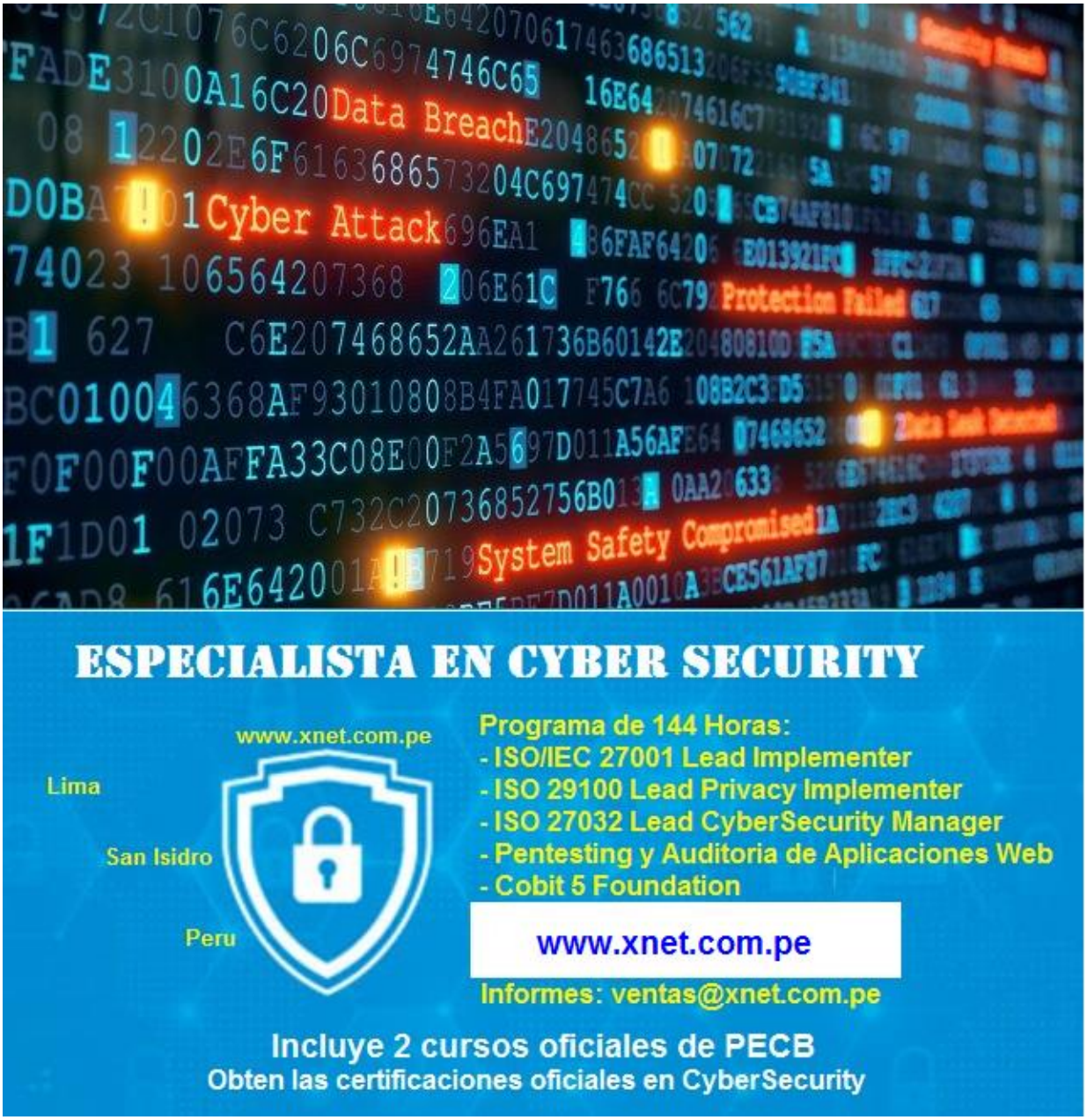
XNET SOLUTIONS
Centro Autorizado de Capacitación PECB

Programa : Especialista en Ciber Security
Con Certificación Internacional en Ciber Seguridad , Protección Datos Personales e ISO 27001 LI

Duración : 144 Horas (5 meses)



SYLLABUS

I. DESCRIPCIÓN

El Programa de Especialista en Ciber Seguridad incluye los cursos de certificación internacional de PECB en ISO 27001 Lead Implementer, ISO 29100 Lead Privacy Implementer (Proteccion de Datos Personales), ISO 27032 Lead CyberSecurity Manager, Pentesting y Auditoria de Aplicaciones Web (OWASP), Cobit 5 Foundation.

Esta dirigido a profesionales de TI que quieran adquirir los conocimientos y certificaciones internacionales para especializarse en cada uno de los cursos del programa permitiendo que puedan liderar los grupos de Gestion, Implementacion y Auditoria para la seguridad de la Información y CiberSeguridad en sus empresas.

Durante el desarrollo del programa el alumno adquirirá los conocimientos necesarios para poder realizar Pentesting o Auditoria de Aplicaciones Web basados en el Marco de trabajo de OWASP, revisaremos el TOP Ten de Owasp y las Guias de Testing para tarea.

Tambien se desarrollara el curso de Cobit 5 Foundation, donde el alumno aprenderá el marco teorico de COBIT 5 para el gobierno y gestión de TI empresarial. COBIT 5 ayuda a maximizar el valor de la información mediante la incorporación de las últimas ideas en gestión empresarial y técnicas de gestión, y proporciona principios aceptados globalmente, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza y el valor de los sistemas de información.

II. METODOLOGÍA

El curso tiene la modalidad presencial. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios y discusión en clase.
En caso de desarrollo de casos o laboratorios practicos, cada alumno contara con 1 PC para el desarrollo de las actividades practicas.

III. REQUISITOS

- No se necesita conocimientos previos, durante cada módulo se irán adquiriendo los conocimientos necesarios

IV. MATERIALES

- Manuales Oficiales de PECB para los cursos con voucher de Certificación
- Manuales Impresos para todos los cursos

CERTIFICADO:

Se incluye 2 voucher para los examen de certificación oficial de PECB para los cursos de los módulos desarrollados.

Adicionalmente se emitirá un certificado de asistencia al curso para los cursos que no incluyen voucher de certificación oficial

V. PLAN DE TEMAS

El programa incluye los siguientes módulos

Módulo 1 : ISO/IEC 27001 Lead Implementer
Módulo 2 : ISO 29100 Lead Privacy Implementer
Módulo 3 : ISO 27032 Lead CyberSecurity Manager
Módulo 4 : Pentesting y Auditoria de Aplicaciones Web (OWASP)
Módulo 5 : Cobit 5 Foundation

Se incluye 2 voucher para el examen de Certificación Oficial de PECB que el alumno deberá elegir entre las siguientes certificaciones:

- **ISO/IEC 27001 Lead Implementer**
- **ISO 29100 Lead Privacy Implementer**
- **ISO 27032 Lead CyberSecurity Manager**

Detalle de cada Modulo:

Módulo 1 : ISO/IEC 27001 Lead Implementer (32 Hrs)

ISO / IEC 27001 La capacitación de implementador líder le permite desarrollar la experiencia necesaria para ayudar a una organización a establecer, implementar, administrar y mantener un Sistema de gestión de seguridad de la información (SGSI) basado en ISO / IEC 27001. Durante este curso de capacitación, también obtendrá un conocimiento profundo de las mejores prácticas de los sistemas de gestión de la seguridad de la información para garantizar la información sensible de la organización y mejorar el rendimiento y la eficacia generales.

Después de dominar todos los conceptos necesarios de los Sistemas de gestión de la seguridad de la información, puede presentarse para el examen y solicitar una credencial "Implementador principal de ISO / IEC 27001 certificado PECB". Con la celebración de un Certificado de implementador principal de PECB, podrá demostrar que posee el conocimiento práctico y las capacidades profesionales para implementar ISO / IEC 27001 en una organización.

LOS OBJETIVOS DE APRENDIZAJE

- Reconozca la correlación entre ISO / IEC 27001, ISO / IEC 27002 y otras normas y marcos normativos
- Dominar los conceptos, enfoques, métodos y técnicas utilizados para la implementación y gestión efectiva de un SGSI
- Aprenda a interpretar los requisitos de ISO / IEC 27001 en el contexto específico de una organización
- Aprenda cómo ayudar a una organización a planificar, implementar, administrar, monitorear y mantener un ISMS de manera efectiva
- Adquiera la experiencia para asesorar a una organización en la implementación de las mejores prácticas del Sistema de gestión de la seguridad de la información

CONTENIDO:

Tema 1: Introducción a ISO / IEC 27001 e inicio de un SGSI

- Objetivos del curso y estructura
- Estándares y marcos regulatorios
- Sistema de gestión de la seguridad de la información (ISMS)
- Principios fundamentales de los sistemas de gestión de la seguridad de la información
- Iniciando la implementación de un SGSI
- Comprender la organización y aclarar los objetivos de seguridad de la información
- Análisis del sistema de gestión existente

Tema 2: Planificar la Implementación de un SGSI

- Liderazgo y aprobación del proyecto ISMS
- Alcance ISMS
- Políticas de seguridad de la información
- Evaluación de riesgos
- Declaración de aplicabilidad y decisión de la alta dirección para implementar el SGSI
- Definición de la estructura organizativa de la seguridad de la información

Tema 3: Implementación de un SGSI

- Definición del proceso de gestión documental
- Diseño de controles de seguridad y redacción de políticas y procedimientos específicos
- Plan de comunicación
- Plan de formación y sensibilización
- Implementación de controles de seguridad
- Administracion de incidentes
- Jefe de operaciones

Tema 4: Seguimiento, medición, mejora continua y preparación de un SGSI para una auditoría de certificación

- Monitoreo, medición, análisis y evaluación
- Auditoría interna
- Revisión de gestión
- Tratamiento de las no conformidades
- Mejora continua
- Preparación para la auditoría de certificación
- Competencia y evaluación de implementadores
- Cerrando el entrenamiento

Duración: 32 horas.

Módulo 2 : ISO 29100 Lead Privacy Implementer (32 Hrs)

Este curso de ISO 29100 Lead Privacy Implementer (Privacidad de Datos Personales) le permite desarrollar la experiencia necesaria para apoyar a una organización en el diseño, la implementación, la operación y el mantenimiento de los sistemas de Tecnología de la Información y la Comunicación (ICT) que manejan y protegen la Información de Identificación Personal (PII). Durante este curso de capacitación, también tendrá la oportunidad de ayudar a una organización a mejorar los programas de privacidad mediante el uso de mejores prácticas y estimular soluciones innovadoras que permitan la protección de la PII dentro de los sistemas de TIC.

Después de dominar todos los conceptos necesarios de ISO/IEC 29100, puede presentarse para el examen y solicitar un certificado de "ISO29100 Lead Privacy Implementer por PECB". Con la celebración de un Certificado de Lider de Implementación de datos personales PECB, usted demostrará que tiene el conocimiento práctico y las capacidades profesionales para implementar y gestionar un marco de privacidad dentro de una organización.

LOS OBJETIVOS DE APRENDIZAJE

- Comprenda los principios de privacidad de ISO / IEC 29100
- Reconocer la correlación entre el concepto de ISO / IEC 29100 e ISO / IEC 27000
- Domine la terminología, los conceptos y los enfoques utilizados para el diseño, la implementación, la operación y el mantenimiento de sistemas TIC que manejan y protegen PII

- Aprender a interpretar el marco de alto nivel para la protección de PII con sistemas TIC en un contexto específico de una organización según lo dispuesto por ISO / IEC 29100
- Aprender cómo asesorar eficazmente a las organizaciones en la definición de sus requisitos de protección de la privacidad relacionados con PII

DETALLES DEL CURSO

DIA 1: Introducción a ISO / IEC 29100 e inicio de un marco de privacidad

- Objetivo y estructura del curso
- Marco normativo y normativo
- Marco de privacidad basado en ISO 29100
- Principios fundamentales de la privacidad
- Legislación de privacidad EE. UU. Y Europa
- Iniciando la implementación del marco de privacidad
- Comprender la organización y aclarar los objetivos de privacidad

DIA 2: Planificar la implementación de un marco de privacidad

- Análisis de los controles existentes
- Liderazgo y aprobación de la privacidad
- Proyecto de marco
- Alcance del marco de privacidad
- Política de privacidad
- Evaluación de riesgo e impacto
- Declaración de control y decisión de la administración para implementar el Marco de privacidad
- Definición de la estructura organizativa de la privacidad

DIA 3: Implementación de un marco de privacidad

- Definición del proceso de gestión documental
- Diseño de controles y redacción de políticas y procedimientos específicos
- Plan de comunicación
- Plan de formación y sensibilización
- Implementación de controles de privacidad
- Gestión de incumplimiento de incidentes y datos
- Jefe de operaciones

DIA 4: Monitoreo, medición, mejora continua y evaluación del marco de privacidad

- Monitoreo, medición, análisis y evaluación
- Auditoría interna
- Revisión de gestión
- Tratamiento de problemas y puntos de preocupación
- Mejora continua
- Competencia y evaluación de implementadores
- Cerrando el entrenamiento

Duración: 32 horas.

Módulo 3 : ISO 27032 Lead CyberSecurity Manager (32 Hrs)

El curso ISO / IEC 27032 Lead Cybersecurity Manager le permite adquirir la experiencia y la competencia necesarias para ayudar a una organización en la implementación y administración de un programa de seguridad cibernética basado en el marco de seguridad cibernética ISO / IEC 27032 y NIST. Durante este curso de capacitación, obtendrá un conocimiento exhaustivo de seguridad cibernética, la relación entre seguridad cibernética y otros tipos de seguridad de TI, y el rol de las partes interesadas en ciberseguridad.

Después de dominar todos los conceptos necesarios de Ciberseguridad, puede presentarse para el examen y solicitar la certificación "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager". Con la celebración de un Certificado de PECB Lead Cybersecurity Manager, podrá demostrar que posee el conocimiento práctico y las capacidades profesionales para apoyar y liderar a un equipo en el manejo de la Ciberseguridad.

LOS OBJETIVOS DE APRENDIZAJE

- Adquirir un conocimiento exhaustivo sobre los elementos y las operaciones de un programa de seguridad cibernética de conformidad con ISO/IEC 27032 y el marco de ciberseguridad del NIST
- Reconocer la correlación entre ISO / IEC 27032, el marco de seguridad cibernética del NIST y otros estándares y marcos operativos
- Dominar los conceptos, enfoques, estándares, métodos y técnicas utilizados para establecer, implementar y administrar con eficacia un programa de Ciberseguridad dentro de una organización

- Aprenda a interpretar las pautas de ISO/IEC 27032 en el contexto específico de una organización
- Dominar la experiencia necesaria para planificar, implementar, administrar, controlar y mantener un programa de ciberseguridad como se especifica en ISO/IEC 27032 y el marco de seguridad cibernética del NIST
- Adquirir la experiencia necesaria para asesorar a una organización sobre las mejores prácticas para administrar la Ciberseguridad

DETALLES DEL CURSO

DIA 1: Introducción a la ciberseguridad y conceptos relacionados según lo recomendado por ISO/IEC 27032

- Objetivos del curso y estructura
- Estándares y marcos regulatorios
- Conceptos fundamentales en Ciberseguridad
- Programa de seguridad cibernética
- Iniciando un programa de ciberseguridad
- Analizando la organización
- Liderazgo

DIA 2: Políticas de ciberseguridad, gestión de riesgos y mecanismos de ataque

- Políticas de seguridad cibernética
- Gestión del riesgo de ciberseguridad
- Mecanismos de ataque

DIA 3: Controles de seguridad cibernética, intercambio de información y coordinación

- Controles de seguridad cibernética
- Intercambio de información y coordinación
- Programa de formación y sensibilización

DIA 4: Gestión de incidentes, monitoreo y mejora continua

- Continuidad del negocio
- Gestión de incidentes de ciberseguridad
- Respuesta y recuperación de incidentes de ciberseguridad
- Pruebas en Ciberseguridad
- Medición del desempeño
- Mejora continua
- Cerrando el entrenamiento

Duración: 32 horas.

Módulo 4: Pentesting y Auditoria de Aplicaciones Web (24 Hrs)

DESCRIPCION DEL CURSO:

Este curso está diseñado para capacitar a profesionales y técnicos en TI en las técnicas y herramientas disponibles, usadas por los hackers para realizar un ataque desde Internet, redes internas a aplicaciones web y entornos basados en servidores web y de aplicaciones.

Objetivo:

Proporcionar al participante los conocimientos teóricos-prácticos que permita desarrollar las competencias necesarias realizar un proceso controlado de Pentesting que permite conocer las vulnerabilidades y de esta manera tomar las medidas preventivas en contra de agresiones maliciosas, valiéndose para ello de los tests de intrusión, que evalúan la seguridad técnica de los sistemas de información, redes de datos, aplicaciones web y servidores expuestos.

Competencias:

- Comprende un ataque a servidores web y aplicaciones a través de Internet
- Realiza una prueba de penetración
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria
- Entender el funcionamiento de los ataques más comunes desde Internet como SQL Injection, Cross Site Scripting, Path Traversal, Session Hijacking, entre otros
- Comprende cómo protegerse de los ataque implementando medida de seguridad
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

Dirigido a:

- Profesionales en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

DETALLES DEL CURSO

Tema 1: Introducción a las Aplicaciones Web

- Funcionamiento de las Aplicaciones Web
- Seguridad de las Aplicaciones Web
- Owasp Top 10
- Owasp Testing Guide

Tema 2: Denegación de Servicio y Session Hijacking

- Técnicas de ataque DoS
- Herramientas de Ataque DoS
- Ataques basado en Session Hijacking
- Técnicas de Session Hijacking
- Tipos de Session Hijacking

Tema 3 : Pentesting de Servidores Web

- Arquitectura de Servidores Web
- Metodología para ataques a servidores web
- Recopilación de Información
- Analizando Metadata
- Footprinting de Servidores Web
- Mirroring de Sitios Web
- Hacking de Contraseñas en Aplicaciones Web
    - ❖ Hydra
    - ❖ DirBuster / WebSlayer

Tema 4: Análisis de Vulnerabilidades de Servidores Web

- Analizadores a Nivel Plataforma
- Analizadores a Nivel Aplicación
- Análisis de Vulnerabilidades a Nivel Plataforma
- Análisis de Vulnerabilidades a Nivel Aplicación
    - ❖ Nessus
    - ❖ Acunetix Web Vulnerability Scanner
    - ❖ Webshag
    - ❖ Skipfish
    - ❖ Nikto
    - ❖ Owasp-Zap

Tema 5: Pentesting de Aplicaciones Web

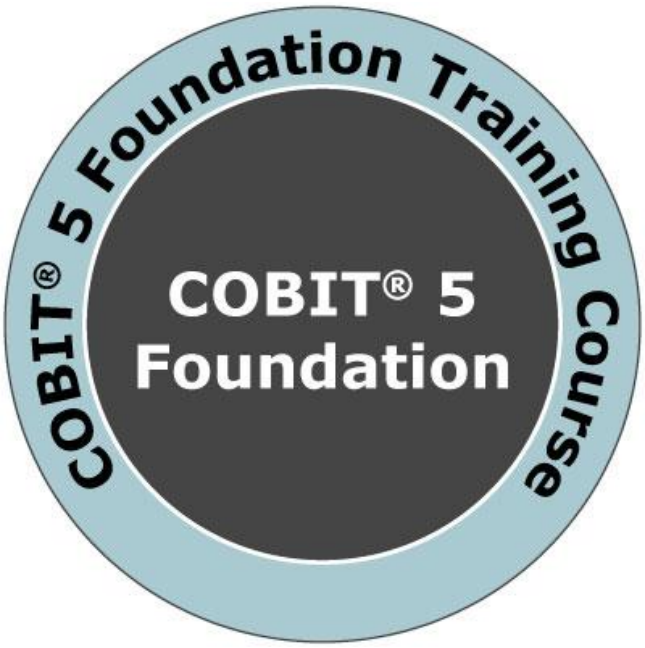
- Cómo funcionan las aplicaciones Web
- Como empezar a hackear una Aplicación Web
- Frameworks de Aprendizaje
- Métodos, Header, Body
- Entradas Inválidas
- Ataques de Directory Traversal
- URL encoding
- Cross Site Scripting
- SQL Injection
- Ejecución de Comandos
- Manejos de Shell

Tema 6: Explotación de Vulnerabilidades

- Trabajando con Exploits
- Metasploit Framework
- La Navaja Suiza del Hacker
- Proceso de Explotación de Vulnerabilidades

Duración: 24 horas.

Modulo 5 : Cobit 5 Foundation (24 Hrs)



COBIT 5 es el único marco comercial para el gobierno y gestión de TI empresarial. COBIT 5 ayuda a maximizar el valor de la información mediante la incorporación de las últimas ideas en gestión empresarial y técnicas de gestión, y proporciona principios aceptados globalmente, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza y el valor de los sistemas de información.

COBIT 5 construye y amplía COBIT 4.1 al integrar otros marcos principales, estándares y recursos, incluyendo Val IT y Risk IT de ISACA, Information Infrastructure Library (ITIL®) y normas relacionadas de la Organización Internacional de Normalización (ISO).
COBIT 5 ayuda a empresas de todos los tamaños a:

- Mantener información de alta calidad para respaldar las decisiones comerciales
- Alcanzar objetivos estratégicos y obtener beneficios comerciales a través del uso efectivo e innovador de TI
- Lograr la excelencia operativa a través de la aplicación confiable y eficiente de la tecnología
- Mantener el riesgo relacionado con TI a un nivel aceptable
- Optimizar el costo de los servicios de TI y la tecnología
- Apoyar el cumplimiento de las leyes, regulaciones, acuerdos contractuales y políticas relevantes

LOS OBJETIVOS DE APRENDIZAJE

- Los principales impulsores para el desarrollo de COBIT 5
- Los beneficios comerciales de usar COBIT 5
- La arquitectura del producto COBIT 5
- Los problemas y desafíos de la administración de TI que afectan a las empresas
- Los 5 principios clave de COBIT 5 para el gobierno y la gestión de TI empresarial
- Cómo COBIT 5 HABILITA que se gobierne y administre de manera holística para toda la empresa
- Cómo los procesos COBIT 5 y el modelo de referencia de proceso (PRM) ayudan a guiar la creación de los 5 principios y los 7 habilitadores de gestión y gestión.
- Los conceptos básicos para la Implementación de COBIT 5
- Los conceptos básicos del nuevo Modelo de Evaluación de Procesos
- Las guías COBIT 5 y cómo se relacionan entre sí

DETALLES DEL CURSO

El esquema del curso incluye lo siguiente:

1. Descripción general y características principales de COBIT 5

- El caso de negocios para COBIT 5
- Las diferencias clave entre COBIT 4.1 y COBIT 5

2. Los principios de COBIT 5

- Satisfacción de las necesidades de las partes interesadas
- Cubrir la empresa de punta a punta
- Aplicación de un marco integrado único
- Permitir un enfoque holístico
- Separar el gobierno de la gestión

3. Los habilitadores de COBIT 5

- Principios, políticas y marcos
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Personas, habilidades y competencias

4. Introducción a la implementación de COBIT 5

- ¿Cuáles son los controladores?
- ¿Dónde estamos ahora?
- ¿Dónde queremos estar?
- ¿Qué se necesita hacer?
- ¿Cómo llegamos allí?
- ¿Llegamos allí?
- ¿Cómo mantenemos el impulso?

5. Modelo de evaluación de la capacidad del proceso

- Elementos esenciales del modelo
- Diferencias entre el Modelo de Madurez COBIT 4.1 y el Modelo de Capacidad de Proceso COBIT 5
- Realizar una evaluación de capacidad

Duración: 24 horas.

VI. INFORMES

El Programa de Certificación en Cyber Seguridad esta compuesto por cursos oficiales de PECB los cuales incluyen la certificación oficial y algunos cursos de apoyo para fortalecer los conocimientos y aumentar las capacidades en el tema.

Estos cursos se dictan generalmente en horarios fuera de oficina o se pueden dictar a solicitud de los participantes.

Para Informes y detalle de horarios y precios, ud puede :

Informes : www.xnet.com.pe
Lugar : Av del Parque Sur 185 – Oficina 501 , San Isidro
Contacto : Jean del Carpio Foronda
Email : ventas@xnet.com.pe
Teléfono : 945045737

VII. DOCENTES

El programa cuenta con la participación de reconocidos profesionales con amplia experiencia académica y profesional, entre los que podemos destacar:

Miguel Ángel Gutiérrez Huamán

Profesional con más de 13 años en gestión de proyectos bajo el enfoque PMBOK, en riesgos de seguridad de la información y continuidad de negocios. Amplia experiencia en la implementación, operación y auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI). Ingeniero Electrónico de la Universidad Católica del Peru, con estudios de Maestría en Project Management en ESAN, Certificado CISA, CISM, CRISC, Lead Auditor IRCA ISO 27001, ISO 31000, COBIT y CEH.

Cuenta con las siguientes certificaciones:
- CERTIFIED INFORMATION SYSTEMS AUDITOR – **CISA**
- CERTIFIED INFORMATION SECURITY MANAGER – **CISM**
- CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL - **CRISC**
- CERTIFIED ISO/IEC 27001 Lead Implementer – **ISO27001 LI**
- CERTIFIED ISO/IEC 27001 Lead Auditor – **ISO27001 LA**
- CERTIFIED ISO/IEC 29100 Lead Privacy Implementer – **ISO 29100**
- CERTIFIED ISO/IEC 27032 Lead CyberSecurity Manager – **ISO 27032**
- EC Council Certified Chief Information Security Officer - **CCISO**
- Certified Lead Auditor IRCA ISO 27001 – **ISO 27001 IRCA**
- Certified ISO 31000 Lead Risk Manager – **ISO 31000**
- Certified Ethical Hacker – **CEH**
- Certified Penetration Testing Engineer **- CPTE**
- Check Point Certified Security Administrator - **CCSA**
- Cisco Certified Network Associate – **CCNA**

Jean del Carpio Foronda.

Ingeniero Electrónico con 15 años de Experiencia en Seguridad Informática y Networking de la Universidad Nacional de Ingeniería con Maestría en Dirección de Operaciones y Postgrado en Data Networking en la Universidad Peruana de Ciencias Aplicadas.

Conocimiento avanzados de TCP/IP, Redes LAN, Redes WAN ATM, Redes VSAT, Soluciones Satelitales, Redes SDH, MPLS, Voz Sobre IP, Telefonía IP, Call Manager, Switching, Seguridad Cisco ASA, IPS, Seguridad de la Información, Implementación de Sistemas de Gestión de la Seguridad de la Información SGSI, ISO27001, Ethical Hacker, Computo Forense, entre otros.

Catedrático de la Maestría de Seguridad Informática y Maestría de Telecomunicaciones de la UTP (Universidad Tecnológica del Perú), instructor de la UPC en el Programa de Especialista en Seguridad, ISO 27001, Hardening aplicaciones Windows, Linux, Auditoria de sistemas de Información.

A participado en Análisis de Ethical Hacking para el Ministerio del Interior, Banco Financiero, INPE, Ministerio de Defensa, Bancos y entidades comerciales.

Cuenta con las certificaciones:
- Certified Ethical Hacking (**CEH)**
- EC Council Security Analyst – **(ECSA)**
- Computer Hacking Forensic Investigator **(CHFI)**
- Certified Penetration Testing Engineer **- CPTE**
- CERTIFIED ISO/IEC 27001 Lead Implementer (**ISO 27001 LI**)
- CERTIFIED ISO/IEC 27032 Lead CyberSecurity Manager – **ISO 27032**
- EC Council Certified Chief Information Security Officer - **CCISO**
- EC Council Ethical Hacking Instructor **(CEI)**
- Certificacion Qualys Guard **(Qualys Guard CERTIFIED SPECIALIST)**
- Certificación **CCNA**, **CCNP**, **CCAI** (Cisco Certified Academy Instructor)
- Fortinet Certified Network Security Administrator **FCNSA**.
- Fortinet Certified NSE 1, NSE 2, NSE 3
- CheckPoint Certified SandBlast Administrator - **CCSA**