UNIVERSIDAD TECNOLÓGICA DE PEREIRA
Facultad de Ingeniería Eléctrica, Electrónica y ciencias de la Computación

Especialización en Redes de Datos
Posgrados Universidad Tecnológica de Pereira

SEMESTRE 2016-2

CURSO: SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001: 2013
HORAS: 48

NOTA: Para los estudiantes de la Especialización en redes de datos de la Universidad Tecnológica de Pereira, este curso es una electiva de su plan de estudios.

OBJETIVO GENERAL

Presentar los conceptos de la norma ISO 27001:2013, de forma que los estudiantes puedan conocer el campo de aplicación e implementación de un Sistema de Gestión de Seguridad de la información e identificar líneas de trabajo en esta temática.

OBJETIVOS ESPECÌFICOS

1. Entregar a los participantes los conocimientos teóricos y prácticos necesarios para que conozcan los riesgos y la manera pueden ayudar a la entidad a evitar pérdidas, reportando las anomalías que identifiquen.

2. Fortalecer habilidades en los participantes mediante el desarrollo de casos de estudio asociados a temas particulares de la seguridad de la información, utilizando herramientas y técnicas para la aplicación de conceptos que permitan mejorar la seguridad de la información en el que hacer del día a día.

3. Desarrollar en los participantes las competencias inherentes al rol que debe desempeñar como guarda de seguridad de la información y el aporte que debe realizar al mantenimiento y mejora del SGSI.

COMPETENCIAS ACADÉMICAS

1. Liderar planes de acción para prevenir y administrar riesgos relativos a la seguridad de la información
2. Diseñar, valorar y evaluar metodologías, sistemas y planes de acción para la gestión del riesgo, continuidad del negocio y recuperación de desastres.
3. Auditar y mejorar sistemas de seguridad de la información.
4. Identificar líneas de trabajo en estas temáticas.

METODOLOGÍA

A través de los módulos de capacitación se abarcan los conceptos, técnicas y herramientas, incluyendo horas prácticas en realización de talleres y estudios de casos, que permitan adquirir habilidades y competencias en la seguridad de la información, para que los funcionarios realicen la custodia y guardia de los activos de información de la entidad.

CONTENIDO RESUMIDO

I. Módulo 1: Fundamentos de seguridad de la información
II. Módulo 2: Gestión de riesgos
III. Módulo 3: Auditoría
IV. Módulo 4: Taller aplicación empresas

CONTENIDO DETALLADO

MODULO 1

FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

- Introducción
- Seguridad de la información
- Condiciones de implementación del modelo.
- Estratificación de la seguridad de la información en las entidades publicas
- Tiempos estimados de implementación por características de entidad.
- Sensibilización sobre el alcance y objetivo de la autoevaluación.
- Definición de la brecha.
- Implementación y ajustes al modelo de seguridad de la información.
- La relación del Responsable de Seguridad de la Información y el Modelo de Seguridad de la Información.
- Auto sostenibilidad del modelo
- Organigrama, roles, funciones y responsabilidades
- Características del guarda de seguridad de la información

MODULO 2

GESTION DE RIESGOS

- Clasificación de activos
- Riesgos y factores de riesgo en seguridad de la información.
- Tipos de riesgos, vulnerabilidades y amenazas
- Metodologías de gestión de riesgos
- Planes de tratamiento
- Planes de contingencia
- Planes de continuidad
- Integración de la gestión de riesgos con otros sistemas de gestión

MODULO 3

- Conceptos de Sistema de Gestión
- Términos y definiciones
- Análisis del Contexto Interno y Externo de Organizaciones
- Gestión del Riesgo de Seguridad de la Información
- Planificación de un Sistema de Gestión de la Seguridad de la Información – Soporte
- Estructura de la norma ISO 27000:2013
- Fundamentos de auditorías a sistemas de gestión
- Planificación, preparación, realización e informe de auditorías a Sistemas de Gestión
- Habilidades del Auditor
- Redacción de hallazgos de auditoría
- Técnicas de Auditoria.

MODULO 4

TALLER APLICACIÓN EMPRESAS

- Ejemplo de proceso con controles de seguridad
- Revisión de un proceso empresarial por parte de los participantes aplicado a su empresa
- Propuesta de aplicación de controles según lineamientos de seguridad.

Actividades de trabajo independiente del estudiante:

- Investigación y análisis de estudios de caso relativos a seguridad de la información.

EVALUACIÓN

- La evaluación se realizará de la siguiente forma:

Actividad	Valor porcentual
Parcial I	30 %
Parcial II	30 %
Proyecto final	40 %

Se evalúan los temas discutidos en clase y las actividades de trabajo independiente.

- Se realizará Role-Play para simulaciones de los ambientes de implementación y prácticas de los diferentes componentes necesarios para seguridad de la información.
- Se realizarán talleres de definición de proyectos de grados.

BIBLIOGRAFÍA

[7] ACIS. Revista asociación colombiana de ingeniería de sistemas. Disponible en http://www.acis.org.co/.

[8] Álvarez, C. S. La ley y la seguridad de la información: Perspectiva regional. ElTiempo, Disponible en: http://www.eltiempo.com/blogs/el\\\\\\\\\\\\\\filado\ \%\\\\\\\\\\\fioscuro\\\\\\\\\\\\\\fide\\\\\\%\\\\\\\fiinternet/2010/03/la-ley-y-la-eguridad-de-la-in.php.
[9] Boehmer, W. Cost-benefit trade-ofi analysis of an isms based on iso 27001. 2009 International ConferenceonAvailabilityReliability and Security, 2009.
[10] ChannelPlanet. Investigación, medios y eventos en tecnología de la información.

[11] Chi-Hsiang, W. Integrated installing iso 9000 and iso 27000 management systems onan organization. IEEE, Security Technology. 43rd Annual 2009 International CarnahanConferenceon, 2009.
[12] de Empresas de Tecnologías de la información y las Comunicaciones., A. M. Guía de seguridad de la información para pymes. Disponibleen: http://www.gdata.es/sobre-g-data/prensa/pressemeldungen/news-details/ article/1348-el-mercado-negro-de-internet.html.
[13] DANE. Departamento de administración nacional de estadística.
[14] Dey, M. Information security management - a practical approach. IEEE, AFRICON2007 , 2007.
[15] de Informática, C. S. Metodología de análisis y gestión de riesgos de los sistemas de información - margerit. Gobierno de España, Disponible en http://administracionelectronica.gob.es/?\\\\\\\\\\\\finfpb=true&\\\\\\\ \\\\\fipageLabel=P80029225129365155099 1&langPae=es%&detalleLista=PAE\\\\\\\\\\\\fi1276529683497133.
[16] Institute, S. E. Sse-cmm. Modelo de seguridad de la información. Versión
[17] INTECO y CERT. Curso - sistemas de gestión de la seguridad de la información según la norma une-iso/iec 27000. 2010.
[18] Intelligent, B. Iso 27000. Disponible en http://www.business-intelligent.com/ iso27000.pdf.
ICONTEC, Norma ISO/IEC 27000:2014 Sistemas de gestión de seguridad de la información – ICONTEC, Información general y vocabulario.
ICONTEC, Norma ISO/IEC 27001:2013 Sistemas de gestión de seguridad de la información - Requisitos
ICONTEC, Norma ISO/IEC 27002:2013 Guía de Buenas Prácticas de seguridad de la información.
ICONTEC, Norma ISO/IEC 27006:2011 Requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información
ICONTEC, Norma ISO 19011:2011 Directrices para la auditoría de los sistemas de gestión.
Ministerio de tecnologías de la información y comunicaciones, Estrategia Gobierno en Linea 3.1.