CURSO TALLER

Implementador Norma ISO 27001 sobre Gestión de Seguridad de la Información

DESCRIPCIÓN DEL CURSO

El curso explicará los fundamentos para liderar una iniciativa en seguridad de la información, teniendo como base principios de gerencia de seguridad, y el uso de 2 normas reconocidas internacionalmente: la ISO 27001 "Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) Requisitos ", y la ISO 177991 "Tecnología de la Información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información". Al final del curso el asistente contará con las herramientas básicas para poder ser agente de cambio en la postura que una empresa debe tener con respecto a los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

OBJETIVOS

Comprender las iniciativas necesarias para Gestionar la Seguridad de la Información de forma pro-activa.

- ☐ Implicaciones de la Gestión del Riesgo: Identificación de Activos de Valor, Amenazas, Vulnerabilidades, Impacto, Metodologías valoración del Riesgo, Plan de Tratamiento de riesgos.

- Adquirir los conocimientos, habilidades y aptitudes necesarias para planificar, desarrollar e implementar un sistema de gestión de la información de una organización basándose en los estándares internacionales aplicables de acuerdo a la normativa ISO 27001:2013

- Aprender, planificar y documentar debidamente un Sistema de Gestión de Seguridad de la Información utilizando los diferentes instrumentos de análisis e información que permitan realizar correctamente una auditoría SGSI.

- ☐ Definición de objetivos de seguridad, y políticas del Sistema de Gestión de la
- ☐ Seguridad de la Información.

- ☐ Definición de la Declaración de Aplicabilidad: Selección e implementación de controles físicos, organizacionales y técnicos.
- ☐ Definición de estructuras de documentación, para la escritura, lectura, aprobación, promoción y control de Políticas, Normas y Procedimientos. Comprender las áreas, objetivos de control, y controles definidos por:

☐ La ISO 17799:2005 (ISO 27002), Código de Practica para la Gerencia de Seguridad de la Información.

_ Política de Seguridad. _ Organización de la Seguridad de la Información. _ Administración de Activos. _ Seguridad en los recursos humanos. _ Seguridad física y ambiental. _ Gerencia de las Comunicaciones y las Operaciones.

_ Control de Acceso. Adquisición, desarrollo y mantenimiento de sistemas de información. _ Manejo de incidentes de seguridad. _ Manejo de Continuidad de Negocio. _ Cumplimiento.

Comprender aspectos de acreditación y auditoria para la certificación del Sistema de gestión de Seguridad de la Información.

☐ Auditorías internas, acciones correctivas y preventivas.

☐ Auditorías externas y certificación.

☐ Comprender los pilares para el lograr la seguridad de la información:

☐ Planeación: Se debe planear para lograr seguridad. Este pilar es el conjunto de actividades para soportar el diseño, creación e implementación de estrategias de seguridad de la información, para lograr así que la estrategia del negocio sea soportada por la estrategia de los sistemas de información, y esta sea soportada por la estrategia de la seguridad de la información.

☐ Políticas: Se deben definir el conjunto de directrices que van a dictar cierto comportamiento en la organización a nivel corporativo, a nivel de ciertas coyunturas/problemáticas y a nivel de sistemas.

☐ Programas: Son el conjunto de operaciones que hacen parte del área de seguridad que buscan el cumplimiento de ciertos objetivos. Se pueden componer de un conjunto de proyectos.

☐ Protección: Es el pilar asociado a la identificación, valoración y mitigación de riesgos con la implementación de mecanismos de protección.(Controles y herramientas de seguridad). Personas: Este pilar tiene que ver con la organización del área de seguridad, la forma como se la va a dar seguridad a las personas que hacen parte de esta, y la forma como esta área le piensa brindar seguridad al

personal.

☐ Gerencia de Proyectos: Gerencia de proyectos, todo conjunto de actividades que se considere como un proyecto debe seguir una metodología estricta de Gerencia de proyectos para garantizar el éxito de las mismas.

METODOLOGÍA

Se realizarán sesiones orientadas a presentar los conceptos fundamentales de cada tema. Para esto se utilizarán: Exposiciones magistrales: con el uso de ayudas audiovisuales, se hará particular énfasis en los conceptos principales y rol que ejercen dentro del modelo de ITIL. Evaluaciones cortas: Se plantearán preguntas de selección múltiple, para la verificación del entendimiento de los conceptos tratados en cada tema.

CONTENIDO

1. INTRODUCCIÓN

Introducción a la Gerencia en Seguridad de la Información. o Reconocer la importancia de las tecnologías de información, y comprender quien es responsable de proteger los activos de información de la organización. o Conocer y comprender la definición y características claves de la seguridad de la información. o Conocer y comprender las características claves asociadas a liderazgo y gerencia. o Reconocer las características que diferencian la gerencia en seguridad de la información de cualquier otro tipo de gerencia.

2. PLANEACIÓN

Planeación de la seguridad.

☐ Reconocer la importancia de lo que significa la planeación, y los principales componentes de ésta cuando se trata de seguridad de la información.

☐ Conocer y comprender los componentes principales para la implementación de un sistema de seguridad de la información dentro de la organización.

3. POLITICAS Y PROGRAMAS

☐ Política de Seguridad de la Información.

☐ Definir la política de seguridad de la información y comprender su rol central en la realización de un programa exitoso de seguridad.

☐ Reconocer los 3 tipos principales de políticas de seguridad de la información, y conocer que realiza cada uno.

☐ Desarrollar, implementar, y mantener varios tipos de políticas en seguridad de la información.

☐ Desarrollo de un programa de seguridad de TI.

☐ Reconocer y comprender las aproximaciones organizacionales a la seguridad de la información.

☐ Listar y describir los componentes funcionales de un programa de seguridad de la información.

☐ Determinar cómo planear y organizar el programa de seguridad de la información según el tamaño de la empresa.

Evaluar los factores internos y externos que influencian las actividades y la organización de un programa en seguridad de la información.

☐ Describir los componentes de un programa de conciencia, educación y entrenamiento en seguridad.

☐ Prácticas y modelos de Gerencia en Seguridad de la Información.

☐ Seleccionar los principales modelos de gerencia en seguridad de la información, y desarrollar habilidades para customizarlos a las necesidades específicas de la organización. Presentación ISO 27001 "Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) Requisitos" (Parte 1) i. Términos y definiciones. ii. Sección 4. Sistemas de Gestión de Seguridad de la Información: explicaciones y consideraciones. iii. Sección 5. Responsabilidad Gerencial. iv. Sección 6. Auditorías Internas. Presentación ISO 17999/27002 "Tecnología de la Información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información". Descripción de áreas y objetivos de control para: i. Política de Seguridad ii. Organización de la Seguridad de la Información. iii. Administración de Activos. iv. Seguridad en los recursos humanos. v. Seguridad física y ambiental. vi. Gerencia de las Comunicaciones y las Operaciones. vii. Control de Acceso viii. Adquisición, desarrollo y mantenimiento de sistemas de información. ix. Gestión de incidentes de seguridad. x. Gestión de Continuidad de Negocio. xi. Cumplimiento Presentación ISO 27001 "Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) Requisitos" (Parte 2) i. Sección 7. Revisión Gerencial del SGSI. ii. Sección 8. Mejora del SGSI.

4. PROTECCIÓN

Gestión de riesgos: Identificación, estimación y control de riesgos.

☐ Definir la gestión de riesgos, y su rol dentro de la organización.

☐ Utilizar técnicas de gestión de riesgos para identificar y priorizar los factores de riesgo a los activos de información.

☐ Valorar el riesgo basado en la probabilidad de eventos adversos y en los efectos que pueden tener sobre los activos de información.

☐ Comprender y seleccionar las opciones de estrategias para la mitigación de riesgos para controlar el riesgo.

☐ Comprender la aproximación OCTAVE para realizar la gerencia del riesgo. Mecanismos de protección:

☐ Conocer y comprender las aproximaciones para el control de acceso, incluyendo la autenticación, autorización, y controles de acceso biométricos.

☐ Definir e Identificar varios tipos de firewalls, y aproximaciones comunes para la implementación de los mismos.

☐ Discutir los principales puntos cuando se manejan accesos remotos y conexiones dialup.

☐ Identificar y describir tipos de sistemas de detección de intrusos, y dos estrategias en las cuales se basan.

☐ Discutir conceptos de criptografía, y comparar y contrastar la inscripción simétrica y asimétrica.

5. PERSONAS Y PROYECTOS Personal y Seguridad

☐ Identificar las habilidades y requisitos para los cargos en seguridad de la información.

☐ Reconocer las certificaciones en seguridad de la información, e identificar el foco de cada una de ellas.

☐ Comprender e implementar las principales restricciones en seguridad cuando se van a contratar este tipo de personas.

☐ Comprender el rol de la seguridad de la información, cuando una persona termina su empleo.

☐ Describir las prácticas de seguridad utilizadas para controlar el comportamiento de un empleado y prevenir el mal uso de la información. Gestión de Proyectos en Seguridad de la información

☐ Comprender la gestión básica de proyectos.

☐ Aplicar los principios de gerencia en un programa de seguridad de la información.

DURACCION: 40 horas profesores certificados en la norma ISO 27001

INCLUYE:

1. Material oficial
2. Examen de certificación
3. Practicas y talleres