

Modulos, Objetivo y Contenido Minimo - ASIC Presencial

Autor Luis Antonio
 martes, 31 de marzo de 2009
 Modificado el martes, 09 de junio de 2009

MODULOS, OBJETIVO Y CONTENIDO MINIMO:

GESTION DE RIESGOS

OBJETIVO.- Desarrollar métodos cualitativos y cuantitativos para efectuar un adecuado análisis de riesgo y en función a ello plantear una serie de estrategias de control de los objetivos del negocio y sus contramedidas, planificación de la auditoria y evaluación de los métodos utilizados por el Negocio para minimizar el impacto que podría ocasionarse a la Tecnología y al Negocio.

CONTENIDO MINIMO:

Introducción a la administración de Riesgos

Roles y responsabilidades

Proceso de administración de Riesgos

Amenazas

Vulnerabilidades

Riesgos

Impactos

Controles y Contramedidas

Clasificación de los Activos de Información Limites (Baselines) de control de Tecnología de información

Monitoreo y Comunicación Documentación NIST 800/30 – Los 9 pasos

- AUDITORIA AL GOBIERNO DE TI **OBJETIVO.-** Asegurar que el auditor de SI entienda y pueda dar garantía que la organización tiene establecidas la estructura, las políticas, los mecanismos de registro y las practicas de monitoreo para satisfacer los requerimientos del gobierno corporativo de TI. **CONTENIDO MINIMO:**

Gobierno Corporativo Practicas de Monitoreo y Aseguramiento para la Dirección y Gerencia Ejecutiva.

Gobierno de Seguridad de la Información Estrategias de Sistemas de Información Políticas y

procedimientos de Seguridad de la información Administración de Riesgo Administración del Personal

Practicas de Sourcing Estructura Organizacional y Responsabilidades de SI Segregación de funciones

dentro de SI Auditoria de la Estructura e Implementación de Gobierno de TI AUDITORIA A LA

GESTION DE SEGURIDAD DE TI **OBJETIVO.-** Asegurar que el auditor de SI entienda y pueda dar garantía que la organización tiene establecidas una adecuada Gestion de Seguridad, que permita mantener al mayor nivel los criterios de integridad, disponibilidad y confidencialidad. **CONTENIDO MINIMO:** Política de Seguridad

Organización de la Seguridad Clasificación de la Información Controles físicos Controles

lógicos Controles Ambientales Plan de Contingencia Adm. Problemas e incidentes

Cumplimiento. AUDITORIA A LA ADMINISTRACION DE PROYECTOS Y APLICACIONES

OBJETIVO.- Asegurar que el auditor de SI, entienda y pueda proveer certeza de que las practicas de administración para los proyectos, el desarrollo, adquisición, pruebas, implementación, mantenimiento y eliminación de aplicaciones e infraestructura, cumplirán los objetivos de la organización. **CONTENIDO MINIMO:** Realización del

Negocio Administración y Gestión de Proyectos Desarrollo de aplicaciones de Negocio Riesgos

asociados con el Desarrollo de Software Estrategias alternativas para el Desarrollo de Aplicaciones

Auditoria a cambios en programas Adquisición de infraestructuras Mantenimiento de los Sistemas de

Información Herramientas para el desarrollo de Sistemas (CASE) Reingeniería del Proceso del Negocio

Controles de Aplicación Auditoria a los controles de aplicación Auditoria del Desarrollo, adquisición y

mantenimiento de Sistemas. Banca Electrónica Cajeros Automáticos ATMs Auditoria de ATMs

AUDITORIA A LA GESTION DE SEGURIDAD FISICA DE LA INFORMACION Y SERVICIOS DE TI

OBJETIVO.- Asegurar que el auditor de SI entienda y pueda proporcionar garantía de que la arquitectura de seguridad (políticas, estándares, procedimientos y controles), asegure la confidencialidad, integridad y disponibilidad de los activos de información. **CONTENIDO MINIMO:** Almacenar, recuperar, transportar y descartar

información confidencial Auditoria de la Estructura de Seguridad de la Información Auditoria de Seguridad de la infraestructura FISICA Auditoria de los Controles ambientales Auditoria de los Controles de

Acceso Físico Computación móvil. Help Desk Auditoria a Help Desk AUDITORIA

A LA INFRAESTRUCTURA DE REDES Y TELECOMUNICACIONES

o **OBJETIVO.-** Asegurar que el Auditor de SI, entienda y pueda proveer seguridad con relación a que las prácticas de gerencia aseguran la entrega de los niveles de servicio requeridos para el soporte de los objetivos de la organización.

o **CONTENIDO MINIMO:**

Conceptos generales de Redes y Telco
 Tipos de Redes: MAN, WAN, LAN, VPN, inalámbricas
 Sistemas Operativos (IOS) y SNMP
 Administración de operaciones de SI, Servicios, Infraestructura (W2K3 y Linux)
 Infraestructura de las Redes de Sistemas de Información
 Administración y Control de RED
 Auditoria de la infraestructura y de las operaciones (ITIL)
 Auditoria del Hardware
 Recomendaciones y buenas practicas

o CONTENIDO DE PRACTICAS:
 Gestión de políticas en Firewalls
 Implementación de VLAN's
 Implementación de VPN's
 Implementación de ACL's

DELITOS INFORMATICOS

OBJETIVO.-

Conocer sobre los delitos informaticos.

AUDITORIA AL PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACION DE DESASTRES

OBJETIVO.- Asegurar que el Auditor entienda y pueda proveer garantía de que el caso de un interrupción, los procesos de continuidad del negocio y recuperación de desastres aseguren el reinicio a su debido tiempo de los servicios de TI mientras que se minimiza el impacto sobre el negocio.

CONTENIDO MINIMO:

Planeación de la Continuidad	Desastres y otras interrupciones	Proceso del BCP	Política de
continuidad del Negocio	Administración de incidentes dentro del BCP	Estrategias de Recuperación	
Alternativas de Recuperación	Organización y Asignación de Responsabilidades	Componentes de un BCP	
Pruebas del Plan	Respaldo (backup) y Recuperación	Auditoria al Plan de Continuidad del Negocio	
Evaluación de Resultados	Evaluación de la seguridad del sitio alternativo	Evaluación de la cobertura de	

Seguros Entrevistas al Personal Clave PROCESOS DE AUDITORIA DE SISTEMAS DE INFORMACION

OBJETIVO.- Garantizar que el Auditor tenga los conocimientos necesarios para proporcionar servicios de auditoria de sistemas de información, en conformidad a los estándares, directrices y mejores practicas de SI para apoyar a la organización a validar que su tecnología de información y sus sistemas de negocio estén protegidos y controlados.

CONTENIDO MINIMO:

control en Auditoria de SI	Planeacion de la Auditoria de SI	Introducción a la Auditoria de SI	Riesgos de
SI (ISACA)	Evaluación de Pistas de Auditoria lógica	Estándares y Directrices para la Auditoria de	
accesos, etc.)	Auditoria por procesos: Metodología COBISO & MATTA.	Evaluación de Controles en TI (edición, validación,	
Lógica de la Información.	Auditoria a los controles automatizados (Aplicativo y BD)	Auditoria a la Seguridad	
controles de aplicación	Evaluación de Controles de Accesos lógicos e Integridad en Datos (Pruebas de	de	
Cumplimiento y Sustantivas).	Uso de CAATs y NO CAATs (importancia y alcance)	Detección de Fraudes	
e irregularidades en Datos.	Control Self Assessment	Elaboración e informe de Hallazgos de Auditoria	
(método de las: 3C, E, R) y papeles de trabajo.	Comunicación de los resultados de Auditoria		

Demostraciones y Prácticas con FULL HERRAMIENTAS

EXAMEN Y APROBACION

Las pruebas son elaboradas bajo el mismo método de los exámenes anuales para optar la certificación internacional CISA, CISM de ISACA Al final de cada Modulo, se tomaran exámenes-modelo vía AULA VIRTUAL de 15 preguntas. Nota mínima de aprobación es de 65 pts. PONDERADO 20 PUNTOS. Y al final del curso (15 días después) se tomara un examen que incluya todos los módulos, compuesto por 100 preguntas en 2.5 Hrs. Nota mínima de aprobación 65 pts, sumándose la NOTA PONDERADA, señalado en el punto anterior. El participante que NO apruebe o NO se presente al examen final, podrá presentarse nuevamente en la fecha del examen final del siguiente curso o se programara una fecha en un plazo máximo de 90 días, previo pago de \$us. 50.- (costos administrativos) Todos lo participantes que tengan una asistencia presencial mayor al 75% de la carga horaria, se harán acreedores a un Certificado de Participación.

CARGA HORARIA		No.		MODULO	
HORAS	TEORIA	PRACT.	LABOR.	1	2
RIESGOS	6 HORAS	SI	SI	NO	2
AUDITORIA AL GOBIERNO DE TI	6 HORAS	SI	SI	NO	2
3	AUDITORIA A LA GESTION DE SEGURIDAD DE TI	3 HORAS			
4	AUDITORIA A LA ADMINISTRACION DE PROYECTOS Y APLICACIONES				
6 HORAS	SI	SI	NO	5	AUDITORIA A LA GESTION
DE SEGURIDAD FISICA DE LA INFORMACION Y SERVICIOS DE TI	6 HORAS	SI			
SI	NO	6			
TELECOMUNICACIONES	6 HORAS	SI	SI	SI	7
DELITOS INFORMATICOS.	6 HORAS	SI	SI	NO	

8	AUDITORIA AL PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACION DE DESASTRES					
3 HORAS	SI	SI	NO	9	PROCESOS DE	
AUDITORIA DE SISTEMAS DE INFORMACION - TALLER				8 HORAS	SI	SI
SI		50 HORAS				