

DIPLOMADO SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE EN EL ESTANDAR 27001 Y PROTECCIÓN DE DATOS

Certificación:

-Auditor Interno en 27001 por SGS a nivel Internacional.
-Diploma de Asistencia por la FEUD

Duración:

120 Horas

Tipo de Curso:

Presencial / E -Learning

Idioma:

Español

CONTACTO

Fundación de Egresados de la Universidad Distrital

Bogotá D.C. / Colombia

Cr. 20 # 32 A - 45

PBX: 7561133

info@egresadosudistrital.edu.co

Medellín

Centro Emp. Ciudad del Río

Cra 48 No 20-114 Torre 2

Oficina 924

Teléfono: (4) 560 7740

infomed@egresadosUdistrital.edu.co

Correo Electrónico

info@egresadosudistrital.edu.co

Más Información

www.egresadosudistrital.edu.co

CONTENIDO TEMÁTICO

Módulo 1: Conceptos base en seguridad de la información

Este módulo introduce al estudiante a los principales conceptos que se han de tener en cuenta en el momento de hablar de Seguridad de la Información.

1. Vulnerabilidades
2. Amenazas
3. Riesgos
4. Estándares internacionales
5. Certificaciones en seguridad de aceptación internacional
6. Modelo de referencia OSI
7. Ingeniería social
8. Tecnologías LAN
9. Tecnologías WAN

Módulo 2: Seguridad de red en dispositivos de capa 2 y 3

Este modulo se basará en la arquitectura y la administración de la seguridad de la red desde la perspectiva de Cisco, para las prácticas, se desarrollaran con equipos como routers y switches, y los laboratorios estarán en conformidad con las mejores prácticas diseñadas y recomendadas por cisco para sus dispositivos.

1. Organizaciones de seguridad en redes.
2. Principios fundamentales de una red segura.
3. Seguridad en dispositivos de capa 2 Introducción a la seguridad de capa 2
 - Ataques de falsificación de direcciones MAC (Laboratorio_ Denegación de servicio)
 - Ataques por desbordamiento de la tabla de direcciones MAC
 - Ataques de manipulación STP
 - Ataques de VLAN
 - Configuración del analizador de puertos conmutados Cisco.
4. Seguridad en dispositivos de capa 2 Introducción a la seguridad de capa 2
 - Seguridad del router de borde.
 - DMZ.
 - Configuración de un acceso administrativo seguro.
 - Seguridad en los protocolos de enrutamiento (Laboratorio con Ospf y Rip)
 - Autenticación, autorización y registro de auditoria.
 - Configuración de autenticación AAA local con CLI.
5. Sniffers
 - Conceptos.
 - Operación de la Nic
 - Modo promiscuo
 - Dominio de Broadcast
 - Puerto mirror
6. Metodologías de ataque.
 - Ataques de contraseña (Laboratorio Utilizando Backtrack)
 - Explotación de la confianza (Laboratorio Utilizando Backtrack)
 - Redirección de puerto (Laboratorio Utilizando Backtrack)
 - Ataque Man in the Middle (Laboratorio Utilizando Backtrack)
 - Desbordamiento de buffer (Laboratorio Utilizando Backtrack)
7. VPN
 - Conceptos Básicos
 - Ipsec
 - SSL (Laboratorio)
 - Site-to-Site
8. Firewal
 - Tipos de Firewall
 - IDS
 - Configuración Iptables
 - Configuración Básica Firewall Check Point R71

DIPLOMADO SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE EN EL ESTANDAR 27001 Y PROTECCIÓN DE DATOS

Certificación:

-Auditor Interno en 27001 por SGS a nivel Internacional.
-Diploma de Asistencia por la FEUD

Duración:

120 Horas

Tipo de Curso:

Presencial / E -Learning

Idioma:

Español

CONTACTO

Fundación de Egresados de la Universidad Distrital

Bogotá D.C. / Colombia

Cr. 20 # 32 A - 45

PBX: 7561133

info@egresadosudistrital.edu.co

Medellín

Centro Emp. Ciudad del Río

Cra 48 No 20-114 Torre 2

Oficina 924

Teléfono: (4) 560 7740

infomed@egresadosUdistrital.edu.co

Correo Electrónico

info@egresadosudistrital.edu.co

Más Información

www.egresadosudistrital.edu.co

CONTENIDO TEMÁTICO

Módulo 3: SEGURIDAD EN APLICACIONES Y BASES DE DATOS

Este módulo está enfocado a proveer herramientas y estrategias para poder administrar y asegurar tecnologías de persistencia como Bases de Datos y otro tipo de aplicaciones y claves importantes para evitar accesos indebidos o actos maliciosos por parte de los usuarios.

1. Servidores de Bases de Datos (Arquitectura, Ventajas y vulnerabilidades)
2. Sistemas en el Web (Administración de seguridad en sistemas distribuidos)
3. Administración de usuarios (Políticas, Recomendaciones, mejores prácticas, Errores frecuentes)
4. Intrusos en el sistema (Origen, Detección, Estadísticas de acceso)
5. Entendiendo la investigación computacional.
6. Ambientes de trabajo: Windows, Unix y Linux.
7. Herramientas actuales para la computación forense.
8. Modelos de seguridad para redes,
9. Seguridad sobre Internet.
10. Controles sobre evidencia digital.
11. Procesamiento de la escena del crimen y de los incidentes.
12. Análisis computacional forense.
13. Evidencia digital en redes
14. Análisis de tráfico de red. Network Intrusion Detection
15. Registros y rastros a través del Modelo OSI/ISO
16. Ejemplos de aplicación
17. Análisis de incidentes de seguridad en redes
18. Investigación del correo electrónico.
19. Análisis e investigación de datos.
20. Pruebas de vulnerabilidad y Ethical Hacking
21. Documentación del proceso

Módulo 4: ANÁLISIS FORENSE Y EVIDENCIA DIGITAL

Investigar delitos informáticos es una tarea que tiene desde sus comienzos un análisis formal, tan formal que es una ciencia actualmente, en este módulo se presenta un abreviado del flujo de procesos estudios forenses digitales

1. Introducción.
2. Recuperación de información
3. Delitos Informáticos directos e indirectos.

1. La computación forense y la investigación forense como profesión.
2. Técnicas de auditoría.

DIPLOMADO SEGURIDAD DE LA INFORMACIÓN CON ENFOQUE EN EL ESTANDAR 27001 Y PROTECCIÓN DE DATOS

Certificación:

-Auditor Interno en 27001 por SGS a nivel Internacional.
-Diploma de Asistencia por la FEUD

Duración:

120 Horas

Tipo de Curso:

Presencial / E -Learning

Idioma:

Español

CONTACTO

Fundación de Egresados de la Universidad Distrital

Bogotá D.C. / Colombia

Cr. 20 # 32 A - 45

PBX: 7561133

info@egresadosudistrital.edu.co

Medellín

Centro Emp. Ciudad del Río

Cra 48 No 20-114 Torre 2

Oficina 924

Teléfono: (4) 560 7740

infomed@egresadosUdistrital.edu.co

Correo Electrónico

info@egresadosudistrital.edu.co

Más Información

www.egresadosudistrital.edu.co

CONTENIDO TEMÁTICO

Módulo 5: GESTIÓN DE CONTINUIDAD DE NEGOCIO Y RIESGOS (BCP, DRP)

En éste módulo se conocerán las mejores prácticas en la gestión del riesgo. Se estudiarán las últimas metodologías y los estándares internacionales este tema.

1. Procedimientos de contingencia
2. Definición de un sitio alterno
3. Respuesta a incidentes
4. Recuperación de la operación de la empresa
5. Estándares y mejores prácticas del NIST y del CERT
6. Ciclo de contingencia
7. Planes de Contingencia y Recuperación de Desastres
8. Esquema de Alerta Análisis de Impactos.
9. Modelo BS 25999
10. El modelo OCTAVE

Módulo 6: PROTECCIÓN DE DATOS Y DERECHO INFORMÁTICO

Hacer conocer las principales actividades y funciones como auditor, haciendo énfasis en los aspectos legales a nivel nacional.

1. Derecho Informático y la importancia en la Seguridad de la Información
2. El entorno jurídico y la protección de la información.
3. Delitos Informáticos, Ley 1273 de 2009
4. Protección de datos
5. Base de datos y su manejo jurídico
6. Legislación
7. Etapas preactivas.
8. Diagnósticos de seguridad
9. Revisión y actualización de procedimiento
10. Evaluación de la seguridad implantada.
11. Políticas de Seguridad de la Información
12. La norma técnica Colombiana NTC 5254.
13. Reciclaje electrónico y su importancia en la seguridad de la información.
Taller

Módulo 7 por SGS: SENSIBILIZACIÓN ESTANDAR ISO 27001

1. Sistema de gestión de seguridad de la información.
2. Conceptos básicos.
3. ¿Qué es la norma ISO/IEC27001:2013?
4. Origen norma ISO/IEC27001:2013.

Módulo 8 por SGS: CURSO AUDITOR INTERNO ESTANDAR ISO 27001

1. Establecimiento del SGSI.
2. Contenido norma ISO/IEC27001:2013.
 - a. Requisitos generales.
 - b. Conceptos de implementación y operación del SGSI.
 - c. Seguimiento y revisión del SGSI.
 - d. Mantenimiento y mejora del SGSI.
 - e. Requisitos de documentación exigidos por la norma.
 - f. Responsabilidad de la dirección.
 - g. Gestión de los recursos, auditorías internas, revisión por la dirección y mejora continua del SGSI.
 - h. Objetivos de control y controles que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.
3. Metodología y ciclo de implementación.
4. Dominios de seguridad.
5. Auditorías Internas de un SGSI. TALLER
6. Examen Internacional