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. GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

1.1. DESCRIBIR EL PAPEL DEL GOBIERNO EN LA CREACIÓN DE VALOR PARA LA EMPRESA.
1.2. EXPLICAR LA IMPORTANCIA DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CONTEXTO DEL GOBIERNO EMPRESARIAL GENERAL.
1.3. DESCRIBIR LA INFLUENCIA DEL LIDERAZGO, LA ESTRUCTURA Y LA CULTURA EMPRESARIAL EN LA EFICACIA DE UNA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN.
1.4. IDENTIFICAR LOS REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTUALES PERTINENTES QUE AFECTAN A LA EMPRESA.
1.5. DESCRIBIR LOS EFECTOS DE LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE RIESGOS EMPRESARIALES.
1.6. EVALUAR LOS MARCOS Y ESTÁNDARES COMUNES UTILIZADOS PARA REGIR UNA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN.
1.7. EXPLIQUE POR QUÉ LAS MÉTRICAS SON FUNDAMENTALES PARA DESARROLLAR Y EVALUAR LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN.

2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2.1. APLICAR ESTRATEGIAS DE EVALUACIÓN DE RIESGOS PARA REDUCIR EL IMPACTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.
2.2. EVALUAR LOS TIPOS DE AMENAZAS QUE ENFRENTA LA EMPRESA.
2.3. EXPLICAR CÓMO LAS LÍNEAS BASE DE CONTROL DE SEGURIDAD AFECTAN EL ANÁLISIS DE VULNERABILIDAD Y DEFICIENCIA DE CONTROL.
2.4. DIFERENCIAR ENTRE LA APLICACIÓN DE TIPOS DE TRATAMIENTO DE RIESGOS DESDE UNA PERSPECTIVA DE SEGURIDAD DE LA INFORMACIÓN.
2.5. DESCRIBIR LA INFLUENCIA DEL RIESGO Y LA PROPIEDAD DEL CONTROL EN EL PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN.
2.6. DESCRIBA EL PROCESO DE MONITOREO Y REPORTE DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

3. PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

3.1. RESUMA LOS COMPONENTES Y RECURSOS UTILIZADOS PARA CONSTRUIR UN PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN.
3.2. DISTINGA ENTRE LOS ESTÁNDARES Y MARCOS COMUNES DE SI DISPONIBLES PARA

CONSTRUIR UN PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN.
3.3. EXPLICAR CÓMO ALINEAR LAS POLÍTICAS, LOS PROCEDIMIENTOS Y LAS DIRECTRICES DE SI CON LAS NECESIDADES DE LA EMPRESA.
3.4. DESCRIBA EL PROCESO DE DEFINICIÓN DE LA HOJA DE RUTA DE UN PROGRAMA DE SI.
3.5. RESUMA LAS MÉTRICAS CLAVE DEL PROGRAMA DE SI UTILIZADAS PARA RASTREAR E INFORMAR EL PROGRESO A LA ALTA DIRECCIÓN.
3.6. EXPLICAR CÓMO ADMINISTRAR EL PROGRAMA IS USANDO CONTROLES.
3.7. CREAR UNA ESTRATEGIA PARA MEJORAR LA CONCIENCIA Y EL CONOCIMIENTO DEL PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN.
3.8. DESCRIBA EL PROCESO DE INTEGRACIÓN DEL PROGRAMA DE SEGURIDAD CON LAS OPERACIONES DE TI Y LOS PROVEEDORES EXTERNOS.
3.9. COMUNICAR LA INFORMACIÓN CLAVE DEL PROGRAMA DE SI A LAS PARTES INTERESADAS RELEVANTES.

4. GESTIÓN DE INCIDENTES

4.1. DISTINGUIR ENTRE GESTIÓN DE INCIDENTES Y RESPUESTA A INCIDENTES
4.2. DESCRIBA LOS REQUISITOS Y PROCEDIMIENTOS NECESARIOS PARA DESARROLLAR UN PLAN DE RESPUESTA A INCIDENTES.
4.3. IDENTIFICAR LAS TÉCNICAS UTILIZADAS PARA CLASIFICAR O CATEGORIZAR LOS INCIDENTES.
4.4. DESCRIBIR LOS TIPOS DE FUNCIONES Y RESPONSABILIDADES NECESARIAS PARA UN EQUIPO EFICAZ DE GESTIÓN Y RESPUESTA A INCIDENTES.
4.5. DISTINGUIR ENTRE LOS TIPOS DE HERRAMIENTAS Y TECNOLOGÍAS DE GESTIÓN DE INCIDENTES DISPONIBLES PARA UNA EMPRESA.
4.6. DESCRIBIR LOS PROCESOS Y MÉTODOS UTILIZADOS PARA INVESTIGAR, EVALUAR Y CONTENER UN INCIDENTE.
4.7. IDENTIFICAR LOS TIPOS DE COMUNICACIONES Y NOTIFICACIONES UTILIZADAS PARA INFORMAR A LAS PARTES INTERESADAS CLAVE SOBRE INCIDENTES Y PRUEBAS.
4.8. DESCRIBA LOS PROCESOS Y PROCEDIMIENTOS UTILIZADOS PARA ERRADICAR Y RECUPERARSE DE INCIDENTES.
4.9. DESCRIBIR LOS REQUISITOS Y BENEFICIOS DE DOCUMENTAR EVENTOS.
4.10. EXPLICAR LA RELACIÓN ENTRE EL IMPACTO EN EL NEGOCIO, LA CONTINUIDAD Y LA RESPUESTA A INCIDENTES.
4.11. DESCRIBIR LOS PROCESOS Y RESULTADOS RELACIONADOS CON LA RECUPERACIÓN ANTE DESASTRES.
4.12. EXPLICAR EL IMPACTO DE LAS MÉTRICAS Y LAS PRUEBAS AL EVALUAR 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.