOS, ORGANIZACIONALES
2.3. ASEGURAR QUE LAS EVALUACIONES DE RIESGOS, LAS EVALUACIONES DE VULNERABILIDAD
2.4. DETERMINAR LAS OPCIONES APROPIADAS DE TRATAMIENTO DEL RIESGO
2.5. EVALUAR LOS CONTROLES DE SEGURIDAD DE LA INFORMACION
2.6. IDENTIFICAR LA BRECHA ENTRE LOS NIVELES DE RIESGO ACTUALES
2.7. INTEGRAR LA GESTION DEL RIESGO DE LA INFORMACION
2.8. MONITOREAR LOS RIESGOS EXISTENTES
2.9. INFORMAR SOBRE EL INCUMPLIMIENTO Y OTROS CAMBIOS EN EL RIESGO DE INFORMACION

3. DESARROLLO Y GESTION DE PROGRAMA DE SEGURIDAD DE LA INFORMACION

3.1. ESTABLECER Y MANTENER EL PROGRAMA DE SEGURIDAD DE LA INFORMACION
3.2. ASEGURAR LA ALINEACION ENTRE EL PROGRAMA DE SEGURIDAD DE LA INFORMACION
3.3. DENTIFICAR, ADQUIRIR, GESTIONAR Y DEFINIR LOS REQUISITOS DE RECURSOS INTERNOS Y EXTERNOS
3.4. ESTABLECER Y MANTENER ARQUITECTURAS DE SEGURIDAD DE LA INFORMACION
3.5. ESTABLECER, COMUNICAR Y MANTENER ESTANDARES, PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION
3.6. ESTABLECER Y MANTENER UN PROGRAMA DE SENSIBILIZACION
3.7. INTEGRAR LOS REQUISITOS DE SEGURIDAD DE LA INFORMACION EN LOS PROCESOS ORGANIZACIONALES
3.8. INTEGRAR LOS REQUISITOS DE SEGURIDAD DE LA INFORMACION EN LOS CONTRATOS Y ACTIVIDADES DE TERCEROS
3.9. ESTABLECER, MONITOREAR Y REPORTAR PERIODICAMENTE

4. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

4.1. ESTABLECER Y MANTENER UNA DEFINICION ORGANIZATIVA DE LOS INCIDENTES DE SEGURIDAD DE LA

INFORMACION

4.2. ESTABLECER Y MANTENER UN PLAN DE RESPUESTA A INCIDENTES

4.3. DESARROLLAR E IMPLEMENTAR PROCESOS PARA ASEGURAR LA IDENTIFICACION OPORTUNA DE INCIDENTES DE SEGURIDAD DE LA INFORMACION.

4.4. ESTABLECER Y MANTENER PROCESOS PARA INVESTIGAR Y DOCUMENTAR LOS INCIDENTES DE SEGURIDAD

4.5. ESTABLECER Y MANTENER PROCESOS DE ESCALAMIENTO Y NOTIFICACION DE INCIDENTES

4.6. ORGANIZAR, CAPACITAR Y EQUIPAR EQUIPOS PARA RESPONDER EFICAZMENTE A LOS INCIDENTES DE SEGURIDAD

4.7. PRUEBE Y REVISE EL PLAN DE RESPUESTA A INCIDENTES

4.8. ESTABLECER Y MANTENER PLANES Y PROCESOS DE COMUNICACION

4.9. LLEVAR A CABO REVISIONES POSTERIORES A LOS INCIDENTES

4.10. ESTABLECER Y MANTENER LA INTEGRACION ENTRE EL PLAN DE RESPUESTA A INCIDENTES

BENEFICIOS

- Al finalizar los participantes estarán capacitados en la administración de seguridad de la información, enfocada a la gerencia. Es una certificación interesante ya que actualmente la demanda de profesionales cualificados en gestión de la seguridad está en aumento.