Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca
Aplicación del ISO 27001:2005

Por

Alberto G. Alexander, Ph.D.
Director Centro para la Excelencia Empresarial
www.centrum.pucp.edu.pe/excelencia
aalexan@pucp.edu.pe

Las organizaciones hoy en día, con la sofisticación tecnológica y la complejidad en el manejo de información, enfrentan distintas amenazas que muchas veces explotan sus vulnerabilidades. El riesgo esta siempre presente. La confidencialidad, integridad y disponibilidad de la información en la empresa, es fundamental para el aumento de la competitividad de la firma. Las organizaciones están obligadas si desean continuar operando, de instaurar "Sistemas de Gestión de Seguridad de Información" que permitan asegurar que tienen identificados sus activos vitales de información, que han determinado de manera sistemática que activos son los de riesgo y puedan con precisión instituir los controles pertinentes.
En el presente ensayo, se utiliza un caso real en la Banca Latinoamericana. Se detallan los pasos metodológicos seguidos para identificar el alcance para establecer el estándar ISO 27001:2005 en el proceso de "cuentas corrientes". Seguidamente se presentan los pasos para efectuar el "análisis y evaluación del riesgo" en el referido proceso.

INTRODUCCIÓN

La experiencia en implantar el modelo de gestión de seguridad de información (SGSI), se desarrolló en un Banco Comercial ubicado en la capital de un país latinoamericano. La institución en el momento de implantar el modelo estaba considerada por sus captaciones como el tercer Banco del país. Su fortaleza estaba en la banca comercial.

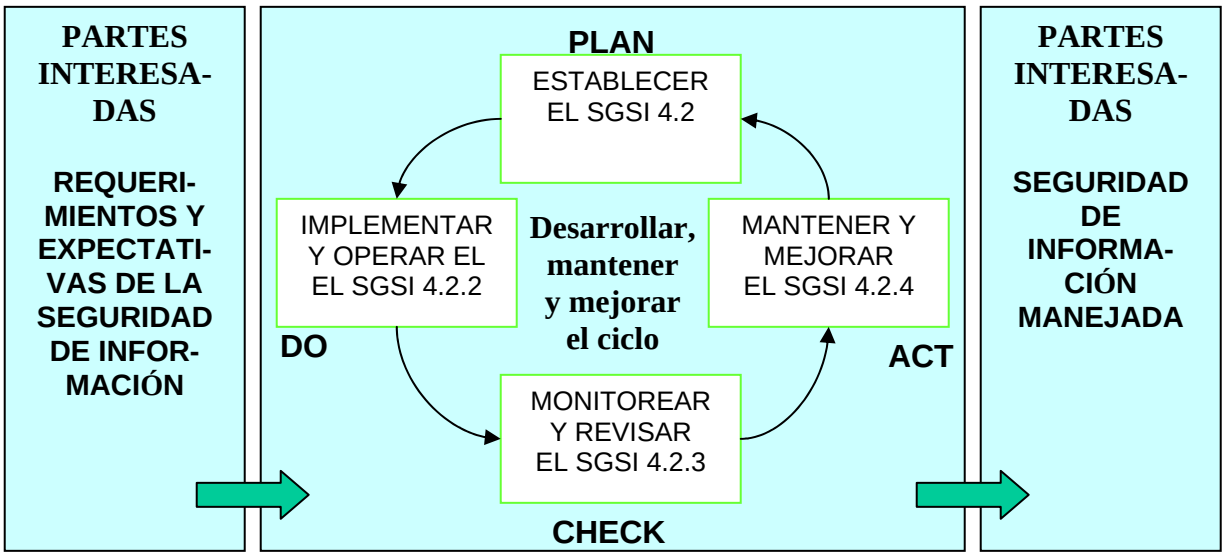
La alta gerencia del Banco, ante el aumento de fraudes y riesgos en el manejo de la información en la mayoría de sus procesos, decidió la implantación del SGSI ISO 27001:2005. Se decidió implantar el modelo, por razones estratégicas, en el proceso de "cuentas corrientes".

NATURALEZA DEL SGSI BS 7799-2:2002

El estándar ISO 27001:2005, es parte del sistema de gestión de la organización. Esta basado en un enfoque de riesgos del negocio., para establecer, implantar, operar, monitorear, mantener y mejorar la seguridad de información. El sistema de gestión incluye, estructura organizacional, políticas, planeación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

Para implantar el modelo, la empresa debe determinar su alcance. La amplitud del modelo puede variar según la conveniencia de la empresa. Se puede aplicar a toda la firma o a algún proceso en particular, cubriendo los activos relevantes de información, sistemas, aplicaciones, servicios, redes y tecnologías usadas para procesar, almacenar y comunicar información.
El ISO 27001:2005, específica los requerimientos para establecer, implantar, operar, monitorear y mejorar un SGSI documentado, dentro del contextote de los riesgos de una organización. El modelo específica los requerimientos para la implantación de controles de seguridad confeccionados a las necesidades individuales de una organización, o partes de ella.
En la figura N° 1, se tiene una representación gráfica de los componentes del estándar. Esta basado en el célebre “modelo shewhart” el cual fue popularizado por el Dr. Deming.

Figura N° 1
Modelo Sistema de Gestión de Seguridad de Información



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."

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 "cuentas corrientes". 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".

A los activos de información, se les debe efectuar una 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."

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

- Activos de información (datos, manuales de usuario, 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..)

Como se aprecia, los activos de información son muy amplios. Es fundamental estar conceptualmente claros qué es un activo de información y conocer sus distintas posibles

modalidades, para así poder realizar un correcto análisis y evaluación del riesgo y poder por lo tanto, establecer adecuadamente el modelo ISO 27001:2005.

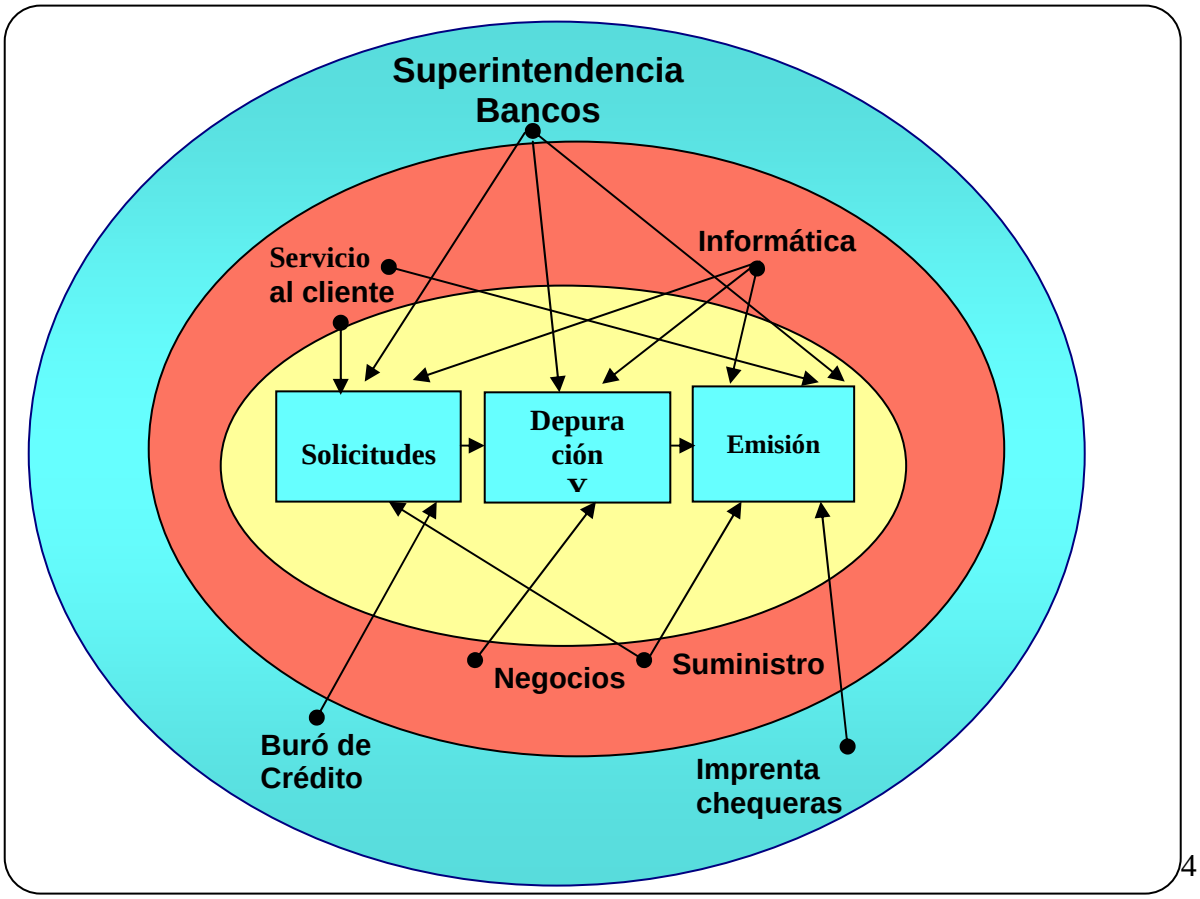
Al determinar el alcance, tal como se hizo en el caso del Banco, que se decidió que fuera el proceso de "cuentas corrientes", es recomendable utilizar el método de las elipses. Con lo cual se trata de visualizar con mucha precisión los distintos subprocesos que componen el alcance. Esto se determina en la elipse concéntrica. (Ver figura N°2) Los procesos básicos que componen el proceso de "cuentas corrientes" son: **(1)** solicitudes, **(2)** depuración**, (3)** emisión. El paso a seguir sería el de determinar con los usuarios y dueños de esos procesos ¿cuáles son los activos de información vitales?.

El segundo paso en la metodología, es el de identificar en la elipse intermedia las distintas interacciones que los subprocesos de la elipse concéntrica, tienen con otros procesos de la organización. Seguidamente, también se deben identificar con los dueños de esos procesos, los activos de información involucrados en las interacciones con la elipse concéntrica. Las flechas indican las interacciones.

En la elipse externa, se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse concéntrica. Las flechas indican la interacción. Aquí también se deben identificar los distintos tipos de activos de información, con miras a averiguar el tipo de memorando de entendimiento que existe o debiera de elaborarse así como los contratos existentes y los grados de acuerdos necesarios.

La metodología de las elipses, es un método sencillo que permite identificar los distintos tipos de activos de información existentes dentro del alcance del modelo.

Figura N°2
Metodología de las Elipses



ANÁLISIS Y EVALUACIÓN DEL RIESGO

Una vez identificados todos los activos de información comprendidos en el alcance, utilizando la metodología de las elipses, se procede a establecer el SGSI, siguiendo las pautas del estándar ISO 27001:2005 en su sección 4.2.1. En esencia lo que se exige es efectuar de manera disciplinada y sistemática un análisis y evaluación del riesgo de los activos identificados para determinar cuales son aquellos que deben ser protegidos para mitigar su riesgo, así como definir también cual es el riesgo residual (el riesgo con el cual la empresa esta decidida a convivir)
En la figura N° 3 se pormenorizan los pasos metodológicos que se siguieron en el Banco para realizar el análisis y evaluación del riesgo, de los activos de información, del proceso de "cuentas corrientes" para cumplir con las exigencias del ISIO 27001:2005.

A continuación se hará una descripción de los pasos seguidos para el manejo de la metodología para el análisis y evaluación del riesgo.

Figura N°3
Metodología para el Análisis y Evaluación del Riesgo

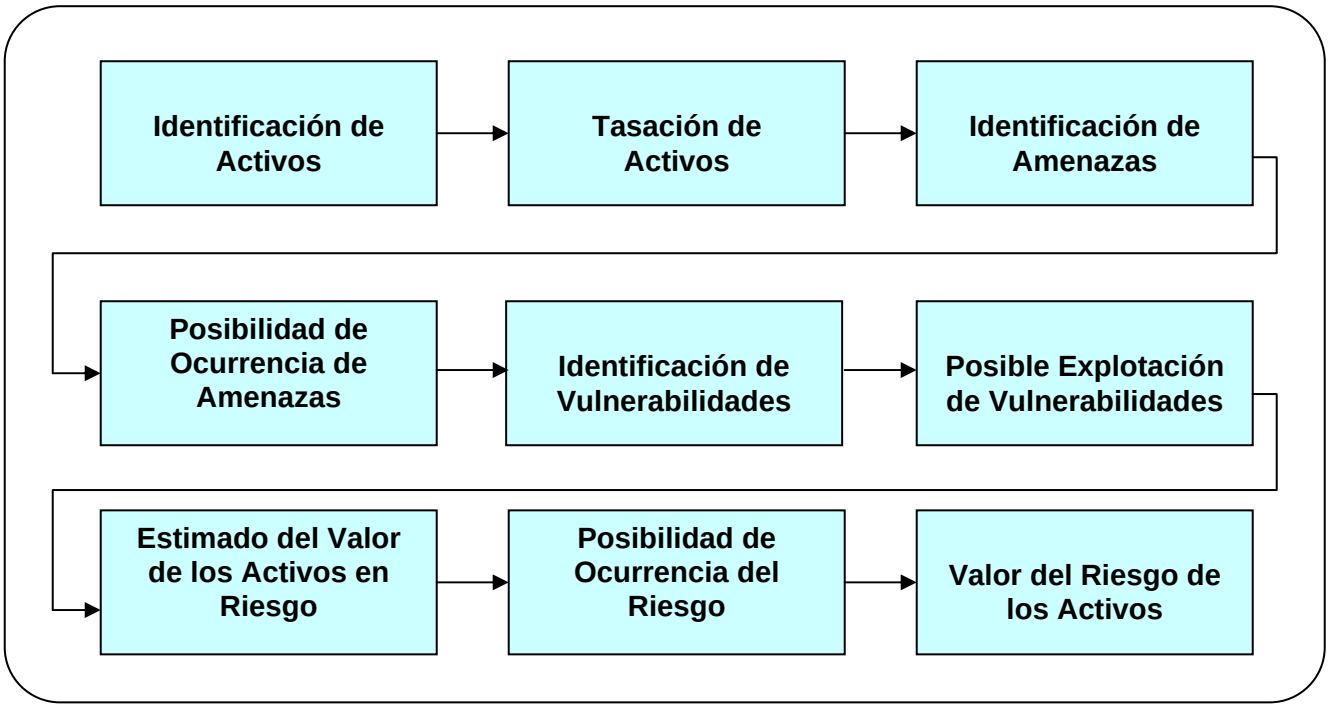


Tabla N°1
Realización del Análisis y Evaluación del Riesgo

Activos	Tasación				Amenazas	Posibilidad ocurrencia	Vulnerabilidad	Posible explotación de vulnera-bilidad	Valor activo	Posible ocurrencia	Total
	Confiden-cialidad	Integri-dad	Disponi-bilidad	Total							
1) Datos del cliente	A	A	A	A	- Plagio - Falsificación - Alteración - Privacidad	B B B A	- Deficiencia org. - Deficiencia envio - Acceso no autorizado - Control documentos	B A A M	A	M	M
2) Factura como documento	A	A	A	A	- Pérdida documento - Retraso en entrega - Ilegibilidad de datos - Cargos incorrectos	A A B M	- Datos incompletos - Desconocimiento rutas - Deficiencia impresión - Errores de procesamiento	A A B A	A	M	M
3) Tarifas	A	A	A	A	- Alteración incorrecta - Ignorancia cambios - Ofertas	B M A	- Acceso no autorizado - Mal entrenamiento - Falta comunicación	M B M	A	B	B
4) Servicios brindados	B	A	A	A	- Mala interpretación - Poco detalle - Servicio no solicitado	M A M	- Personal no calificado - Reducción costo - Error digitación	M A M	A	M	M
5) Software de facturación	A	A	A	A	- Errores de código - Códigos maliciosos - Fallos técnicos - Errores usuario - Falta seguridad	M A M B A	- Personal no calificado - Controles acceso - Energía eléctrica - Mal entrenamiento - Falta políticas	B M A B A	A	A	A
6) Medio de comunicación y/o entrega	A	A	A	A	- Fallas funciona-miento - Falta seguridad - Falta personal	A A B	- Energía eléctrica - Errores configuración - Poca disponibilidad	A M B	A	A	A

Leyenda: Alto……A
Mediano…..M
Bajo…… B

En la tabla N° 1, se fueron vaciando los resultados del análisis y evaluación del riesgo. El primer paso que se siguió fue la **(1**) Identificación de Activos.- Como resultado del uso de la metodología de las elipses, se identificaron seis activos de información vitales. Luego se procedió a la **(2)** Tasación de Activos.- Para poder identificar la protección apropiada a los activos, es necesario tasar su valor en términos de la importancia a la gestión comercial, o dadas ciertas oportunidades determinar su valor potencial .

En el caso de los activos de información del proceso de "cuentas corrientes", se tasó su impacto en relación a su confidencialidad, integridad y disponibilidad. Se manejó una escala cualitativa que variaba entre: ALTO, MEDIANO y BAJO.
Una ves realizada la tasación se efectuó la **(3)** Identificación de Amenazas.- Una amenaza tiene el potencial de causar incidentes indeseables, los cuales podrían resultar causando daño al sistema, la organización y sus activos. A través de la dinámica de grupos utilizando la técnica de la "lluvia de ideas", se hallaron las principales amenazas por cada activo de información.
El paso siguiente fue establecer la **(4)** Posibilidad de Ocurrencia de Amenazas.- No todas las amenazas tienen la misma posibilidad de ocurrencia. Habrán algunas que su presencia es remota y otras su probabilidad de que ocurran podrían ser altas. Por cada amenaza, el "comité gestor", basado en su experiencia y conocimiento de los activos y las amenazas, evaluó la posibilidad de ocurrencia para cada amenaza.
Continuando con la metodología, se procedió a la **(5)** Identificación de Vulnerabilidades.- Las vulnerabilidades son debilidades asociadas con cada activo de información. Son condiciones que pueden permitir que las amenazas las exploten y causen daño. Aquí el comité gestor, a través de la dinámica de grupos, estableció por cada amenaza las vulnerabilidades relacionadas con cada activo de información. Seguidamente se identificó, la **(6)** Posible Explotación de Vulnerabilidades.- También a través de la dinámica de grupos el "comité gestor", evaluó la posible explotación de vulnerabilidades por cada amenaza.
El paso siguiente de la metodología es el de evaluar el riesgo. El riesgo se evalúa contemplando dos elementos básicos**: (7)** Estimado del Valor de los Activos en Riesgo.- Este elemento es fundamental para evaluar el riesgo. Aquí lo que se pretende es determinar el daño económico que el riesgo pudiera causar a los activos de información. En el caso de "cuentas corrientes" el "comité gestor" estableció el estimado. **(8)** Posibilidad de Ocurrencia del Riesgo.- Aquí el "comité gestor", visualizando por cada activo sus impactos, amenazas y posibilidad de ocurrencia así como las vulnerabilidades y su posibilidad de ser explotadas, determinó la posibilidad de ocurrencia del riesgo por cada activo de información.
Finalmente se estableció el **(9)** Valor del Riesgo de los Activos.- Se concluyó siguiendo de manera sistemática la metodología, que los activos de información: **a)** Software de Información y **b)** Medio de Comunicación y/o Entrega eran los activos de información considerados de riesgo, y por lo tanto serían aquellos a los cuales habría que identificar del Anexo A sus respectivos controles.

TRATAMIENTO DEL RIESGO

En la cláusula 4.2.1 (g) se plantea de manera muy precisa que

Se deben seleccionar objetivos de control y controles apropiados del anexo A del estándar ISO 27001:2005 y la selección se debe justificar sobre la base de las conclusiones de la evaluación del riesgo y tratamiento del riesgo

En el caso del proceso de “cuentas corrientes”, una vez efectuado el análisis y evaluación del riesgo, se decidió mitigar los riesgos encontrados en los activos de información: a) software de información y b) medio de comunicación y/o entrega. El criterio establecido para aplicar los controles apropiados del anexo A á estos activos fue el resultado de ALTO RIESGO en la evaluación del riesgo realizada. Los activos de información: c) datos del cliente, d) factura como documento y e) servicios brindados, se decidió transferir sus riesgos comerciales a una empresa aseguradora. El activo de información “tarifas” el cual, como resultado de la evaluación del riesgo, se le consideró un riesgo aceptable, por ser evaluado como de bajo riesgo y visualizarlo compatible con las políticas de la organización.

Es importante entender, que el conjunto de decisiones tomadas con cada activo de información, como consecuencia de la evaluación del riesgo, se define como “tratamiento del riesgo”. El ISO/IEC guía 73 – 2002: Risk management – vocabulary- guidelines for use in standards”, lo determina “como el proceso de selección e implementación de medidas para modificar el riesgo”. Las medidas de tratamiento del riesgo pueden contemplar acciones como: evitar, optimizar, transferir o retener el riesgo.

ENUNCIADO DE APLICABILIDAD

En la cláusula 4.2.1 (h) se exige que se documente un “enunciado de aplicabilidad”. En la cláusula 4.3.1 (g) se hace mención también al enunciado de aplicabilidad, considerándolo un documento importante del SGSI.

Un enunciado de aplicabilidad es:
Un documento en el cual deben documentarse los objetivos de control y los controles seleccionados, así como las razones para su selección. También debe registrarse la exclusión de cualquier objetivo de control y controles enumerados en el anexo A.

El “enunciado de aplicabilidad” es un documento importante del SGSI. Sirve para mostrar a terceros la racionalidad al haber escogido ciertos objetivos de control y controles para mitigar ciertos riesgos identificados.

En la tabla Nº 2 se muestra a nivel de ilustración un enunciado de aplicabilidad como producto del análisis y evaluación del riesgo efectuado al proceso de cuentas corrientes.

Tabla N°2

Enunciado de Aplicabilidad Cuentas Corrientes

Activo de Información	Objetivo de Control	Control	Justificación
Software de Facturación	A.3.1	A.3.1.1 A.3.1.2	Proporcionar direccionalidad en la seguridad de información.
	A.6.1	A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4	Minimizar errores humanos en la seguridad de información.
	A.6.2	A.6.2.1	Capacitación del usuario
	A.6.3	A.6.3.1 A.6.3.2 A.6.3.3 A.6.3.4 A.6.3.5	Minimizar los incidentes de seguridad y aprender de ellos.
	A.7.1	A.7.1.2	Evitar el acceso físico no autorizado.
	A.7.2	A.7.2.1 A.7.2.2	Evitar la pérdida de activos e interrupción del servicio.
	A.9.1	A.9.1.1	Controlar el acceso a la información.
	A.9.5	A.9.5.2 A.9.5.3	Evitar el acceso no autorizado a la computadora.

Activo de Información	Objetivo de Control	Control	Justificación
Medio de Comunicación y/o Entrega	A.3.1	A.3.1.1 A.3.1.2	Proporcionar direccionalidad en la seguridad de información.
	A.6.1	A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4	Minimizar errores humanos en la seguridad de información.
	A.6.2	A.6.2.1	Capacitación del usuario
	A.6.3	A.6.3.1 A.6.3.2 A.6.3.3 A.6.3.4 A.6.3.5	Minimizar los incidentes de seguridad y aprender de ellos.
	A.7.2	A.7.2.2	Evitar la pérdida de activos e interrupción del servicio
	A.8.1	A.8.1.2	Asegurar la operación correcta de los medios de procesamiento de información.

NOTA: Las cláusulas de control A.11 y A.12 no se han incluido en la ilustración de enunciado de aplicabilidad. En un caso real habría que añadirlos.

CONCLUSIONES

El establecimiento, implantación, operación, monitoreo, mantenimiento y mejoramiento del ISO 27001:2005, requiere de un ingrediente básico, el cual es el rol protagónico que debe cumplir la alta gerencia. Es un estándar para la gestión y la gerencia no puede delegar su rol.

En el caso presentado, la alta gerencia siempre dio su apoyo visible en todas las fases del proceso de análisis y evaluación del riesgo. El comité gestor, siempre estuvo comprometido con el establecimiento del modelo, y desarrolló, a través del entrenamiento, las pericias pertinentes para su manejo.

Es importante entender, que el objetivo de la evaluación del riesgo es la de identificar y ponderar los riesgos a los cuales los sistemas de información y sus activos están expuestos, con miras a identificar y seleccionar controles apropiados.

La selección de los controles se debe justificar sobre la base de las conclusiones de la evaluación y tratamiento del riesgo. Los objetivos de control y los controles seleccionados, así como las razones para su selección deben documentarse en el “enunciado de aplicabilidad.

Como se ha podido apreciar en el caso del proceso de "cuentas corrientes", la evaluación del riesgo esta basada en los valores de los activos y en los niveles de los requerimientos de seguridad, considerando la existencia de los controles actuales.

La evaluación del riesgo envuelve la consideración sistemática de dos elementos claves:

- Consecuencias: El daño a la actividad comercial, como resultado de una ruptura de seguridad de información, considerando las consecuencias potenciales, de pérdida o fallas en la confidencialidad, integridad y disponibilidad de la información.

- Probabilidad: La posibilidad realista de que una ruptura ocurra

Siempre se debe tener claro, que no existe un método "bueno" o "malo" para calcular los riesgos. El único requisito es que los conceptos de determinar los activos de información, su tasación, la identificación de amenazas y vulnerabilidades se cumplan.