IMPLANTACIÓN DEL ISO 27001:2005 "SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN"

Alberto G. Alexander, Ph.D, CBCP
Auditor Sistemas de Gestión de Seguridad de Información
Certificado IRCA (International Registered of Certified Auditors)

E-mail: aalexan@pucp.edu.pe
www.centrum.pucp.edu.pe/excelncia

CENTRUM
CENTRO DE NEGOCIOS
Pontificia Universidad Católica del Perú

¿Su base de datos está protegida de manos criminales?

¿Cuánto pagaría la competencia por su información confidencial?

¿Su empresa tiene un plan para continuar operando después de un desastre?

¿Se tiene una política formal y se han adoptado controles adecuados para protección contra los riesgos del uso de telecomunicaciones móviles?

¿Se tienen procedimientos y controles para protección de software maliciosos?

¿Los activos de su empresa han sido inventariados y tasados?

INFORMACIÓN EN LA EMPRESA

Un reciente reporte del House Banking Committee de Estados Unidos, muestra que el sector financiero perdió 2.4 billones de dólares por ataques computarizados en 1998 –más del triple que en 1996. No es sorprendente, considerando que por día se transfieren electrónicamente 2 trillones de dólares, mucho de lo cual pasa a través de líneas que según el FBI no son muy seguras. (Fortune 500, 2003).

Casi el 80% de los valores intelectuales de las corporaciones son electrónicos, de acuerdo a la Cámara de Comercio estadounidense, y un competidor puede subir hasta las nubes si roba secretos comerciales y listas de clientes. (Sloan Review, 2003).

Los hackers son expertos en ingeniería social –consiguiendo personas de dentro de las compañías para sacarles contraseñas y claves de invitados. “Si te levantas a la secretaria ganaste, dice Dill Dog”. (Famoso hacker).

INFORMACIÓN EN LA EMPRESA

El fraude celular no escapa a ninguna compañía telefónica en el mundo. Telcel y Movilnet en el caso de Venezuela afirman que en el año 1997 las pérdidas por concepto de clonación se ubicaaron en 1,800 millones de dólares, lo que los ha impulsado a mejorar su sistema de gestión de seguridad de información.

La clonación ocurre cuando los “clonadores” capturan la transmisión de los números de identificación (ESN: número asignado), bien sea rastreando los datos o sobornando a un empleado de la operadora y la copian en otros equipos no autorizados.

(Cielorojo/computación 19/01/04).

INFORMACIÓN EN LA EMPRESA

La información en la empresa es uno de los más importantes activos que se poseen.

Las organizaciones tienen que desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información.

La información está sujeta a muchas amenazas, tanto de índole interna como externa.

¿Qué tan VULNERABLE es la información en su organización?

ISO 27001:2005 SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

El nuevo estándar internacional, el ISO 27001:2005, está orientado a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas.

HISTORIA DEL ESTÁNDAR BS 7799 E ISO 17799

- Grupo de trabajo de la industria se establece en 1993
- Código de práctica - 1993
- British standard - 1995
- BS 7799 parte 2 - 1998
- BS 7799 parte 1 - 1998
- BS 7799 parte 1 y parte 2 revisada en 1999
- BS / ISO / IEC – 17799 - 2000

ISO 27001:2005- SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

ISO / IEC 17799 : 2005

- Código de práctica de seguridad en la gestión de la información – Basado en BS 7799 – 1 : 2000.
- .Recomendaciones para buenas prácticas
- No puede ser utilizado para certificación

ISO 27001:2005

- Especificación para la gestión del sistema de seguridad de información
- .Es utilizado para la certificación

INFORMACIÓN

“La información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente”.

ISO 17799:2005

¿QUÉ ES SEGURIDAD DE INFORMACIÓN?

Seguridad de información es mucho más que establecer “firewalls”, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar en la bóveda los “backups”.

Seguridad de información es determinar qué requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo.

La seguridad de información se caracteriza por la preservación de:

a) **CONFIDENCIALIDAD** : La información está protegida de personas no autorizadas.

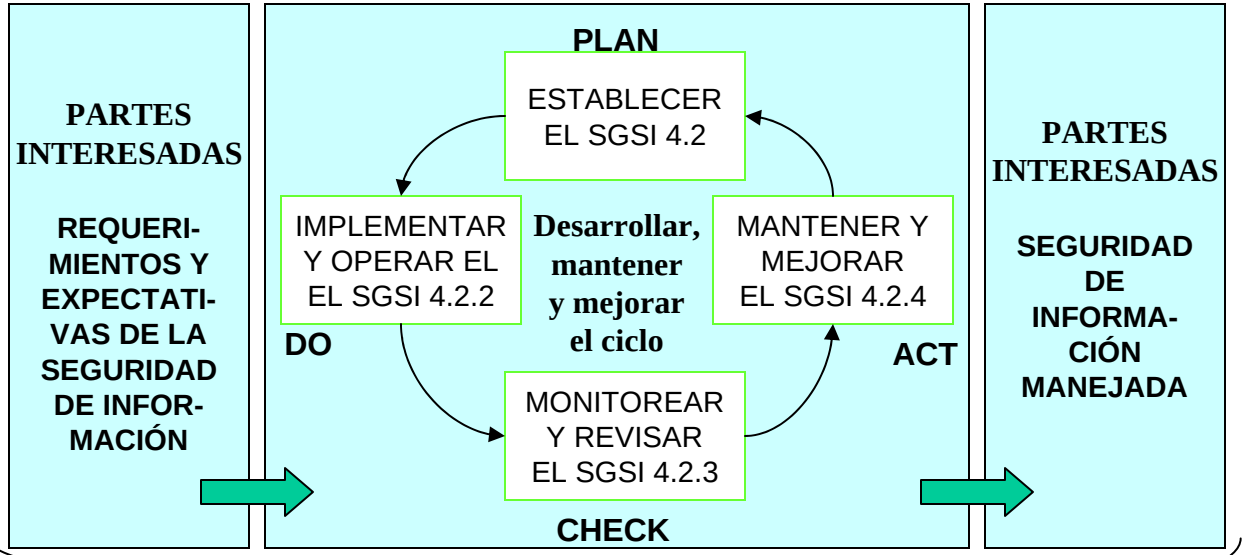
b) **INTEGRIDAD** : La información está como se pretende, sin modificaciones inapropiadas.

c) **DISPONIBILIDAD** : Los usuarios tienen acceso a la información y a los activos asociados cuando lo requieran.

NATURALEZA Y DINÁMICA DEL ISO 27001:2005

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

MODELO PDCA APLICADO A LOS PROCESOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN SGSI



4.3 Requerimientos de documentación
- 4.3.2 Control de documentos
- 4.3.3 Control de registros

5.0 Responsabilidad de la gerencia
- 5.1 Compromiso de la gerencia
- 5.2 Gestión de recursos
  - 5.2.1 Provisión de recursos
  - 5.2.2 Capacitación, conocimiento y capacidad

6.0 Revisión gerencial
- 6.4 Auditorias internas

7.0 Mejoramiento del SGSI
- 7.1 Mejoramiento continuo
- 7.2 Acción correctiva
- 7.3 Acción preventiva

HOJA DE RUTA PARA CUMPLIR CON EL ISO 27001:2005

CLÁUSULAS	ACTIVIDADES ORGANIZACIONALES
Establecer el SGSI (Sección 4.2.1)	a) Definir el alcance del SGSI b) Definir un sistemático enfoque para evaluación del riesgo c) Identificar el riesgo d) Evaluar el riesgo e) Definir política SGSI f) Identificar y evaluar opciones para el tratamien-to del riesgo g) Seleccionar objetivos de control y controles h) Preparar un enunciado de aplicabilidad i) Obtener aprobación de la gerencia

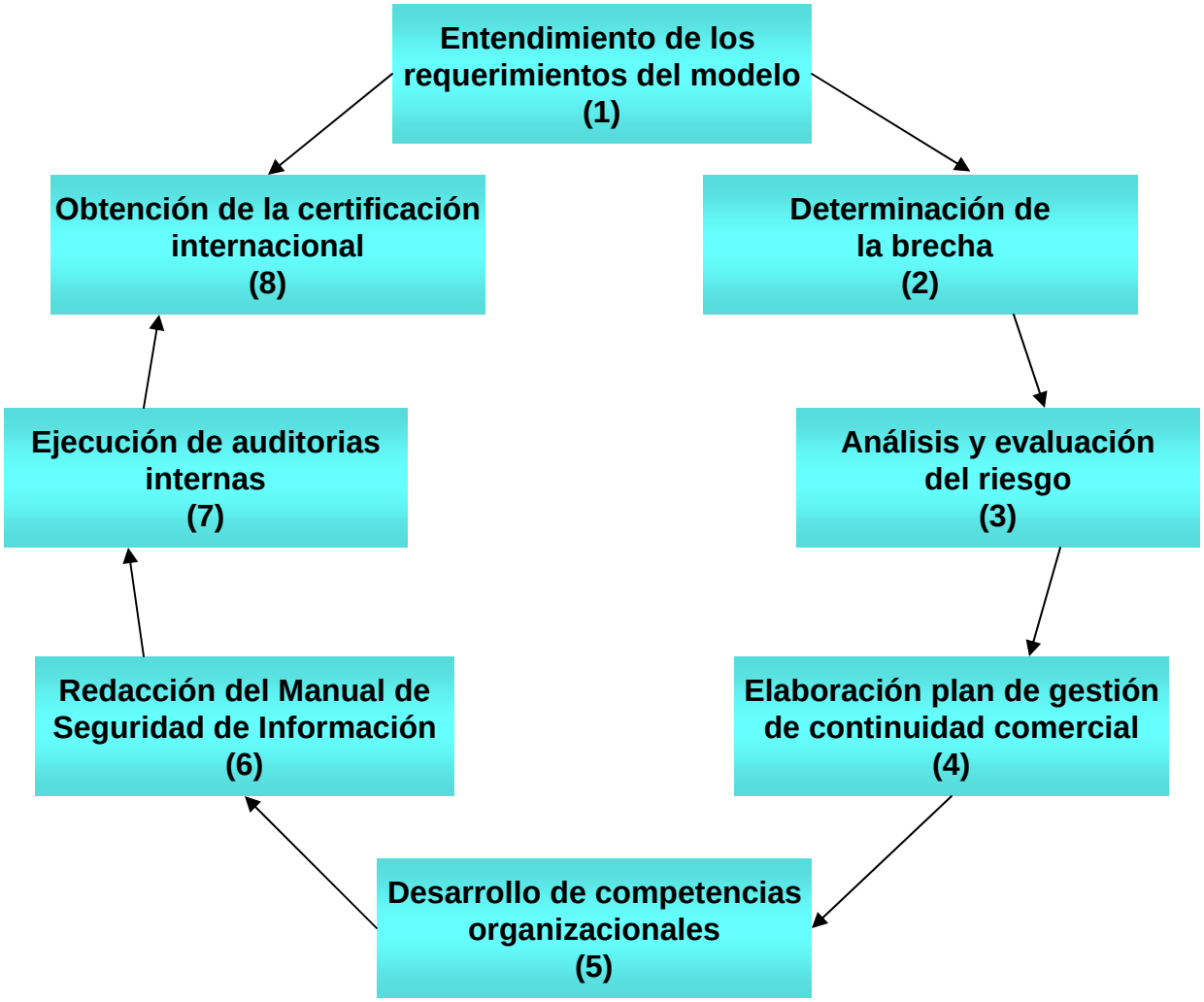
HOJA DE RUTA PARA CUMPLIR CON EL BS 7799-2:2002

CLÁUSULAS	ACTIVIDADES ORGANIZACIONALES
Implementar y operar el SGSI **(Sección 4.2.2)**	a) Formular un plan para tratamiento del riesgo b) Implementar el plan de tratamiento del riesgo c) Implementar todos los objetivos de control y controles seleccionados d) Implementar programa de entrenamiento y toma de conciencia e) Gestionar operaciones f) Gestionar recursos

HOJA DE RUTA PARA CUMPLIR CON EL ISO 27001:2005

CLÁUSULAS	ACTIVIDADES ORGANIZACIONALES
Monitorear y revisar el SGSI **(Sección 4.2.3)**	a) Ejecutar procedimientos de monitoreo b) Efectuar revisiones regulares de la eficacia del SGSI c) Revisar el nivel del riesgo residual y del riesgo aceptable d) Conducir las auditorias internas del SGSI e) Registrar todos los eventos que tienen un efecto en el desempeño del SGSI
Mantener y mejorar el SGSI **(Sección 4.2.4)**	a) Implementar las mejoras identificadas b) Tomar apropiadas acciones correctivas y preventivas c) Comunicar los resultados a todas las partes interesadas d) Asegurar que las mejoras alcancen los objetivos deseados

CICLO METODOLÓ-GICO PARA LA IMPLANTACIÓN DEL MODELO ISO 27001:2000



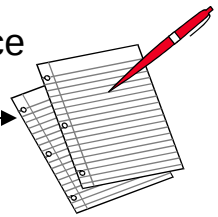
METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ISO 27001:2005

PASO I

Entendimiento de los requerimientos del modelo

Taller estratégico con la gerencia para analizar requerimientos del modelo ISO 27001:2005

Definir alcance del modelo

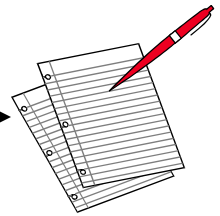


PASO II

Determinación de la brecha

Efectuar "Gap Analysis"

Informe a la gerencia



Determinar la brecha y estimar presupuesto y cronograma

METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ISO 27001:2005

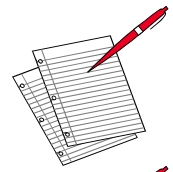
PASO III

Análisis y evaluación del riesgo

-Amenazas,
-Vulnerabilidades
-Impactos

Efectuar un análisis y evaluación del riesgo → Evaluación del riesgo

Política de seguridad → Política documentada



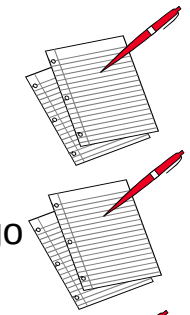
PASO IV

Elaboración Plan de gestión de continuidad comercial

Plan de continuidad comercial del negocio → Plan de continuidad comercial documentado

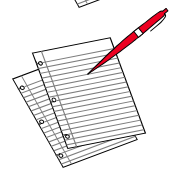
Enfoque de la gerencia para tratar el riesgo

Gerencia del riesgo → Plan de tratamiento del riesgo



Utilización de Anexo A de la norma

Seleccionar controles y objetivos de control a implantar → Tabla de controles



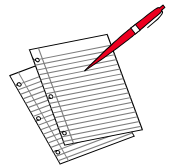
METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ISO 27001:2005

PASO V

Desarrollo de competencias organizacionales

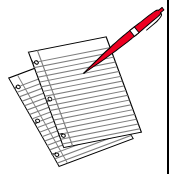
Enunciado de aplicabilidad →

Elaborar un enunciado de aplicabilidad → Enunciado de aplicabilidad documentado

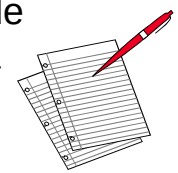


Entrenamiento en documentación de procedimientos, instruc-ciones de trabajo

Taller estratégico para manejo de la acción correctiva y preventiva → Procedimiento para manejo de la acción correctiva



Taller estratégico para el manejo de la auditoria interna → Procedimiento de auditoria interna documentado



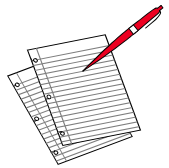
METODOLOGÍA DETALLADA PARA IMPLANTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ISO 27001:2005

PASO VI

Redacción del manual de Seguridad de Información

Elaboración del manual de seguridad de información

Manual de Seguridad de Información Documentado

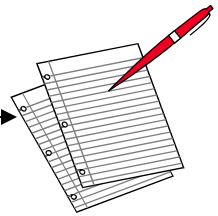


PASO VII

Ejecución de Auditorias Internas

Efectuar auditoria interna

Informe de la auditoria interna

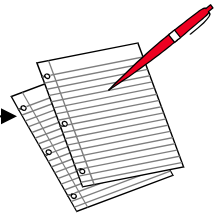


PASO VIII

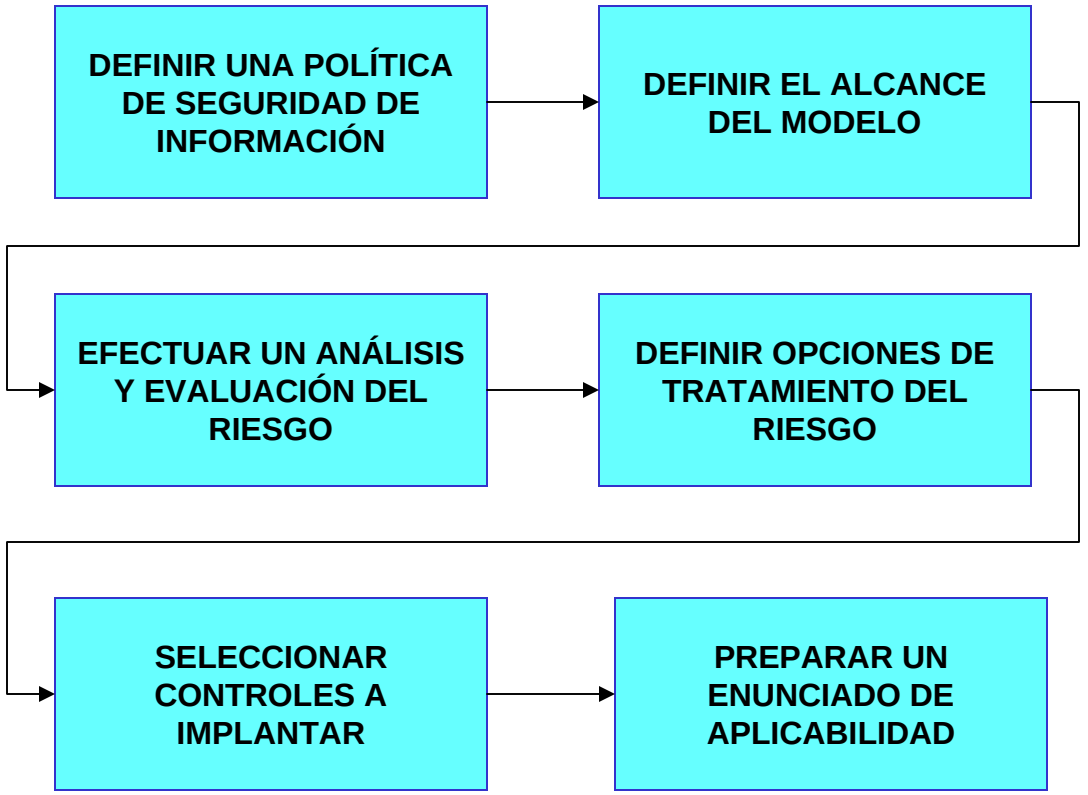
Obtención de la certificación internacional

Auditoria de empresa certificadora

Entrega de informe



ENFOQUE DE LAS SEIS FASES ESENCIALES DEL PROCESO DE IMPLANTACIÓN ISO 27001:2005



CASO PRÁCTICO DE IMPLANTACIÓN DEL ISO 27001:2005 EN UNA ORGANIZACIÓN FINANCIERA

ÁREA: AHORROS-CAPTACIONES

DEFINICIÓN DEL ALCANCE DEL MODELO EN EL BANCO

En la sección 4.2 (a) del estándar, se exige como punto de partida para establecer el SGSI que la empresa: “defina el alcance del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología”.

IDENTIFICA-CIÓN DE ACTIVOS DE INFORMACIÓN

Una vez determinado el alcance del modelo en la empresa, se debe proceder a identificar los distintos activos de información, los cuales se convierten en el eje principal del modelo.

Es importante mencionar que, en el caso del banco, se conformó un grupo multidisciplinario, compuesto por los dueños de los subprocesos que conformaban el proceso escogido en el alcance. También en el grupo se incluyó a los clientes vitales y proveedores internos de ahorros/captaciones. Posteriormente, una vez identificados los activos de información, se incluyeron en el grupo a los dueños de los activos de información. Al grupo multidisciplinario, se le denominó comité gestor.

ANÁLISIS Y EVALUACIÓN DEL RIESGO

A los activos de información se les debe efectuar un análisis y evaluación del riesgo, e identificar los controles del anexo A del estándar que tendrán que implementarse para mitigar el riesgo.

Es importante en este punto, clarificar qué es un activo de información en el contexto del ISO 27001:2005. Según el ISO 17799:2005 (Código de Práctica para la Gestión de Seguridad de Información) un activo de información es: "algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

ANÁLISIS Y EVALUACIÓN DEL RIESGO

Los activos de información son clasificados por el ISO 17799:2005 en las siguientes categorías:

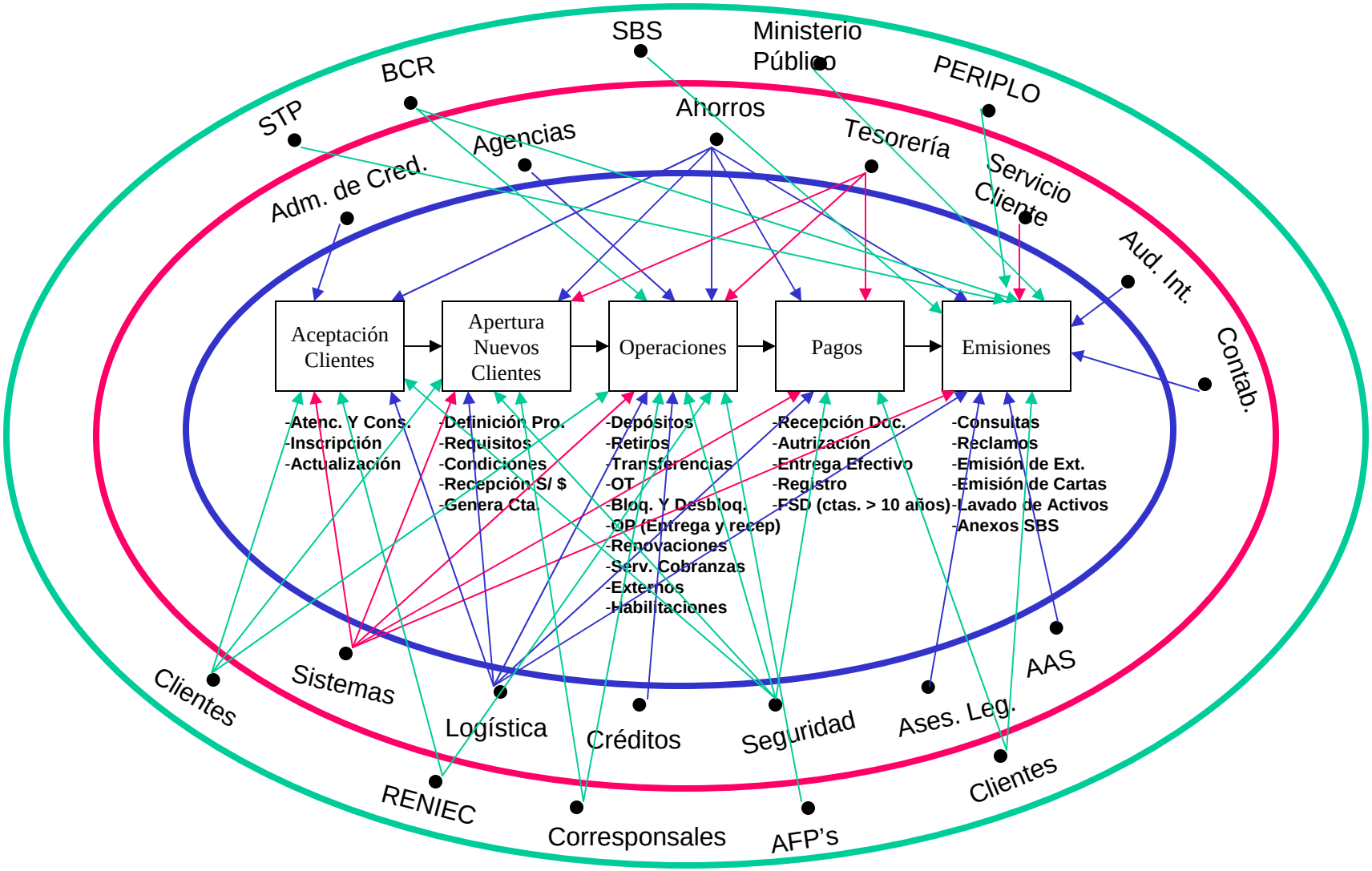
-**Activos de información (datos, manuales, usuarios, etc.)**
-**Documentos de papel (contratos)**
-**Activos de software (aplicación, software de sistemas, etc.)**
-**Activos físicos (computadoras, medios magnéticos, etc.)**
-**Personal (clientes, personal)**
-**Imagen de la compañía y reputación**
-**Servicios (comunicaciones, etc.)**

ALCANCE DEL SGSI

Al establecer el alcance, en la organización financiera se determinó que fuera el área de ahorros y captaciones.

Para dicho efecto, se utilizó el método de las elipses para determinar los activos de información.

AHORROS CAPTACIONES



TASACIÓN DE ACTIVOS DE INFORMACIÓN

ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
- Base de datos ahorros	4	4	4	4
- Base de datos clientes	5	5	4	5
- Equipo de cómputo	2	2	4	2
- Línea dedicada	2	2	5	3
- Internet	2	1	3	2
- Servidor de archivos	5	5	4	5
- Servidor	5	4	4	4
- Copias de backup	5	5	3	4
- Switchers	1	1	5	2
- Router's	1	1	5	2
- Modem	1	1	5	2
- Líneas telefónicas	4	2	3	3
- Central telefónica	4	2	3	3
- Disco duro	5	5	3	4
- Cámaras de video	1	1	5	2
- Teléfonos	4	1	3	3

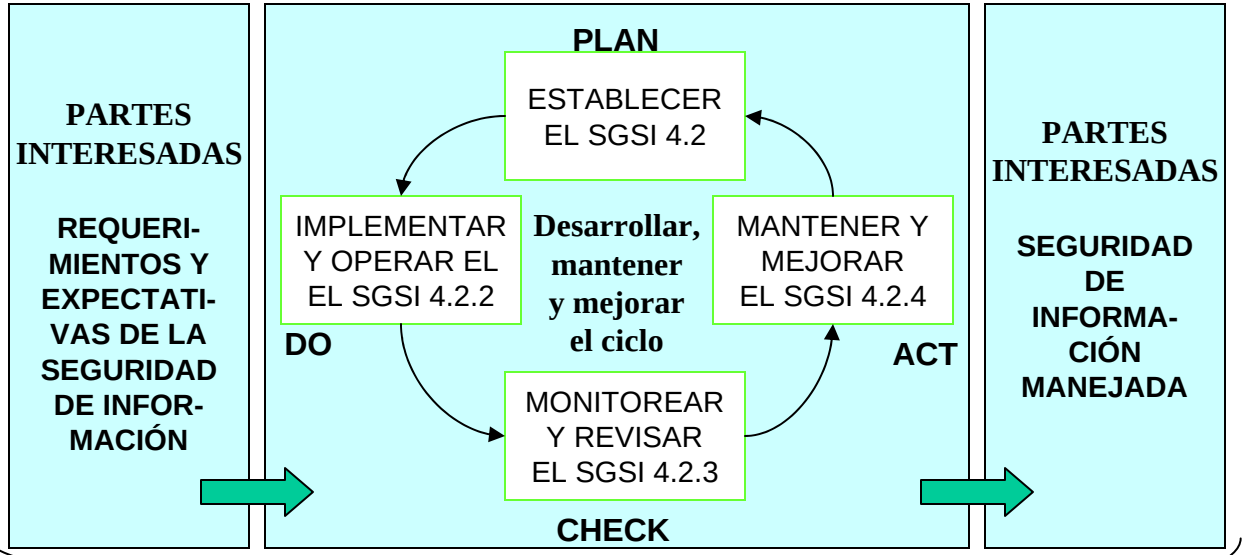
DISTRIBUCIÓN DE ACTIVOS Y SUS PROPIETARIOS

ACTIVOS DE INFORMACIÓN	PROPIETARIOS
1. BASE DE DATOS CLIENTES	SERVICIO AL CLIENTE
2. SERVIDOR	SISTEMAS
3. JEFE DE AHORROS	AHORROS
4. BASE DE DATOS AHORROS	SISTEMAS
5. CLAVES	AHORROS
6. SERVIDOR DE ARCHIVOS	SISTEMAS
7. COPIAS DE BACKUP	SISTEMAS
8. DISCO DURO Y GRAB. (Videos)	SISTEMAS
9. REGISTROS DE CLIENTES	AHORROS
10. FORMATOS	AHORROS
11. VOUCHER'S	ADM. DE CRÉDITOS
12. FORMATO LAVADO ACTIVOS	AHORROS

ANÁLISIS Y EVALUACIÓN DEL RIESGO

ACTIVOS DE INFORMACIÓN	AMENAZAS	POSIBILIDAD OCURRENCIA	VULNERABILIDADES	POSIBILIDAD QUE AMENAZA PENETRE VULNERABILIDAD	VALOR DE ACTIVOS DE RIESGOS	POSIBILIDAD DE OCURRENCIA DE AMENAZA	TOTAL	CRITICIDAD	CRITERIO PARA ACEPTAR EL RIESGO	OBJETIVOS DE CONTROL	CONTROLES	NIVELES DE ACEPTACION DEL RIESGO
1. BASE DE DATOS AHORROS	- Hckers - Deterioro fisico	2 4	- Falta de antivirus - Libre acceso	2 5	4	4	16	C	- Verificación semanal de actualizaciones - El sistema permite control automático de incidentes	A.5.1 Promocionar dirección gerencial y apoyo a la S.I. A.6.1 Seguridad del equipo: evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades comerciales. A.6.2 Proteger la integridad del software y la información del daño de software malicioso. A.7.1Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	A.5.1.1 A.5.1.2 A.7.2.4 A.6.2.1 A.7.1.1 A.7.1.2	
2. SERVIDOR	- Virus - Rayos	2 4	- Software desactualizado - Falta para rayos	3 4	4	4	16	C	- Parches de software - Verificación semanal de actualizaciones.	A.9.2. Proteger la integridad del software y la información del daño de software malicioso.	A.9.2.1	
3. BASE DE DATOS CLIENTES	- Errores en digitación	4	- Mala programación - Mala validación y pruebas	2 5	5	4	20	C	- Verificación diaria de actualizaciones - El sistema permite registro e impresión de incidentes - Parches de software	A.9.2 Minimizar el riesgo de fallas en los sistemas. A.10.1 Asegurar que se incorpore seguridad en los sistemas de información. A.10.2 Evitar la pérdida, modificación o mal uso de la data del usuario en los sistemas de información. A.10.3 Asegurar que los proyectos T.I. y las actividades de apoyo se reducen de manera segura.	A.9.2.1 A.9.2.2 A.10.1.1 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.1 A.10.3.3	

MODELO PDCA APLICADO A LOS PROCESOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN SGSI



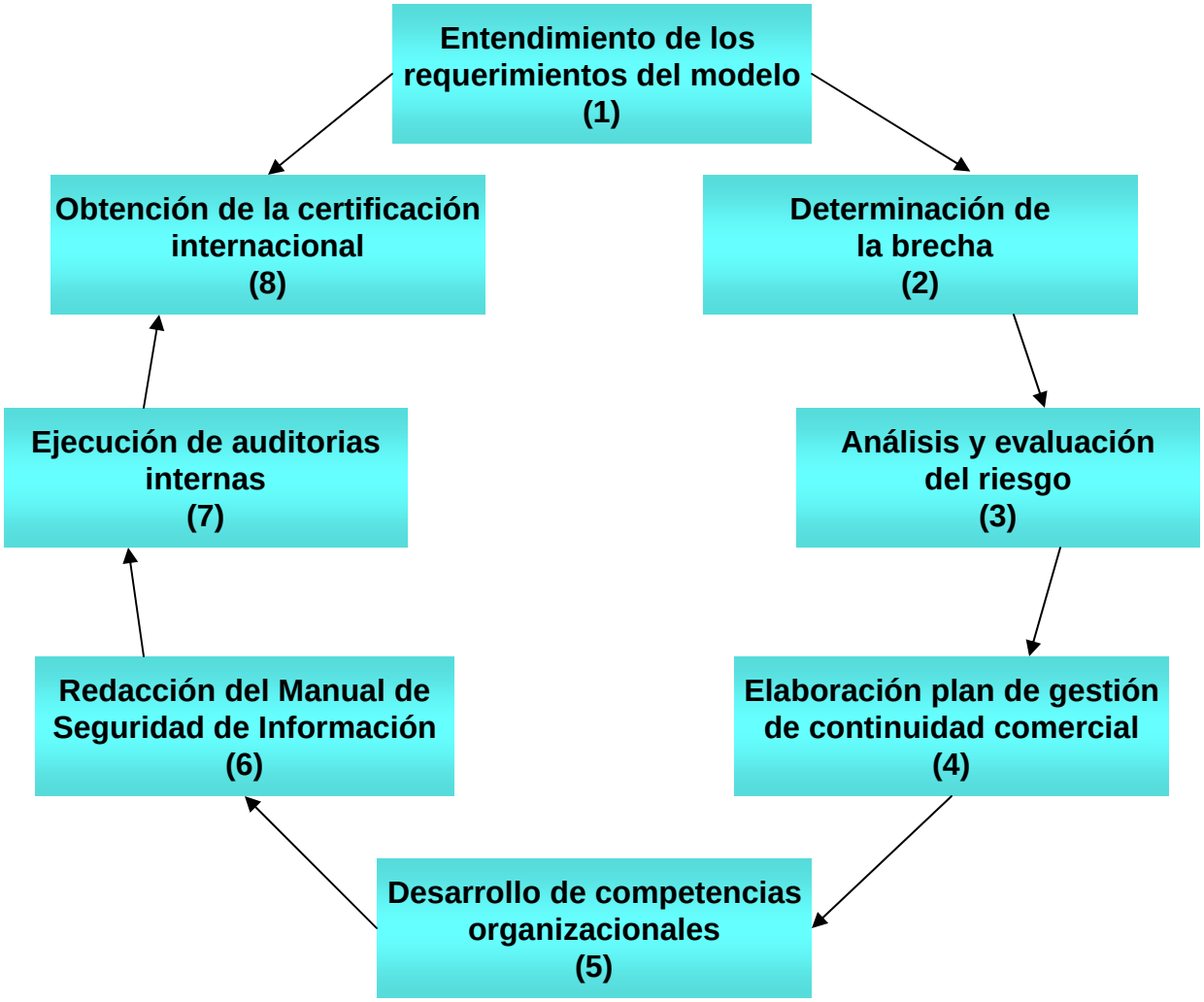
4.3 Requerimientos de documentación
- 4.3.2 Control de documentos
- 4.3.3 Control de registros

5.0 Responsabilidad de la gerencia
- 5.1 Compromiso de la gerencia
- 5.2 Gestión de recursos
  - 5.2.1 Provisión de recursos
  - 5.2.2 Capacitación, conocimiento y capacidad

6.0 Revisión gerencial
- 6.4 Auditorias internas

7.0 Mejoramiento del SGSI
- 7.1 Mejoramiento continuo
- 7.2 Acción correctiva
- 7.3 Acción preventiva

CICLO METODOLÓ-GICO PARA LA IMPLANTACIÓN DEL MODELO ISO 27001:2005



RESULTADOS DEL COMPUTER CRIME AND SECURITY SURVEY/ FBI 2005

-**Los ataques de virus continúan como la principal fuente de grandes pérdidas financieras.**
-**El uso no autorizado de sistemas de computación ha incrementado.**
-**Los incidentes en los web sites han aumentado dramáticamente.**
-**El outsourcing de actividades de seguridad de información no ha crecido.**
-**87% de los encuestados conducen auditorias de seguridad.**
-**La mayoría de empresas ven el entrenamiento al usuario como algo muy importante.**

VISA ACCOUNT INFORMATION SECURITY STANDARDS

Los 15 requerimientos son una lista de chequeo para lograr conformidad con el estándar.

1. **Establecer política para la contratación de personal.**
2. **Restringir acceso a datos.**
3. **Asignar al personal un sistema de identificación único para ser validado al acceder a datos.**
4. **Controlar el acceso a datos.**
5. **Instalar y mantener un “firewall” network si los datos son accedidos desde la internet.**
6. **Encriptar datos mantenidos en bases de datos.**
7. **Encriptar datos enviados a través de redes.**
8. **Proteger sistemas y datos de virus.**

VISA ACCOUNT INFORMATION SECURITY STANDARDS

9. Mantener al día los parches a software
10. No utilizar “passwords” para sistemas y otros parámetros de seguridad proporcionado por terceros.
11. No dejar desatendidos computadoras, diskettes con datos.
12. De manera segura, destruir datos cuando ya no son necesarios.
13. De manera regular verificar el desempeño de sistemas y procedimientos.
14. Inmediatamente investigar y reportar a VISA cualquier perdida de cuentas o información de las transacciones.
15. Utilizar sólo proveedores de servicios que cumplan estos requisitos

IMPLANTACIÓN DEL ISO 27001:2005 "SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN"

Alberto G. Alexander, Ph.D, CBCP
Auditor Sistemas de Gestión de Seguridad de Información
Certificado IRCA (International Registered of Certified Auditors)

E-mail: alexand@terra.com.pe

CENTRUM
CENTRO DE NEGOCIOS
Pontificia Universidad Católica del Perú