

Como Implantar un Sistema de Gestión de Seguridad de Información ISO 27001:2005 NUEVO ESTÁNDAR INTERNACIONAL

INTRODUCCIÓN

Desde el 15 de Octubre del 2005, el estándar internacional BS 7799-2:2002 quedó en la obsolescencia. El ISO 27001:2005, el primer representante de la nueva familia de estándares ISO 27000 lo reemplaza como "Sistema de Gestión de Seguridad de Información".

No hay duda ni siquiera para el más escéptico, que el comercio entre organizaciones y el de organizaciones con consumidores, será casi en su totalidad a través del uso de internet en los próximos años. Hoy en día suena difícil escuchar que un Banco no da servicios electrónicos, o que determinada organización no tenga un portal en la red.

Todos estos adelantos tecnológicos han desarrollado una necesidad imperiosa que las empresas tienen que solucionar, el cual es darle a sus clientes seguridad de que se tiene un sistema confiable de información y que se puede proteger su integridad. El mercado no trabajará con proveedores que no tengan un sistema que minimice el riesgo en el manejo de la información.

Los riesgos comerciales a los que una organización está sometida son interminables. Los activos de información que se manejan en la empresa moderna son importantísimos para su desempeño estratégico. Imaginémonos los virus que se proliferan en la red, los hackers siempre al acecho, intrusos que penetran a nuestro sistema informático y se llevan la información de los clientes, estados financieros que llegan fácilmente a manos de terceros y bases de datos que son usurpadas.

Si las empresas no establecen sistemas que aseguren la:

(1) integridad (la información esta como se pretende, sin modificaciones inapropiadas o corrupción).

(2) Confidencialidad (la información esta protegida de personas no autorizadas).

(3) Disponibilidad (usuarios autorizados pueden acceder aplicaciones y sistemas cuando lo requieran para desempeñar sus funciones), jamás podrán mantenerse compitiendo en el mundo globalizado.

El riesgo, entendido como la probabilidad de que una amenaza en particular ataque una determinada vulnerabilidad en la empresa, siempre esta latente. La idea para minimizar la posibilidad de riesgo en el manejo de la información, consiste en establecer un Sistema de Gestión de Seguridad de Información (SGSI) en la empresa que permita llevar a sus niveles mínimos el riesgo y permita asegurarle a terceros que se tiene un sistema confiable de información.

QUIENES DEBEN ASISTIR A ESTE SEMINARIO

- Directores de Operaciones o gerentes de áreas con responsabilidad ejecutiva en el negocio.
- Especialistas del área de informática interesados en conocer como se implanta el estándar ISO 27001:2005. "Sistema de Gestión de Seguridad de Información.
- Gerentes y especialistas en seguridad de información interesados en conocer como se establece un sistema de análisis y evaluación del riesgo.

BENEFICIOS DE ASISTIR A ESTE SEMINARIO.-

Al final de este seminario los participantes:

- Entenderán la naturaleza y los requerimientos del estándar ISO 27001:2005 y el código de práctica para la gestión de seguridad de información del ISO
- 17799:2005.
- Conocerán en detalle como se procede a implantar el ISO 27001:2005 "Sistema de Gestión de Seguridad de Información."

- Sabrán como se procede metodológicamente para analizar y evaluar el riesgo de información en una empresa y a mitigar a través de controles el riesgo.
- Aprenderán como opera un plan de continuidad comercial del negocio.
- Podrán gestionar un proyecto de implantación del ISO 27001:2005 "Sistema de Gestión de Seguridad de Información" en una empresa determinada.

EXPOSITOR



Alberto G. Alexander Ph.D. The University of Kansas, 1977, M.A. Northern Michigan University, 1974, Licenciatura en Administración, Universidad de Lima, 1972. El Dr. Alexander posee una amplia experiencia académica en Instituciones de Post-Grado. Ha sido profesor a dedicación exclusiva en la Dirección de Post-Grado de la Universidad de Carabobo, Valencia - Venezuela (1977-1978). Fue profesor de Post-Grado de la Universidad Católica Andrés Bello, Caracas - Venezuela (1978-1979). Se desempeñó como profesor residente del Instituto de Estudios Superiores de Administración (IESA), Caracas - Venezuela (1978-1983). Ha sido profesor afiliado de la Escuela de Administración de Negocios para Graduados (ESAN), Lima - Perú. El Dr. Alexander posee una amplia experiencia en el diseño y dictado de Programas de Desarrollo Gerencial para Ejecutivos. Sus áreas de interés, así como de experiencia en la Docencia y en Consultoría, son: Productividad, Calidad Total, Modelos de Aseguramiento de la Calidad, Sistema de Recursos Humanos y Planificación Estratégica. Ha publicado artículos y ensayos en revistas internacionales. Es ganador del Concurso Nacional Venezolano de Productividad "Don Eugenio Mendoza", patrocinado por **FEDECAMARAS**, en el año 1980. En el año 1990, la Federación Venezolana de Prensa le otorgó "EL SOL DORADO", en reconocimiento a sus aportes para el desarrollo y bienestar de Venezuela. El Dr. Alexander posee una amplia experiencia internacional en el asesoramiento a empresas en áreas tales como: Modelos de Aseguramiento de la Calidad: ISO 9000, Reingeniería de Procesos, Mejoramiento de la Calidad, Reducción de Costos de la Mala Calidad y Sistemas de Recursos Humanos. Es miembro activo de American Society for Quality. Es **auditor líder**

de **Sistemas de Gestión de la Calidad ISO 9000**, certificado por el International Register of Certificated Auditors (IRCA), Inglaterra. **Auditor de "Sistemas de Gestión de Seguridad de Información"** certificado por el Internacional Register of Certificated Auditors" (IRCA) Inglaterra. Entrenado como auditor lider en **ISO 14000** certificado ante el EARA (Inglaterra) y el RAB (USA). Auditor de Sistemas **TL 9000**, certificado ante el **QuEST (USA)**. **Autor de los libros:** La Mala Calidad y sus Costos, 1994. Aplicación del ISO 9000 y Cómo Implementarlo, 1995. Ambos ejemplares publicados por la Editorial Addison Wesley, U.S.A., Manual para Documentar Sistemas de Calidad. Prentice Hall Hispanoamerica, 1999, México, Metodología Para el Mejoramiento Continuo. Prentice Hall Hispanoamericana 2001, México, e Implantación Estratégica del ISO 9000 versión 2000. Fondo Editorial Pontificia Universidad Católica del Perú. 2003, Perú. Metodología para Documentar el ISO 9000 versión 2000, Prentice Hall, 2005, México. Su mas reciente publicación es Diseño y Gestión de un Sistema de seguridad de Información: Óptica 27001:2005, Editorial Alfaomega, Colombia, 2007. Se ha desempeñado como Director Gerente de la firma **EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.**, con sede en Caracas - Venezuela. Actualmente actua en las mismas funciones para las operaciones de latinoamerica, desde Lima, Perú. www.eficienciagerencial.com

ESTRUCTURA DEL PROGRAMA

Herramientas Metodológicas a Utilizar:

- Clases Lectivas: Presentación explícita del contenido y de los aspectos conceptuales y técnicos asociados a cada tema en formato Powerpoint.
- Análisis de Casos y Distribución de Lecturas: Las explicaciones conceptuales se combinarán con el análisis de casos prácticos que permitirán profundizar en los diferentes aspectos tratados.
- Juegos de Simulación: Se utilizarán juegos de simulación que replicarán situaciones reales en las empresas al tratar de implantar el modelo.

1. Naturaleza y Dinámica del estándar ISO 27001:2005 "Sistema de Gestión de Seguridad de Información".

Temario

- El ISO 27001:2005 y la nueva familia ISO 27000.
- Qué es información y su relación con el riesgo.
- Funcionamiento del modelo ISO 27001:2005 y el enfoque de procesos.
- Interpretación de los requerimientos del modelo ISO 27001:2005.
- Ejercicio de simulación: Interpretación de los requerimientos del estándar ISO 27001:2005.
- BASILEA II y las exigencias para el manejo del riesgo operativo.

2. Análisis e Interpretación de los controles del estándar ISO 27001:2005

Temario

- Estructura de los controles del estándar.
- Los controles obligatorios del modelo.
- Los procedimientos y las políticas exigidas por los controles del estándar.
- Interpretación de los requerimientos de cada uno de los controles del estándar.
- Caso Práctico: Interpretación de los controles.

3. Establecimiento de un Sistema de Gestión de Seguridad de Información

Temario

- Determinación del alcance del modelo: Utilización de la metodología de las elipses.
- Identificación de los activos de información y métodos para efectuar una tasación.
- Metodología para determinar las amenazas de los activos.
- Técnicas para definir las vulnerabilidades de los activos.
- Caso: Estableciendo un Sistema de Gestión de Seguridad de Información.

4. Realización del análisis y evaluación del riesgo

Temario

- Componentes del análisis del riesgo
- Enfoque cuantitativo y cualitativo para evaluar el riesgo.
- Determinación del riesgo residual.
- Elaboración de un plan de tratamiento del riesgo y diseño de una política de seguridad de información.
- Caso: Analizando y evaluando el riesgo en una empresa.

5. Identificación de los controles para minimizar el riesgo evaluado

Temario

- Aspectos estratégicos al escoger los controles del anexo A del estándar.
- Aprender a utilizar como guía para implantar controles al ISO 17799:2005.
- Estructura de la documentación exigida para implantar los controles.
- Diseño de procedimientos y políticas para instaurar controles.
- Elaboración de un enunciado de aplicabilidad
- Caso: Estableciendo controles para mitigar el riesgo.

6. Implantación y Operación de un Sistema de Gestión de Seguridad de Información

Temario

- Rol de la gerencia, acciones y responsabilidades para el manejo de los riesgos de seguridad.
- Acciones para implementar los controles seleccionados.
- Las revisiones gerenciales y el diseño y puesta en marcha de las auditorías internas.
- Manejo de las acciones correctivas y preventivas.
- Caso: Diseñando un plan de continuidad del negocio.

7. Metodología para Implantar el ISO 27001:2005.

“Sistema de Gestión de Seguridad de Información” en una Empresa

Temario

- Funcionamiento del ciclo metodológico para implantar el modelo en una empresa.
- Establecimiento estratégico del alcance del modelo.
- Estructura requerida para gestionar el proyecto de implantación en una empresa.
- Proceso de certificación internacional del modelo.
- Caso: Implantación del ISO 27001:2005 en una empresa.

MATERIAL DIDÁCTICO

Cada participante recibirá:

- La presentación y la documentación completa preparada por el expositor para la actividad. Este material se convertirá en una guía para implantar el modelo en sus respectivas empresas.
- Una copia en castellano del estándar ISO 27001:2005 y del ISO 17799:2005.

INFORMACIÓN E INSCRIPCIÓN

E-Mail: servicios@eficienciagerencial.com

Website: www.eficienciagerencial.com

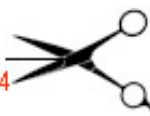
Dirección: Av. Del Pinar # 134, Edificio El Pinar II, Ofic. 803, Chacarilla del Estanque, Santiago de Surco, Lima – Perú

Teléfonos: (511) 3721441 / 3721415

Fax: (511) 436 6144

Este seminario puede confeccionarse y adaptarse a las necesidades específicas de la empresa y ser dictado de manera exclusiva.

Favor completar y enviar vía email a cursos@eficienciagerencial.com o por fax al (511) 436-6144



FORMULARIO DE INSCRIPCIÓN

COMO IMPLANTAR UN SGSI ISO 27001:2005

INFORMACIÓN DE LA EMPRESA

Nombre de la Empresa _____
RUC _____
Actividad Especifica de la Empresa _____
Dirección _____
Ciudad _____ Provincia _____
Teléfono _____ Fax _____

INFORMACIÓN DEL PARTICIPANTE

Nombres y Apellidos _____
Cargo _____
Email Empresa _____ Email Personal _____
Teléfono (Empresa) _____ Teléfono (Móvil) _____
Sexo

F	M
---	---

 Fecha Nacimiento (Día/Mes) _____

¿Cómo desea que aparezcan sus datos en su certificado de participación?
(Indique Nombres y Apellidos)

Objetivos: ¿Qué espera lograr asistiendo a este seminario?

¿Cómo se enteró del curso?

Prensa Revista Email Google Website Un amigo

Otros, indique _____

DATOS DE FACTURACIÓN

Formas de Pago (*) Depósito en cuenta bancaria Pago en línea vía web EGP
<http://www.eficienciagerencial.com/tienda>
Facturar a Participante Empresa

Si eligió **facturar a empresa** llene la siguiente información:

Persona responsable de la inscripción _____
Departamento _____ Posición _____
Teléfono _____ Fax _____

(*) Datos para depósito en cuenta bancaria:

Abono en cuenta ahorro US \$:

- Banco: BBVA
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.
Cuenta US \$ N° 0011-0194-0200289850-86

Abono en cuenta corriente en nuevos soles S/:

- Banco: SCOTIABANK
Beneficiario: EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.
Cuenta N° 6459374

POLÍTICAS DE CANCELACIÓN Y REEMBOLSOS

1. Nos reservamos el derecho de cancelar el curso si no se cumplen con las condiciones estipuladas, en este caso el costo de inscripción será reembolsado a los participantes.
2. No nos hacemos responsables por gastos de pasaje u hospedaje en el cual el participante haya incurrido. Toda notificación de cambio o cancelación por parte de nuestra empresa será indicada no menos de quince (15) días antes del inicio del curso.
3. Los asistentes que den por cancelada su participación en el curso quince (15) días antes del inicio del curso tendrán un cargo del 20% del valor de la inscripción del curso, correspondiente a gastos administrativos.

Cancelaciones después de este período no tendrán reembolso, sin embargo el cupo puede ser usado por otro participante de la misma empresa

4. Sólo el envío de la solicitud de inscripción debidamente llenada y el pago adelantado del importe del evento formalizará la inscripción.
5. El curso debe ser pagado en su totalidad antes de la fecha de inicio.