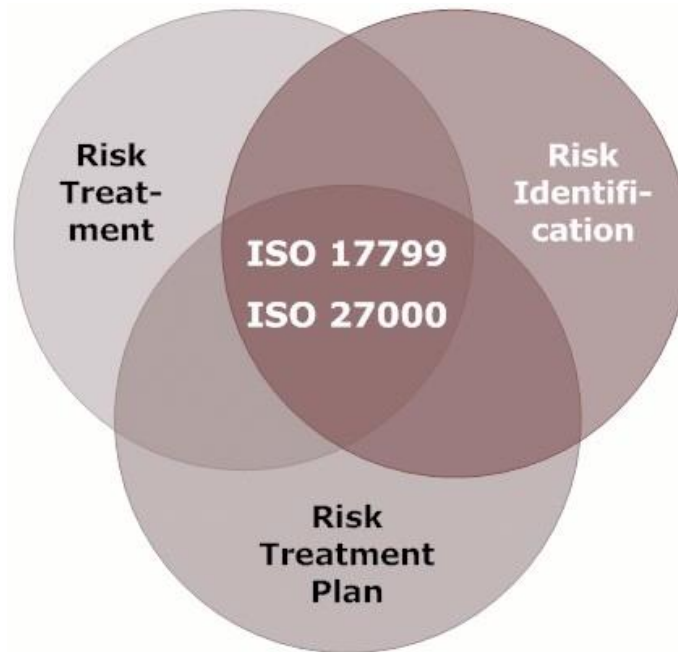


ii. Consultoría en Políticas de Seguridad BS7799 – ISO 17799 – ISO 27000



1. Políticas y Procedimientos de Seguridad

Tópicos de la Norma BS 7799 en relación con su reglamento ISO/IEC 17799 – 2000 – 27000 Para la obtención de un ISMS

Un Sistema Administrativo de Seguridad de la Información (Information Security Management System ISMS) es una forma sistemática de administrar la información sensible de una compañía, para que permanezca segura. Abarca a las personas, los procesos y las Tecnologías de la Información. BSI ha publicado un reglamento de prácticas para estos sistemas, el ISO/IEC 17799, que está siendo internacionalmente adoptado.

La seguridad de la información no termina al implementar el más reciente "firewall", o al subcontratar a una compañía de seguridad las 24 horas. La forma total de la Seguridad de la Información, y la integración de diferentes iniciativas de seguridad, necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema Administrativo de Seguridad de la Información - que le permite a la empresa, poder coordinar sus esfuerzos de seguridad con mayor efectividad.

Tópicos de SRB para una ISMS aplicando BS7799 con su reglamento ISO/IEC 17799:2000

1.- Política de seguridad

- 1.1.- Marco teórico y práctico general, en el apoyo a la seguridad de la información
- 1.2.- Estructura reglamentaria a favor del foco de negocio de cada empresa

2.- Seguridad Organizacional

- 2.1.- Infraestructura de seguridad de la información
- 2.2.- Seguridad del activo de la empresa
- 2.3.- Externalización que afectan a los activos o Información a la empresa

3.- Clasificación y control de Bienes o activos

- 3.1.- Responsabilidad de los Bienes
- 3.2.- Clasificación de la información

4.- Seguridad del Personal

- 4.1.- Seguridad en la definición de trabajo y recursos
- 4.2.- Entrenamiento del usuario
- 4.3.- Respuesta a los incidentes de seguridad y mal funcionamiento

5.- Seguridad Ambiental y Física

- 5.1.- Área segura
- 5.2.- Seguridad de los Equipos
- 5.3.- Controles Generales

6.- Gestión de la operación y las comunicaciones

- 6.1.- Responsabilidad y procedimiento de la operación
- 6.2.- Aceptación y planificación del sistema
- 6.3.- Protección contra el Software malicioso
- 6.4.- Administración interna
- 6.5.- Gestión de Red, Seguridad y manipulación de dispositivos.
- 6.6.- Intercambio de información y software

7.- Control de Acceso

- 7.1.- requisito del negocio para el control de acceso
- 7.2.- Gestión de acceso de usuario
- 7.3.- Responsabilidad del usuario
- 7.4.- control de acceso a la red
- 7.5.- control de acceso a la operación del sistema
- 7.6.- control de acceso a las aplicaciones
- 7.7.- monitoreo de uso y acceso al sistema
- 7.8.- control de acceso a computadores móviles y tele trabajo

SRB CHILE

Huerfanos 835
Oficina 2103, Santiago

SRB ARGENTINA

Av. Pueyrredon 538 PB 2do
Of. 5 C1032ABS Buenos Aires Nro. 562-238, Miami, FL

SRB USA

7831 NW 72 Avenue
Nro. 562-238, Miami, FL

Teléfonos: (+56 2) 956 3034 – 2437547

www.srb.cl info@srb.cl

8.- Desarrollo y mantenimiento del sistema

- 8.1.- requisito de la seguridad del sistema
- 8.2.- Control criptográfico
- 8.3.- Seguridad de los archivos del sistema
- 8.4.- Seguridad en los procesos de desarrollo y apoyo

9.- Gestión de la continuidad del negocio

- 9.1.- Manejo en los aspectos de la continuidad del negocio
- 9.2.- Análisis de externalidades positivas y negativas
- 9.3.- Análisis de Contingencia en todos los posibles escenarios.

10.- Cumplimiento

- 10.1.- Cumplimiento de los requisitos legales
- 10.2.- Revisión de la política de seguridad y cumplimiento técnico
- 10.3.- Consideraciones de auditoría del sistema
- 10.4.- Procesos continuos

SRB CHILE

Huerfanos 835
Oficina 2103, Santiago

SRB ARGENTINA

Av. Pueyrredon 538 PB 2do
Of. 5 C1032ABS Buenos Aires

SRB USA

7831 NW 72 Avenue
Nro. 562-238, Miami, FL

Teléfonos: (+56 2) 956 3034 – 2437547

www.srb.cl info@srb.cl