XNET SOLUTIONS
Centro de Entrenamiento Autorizado de PECB

Programa : Especialista en Gestión de la Seguridad de la Información- SGSI
Con Certificación Internacional en ISO 27001 e ISO 31000

Duración : 152 Horas (5 - 6 meses)

SYLLABUS

I. DESCRIPCIÓN

La información se ha convertido en un activo fundamental que debe ser protegido para que las firmas puedan sobrevivir y competir. La protección de la confidencialidad, disponibilidad e integridad de la información en las empresas, debe ser una preocupación estratégica. Los activos de información están sujetos constantemente a una serie de amenazas que buscan penetrar las vulnerabilidades organizacionales.

El estándar internacional ISO 27001:2013, que busca como propósito la implantación en las empresas de un Sistema de Gestión de Seguridad de Información (SGSI), con el fin de asegurar la instauración de controles como producto del análisis y evaluación del riesgo para minimizar daños a la organización a través de la prevención y reducción del impacto de los incidentes de seguridad.

Un SGSI le da la confiabilidad a un proveedor de poder continuar ofreciendo sus productos en los mercados. Garantiza que el riesgo que podría generar un desastre está mitigado por los controles que se han implantado. Da confianza de que existe continuidad del negocio.

El Programa de Especialización en Gestión de la Seguridad de la Información incluye los cursos de certificación internacional de PECB en ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, ISO 31000 Risk Manager y tiene como objetivo el poder formar profesionales que puedan liderar procesos de implementación, control y Auditoria de Sistemas de Gestión de Seguridad de la Información que cumplan con los requisitos de la Norma Internacional ISO 27001 obteniendo durante el desarrollo del Programa los

conocimientos necesarios y las certificaciones internaciones en ISO 27001 Implementador/Auditor Líder e ISO 31000 Gestión de Riesgos.

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 31000 Risk Manager (24Hr)
Módulo 2 : ISO/IEC 27001 Lead Implementer (32Hr)
Módulo 3 : Elaboración de la Documentación del SGSI (32Hr)
Módulo 4 : Balanced Score Card de Seguridad de la Información (24Hr)
Módulo 5 : ISO/IEC 27001 Lead Auditor (40Hr)

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/IEC 27001 Lead Auditor**
- **ISO/IEC 31000 Risk Manager**

Detalle de cada Modulo:

Módulo 1 : ISO/IEC 31000 Risk Manager (24 Hrs)

Este curso permite a los participantes obtener un conocimiento exhaustivo de los principios, el marco y el proceso fundamentales de Risk Management basados en ISO 31000. Durante este curso de capacitación, también obtendrá un conocimiento profundo de las mejores prácticas de Risk Management y podrá aplicarlos de manera efectiva en una organización para implementar efectivamente un proceso de Gestión de Riesgos.

Después de familiarizarse con todos los conceptos necesarios de Risk Management, puede presentarse para el examen y solicitar una credencial "PECB Certified ISO 31000 Risk Manager". Al tener un Certificado PECB, usted demostrará que tiene conocimientos prácticos y habilidades para gestionar eficazmente un proceso de riesgo en una organización.

LOS OBJETIVOS DE APRENDIZAJE

- Comprender la implementación de procesos de gestión de riesgos basados en ISO 31000
- Comprender los conceptos y procesos fundamentales de la Gestión de riesgos
- Reconocer la correlación entre ISO 31000, IEC / ISO 31010 y otras normas y marcos normativos
- Comprender los enfoques, métodos y técnicas utilizados para gestionar el riesgo dentro de una organización
- Aprenda a interpretar los principios y directrices de ISO 31000

DETALLES DEL CURSO

Tema 1: Introducción a los principios y el marco de ISO 31000

- Objetivos del curso y estructura
- Marco normativo y normativo
- Introducción a los conceptos y principios de ISO 31000
- Marco de gestión de riesgos
- Iniciando la implementación del proceso de gestión de riesgos
- Establecimiento de contexto

Tema 2: Procesos de gestión de riesgos basados en ISO 31000

- Identificación de riesgo
- Análisis de riesgo
- Evaluación de riesgo
- Tratamiento de riesgo
- Aceptación de riesgo
- Comunicación y consulta de riesgos
- Monitoreo y revisión de riesgos

Tema 3: Técnicas de evaluación de riesgos basadas en IEC / ISO 31010

- Metodologías de gestión de riesgos basadas en ISO 31010 (parte 1)
- Metodologías de gestión de riesgos basadas en ISO 31010 (parte 2)
- Competencia, evaluación y cierre de la capacitación

Duración: 24 horas.

Módulo 2 : 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 3 : Elaboración de la Documentación del SGSI (32 Hrs)

La implantación de un **SGSI** (Sistema de Gestión de Seguridad de la Información) basado e**n ISO 2700**1 implica la correcta elaboración y recopilación de la Documentación, para garantizar la confidencialidad, integridad y disponibilidad de la información asociada a dicho SGSI.

En la nueva **ISO 27001:2013** se habla de información documentada para hacer referencia a los denominados documentos y registros diferenciados en la anterior versión.

CONTENIDO:

- Documentación requerida por el estándar ISO 27001:2013.
- Principios para elaborar procedimientos.
- Metodología para el manejo de la información documentada.
- Documentación de políticas e instrucciones de trabajo.
- Gestión de la información documentada controlada.
- Manejo de un proyecto de documentación.

Documentos obligatorios y registros requeridos por ISO 27001:2013

Aquí están los documentos que necesita elaborar si quiere cumplir con la norma ISO 27001

- Análisis de Contexto (cláusula 4.1)
- Requerimientos de Seguridad de las Partes Interesadas (cláusula 4.2)
- Alcance del sistema de gestión de seguridad de la información (cláusula 4.3)
- Interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas (cláusula 4.3.c)
- Política de seguridad de la información (cláusulas 5.2)
- Gestión de Riesgos y Oportunidades del SGSI (cláusula 6.1.1)
- Metodología de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información(cláusula 6.1.2)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Objetivos de Seguridad de la Información (cláusula 6.2)
- Informe sobre evaluación de riesgos (cláusula 8.2)
- Definición de roles y responsabilidades de seguridad (cláusula 5.3)
- Evidencia de la competencia (cláusula 7.2)
- Plan de Comunicaciones del SGSI (cláusula 7.4)
- Control de Documentos internos y externos del SGSI (cláusula 7.5)
- Evaluación del desempeño del SGSI (cláusula 9.1)
- Auditoría Interna del SGSI (cláusula 9.2)
- Revisión por la Dirección del SGSI (cláusula 9.3)
- Mejora continua del SGSI (cláusula 10)

Y aquí están los registros obligatorios:

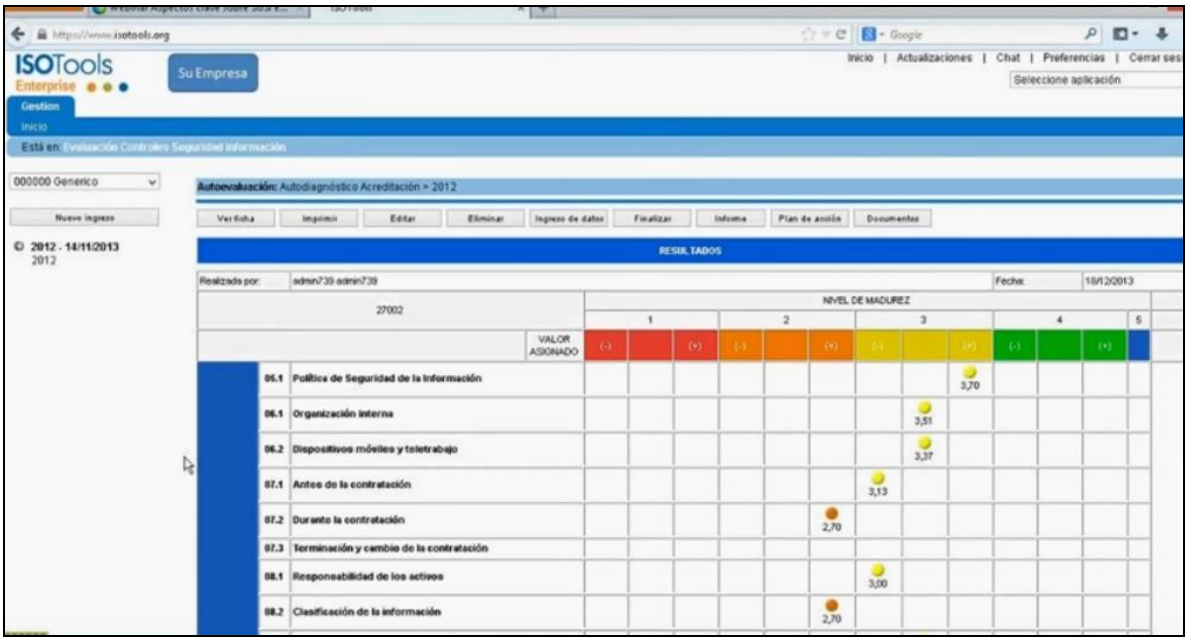
- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)
- Registros de gestión de riesgos y oportunidades del SGSI (cláusula 6.1.1)
- Registros de gestión de riesgos de seguridad de la información (cláusula 6.1.2)
- Seguimiento y resultados de medición (cláusula 9.1)
- Programa de auditoria interna (cláusula 9.2)
- Resultados de auditorías internas (cláusula 9.2)
- Resultados de la Revisión por Dirección (cláusula 9.3)
- Resultados de acciones correctivas (cláusula 10.1)
- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3)

Documentos no obligatorios
Hay numerosos documentos no obligatorio que pueden ser utilizados para la implementación de la ISO 27001, especialmente para los controles de seguridad del anexo A. Sin embargo, estos documentos no son obligatorios pero comúnmente son los más usados:

- Política BYOD (Bring Your Own Device = Trae tu propio dispositivo) (cláusula A.6.2.1)
- Política de dispositivo sobre dispositivos móviles y tele-trabajo (cláusula A.6.2.1)
- Política de clasificación de la información (cláusulas A.8.2.1, A.8.2.2 y A.8.2.3)
- Política de claves (cláusulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3)
- Política de eliminación y destrucción (cláusulas A.8.3.2 y A.11.2.7)
- Procedimientos para trabajo en áreas seguras (cláusula A.11.1.5)
- Política de pantalla y escritorio limpios (cláusula A.11.2.9)
- Política de gestión de cambios (cláusulas A.12.1.2 y A.14.2.4)
- Política de Copias de seguridad (cláusula A.12.3.1)
- Política de transferencia de información (cláusulas A.13.2.1, A.13.2.2, y A.13.2.3)
- Análisis de impacto en el negocio (BIA) (cláusula A.17.1.1)
- Plan de pruebas y verificación (cláusula A.17.1.3)
- Plan de mantenimiento y revisión (cláusula 17.1.3)
- Estrategia de continuidad de negocio (cláusula A.17.2.1)

Herramienta : ISO Tools

Aprendizaje en el uso de la herramienta ISO Tools para la ISO 27001



Duración: 32 horas.

Módulo 4 : Balanced Score Card de Seguridad Información (24 Hrs)

Objetivos del Curso:

La norma **ISO 27001** nos ofrece los requisitos necesarios para poder implementar con éxito un Sistema de Gestión de Seguridad de la Información en las organización, no obstante debemos tener en cuenta muchas más opciones.

Medir el desempeño es uno de los procesos fundamentales de las organización, bien sea en el ámbito corporativo, de tecnología de la información o de la seguridad TI.

Uno de los principales instrumentos que se ha adoptado por muchas organizaciones es el **Balanced Scorecard** (BSC), que se puede entender en español como Cuadro de Mando.

El Cuadro de Mando mide el desempeño de las organizaciones en el futuro. Se motiva gracias a que los sistemas de medición del desempeño que han sido utilizados hasta ese momento se han quedado obsoletos, ya que se encuentran orientados a los indicadores financieros.

El cuadro de mando incluye un esquema de medición que tiene en consideración cuatro perspectivas diferentes para el desempeño de las organizaciones:

- La perspectiva financiera: mide el desempeño de la organización que se encuentra basado en los indicadores económicos establecidos por la gerencia. Los indicadores se relacionan de una alguna forma con todos los aspectos de utilidad, de rendimiento sobre las inversiones y sobre la protección de la información, donde entra la norma **ISO 27001**.

- La perspectiva de clientes: ofrece mediciones sobre diferentes aspectos que se encuentran relacionados con los clientes de la organización, como puede ser el nivel de satisfacción de dicho clientes, la retención de clientes, los nuevos clientes, etc.

- La perspectiva de procesos: facilita la identificación y la medición de los procesos en los que la organización puede generar un incremento del desempeño. Todos los procesos que se encuentran relacionados con los servicio a los clientes, como puede ser la satisfacción de dichos clientes también influye mucho la seguridad de la información, es decir, la norma **ISO 27001**.

- La perspectiva de aprendizaje y crecimiento: se tratan las infraestructuras de la organización, ya que deben asegurar una mejora y un crecimiento a largo plazo. Todas las mediciones de las tres perspectivas anteriores puede generar brechas, por lo que el fin que persigue BSC junto a la norma **ISO 27001** es la eliminación de dichas brechas, optimizando los sistemas y alineando los procedimientos con las rutinas de trabajo.

Una de las principales aportaciones más importantes del **Sistema de Gestión de Seguridad de la Información** junto a **Balanced Scorecard** es que ofrece la perspectiva del conjunto de aspectos más importantes de la organización. Todos los directivos responsables que pueden generar información sobre los diferentes indicadores de la organización son utilizados para fundamentar las decisiones.

Otra característica muy importante es que facilita la relación de los planes de negocio corporativos con el objetivo departamental y con los objetivos de desempeño individual de los colaboradores.

Se ha desarrollado un modelo de cuadro de mando para la **tecnología de la información**, teniendo como base las cuatros perspectivas que hemos mencionado antes y adaptándolas a una función de **tecnología de la información**.

Contenido:

1. Conceptos del **BSC** y metodología de integración del plan estratégico al BSC de seguridad de la información.
2. Modelamiento e Identificación de estrategias de seguridad de la información
3. Alineamiento a la Visión, misión y estrategia de la empresa , mediante el BSC.
4. Diseño del mapa estratégico y selección de indicadores de seguridad de la información
5. Implementación de tableros de gestión (scorecards o Dashboards)
6. Caso prácticos de implementación del BSC de seguridad de la información

Duración: 24 horas.

Módulo 5 : ISO/IEC 27001 Lead Auditor (40 Horas)

La capacitación de Auditor Líder ISO / IEC 27001 le permite desarrollar la experiencia necesaria para realizar una auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) mediante la aplicación de principios, procedimientos y técnicas de auditoría ampliamente reconocidos. Durante este curso de capacitación, adquirirá los conocimientos y habilidades necesarios para planificar y llevar a cabo auditorías internas y externas.

Con base en ejercicios prácticos, podrá dominar las técnicas de auditoría y ser competente para administrar un programa de auditoría, un equipo de auditoría, la comunicación con los clientes y la resolución de conflictos.

Después de adquirir la experiencia necesaria para realizar esta auditoría, puede presentarse para el examen y solicitar una credencial **"PECB Certified ISO/IEC 27001 Lead Auditor"**. Al tener un Certificado de auditor líder de PECB, usted demostrará que tiene las capacidades y competencias para auditar a las organizaciones según las mejores prácticas.

LOS OBJETIVOS DE APRENDIZAJE

- Comprender las operaciones de un Sistema de gestión de la seguridad de la información basado en ISO/IEC 27001
- Reconozca la correlación entre ISO/IEC 27001, ISO/IEC 27002 y otras normas y marcos normativos
- Comprender el papel del auditor para: planificar, liderar y dar seguimiento a una auditoría del sistema de gestión de acuerdo con ISO 19011
- Aprenda a liderar un equipo de auditoría y auditoría
- Aprenda a interpretar los requisitos de ISO/IEC 27001 en el contexto de una auditoría del SGSI
- Adquirir las competencias de un auditor para: planificar una auditoría, dirigir una auditoría, redactar informes y realizar un seguimiento de una auditoría de conformidad con ISO 19011

DETALLES DEL CURSO

Sesión 1: Introducción a los sistemas de gestión de la seguridad de la información (ISMS) e ISO / IEC 27001

- Objetivos del curso y estructura
- Estándares y marcos regulatorios
- Proceso de certificación
- Principios fundamentales de los sistemas de gestión de la seguridad de la información
- Sistemas de gestión de seguridad de la información (SGSI)

Sesión 2: Principios de auditoría, preparación y lanzamiento de una auditoría

- Conceptos y principios fundamentales de auditoría
- Enfoque de auditoría basado en la evidencia
- Iniciando la auditoría
- Etapa 1 auditoría
- Preparación de la auditoría de la etapa 2 (auditoría en el sitio)
- Etapa 2 de auditoría (Parte 1)

Sesión 3: Actividades de auditoría en el sitio

- Etapa 2 de auditoría (Parte 2)
- Comunicación durante la auditoría
- Procedimientos de auditoría
- Crear planes de prueba de auditoría
- Redacción de hallazgos de auditoría e informes de no conformidad

Sesión 4: Cierre de la auditoría

- Documentación de la auditoría y revisión de la calidad de la auditoría
- Cierre de la auditoría
- Evaluación de planes de acción por el auditor
- Beneficios de la auditoría inicial
- Administrar un programa de auditoría interna
- Competencia y evaluación de auditores
- Cerrando el entrenamiento

Duración: 40 horas.

VI. INFORMES

El Programa de Certificación en Seguridad de la Información (SGSI) está 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. DOCENTE

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**