Oficiales de Seguridad

Código: SEG-107

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas

En este curso repasaremos los conceptos de seguridad, riesgos, vulnerabilidad y amenazas.
El participante será capaz de implementar, mantener, actualizar y mejorar la GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN en su organización.

AUDIENCIA

- Consultores Senior en Seguridad de la Informacio?n, auditores y profesionales en a?reas de gestio?n de la Seguridad de la Informacio?n.

PRE REQUISITOS

- Conocimientos en seguridad de la información.

OBJETIVOS

- Repasar los conceptos de seguridad, riesgos, vulnerabilidad y amenazas.
- Funciones de un oficial de seguridad de la información.
- Estructura organizacional de seguridad.
- Funciones y responsabilidades del oficial de SI.

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

CONTENIDO

1. GOBIERNO DE TI

1.1. SEGURIDAD INFORMÁTICA, SEGURIDAD DE LA INFORMACIÓN, CYBERSECURITY
1.2. GOBIERNO RIEGO Y CUMPLIMIENTO
1.3. ALINEACIÓN ESTRATÉGICA USANDO COBIT 5.0
1.4. COBIT 5 OVERVIEW
1.5. GOBIERNO Y GESTIÓN
1.6. GOBIERNO EFECTIVO
1.7. ROLES EN LA SEGURIDAD DE LA INFORMACIÓN: CONSEJOS DE DIRECCIÓN, DIRECCIÓN EJECUTIVA, DIRECTOR DE SEGURIDAD, OPERADORES DE SEGURIDAD
1.8. MÉTRICAS DEL GOBIERNO
1.9. DESARROLLO DE UNA ESTRATEGIA DE SÍ

2. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

2.1. GAP ANALISIS (ANÁLISIS DE BRECHAS)
2.2. IDENTIFICACIÓN DE PROCESOS CRÍTICOS DEL NEGOCIO
2.3. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN
2.4. VALORACIÓN DE ACTIVOS DE INFORMACIÓN
2.5. ANÁLISIS DE RIESGO TECNOLÓGICO
2.6. ESTABLECIMIENTO DE ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN
2.7. GESTIÓN DE RIESGO (ISO 31000)

3. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

3.1. PLAN DE TRATAMIENTO DE RIESGO
3.2. IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD (POLÍTICAS, PROCEDIMIENTOS, MANUALES OPERATIVOS, CONTROLES TÉCNICOS Y SOLUCIONES)
3.3. ANÁLISIS DE IMPACTO AL NEGOCIO (ISO 22301)
3.4. PLANES DE CONTINUIDAD Y PLANES DE CONTINGENCIA (ISO 22301)
3.5. DESARROLLO E IMPLEMENTACIÓN DE COMITES DE SEGURIDAD (GESTIÓN Y OPERACIONES)

4. GESTIÓN DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

4.1. FASES DEL PENETRATION TESTING
4.2. DIFERENCIAS ENTRE ANÁLISIS DE VULNERABILIDADES PENTESTING Y EH
4.3. TOOLS OVERVIEW
4.4. DISEÑO DE LA PRUEBA
4.5. ENTREGABLES
4.6. DEFENSIVE VRS OFFENSIVE
4.7. WEB HACKING
4.8. WIRELESS HACKING
4.9. SANDBOX
4.10. HONEYPOTS
4.11. INTRUSSION PREVENTION

4.12. MONITORING & MANGEMENT

4.13. PRINCIPALES ATAQUES COMO FUNCIONAN Y CONTRAMEDIDAS

5. INFRAESTRUCTURAS DE SEGURIDAD

5.1. MODELO OSI

5.2. DEFENSA EN PROFUNDIDAD

5.3. FIREWALLING AISLAMIENTO Y SEGMENTACIÓN, FAIL OVER Y REDUNDANCIA

5.4. TIPOS DE FIREWALL

5.5. PACKET FILTERING

5.6. APLICATION FIREWALLS

5.7. STETFULL INSPECTION

5.8. MONITOREO Y DETECCIÓN DE TRÁFICO

5.9. MONITOREO DETECTION Y LOGING

5.10. IPS, IDS,HIDS

5.11. DATASECURITY (DLP & ENCRYPTION)

5.12. ACCESS CONTROL

5.13. DATA PROTECTION

6. INFRAESTRUCTURAS DE SEGURIDAD EXAMEN TOTAL

6.1. BYD ESTRATEGIES

6.2. SEGURIDAD EN LA VIRTUALIZACIÓN

6.3. SEGURIDAD EN PROFUNDIDAD

6.4. TIPO DE DEFENSA EN PROFUNDIDAD

6.5. ENCRYPTION TECHNIQUES

6.6. VPNS

6.7. WIRELESS CAMPUS

6.8. VULNERABILTY MANAGEMENT

6.9. NETWORK MANAGEMENT

6.10. FAULT, CONFIGURATION,ACCOUNTING & SECURITY

6.11. PUERTOS PROTOCOLOS

6.12. VOIP SECURITY

6.13. APPLICATION SECURITY RISK

7. EVALUACIÓN

7.1. EVALUACIÓN & ROLLPLAYING

BENEFICIOS

- Al finalizar este curso tendrá sólidos conocimientos de las funciones de un oficial de seguridad de la información.