CURSO DE EXTENSIÓN
SÍLABO SEGURIDAD INFORMÁTICA

INFORMACIÓN GENERAL

Programa	**:**	Actualización
Curso	**:**	Seguridad de Información
Modalidad	**:**	Presencial
Horas Lectivas	**:**	24 horas lectivas.

I. SUMILLA

En curso está enfocado para comprender las diferentes fases para establecer, implementar, mantener y mejorar un conjunto de requerimientos de seguridad que nos exige la ISO/IEC 27001:2013. Así mismo los participantes comprendan un conjunto de controles de seguridad de la información comúnmente aceptados, según la ISO/IEC 27002:2013, lo que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles nos permiten asegurar que se cumplan los objetivos específicos de seguridad de información.

II. OBJETIVO GENERAL:

Conocer y aplicar la seguridad de la información basados en marcos de referencia internacional y nacional.

III. OBJETIVOS

Al finalizar el curso el participante:

1. Conocerá los fundamentos de seguridad de la información.
2. Comprender los componentes y la operación de un SGSI basado en la ISO/IEC 27001:2013
3. Dominar los conceptos, enfoques, normas, métodos y técnicas para la implementación y gestión eficaz de un SGSI.
4. Comprende los controles de seguridad de seguridad de la información comúnmente aceptados, según la ISO/IEC 27002 y su aplicación en sus actividades de trabajo.

IV. ESTRUCTURA TEMÁTICA

PRIMERA UNIDAD DE APRENDIZAJE: Fundamentos de Seguridad de la Información
Objetivo Específico: Comprender los fundamentos de seguridad de la información
Temas
Concepto y valor de la información.
Los pilares de la Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad..
La Norma ISO/IEC 27001-2013: terminología y relación con otros ISOs.
Conceptos de amenaza y riesgo y sus relaciones.
Ejemplo de Política y Objetivos de Seguridad de la Información

SEGUNDA UNIDAD DE APRENDIZAJE: Interpretación de la ISO/IEC 27001:2013
Objetivo Específico: Comprender los componentes y la operación de un SGSI basado en la ISO/IEC 27001:2013.
Temas
Que es la ISO
Principios de la ISO
Normas relacionadas del Sistema de Gestión de Seguridad de la Información
Estructura de la ISO/IEC 27001:2013
Introducción a la ISO/IEC 27001:2013
Contexto de la organización
Liderazgo
Planificación
Apoyo
Operación
Evaluación de desempeño
Mejora
Anexo A: Objetivos de control

TERCERA UNIDAD DE APRENDIZAJE: Implementación de la ISO/IEC 27001:2013
Objetivo Específico: Dominar los conceptos, enfoques, normas, métodos y técnicas para la implementación y gestión eficaz de un SGSI.
Temas
Ventajas de implementar un SGSI
Fases para implementar un SGSI
Análisis de brecha (modelo CMMI)
Proceso de certificación
Información documentada
Ley de Protección de Datos Personales
Clasificación de banco de datos personales

CUARTA UNIDAD DE APRENDIZAJE: Controles de Seguridad de la Información según la ISO/IEC 27002:2013, dominios 5 a la 8
Objetivo Específico: Comprende los controles de seguridad de seguridad de la información comúnmente aceptados, según la ISO/IEC 27002 y su aplicación en sus actividades de trabajo.
Temas
Que es la ISO/IEC 27002:2013
Estructura de la ISO/IEC 27002:2013
Requisitos de seguridad
Categorías de controles
Dominio 5: Políticas de Seguridad de la Información
Dominio 6: Organización de la Seguridad de la Información
Dominio 7: Seguridad relativa a los recursos humanos
Dominio 8: Gestión de activos

QUINTA UNIDAD DE APRENDIZAJE: Controles de Seguridad de la Información según la ISO/IEC 27002:2013, dominios 9 al 18
Objetivo Específico: Comprende los controles de seguridad de seguridad de la información comúnmente aceptados, según la ISO/IEC 27002 y su aplicación en sus actividades de trabajo.
Temas
Dominio 9: Control de acceso
Dominio 10: Criptografía

Dominio 11: Seguridad física y del entorno
Dominio 12: Seguridad de la operaciones
Dominio 13: Control de software de explotación
Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información
Dominio 15: Relación con proveedores
Dominio 16: Gestión de incidentes de seguridad de la información
Dominio 17: Aspectos de la seguridad de la información para la continuidad de negocios
Dominio 18: Cumplimiento

V. ACTIVIDADES DE APRENDIZAJE

Para el cumplimiento de los objetivos del curso se han seleccionado, las siguientes actividades:

- Exposiciones y diálogo.
- Enseñanza activa.
- Momentos para reflexionar y analizar.
- Debate.
- Trabajos individuales.
- Trabajos grupales.

VI. METODOLOGÍA

Para lograr un aprendizaje donde el participante construya su propio conocimiento el curso será desarrollado mediante exposiciones (grupales o individuales), diálogo entre el docente y participante promoviendo en todo momento la conversación reflexiva. Los trabajos grupales se desarrollarán de manera cooperativa y participativa. Empleando dinámicas de motivación e integración, orientadas a crear un ambiente de confianza que permita la libre expresión de ideas de los participantes. Para lo que se empleará lo siguiente:

- El método de la exposición para la observación de los principios de la enseñanza activa partiendo de la experiencia de los participantes y derivar de ello las consecuencias técnicas (Mayéutica).
- La técnica del cuchicheo para promover el comentario de las experiencias propias de los participantes.
- Debates que promuevan el análisis y reflexión sobre el quehacer personal, institucional.
- Medios audiovisuales con la finalidad de relacionar y ubicarnos en la situación presentada.

VII. RECURSOS DIDACTICOS

- Exposiciones y diálogo.
- Enseñanza activa.
- Momentos para reflexionar y analizar.
- Debate.
- Trabajos individuales.

VIII. EVALUACIÓN

Durante el desarrollo del curso, la evaluación será permanente mediante las intervenciones, los trabajos grupales e individuales.

Parámetro	Ponderaciones
Participación activa	25%
Examen de fundamentos e interpretación de la ISO/IEC 27001	25%
Examen de aplicación de la ISO/IEC 27001	25%
Examen de la aplicación de ISO/IEC 27002	25%
TOTAL	**100%**

El sistema de calificación a aplicar será de cero (0) a veinte (20). La nota mínima para aprobar el curso será 14.

Para la emisión del certificado se considera la asistencia al 100%.

IX. FUENTES DE INFORMACIÓN

(s.f.). *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements*.

(2014). *NTP ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos*. INDECOPI.

(2014). *UNE ISO/IEC 27002:2013 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información*.