

Seminario



Las medidas de seguridad y la Protección de los Datos Personales

La implementación de medidas de seguridad en la óptica empresarial:

Silvia G. Iglesias

siglesias@itsb.com.ar

www.itsb.com.ar

Agenda

- ⇒ La Seguridad de la Información
- ⇒ Normas ISO que Exigen el cumplimiento de la Las Leyes de Protección de Datos Personales
- ⇒ ISO/IEC 27002/05 y 27002/05
- ⇒ La Disposición 11/06
- ⇒ Tips de Implementación

Seguridad de la Información

- Es una **Decisión Estratégica** que forma parte del aseguramiento de la **Calidad y la Continuidad de los Negocios**
- Es **Imprescindible** para una **correcta Planificación y Evaluación de Resultados**

Seguridad de la Información

Objetivo

- **La Confidencialidad**
- **La Integridad**
- **La Disponibilidad**

Comenzando por los Datos Personales

Working Draft 3 ISO 26000
[Core issues][Fundamental subjects] at a glance



Comenzando por los Datos Personales

- **6.7 Tema de consumidores**
- **6.7.8 Protección de la privacidad y de los datos de los consumidores**

- **OECD - Organization for Economic Co-operation and Development**
 - Guidelines for Multinational Enterprises: Review, 2000.
 - Guidelines for the Security of Information Systems and Networks: Towards a culture of security,
 - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
 - Recommendation on Dispute Resolution and Redress,

- **ISO/IEC 27001/05 y 27002/05**

Comenzando por los Datos Personales

- ISO/IEC 27001/05 y 27002/05
- 15.1 Cumplimiento de Requisitos Legales
- 15.1.4 Protección de los datos y privacidad de la información personal
- Objetivo de Control

Es conveniente que la protección y privacidad de los datos esté garantizada según se requiera en las legislaciones y regulaciones relevantes, y si es aplicable, en las cláusulas contractuales.

Las ISO/IEC 27001/05 y 27002/05

ISO/IEC 27001/05

**Sistema de Gestión de la
Seguridad de la Información**
*ALINEADA CON ISO 9000/00 Y
14000/05*

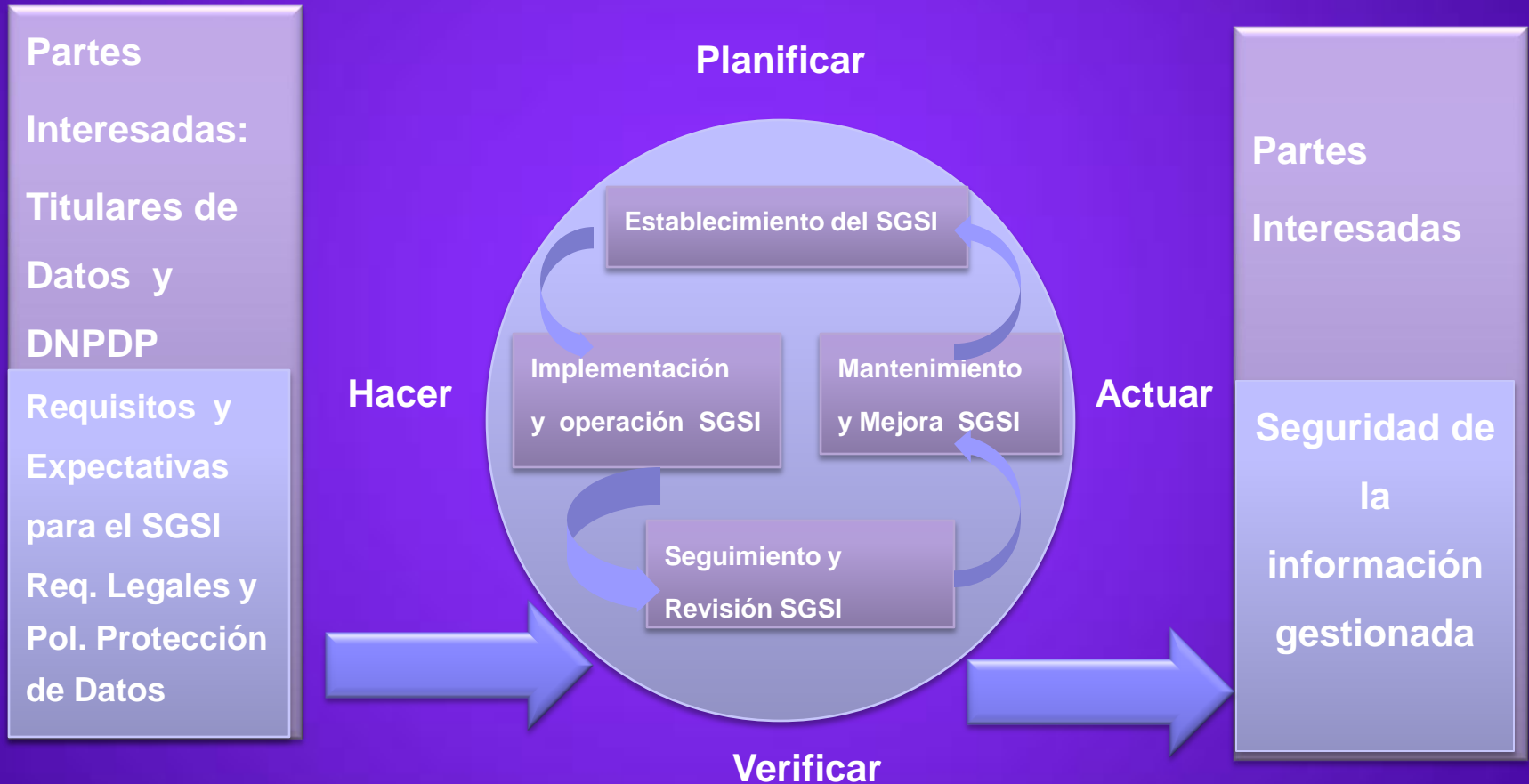
ISO/IEC 27002/05

**Guía de Buenas Prácticas en
Seguridad de la Información**
No se puede certificar

Características de la ISO/IEC 27001/05 - PDCA

Planificar (P) Establecer el SGSI	Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (D) Implementar y operar el SGSI	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (C) Hacer seguimiento y revisar el SGSI	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica del SGSI, y reportar los resultados a la dirección, para su revisión.
Actuar (A) Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección u otra información relevante, para lograr la mejora continua del SGSI.

Características de la ISO/IEC 27001/05 (PDCA) Aplicada al Hábeas Data



Contenido de la ISO/IEC 27002/05

- 1 Objeto
- 2 Términos y Definiciones
- 3 Estructura del Standard
- 4 Aseguramiento y tratamiento del Riesgo
- 5 Política de Seguridad
- 6 Organización de la Seguridad de la Información
- 7 Gestión del los Activos
- 8 Recursos Humanos

Contenido de la ISO/IEC 27002/05

- 9 Seguridad Física y Ambiental
- 10 Comunicación y Operación del Sistema de Seguridad
- 11 Control de Accesos
- 12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
- 13 Gestión de los Incidentes de Seguridad
- 14 Continuidad del Negocio
- 15 Cumplimientos Legales y Normativos

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Documento de Seguridad que contendrá:
Medidas de Seguridad de Nivel Básico

- Funciones y obligaciones del personal. Organización de la Seguridad en ISO/IEC 27001/05 y 27002/5
- Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan. Adquisición, Desarrollo y Mantenimiento de los Sistemas ISO/IEC 27001/05 y 27002/05
- Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Adquisición, Desarrollo y Mantenimiento de los Sistemas ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Básico

- Registros de incidentes de seguridad, su gestión y respuesta. Gestión de los Incidentes de Seguridad ISO/IEC 27001/05 y 27002/05
- Procedimientos para efectuar las copias de respaldo y de recuperación de datos. Gestión de las Operaciones y las Comunicaciones ISO/IEC 27001/05 y 27002/05
- Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso. Control de Accesos ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Básico

- Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información. Control de Accesos ISO/IEC 27001/05 y 27002/05
- Control de acceso de usuarios a datos. Control de Accesos ISO/IEC 27001/05 y 27002/05
- Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) Gestión de Comunicaciones y Operaciones ISO/IEC 2001/05 y 27002/05
- Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal Gestión de Comunicaciones y Operaciones ISO/IEC 2001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Medio

- Deberá nombrarse un Responsable (u órgano específico) de Seguridad. Organización de la Seguridad en ISO/IEC 27001/05 y 27002/5
- Realización de Auditorías (internas o externas) Cumplimiento ISO/IEC 27001/05 y 27002/05
- Los informes de Auditoría son para el Responsable del Archivo. La DNPDP deberá considerarlo obligatoriamente, con carácter no vinculante Organización de la Seguridad ISO/IEC 27001/05 y 27002/05
- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Control de Accesos ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Medio

- Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal. Control de Accesos y Protección Física y Ambiental ISO/IEC 27001/05 y 27002/05
- Gestión de Soportes e información contenida en ellos:
 - Registro de entradas y salidas. Control de Accesos ISO/IEC 27001/05 y 27002/05
 - Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida o transferida para back up o guarda. Gestión de las Comunicaciones y las Operaciones ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Medio

- Deberá disponerse de un procedimiento de recuperación de la información de respaldo y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales. Gestión de las Comunicaciones y las Operaciones y Gestión de los Incidentes de Seguridad ISO/IEC 27001/05 y 27002/05
- Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Gestión de las Comunicaciones y las Operaciones y Gestión de los Incidentes de Seguridad ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Medio

- Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Crítico

- En la distribución de soportes se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte. Gestión de las Comunicaciones y las Operaciones ISO/IEC 27001/05 y 27002/05
- Los Registro de accesos deberá disponer que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo por el término de un TRES (3) años. Control de Accesos ISO/IEC 27001/05 y 27002/05

Ley 25.326 de Hábeas Data

Normativa de Seguridad

Medidas de Seguridad de Nivel Crítico

- Las Copias de Respaldo deberán tener un resguardo externo, situado fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales. Protección Física y Ambiental y Gestión de las Comunicaciones y las Operaciones ISO/IEC 27001/05 y 27002/05
- En la Transmisión de datos, los mismos deberán cifrarse previamente o utilizar cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas. Gestión de las Comunicaciones y las Operaciones ISO/IEC 27001/05 y 27002/05)

Tips para la Implementación

Recursos Humanos:

Capacitación en Protección de Datos

Cultura en Protección de Datos

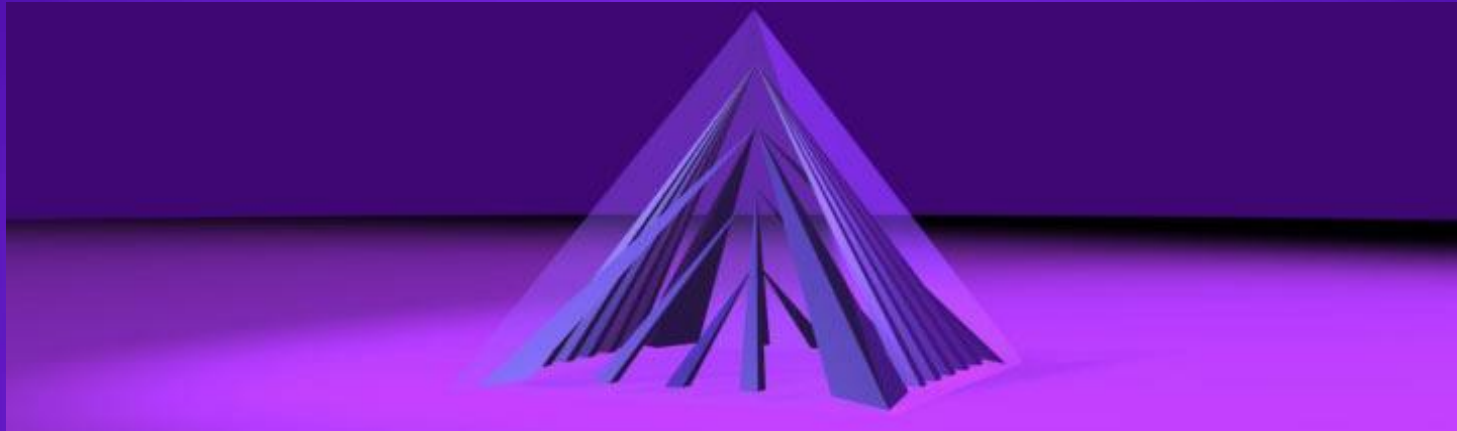
Política de cumplimiento

Identificación de los Circuitos de Traslado y Transferencia de Datos

Diseño adecuado del circuito

Resguardo de los Datos en Papel

Identificación de las tareas tercerizadas



Muchas Gracias por su participación

Consultas a

Silvia Iglesias

siglesias@itsb.com.ar

www.drasilviaiglesias.blogspot.com