PROGRAMA DEL CURSO "SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD (SGSI) BAJO EL ESTÁNDAR ISO 27.001"

1.- Descripción del curso

La creciente dependencia de la tecnología en todos los ámbitos de la vida cotidiana ha hecho que la ciberseguridad se convierta en una prioridad para las organizaciones de todos los tamaños. En este contexto, el **Sistema de Gestión de la Ciberseguridad (SGSI)** bajo el estándar **ISO 27.001** se presenta como una solución robusta para proteger los activos de información y garantizar la confidencialidad, integridad y disponibilidad de los datos.

Descripción del SGSI bajo el estándar ISO 27.001

El SGSI es un enfoque sistemático para gestionar y proteger la información sensible de una organización. La norma ISO 27.001 establece los requisitos y directrices para establecer, implementar, mantener y mejorar continuamente un SGSI. Esta norma internacional es reconocida globalmente y proporciona un marco que ayuda a las organizaciones a gestionar sus riesgos de ciberseguridad de manera efectiva.

Principales Componentes del SGSI

El SGSI incluye varios componentes clave, tales como:

- **Política de Ciberseguridad**: Define la dirección y el propósito del SGSI, estableciendo un marco para la gestión de la seguridad de la información.
- **Evaluación de Riesgos**: Este proceso implica identificar, analizar y evaluar los riesgos asociados con la información y los sistemas de la organización.
- **Controles de Seguridad**: Se implementan controles para mitigar los riesgos identificados. Estos pueden incluir medidas técnicas, administrativas y físicas.
- **Monitoreo y Revisión**: Se establecen mecanismos para el seguimiento continuo de la eficacia del SGSI y la revisión periódica de su desempeño.

2.- Objetivos del Aprendizaje

El objetivo principal del aprendizaje sobre el SGSI bajo el estándar ISO 27.001 es proporcionar a los participantes una comprensión clara de cómo implementar un sistema efectivo de gestión de ciberseguridad. Al finalizar el curso, los participantes deberían ser capaces de:

2.1 Comprender los principios y requisitos de la norma ISO 27.001

2.2 Identificar y evaluar los riesgos cibernéticos en su organización

2.3 Diseñar y aplicar controles de seguridad adecuados

2.4 Implementar un ciclo de mejora continua para el SGSI

3.- Metodología

La metodología utilizada para la enseñanza del SGSI bajo ISO 27.001 se basa en un enfoque práctico y participativo. Los participantes se involucran en actividades teóricas y prácticas que les permiten aplicar los conceptos aprendidos a casos reales. La metodología incluye:

1. **Clases Teóricas**: Se imparten conceptos fundamentales sobre ciberseguridad y la norma ISO 27.001.
2. **Estudios de Caso**: Se analizan ejemplos reales de implementaciones de SGSI en diferentes organizaciones.
3. **Talleres Prácticos**: Los participantes trabajan en grupos para desarrollar un SGSI adaptado a su contexto específico.
4. **Simulaciones**: Se realizan ejercicios de simulación para evaluar la respuesta ante incidentes de ciberseguridad.

4.- Duración

El curso sobre el SGSI bajo el estándar ISO 27.001 tiene una duración total de **40 horas**, distribuidas en sesiones de 5 días. Cada día se dedicarán 8 horas a la enseñanza y la práctica de los conceptos clave del SGSI. Esta estructura permite a los participantes asimilar la información de manera efectiva y aplicar lo aprendido en un entorno colaborativo.

5.- Módulos del Curso

El curso está dividido en varios módulos que cubren todos los aspectos importantes del SGSI bajo ISO 27.001. A continuación se detallan los módulos:

Módulo 1: Introducción a la Ciberseguridad y la ISO 27.001

- Conceptos básicos de ciberseguridad.
- Historia y evolución de la norma ISO 27.001.
- Importancia de la ciberseguridad en el contexto actual.

Módulo 2: Establecimiento del SGSI

- Definición de la política de seguridad de la información.
- Identificación de los interesados y sus expectativas.
- Alcance y límites del SGSI.

Módulo 3: Evaluación de Riesgos

- Métodos y técnicas de evaluación de riesgos.
- Análisis de impacto en el negocio (BIA).
- Identificación y tratamiento de riesgos.

Módulo 4: Implementación de Controles de Seguridad

- Tipos de controles de seguridad (preventivos, detectivos y correctivos).
- Implementación de controles técnicos y administrativos.
- Formación y concienciación del personal.

Módulo 5: Monitoreo y Revisión del SGSI

- Establecimiento de indicadores de rendimiento.
- Auditoría y revisión del SGSI.
- Mejora continua y gestión de cambios.

Módulo 6: Preparación para la Certificación

- Proceso de certificación ISO 27.001.
- Documentación requerida para la auditoría.
- Consejos para superar la certificación.

6.- Modalidad

El curso se ofrecerá en modalidad **presencial** y **virtual**, permitiendo a los participantes elegir la opción que mejor se adapte a sus necesidades.

- **Modalidad Presencial**: Se llevará a cabo en un aula equipada con tecnología adecuada para facilitar la enseñanza y el aprendizaje. Los participantes podrán interactuar directamente con los instructores y entre sí.
- **Modalidad Virtual**: Se impartirá a través de una plataforma de aprendizaje en línea, donde los participantes podrán acceder a materiales de estudio, participar en foros de discusión y realizar actividades prácticas desde cualquier lugar.

7.- Conclusión

El Sistema de Gestión de la Ciberseguridad bajo el estándar ISO 27.001 es esencial para cualquier organización que busque proteger sus activos de información y cumplir con las normativas de seguridad. A través de una formación adecuada y la implementación de un SGSI, las organizaciones pueden no solo protegerse contra amenazas cibernéticas, sino también mejorar su reputación y confianza entre sus clientes y socios.