UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

REFORMULACIÓN DEL PLAN ANUAL DE AUDITORIA DE SISTEMAS, PARA AGREGAR VALOR EN UNA ENTIDAD FINANCIERA

INFORME DE SUFICIENCIA PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

JIMMY CARLO VILLARREAL ALBUJAR

LIMA, PERÚ

2009

Dedicatoria

A mis padres, hermanos, enamorada y amigos, por su amor, comprensión y apoyo incondicional…

Agradecimientos

A Dios por darme la bendición de estar rodeado de personas maravillosas que me apoyan, alientan y brindan su amor en cada momento de mi vida.

A mis padres, que son mi mayor admiración y orgullo, a mis hermanos por su amor y apoyo incondicional, a mis pocos y buenos amigos, a los que apoyaré siempre y en especial a mi enamorada por haber cambiado mi vida y llenado mi mundo de felicidad e ilusión.

A mis amigos del Banco, por su experiencia y apoyo en mi desarrollo profesional.

INDICE

DESCRIPTORES TEMÁTICOS

Auditoría

Auditoría de Sistemas

Banca

Bancos

Cobit

Entidad Bancaria

Entidad Financiera

ISACA

ISO

Plan anual

Sistemas

RESUMEN

El presente informe tiene como objetivo, establecer una estrategia que permita al área de Auditoría de Sistemas de un Banco, cambiar de una auditoria de cumplimiento normativo (tradicional), a una auditoría que genere valor mediante el alineamiento al rumbo estratégico de la organización.

Para dicho fin, se realizó un diagnóstico funcional y estratégico del Banco (objetivos, procesos, sistemas críticos, situación de la plataforma tecnológica, entre otros aspectos), se desarrolló un marco teórico con los distintos estándares y buenas prácticas relacionadas a la seguridad de información, auditoría de tecnologías de información y normas del ente Supervisor (SBS); y con dicha información, se plantearon alternativas de solución al problema, se realizó un análisis costo beneficio y se desarrolló un proceso de toma de decisiones.

De las dos alternativas de solución propuestas, y luego de efectuado el proceso de toma de decisiones, la alternativa de solución seleccionada fue: "Disminuir el número de informes de verificación del cumplimiento de normas internas y externas, considerando que uno de ellos debe agrupar la mayor cantidad de aspectos sobre los cuales, el Banco cuenta con controles adecuados (Informe de verificación del cumplimiento de la Circular SBS G-105-2002). Asimismo, incluir informes de evaluación del funcionamiento y seguridad de la información de los sistemas críticos del Banco, con un nivel de criticidad definido por el área de Auditoría Interna".

Como resultado de aplicar la alternativa de solución seleccionada, se obtuvieron informes con observaciones y recomendaciones reconocidas por

el Directorio y sus Gerencias, mejorando notablemente la imagen del Área de Auditoría Interna y en especial del Área de Auditoría de Sistemas.

INTRODUCCIÓN

Actualmente la información es uno de los principales activos de las entidades financieras, ya que representan por ejemplo, saldos de depósitos, movimientos, estados financieros, créditos, datos de clientes, entre otros. Del mismo modo, son igual de importantes los activos relacionados a la información, es decir, donde se almacena, transporta, procesa y presenta la información.

Sin embargo, conforme cambia y mejoran las tecnologías de información, también se incrementan los riesgos asociados a dichas tecnologías, que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

Como parte de las funciones del área de Auditoría de Sistemas, se realizan evaluaciones para verificar la existencia y aplicación de controles sobre las tecnologías de información (cumplimiento normativo), a fin de minimizar los riesgos asociados. Sin embargo, dichas evaluaciones no están orientadas, necesariamente, a actividades que generan valor a la organización.

En tal sentido, el presente informe tiene como objetivo, establecer una estrategia que permita al área de Auditoría de Sistemas de un Banco, cambiar de una auditoria de cumplimiento normativo (tradicional), a una auditoría que genere valor mediante el alineamiento al rumbo estratégico de la organización.

CAPÍTULO I.
PENSAMIENTO ESTRATÉGICO

I.1. LINEAMIENTOS ESTRATÉGICOS DEL BANCO

Misión

"Ser el Banco líder en la atención de empresas del sector no corporativo, personas del estrato socioeconómico medio y microempresarios calificados con potencial para operar el sistema financiero, diferenciándonos de nuestros competidores en la calidad de servicio, eficiencia y oportunidad con la que resolvemos sus necesidades financieras".

Visión

"Contribuir con el progreso sostenible de nuestros clientes, colaboradores, accionistas y del país a través de la eficiente gestión de productos y servicios financieros que generen valor agregado a nuestros clientes, anticipándonos siempre a sus necesidades y asegurando altos estándares de calidad de servicio".

Objetivos estratégicos

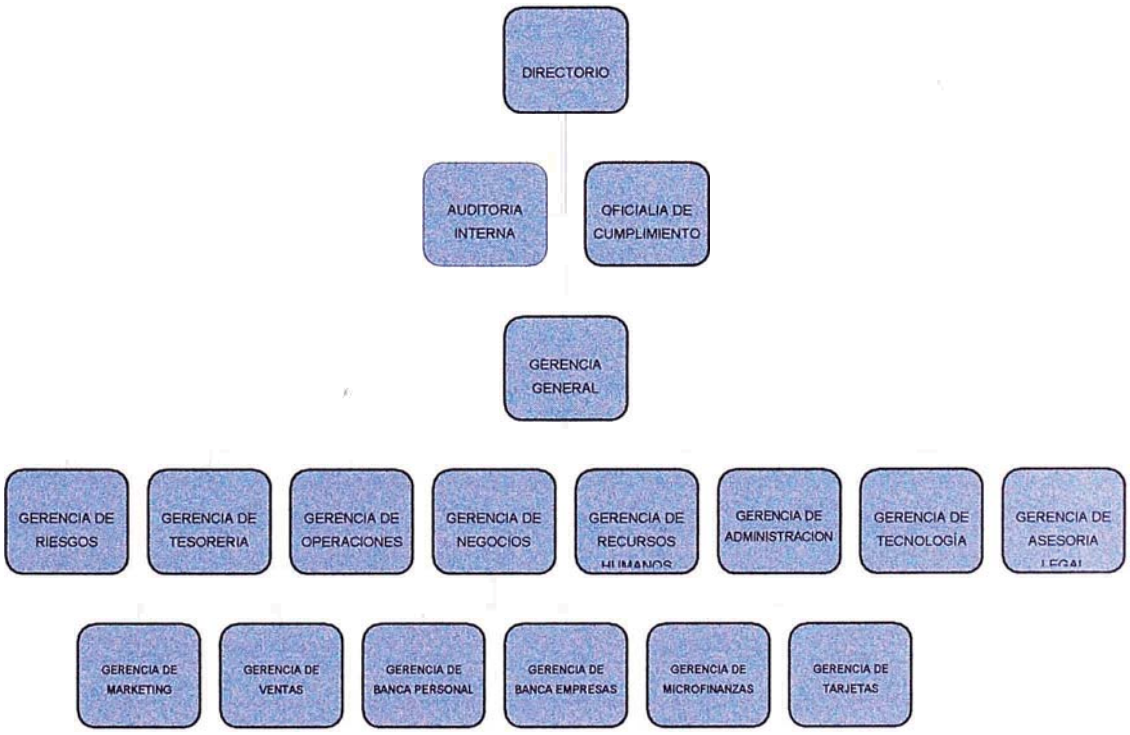
1. Incrementar la rentabilidad del Banco.
2. Diversificar los ingresos por producto y segmento de clientes.
3. Reducir la deserción de clientes.

4. Reducir costos por provisiones.
5. Incrementar la venta cruzada de productos.
6. Mejorar los canales de atención.
7. Reducir el número de errores de operación.
8. Automatizar procesos críticos.
9. Reducir el tiempo de atención.
10. Desarrollar competencias y especialización

I.2. DIAGNOSTICO FUNCIONAL

I.2.1. ORGANIZACIÓN

El organigrama del Banco es el siguiente:



I.2.2. CLIENTES

Personas del estrato socioeconómico medio, empresas pequeñas y medianas y microempresas.

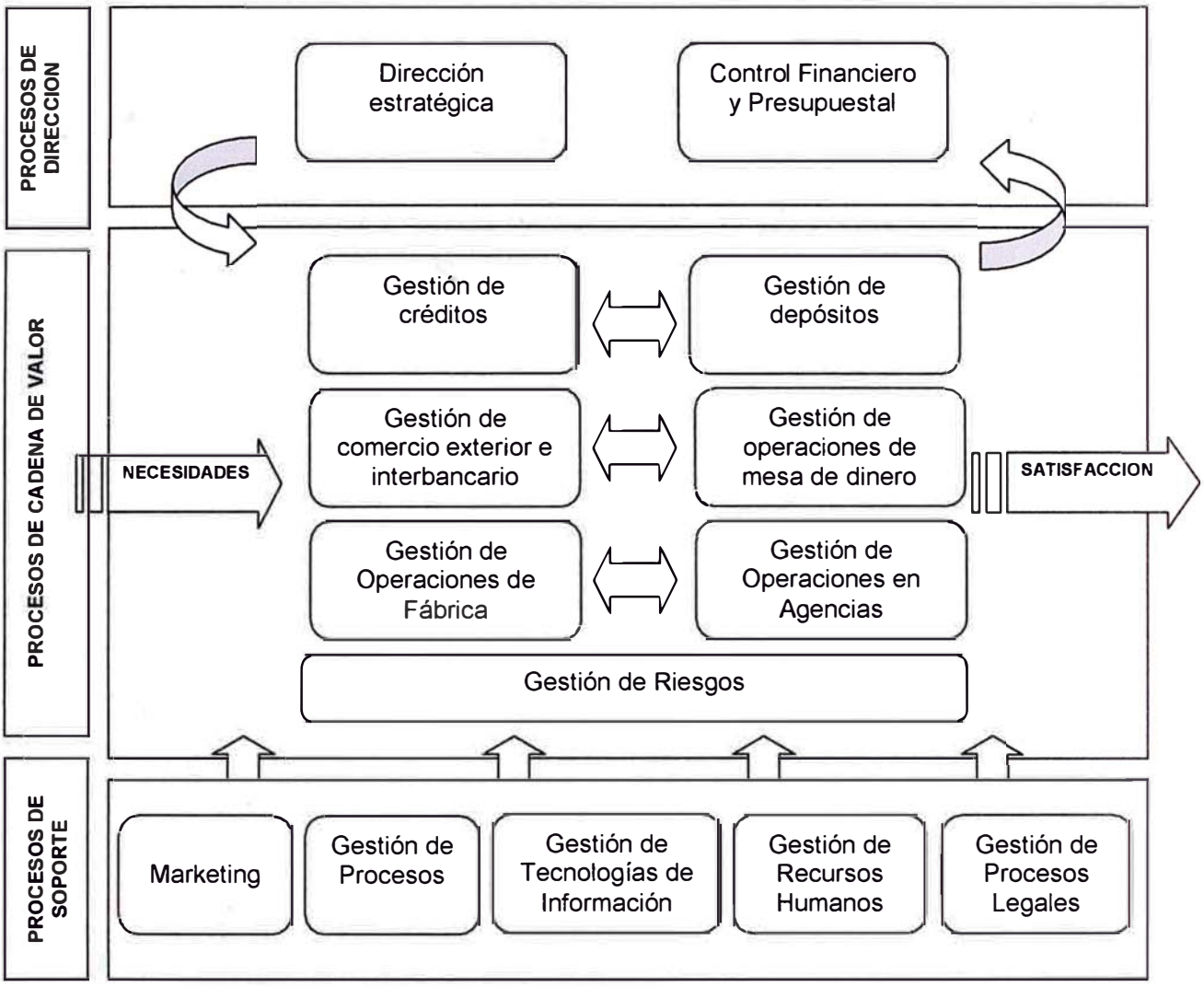
I.2.3. PROVEEDORES

Entre los principales proveedores del Banco, podemos mencionar a empresas que brindan los siguientes servicios y/o productos:

- Servicios públicos (luz, agua, desagüe, teléfono).
- Mantenimiento de servidores, estaciones de trabajo y equipos de comunicación.
- Soporte técnico y mesa de ayuda.
- Impresión de estados de cuenta, avisos y otros.
- Transporte de remesas.
- Pólizas de Seguros.
- Internet, Hosting, housing y redes de comunicación.
- ATM's (Cajeros automáticos)
- Procesamiento de Tarjetas de Crédito.
- Mensajería.
- Outsourcing de desarrollo de sistemas.
- Dispositivos de almacenamiento.
- Otros Bancos, entre otros.

I.2.4. PROCESOS

El mapa de los principales procesos del Banco es el siguiente:

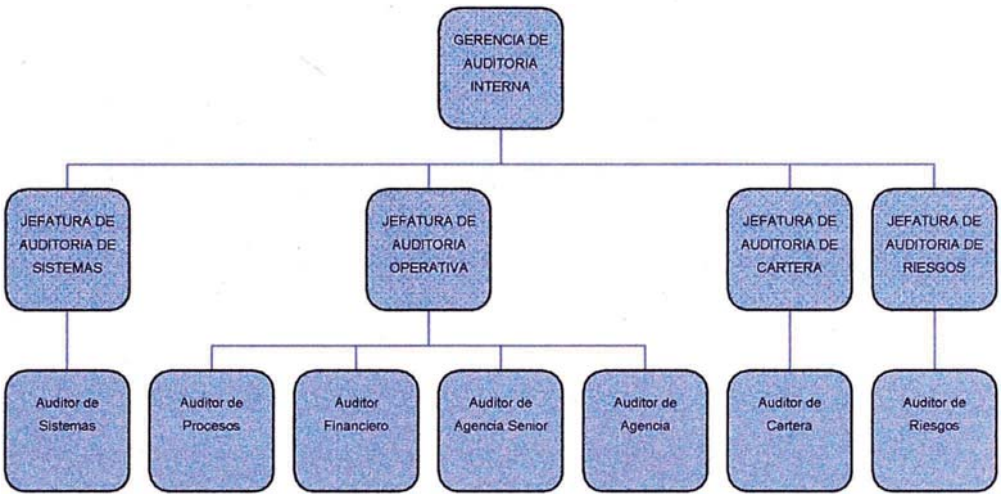


I.2.5. OTRA INFORMACION SIGNIFICATIVA

La distribución y comparación de personal (principal activo del Banco) en los periodos de 2006 y 2007, fue el siguiente:

Personal	2006	2007
Gerente General	1	1
Gerentes	22	17
Sub - Gerentes	20	10
Funcionarios	56	174
Empleados	396	629
TOTAL	495	831

El área de Auditoría Interna, encargada de evaluar el sistema de control interno del Banco, está conformada por 12 personas, distribuidas de la siguiente manera:



El área de Auditoría de Sistemas, se encarga de la evaluación del cumplimiento de las normas internas referidas a seguridad de la información y del reglamento establecido por la SBS (Circular SBS G-105-2002 Riesgos de tecnologías de información), asimismo, apoya a las demás áreas de auditoría en la generación de información de los sistemas y de ser necesario en la revisión de un sistema no contemplado en la planificación del Área de Auditoría de Sistemas.

I.3. DIAGNOSTICO ESTRATEGICO

I.3.1. ANALISIS INTERNO

Como parte del análisis interno realizado por el Banco, se han identificado las siguientes fortalezas y debilidades:

Fortalezas:

- Especialización en nichos de mercado, gracias a un know how adquirido en el tiempo para sus principales productos.
- Base de clientes de banca masiva fidelizada.

- Capacidad patrimonial acumulada, necesaria para desarrollar un crecimiento sostenido.
- Buen nivel de liquidez.

Debilidades:

- Baja presencia en el mercado, por falta de imagen de la entidad y sus productos.
- Clientes con niveles de morosidad sobre el promedio del sistema financiero.
- Procesos críticos que aún no han sido optimizados.
- Deficiencias operativas por alta rotación de personal.
- Bajos niveles de colocación en un alto porcentaje de productos.

I.3.2. ANALISIS EXTERNO

Como parte del análisis externo realizado por el Banco, se han identificado las siguientes oportunidades y amenazas:

Oportunidades:

- Estabilidad y crecimiento económico en 3 a 5 años.
- Incremento de la demanda y consumo internos.
- Nuevos polos de desarrollo a nivel nacional.
- Posibles adquisiciones y/o alianzas estratégicas.

Amenazas:

- Fuerte competencia en el sistema financiero (nuevas entidades financieras), con posibles reducciones de tasas de interés para adquirir y mantener cartera de clientes.
- Migración de recursos del público a fondos mutuos, reducen el nivel de captación de fondos.

CAPÍTULO II.
MARCO TEÓRICO Y METODOLÓGICO

II.1. TEORÍA Y METODOLOGÍA DE REFERENCIA

La Superintendencia de Banca y Seguros (SBS), ha establecido entre otras disposiciones y leyes para el sistema financiero peruano, la Circular N° G-105-2002 Riesgos de tecnología de información (ver Anexo 2), la misma que establece:

"…Auditoría de sistemas

Artículo 17º. Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria del Reglamento…".

Como parte de los procedimientos de auditoría de sistemas aplicados en el Banco, se realiza un aseguramiento de controles mediante el cumplimiento y evaluación de la normativa interna vigente. Se contempla un marco de buenas prácticas de control interno

establecidas por ISACA (Information System Audit and Control Association) en su documento COBIT (consenso de expertos, cuyas prácticas se enfocan más en el control y menos en la ejecución, ayudando a optimizar las inversiones en TI y asegurando la entrega del servicio); así como las Guías globales de auditoría de tecnología de información (GTAG's) proporcionadas por el Instituto de Auditores Internos, y los estándares de seguridad de información ISO/IEC 17799.

Al respecto, como parte de las buenas prácticas y guías establecidas en COBIT 4.0, ISACA define controles (generales y de aplicación) en procesos de TI básicos y que son claramente identificables en cualquier organización, y que de acuerdo a los objetivos y metas de TI y de la organización, se pueden adecuar aquellos controles sugeridos en COBIT y necesarios para asegurar los procesos "críticos" de la organización, a fin de asegurar que se logren dichos objetivos y metas, y se minimicen los riesgos de TI (ver Anexo 4).

Asimismo, las Guías globales de auditoría de tecnología de información (GTAG's) proporcionadas por el Instituto de Auditores Internos, establecen 11 guías detalladas respecto a controles sobre las tecnologías de información, gestión de riesgos, auditoría de la gestión de TI, TI tercerizadas, auditorías sobre controles de aplicación, gestión de continuidad de negocio, entre otros aspectos.

Por otro lado, los estándares de ISO/IEC 17799:2007, establecen buenas prácticas para la seguridad de información, en aspectos tales como: evaluación y tratamiento del riesgo, gestión de incidentes, gestión de continuidad de negocios, desarrollo y mantenimiento de sistemas, administración de operaciones y comunicaciones, entre otros (ver Anexo 3).

CAPÍTULO III.
PROCESO DE TOMA DE DECISIONES

III.1. IDENTIFICACION DE PROBLEMA

Hasta fines del año 2007, la auditoria realizada en el Banco estaba orientada a la verificación del cumplimiento de normas SBS y normas internas. El Directorio y la Gerencia General requieren contar con un Área de Auditoría Interna, que genere observaciones y recomendaciones de valor, alineados al rumbo estratégico del Banco, que mejoren la eficiencia y efectividad en las operaciones, pero sin dejar de verificar el cumplimiento de normas.

La Gerencia de Auditoría Interna, ha solicitado a la Jefatura de Auditoría de Sistemas, reformular el plan anual de auditoria de sistemas para el año 2008, a fin de satisfacer las expectativas del Directorio y la Gerencia General, en aspectos referidos a tecnologías de información.

III.2. PLANTEAMIENTO DE ALTERNATIVAS DE SOLUCION

Para reformular el Plan anual de auditoria de sistemas, se utilizaron enfoques y procedimientos establecidos en el marco de trabajo de COBIT 4.0, estándares y buenas prácticas de seguridad de información ISO/IEC 17799 y guías de control para tecnologías de información (GAIT's) proporcionadas por el Instituto de Auditores Internos.

Asimismo, las 2 alternativas planteadas incluyen la verificación del cumplimiento de lo señalado en la Circular SBS G-105-2002 Riesgos

de tecnología de información y lo establecido en políticas, normas y procedimientos de seguridad información del Banco.

Alternativa 1:

Mantener el número de informes (4) de verificación del cumplimiento de normas internas y externas programados durante el 2007, reduciendo su alcance y periodo de revisión, a fin de poder incluir informes de evaluación del funcionamiento y seguridad de la información de los sistemas críticos (10), de acuerdo al Mapa de sistemas críticos definidos por el Área de Tecnología (actualizado cada 2 años).

Alternativa 2:

Disminuir el número de informes de verificación del cumplimiento de normas internas y externas (a 2), considerando que uno de ellos debe agrupar la mayor cantidad de aspectos sobre los cuales, el Banco cuenta con controles adecuados (Informe de verificación del cumplimiento de la Circular SBS G-105-2002). Asimismo, incluir informes de evaluación del funcionamiento y seguridad de la información de los sistemas críticos del Banco (10), con un nivel de criticidad definido por el área de Auditoría Interna (actualizado trimestralmente).

III.3. SELECCIÓN DE UNA ALTERNATIVA DE SOLUCIÓN

En reunión con el Auditor General y los Jefes de Auditoría de Operativa, Riesgos, Cartera y Sistemas, procedimos a calificar las alternativas propuestas, para cada uno de los 6 criterios de evaluación definidos en el capítulo IV sección A:

	Criterios de evaluación	Alternativa 1	Alternativa 2	Selección
1.	Número de aspectos exigidos por la SBS evaluados en los informes de Auditoría de Sistemas (sobre un total de 19).	19	19	Cualquiera
2.	Mayor número de normas internas, relacionadas a seguridad de información,	10	12	Alternativa 2

	Criterios de evaluación	Alternativa 1	Alternativa 2	Selección
	evaluadas en los informes de Auditoría de Sistemas.			
3.	Mayor número de procesos críticos (soportados por sistemas críticos) evaluados durante el año.	6	10	Alternativa 2
4.	Mayor número de informes relacionados a sistemas críticos que consideran la evaluación de incidencias presentadas y frecuencia de modificaciones realizadas.	6	10	Alternativa 2
5.	Menor número de sistemas críticos evaluados en años anteriores en cuyos informes no resultaron observaciones o recomendaciones con un riesgo medio o alto.	1	1	Cualquiera
6.	Mayor frecuencia de actualización del inventario de sistemas críticos.	Cada 2 años	Trimestral	Alternativa 2

Como resultado de la calificación asignada en cada uno de los 6 criterios de evaluación, se determinó que en 2 de ellos resultaba igual escoger cualquiera de las 2 alternativas propuestas; sin embargo, en 4 de ellos se calificó mejor la alternativa 2, quedando ésta como alternativa de solución.

III.4. PLANES DE ACCION PARA DESARROLLAR LA SOLUCION PLANTEADA

Se definieron 3 planes de acción para desarrollar la solución planteada:

1. Desarrollo de un cronograma preliminar de los informes de auditoría de sistemas programados para el 2008. (Ver Anexo 2).
2. Desarrollo de una guía estándar para la evaluación de aspectos de seguridad de información con estándares ISO. (Ver Anexo 3).
3. Desarrollo de informes de evaluación del funcionamiento y seguridad de la información de los sistemas críticos del Banco, utilizando la Circular SBS G-105-2002, la guía estándar

desarrollada, el marco de trabajo COBIT y GTAG's del Instituto de Auditores Internos.

CAPÍTULO IV. :
ANÁLISIS BENEFICIO – COSTO

IV.1. SELECCIÓN DE CRITERIOS DE EVALUACIÓN

En reunión con el Auditor General y los Jefes de Auditoría de Operativa, Riesgos, Cartera y Sistemas, se definieron los siguientes 6 criterios de evaluación:

1. Mayor número de aspectos exigidos por la SBS evaluados en los informes de Auditoría de Sistemas.

   Teniendo en cuenta que los aspectos exigidos por la SBS, en su Circular G-105-2002, detallan el cumplimiento de 19 artículos.

2. Mayor número de normas internas, relacionadas a seguridad de información, evaluadas en los informes de Auditoría de Sistemas.

   Teniendo en cuenta que, en el Banco, existen 12 normas internas relacionadas a controles en seguridad de información.

3. Mayor número de procesos críticos (soportados por sistemas críticos) evaluados durante el año.

   Teniendo en cuenta que de acuerdo a los recursos del área de Auditoría de Sistemas, sólo se pueden elaborar 12 informes en un año, por lo que, de acuerdo al número de informes de cumplimiento de normas y aspectos exigidos por la SBS programados, la diferencia serán informes de sistemas críticos.

4. Mayor número de informes relacionados a sistemas críticos que consideran la evaluación de incidencias presentadas y frecuencia de modificaciones realizadas.

   Evaluar estos aspectos permitirá conocer la capacidad de respuesta del Banco frente a fallas en los sistemas, y que el área de Auditoría Interna proporcione recomendaciones para el aseguramiento de la continuidad operativa del Banco, así como haga de conocimiento al Directorio las debilidades del Banco.

5. Menor número de sistemas críticos evaluados en años anteriores en cuyos informes no resultaron observaciones o recomendaciones con un riesgo medio o alto.

   Este aspecto, permitirá "evitar" el orientar recursos a la evaluación de aspectos que son adecuadamente cubiertos por los controles del Banco.

6. Mayor frecuencia de actualización del inventario de sistemas críticos.

   Este aspecto, permitirá seleccionar los sistemas críticos de acuerdo a los constantes cambios en los objetivos y metas de TI, y que generalmente son comentados en el Directorio y Comités de Gerencia en los cuales participa el área de Auditoría Interna, y que no necesariamente son plasmados en el inventario de sistemas críticos actualizado por el área de Tecnología.

IV.2. RESULTADOS DE LA SOLUCION PLANTEADA

Los principales resultados obtenidos con la solución planteada fueron los siguientes:

1. En los 6 Comités de Auditoría realizados mensualmente, se presentaron ante el Directorio el 75% de las observaciones resultantes de los informes de Auditoría de Sistemas, ya que

representaban un riesgo alto para el Banco y las recomendaciones propuestas se encontraban alineadas a los objetivos estratégicos.

2. Mejora de la imagen del Área de Auditoría Interna en el Banco, ya que se mostraba como un área técnica, con capacidad para identificar riesgos y contribuir con recomendaciones de valor.
3. Mejora en el flujo de información en el Área de Auditoría Interna, ya que se contaba con acceso a las incidencias presentadas en el Banco y a los nuevos proyectos tecnológicos solicitados y aprobados, lo cual permitía una mejor decisión al seleccionar un sistema a evaluar.
4. Mejor conocimiento de la realidad del Banco, al mantener registros estadísticos de transacciones, accesos, ventas por productos, variaciones en saldos contables, reclamos, entre otros aspectos.
5. Las observaciones resultantes representaban riesgos cuyo impacto era cuantificado en un periodo de tiempo o para una muestra seleccionada, lo cual permitía a las demás Gerencias del Banco, tomar mejores decisiones para solucionar los errores y/o problemas detectados.
6. Se generó una mejor interacción con las áreas del Banco, ya que no veían al Área de Auditoría Interna, como un área que venía a decirle sus errores o a señalar sus incumplimientos, por el contrario, plantearía mejoras en el control interno para alcanzar los objetivos propuestos por el Banco.

CAPÍTULO V. :
CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Para reformular un plan anual de auditoría de sistemas con la finalidad de que agregue valor a la organización, se requiere:

- Realizar un diagnóstico estratégico, a fin de conocer los objetivos y estrategias, y realizar un diagnóstico de las estrategias y objetivos del área de tecnología.
- Establecer canales formales para la recepción de información clave, como por ejemplo, incidencias en la infraestructura de tecnología de información, cambios en el ambiente operativo tecnológico, nuevos proyectos de adquisición y desarrollo, entre otros.
- Evaluar los estándares y normas regulatorias vigentes a fin de establecer guías que permitan planificar y ejecutar la auditoria de sistemas, acorde al cumplimiento normativo y aspectos aplicables a la realidad de la organización.

RECOMENDACIONES

- El área de Auditoría de Sistemas debería contar con un mapa de sistemas críticos, definidos en conjunto con el Área de Auditoría Interna, de acuerdo al nivel de riesgo e impacto identificado.

- Realizar una evaluación permanente de los sistemas críticos del Banco, ampliando las muestras, de ser posible realizar revisiones integrales de inconsistencias en las bases de datos, utilizando procedimientos automáticos.
- Se debería estar permanentemente informado y actualizado en conocimientos de estándares de seguridad de información y buenas prácticas de auditoría de sistemas.
- Se debería contar con capacitación para el manejo de herramientas que permitan la evaluación de sistemas de información.

GLOSARIO

Controles Generales: Son aquellos controles que corresponden a los procesos de TI, como son: el desarrollo y mantenimiento de sistemas, las operaciones del centro de cómputo, la seguridad de acceso, las comunicaciones, entre otros.

Controles de aplicación: Son aquellos controles incrustados en las aplicaciones y/o sistemas de información, como son: los controles de acceso, segregación funcional, logs de auditoría, controles de procesamiento, controles de entrada y de salida, entre otros.

Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada.

Riesgo de operación: Entiéndase por riesgo de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

Riesgos de tecnología de información: Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.

Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

BIBLIOGRAFIA

Circular SBS G-105-2002 Riesgos de tecnología de información, publicada el 22 de febrero de 2002.

COBIT 4.0 Objetivos de control para la información y tecnologías relacionadas, vigente desde abril 2007, elaborado por ISACA (organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información).

GTAG's Guías Globales de Auditoría de Tecnología de Información, elaboradas por el Instituto de Auditores Internos de Estados Unidos.

ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición, publicada en enero 2007 por INDECOPI.

ANEXOS

ANEXO 1: CRONOGRAMA DE INFORMES PROGRAMADOS PARA EL EJERCICIO 2008

	Informe de Auditoría de Sistemas	Plazo
1	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el Sistema Central del Banco.	Febrero
2	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el sistema de cobro de intereses y comisiones.	Marzo
3	Evaluación de los controles establecidos para la Gestión de Continuidad de Negocio.	Abril
4	Verificación del cumplimiento de la Circular SBS G-105-2002 Riesgos de tecnología de información y normas internas relacionadas	Mayo
5	Evaluación de los controles sobre el funcionamiento y la seguridad de la información reportada a las centrales de riesgo.	Junio
6	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el sistema de microfinanzas.	Julio
7	Evaluación de los controles establecidos sobre las operaciones, comunicaciones y red interna del Banco	Agosto
8	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el sistema de generación de reportes de control.	Setiembre
9	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el sistema de banca electrónica.	Octubre
10	Verificación del cumplimiento de la Circular SBS G-105-2002 Riesgos de tecnología de información y normas internas relacionadas	Noviembre
11	Evaluación de los controles establecidos para la Gestión de Continuidad de Negocio.	Diciembre
12	Evaluación de los controles sobre el funcionamiento y la seguridad de la información en el Sistema Central del Banco.	Enero 2009

ANEXO 2: Circular SBS G-105-2002

Lima, 22 de febrero de 2002

CIRCULAR Nº G-105-2002

Ref.: Riesgos de tecnología de información

Señor

Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias, en adelante Ley General, y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001, con la finalidad de establecer criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información, a que se refiere el artículo 10º del Reglamento para la Administración de los Riesgos de Operación, aprobado mediante la Resolución SBS Nº 006-2002 del 4 de enero de 2002, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º .- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

b. Ley General: Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

c. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada.

d. Reglamento: Reglamento para la Administración de los Riesgos de Operación aprobado por Resolución SBS N° 006-2002 del 4 de enero de 2002.

e. Riesgo de operación: Entiéndase por riesgo de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

f. Riesgos de tecnología de información: Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.

g. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

h. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

Responsabilidad de la empresa

Artículo 3°.- Las empresas deben establecer e implementar las políticas y procedimientos necesarios para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo en los procesos críticos asociados a dicho riesgo, considerando las disposiciones contenidas en la presente norma, en el Reglamento, y en el Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.

La administración de dicho riesgo debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

I. Eficacia. La información debe ser relevante y pertinente para los objetivos de negocio y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la empresa.

II. Eficiencia. La información debe ser producida y entregada de forma productiva y económica.

III. Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

IV. Integridad. La información debe ser completa, exacta y válida.

V. Disponibilidad. La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

VI. Cumplimiento normativo. La información debe cumplir con los criterios y estándares internos de la empresa, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

Estructura organizacional y procedimientos

Artículo 4°.- Las empresas deben definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan.

Administración de la seguridad de información

Artículo 5º.- Las empresas deberán establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante "Plan de Seguridad de la información - (PSI)". El PSI debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.

Las actividades mínimas que deben desarrollarse para implementar el PSI, son las siguientes:

a. Definición de una política de seguridad.

b. Evaluación de riesgos de seguridad a los que está expuesta la información

c. Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.

d. Plan de implementación de los controles y procedimientos de revisión periódicos.

e. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Las empresas bancarias y las empresas de operaciones múltiples que accedan al módulo 3 de operaciones a que se refiere el artículo 290º de la

Ley General deberán contar con una función de seguridad a dedicación exclusiva.

Subcontratación (outsourcing)

Artículo 6º.- La empresa es responsable y debe verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en la Primera Disposición Final y Transitoria del Reglamento. Asimismo, la empresa debe asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Las empresas que a la fecha de vigencia de la presente norma se encontrasen en la situación antes señalada, deberán solicitar la autorización correspondiente. Para la evaluación de estas autorizaciones, las empresas deberán presentar documentación que sustente lo siguiente:

a) La forma en que la empresa asegurará el cumplimiento de la presente circular y la Primera Disposición Final y Transitoria del Reglamento.

b) La empresa, así como los representantes de quienes brindarán el servicio de procesamiento en el exterior, deberán asegurar adecuado acceso a la información con fines de supervisión, en tiempos razonables y a solo requerimiento.

Aspectos de la seguridad de información

Artículo 7°.- Para la administración de la seguridad de la información, las empresas deberán tomar en consideración los siguientes aspectos:

7.1 Seguridad lógica

Las empresas deben definir una política para el control de accesos, que incluya los criterios para la concesión y administración de los accesos a los sistemas de información, redes y sistemas operativos, así como los derechos y atributos que se confieren.

Entre otros aspectos, debe contemplarse lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios. Revisiones periódicas deben efectuarse sobre los derechos concedidos a los usuarios.

b) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.

c) Controles especiales sobre utilidades del sistema y herramientas de auditoría.

d) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.

e) Usuarios remotos y computación móvil.

7.2 Seguridad de personal

Las empresas deben definir procedimientos para reducir los riesgos asociados al error humano , robo, fraude o mal uso de activos, vinculados al riesgo de tecnología de información. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la definición de roles y responsabilidades establecidos sobre la seguridad de información, verificación de antecedentes, políticas de rotación y vacaciones, y entrenamiento.

7.3 Seguridad física y ambiental

Las empresas deben definir controles físicos al acceso, daño o interceptación de información. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

Se definirán medidas adicionales para las áreas de trabajo con necesidades especiales de seguridad, como los centros de procesamiento, entre otras zonas en que se maneje información que requiera de alto nivel de protección.

7.4 Clasificación de seguridad

Las empresas deben realizar un inventario periódico de activos asociados a la tecnología de información que tenga por objetivo proveer la base para una posterior clasificación de seguridad de dichos activos. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

Administración de las operaciones y comunicaciones

Artículo 8º.- Las empresas deben establecer medidas de administración de las operaciones y comunicaciones que entre otros aspectos contendrán lo siguiente:

Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.

Control sobre los cambios del ambiente de desarrollo al de producción.

Separación de funciones para reducir el riesgo de error o fraude.

- Separación del ambiente de producción y el de desarrollo.
- Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
- Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
- Seguridad sobre correo electrónico.
- Seguridad sobre banca electrónica.

Desarrollo y mantenimiento de sistemas informáticos - Requerimientos de seguridad

Artículo 9º.- Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.

b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.

c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.

d) Controlar el acceso a las librerías de programas fuente .

e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

Procedimientos de respaldo

Artículo 10º.- Las empresas deben establecer procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con lo requerido en el Plan de Continuidad.

La empresa debe conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

Planeamiento para la continuidad de negocios

Artículo 11º.- Las empresas, bajo responsabilidad de la Gerencia y el Directorio, deben desarrollar y mantener un "Plan de Continuidad de Negocios" (PCN), que tendrá como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

Criterios para el diseño e implementación del Plan de Continuidad de Negocios

Artículo 12º.- Para el desarrollo del PCN se debe realizar previamente una evaluación de riesgos asociados a la seguridad de la información. Culminada la evaluación, se desarrollarán sub-planes específicos para mantener o recuperar los procesos críticos de negocios ante fallas en sus activos, causadas por eventos internos (virus, errores no esperados en la implementación, otros), o externos (falla en las comunicaciones o energía, incendio, terremoto, proveedores, otros).

Prueba del Plan de Continuidad de Negocios

Artículo 13º.- La prueba del PCN es una herramienta de la dirección para controlar los riesgos sobre la continuidad de operación y sobre la

disponibilidad de la información, por lo que la secuencia, frecuencia y profundidad de la prueba del PCN, deberá responder a la evaluación formal y prudente que sobre dicho riesgo realice cada empresa.

En todos los casos, mediante una única prueba o una secuencia de ellas, según lo considere adecuado cada empresa de acuerdo a su evaluación de riesgos, los principales aspectos del PCN deberán ser probados cuando menos cada dos años.

Anualmente, dentro del primer mes del ejercicio , se enviará a la Superintendencia el programa de pruebas correspondiente, en que se indicará las actividades a realizar durante el ciclo de 2 años y una descripción de los objetivos a alcanzar en el año que se inicia.

Cumplimiento normativo

Artículo 14º.- La empresa deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

Privacidad de la información

Artículo 15º.- Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme la normatividad vigente sobre la materia.

Auditoría Interna y Externa

Artículo 16º.- La Unidad de Auditoría Interna deberá incorporar en su Plan Anual de Trabajo la evaluación del cumplimiento de lo dispuesto en la presente norma.

Asimismo, las Sociedades de Auditoría Externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la

entidad cuenta con políticas y procedimientos para la administración de los riesgos de tecnología de información, considerando asimismo, el cumplimiento de lo dispuesto en la presente norma.

Auditoría de sistemas

Artículo 17º.- Las empresas bancarias y aquellas empresas autorizadas a operar en el Módulo 3 conforme lo señalado en el artículo 290° de la Ley General, deberán contar con un servicio permanente de auditoría de sistemas, que colaborará con la Auditoría interna en la verificación del cumplimiento de los criterios de control interno para las tecnologías de información, así como en el desarrollo del Plan de Auditoría.

El citado servicio de auditoría de sistemas tomará en cuenta, cuando parte del procesamiento u otras funciones sean realizadas por terceros, que es necesario conducir su revisión con los mismos estándares exigidos a la empresa, por lo que tomará en cuenta las disposiciones indicadas en la Primera Disposición Final y Transitoria del Reglamento.

Las empresas autorizadas para operar en otros módulos, para la verificación del cumplimiento antes señalado, deberán asegurar una combinación apropiada de auditoría interna y/o externa, compatible con el nivel de complejidad y perfil de riesgo de la empresa. La Superintendencia dispondrá un tratamiento similar a las empresas pertenecientes al módulo 3, cuando a su criterio la complejidad de sus sistemas informáticos y su perfil de riesgo así lo amerite.

Información a la Superintendencia

Artículo 18°.- El informe anual que las empresas deben presentar a la Superintendencia, según lo dispuesto en el Artículo 13° del Reglamento, deberá incluir los riesgos de operación asociados a la tecnología de información, como parte integral de dicha evaluación, para lo cual se

sujetará a lo dispuesto en dicho Reglamento y a lo establecido en la presente norma.

Sanciones

Artículo 19°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plan de adecuación

Artículo 20°.- En el Plan de Adecuación señalado en el segundo párrafo de la Cuarta Disposición Final y Transitoria del Reglamento, las empresas deberán incluir un sub-plan para la adecuación a las disposiciones contenidas en la presente norma.

Plazo de adecuación

Artículo 21°.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vence el 30 de junio de 2003.

ANEXO 3: GUÍA PARA LA EVALUACIÓN DE ASPECTOS DE SEGURIDAD DE INFORMACIÓN ADECUADOS CON ESTÁNDARES ISO

Alcance

Esta guía cubre todos los 39 objetivos de control listados en las secciones 5 a 15 de ISO/IEC 17799:2005 Tecnología de la información: Código de buenas prácticas para la gestión de la seguridad de la información, incluyendo adicionalmente la sección 4, relacionada a la evaluación y tratamiento de riesgos de tecnología de información.

Objetivo

Este documento pretende complementar y detallar la evaluación de los aspectos de seguridad de información del Banco, aplicando estándares ISO/IEC de gestión de seguridad de la información.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
4. Evaluación y tratamiento de riesgos			
4.1	Evaluación de riesgos de seguridad	Verifique la aplicación de un método de gestión de riesgos de seguridad de la información, con preferencia por métodos	Porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		documentados, estructurados y generalmente aceptados.	
4.2	Tratamiento de riesgos de seguridad	Verifique si por los riesgos identificados, existe evidencia de que la gerencia (específicamente, los propietarios de activos de información) necesitan evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones deberían documentarse y detallarse en un Plan de Tratamiento de Riesgos (PTR). Por otro lado, es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información identificados y que se estiman dentro de la "tolerancia al riesgo" de la organización, sin embargo, debe existir	Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia. Costes de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI. Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios. Porcentaje de riesgos de seguridad de la información con "tolerancia al riesgo" no documentados.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		documentación que sustente tal decisión.	
5. Política de seguridad			
5.1	Política de seguridad de la información	Verifique la existencia de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Evalúe la determinación y cumplimiento de la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones.	Cobertura de la política, es decir, porcentaje de secciones de ISO/IEC 17799:2005 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o autoevaluación).

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
6. Aspectos organizativos de la seguridad de la información			
6.1	Organización interna	Verifique la definición formal y existencia de una organización interna orientada a la gestión de riesgos de seguridad de la información.	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.
6.2	Terceros	Verifique si existe un inventario de conexiones de red y flujos de información significativos con terceras partes, evalúe sus riesgos y revise los controles de seguridad de información existentes	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras. Porcentaje de cláusulas cumplidas por

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		respecto a los requisitos. Considere la existencia de contratos con cláusulas específicas y evalúe el cumplimiento de dichas cláusulas a los *partners* más críticos, tales como *outsourcing* de TI, proveedores de servicios de seguridad TI, etc.	terceros. Porcentaje de servicios con terceros cuyos contratos no cuentan con cláusulas mínimas exigidas.
7. Gestión de activos			
7.1	Responsabilidad sobre los activos	Verifique la existencia de un inventario de activos de información, que señale entre otros aspectos, los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.).	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
			necesario y para mantener dichos riesgos en niveles aceptables.
7.2	Clasificación de la información	Verifique la existencia de procedimientos formales para la evaluación de la clasificación de la información y activos relacionados, y que exista una frecuencia para la realización de dicho procedimiento.	Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").
8. Seguridad ligada a los recursos humanos			
8.1	Antes de la contratación	Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del	Porcentaje de nuevos empleados o *pseudoempleados* (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.	
8.2	Durante la contratación	La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc. Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.	Respuesta a las actividades de concienciación en seguridad medidas por, p. ej., el número de emails y llamadas relativas a iniciativas de concienciación individuales.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
8.3	Cese o cambio de puesto de trabajo	La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Examine qué accesos necesita revocar en primer lugar cuando un empleado presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables? Haga un seguimiento del uso del email por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).	Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
9. Seguridad física y ambiental			
9.1	Áreas seguras	Verifique y pruebe los procedimientos de control de acceso al Centro de Procesamiento de Datos. Solicite y evalúe las condiciones físicas y ambientales definidas para el Centro de Procesamiento de Datos. Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar un mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Asegúrese de verificar que los procedimientos internos contemplan el retiro de todos los pases de empleado y de	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		visita cuando se vayan. Verifique que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso.	
9.2	Seguridad de los equipos	Verifique si los vigilantes de seguridad impiden a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) retirar equipos informáticos de las instalaciones sin autorización escrita.	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.
10. Gestión de comunicaciones y operaciones			
10.1	Responsabilidades y procedimientos de operación	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades,	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		identificadas en el manual de política de seguridad de la organización.	que ha llevado parchear al menos la mitad de los sistemas vulnerables esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón).
10.2	Gestión de la provisión de servicios por terceros	Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. Revise y evalué las cláusulas de seguridad de información, penalidades, auditoría, entre otras, establecidas en contratos firmados con terceros.	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.
10.3	Planificación y aceptación del sistema	Evalué los procedimientos definidos para la planificación y aceptación del sistema	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
			rechazados frente a cambios exitosos. Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similares y (b) cuya conformidad con dichos estándares ha sido comprobada mediante *benchmarking* o pruebas.
10.4	Protección contra código malicioso y móvil	Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación). No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo emails de remitentes desconocidos o descargando archivos de sitios no confiables.	Tendencia en el número de virus, gusanos, troyanos o *spam* detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.
10.5	Copias de seguridad	Verifique la existencia y aplicación de procedimientos de backup y recuperación	Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización. Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Verifique si la información más sensible, se encuentra encriptada.	exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.
10.6	Gestión de la seguridad de las redes	Evalúe los estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
10.7	Manejo de los soportes	Verifique los procedimientos de control para los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Verifique si existen y se aplican procedimientos de encriptación para los datos sensibles o valiosos antes de ser transportados.	Porcentaje de soportes de backup o archivo que están totalmente encriptados.
10.8	Intercambio de información	Verifique la existencia y aplicación de procedimientos de control establecido para el intercambio de información, por email, FTP, entre otros.	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.
10.9	Servicios de comercio electrónico	Evalúe los procedimientos de control establecido para el comercio electrónico.	"Estado de la eSeguridad", es decir, un informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de penetración, incidentes actuales o

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
			recientes, vulnerabilidades actuales conocidas, cambios planificados, etc.
10.10	Supervisión	Analice la criticidad e importancia de los datos monitoreados y verifique si existen otros datos críticos no considerados y que afectan los objetivos globales de negocio de la organización en relación a la seguridad de la información.	Porcentaje de sistemas cuyos *logs* de seguridad (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de *logs* y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los *logs* de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.
11. Control de accesos			
11.1	Requisitos de	Verifique que existen propietarios de activos de información, y que cuentan con	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios"

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
	negocio para el control de accesos	la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.	adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo o encargado revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.
11.2	Gestión de acceso de usuario	Verifique la existencia y aplicación de procedimientos formales para la gestión de accesos de usuarios, con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la dirección de seguridad de la información. Verifique si se cuentan con herramientas para realizar el monitoreo de accesos y si son utilizadas.	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes").

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
11.3	Responsabilidades del usuario	Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Verifique si existen procedimientos de monitoreo.	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentadas y (b) formalmente aceptadas.
11.4	Control de acceso a la red	Evalúe los controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).	Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).
11.5	Control de acceso al sistema operativo	Evalúe los estándares de seguridad básica para todas las plataformas informáticas y de comunicaciones.	Estadísticas de vulnerabilidad de sistemas y redes, como nº de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
			prioridades/categorías del fabricante o propias).
11.6	Control de acceso a la aplicación y a la información	Evalúe la aplicación de controles en las aplicaciones y *middleware*.	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)".

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
11.7	Ordenadores portátiles y teletrabajo	Evalúe el cumplimiento de las políticas establecido para equipos informáticos portátiles (es decir, *laptops*, PDAs, etc.). Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.	"Estado de la seguridad en entorno portátil / teletrabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (*laptops*, PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, *firewalls* personales, etc.
12. Adquisición, desarrollo y mantenimiento de los sistemas de información			

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
12.1	Requisitos de seguridad de los sistemas de información	Evalúe si se cumplen los requisitos de seguridad de los sistemas de información.	Sistemas de información que no cuentan con requisitos mínimos de seguridad implementados.
12.2	Procesamiento correcto en las aplicaciones	Evalúe y pruebe los controles en las aplicaciones como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc. Identifique inconsistencias en la información generado por las aplicaciones.	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.
12.3	Controles criptográficos	Verifique el uso de estándares de encriptación para información sensible.	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
			meses).
12.4	Seguridad de los archivos de sistema	Verifique si se aplican los procedimientos de seguridad recomendados por el fabricante o por expertos.	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares.
12.5	Seguridad en los procesos de desarrollo y soporte	Evalúe los controles relacionados a la seguridad de la información en el ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Analice y evalúe las incidencias	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		presentadas en el proceso de desarrollo y soporte.	
12.6	Gestión de la vulnerabilidad técnica	Verifique si existen procedimientos para la actualización de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update, WSUS, entre otros). Verifique si se aplicaron los parches críticos.	Número de servidores, estaciones de trabajo, laptops con software base desactualizado.
13. Gestión de incidentes en la seguridad de la información			
13.1	Notificación de eventos y puntos débiles de la seguridad de la	Verifique la existencia y aplicación de procedimientos que permitan informar incidentes, eventos y problemas de seguridad.	Estadísticas del *helpdesk* de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
	información		información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.
13.2	Gestión de incidentes de seguridad de la información y mejoras	Verifique la existencia y aplicación de procedimientos de revisión postincidente y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.	Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida. Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.
14. Gestión de la continuidad del negocio			

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.). Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio. Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de *failover*, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante tests apropiados en los últimos 12 meses.

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		desastre. Evalúe la frecuencia de la evaluación de riesgos y análisis de impacto en el negocio. Evalúe los procedimientos de contingencia, gestión de crisis, recuperación de TI, entre otros. Obtenga consejos de implantación en BS 25999 Gestión de la Continuidad de Negocio.	
15. Cumplimiento			
15.1	Cumplimiento de los requisitos legales	Verifique si se han establecido en normas internas aspectos relacionados con normas legales, por ejemplo, tiempo mínimo para mantener información histórica, procedimientos para el cambio de datos de	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).

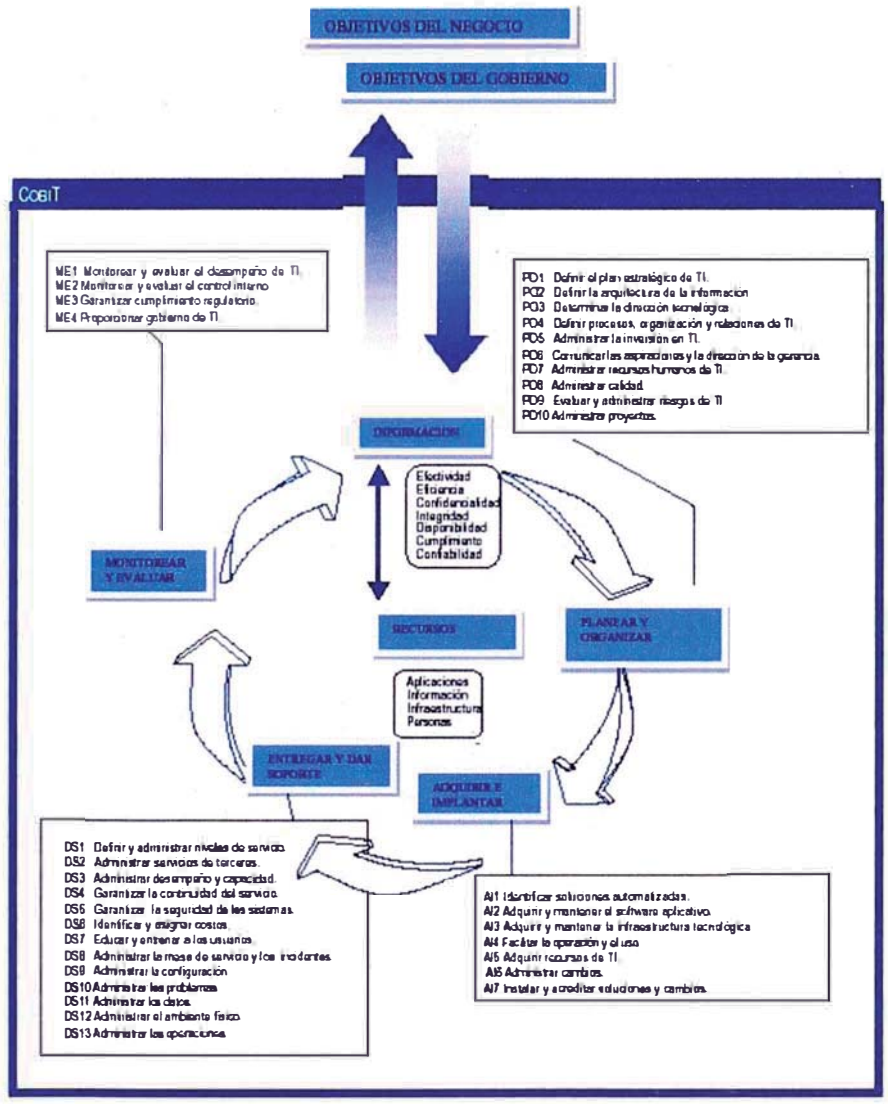
Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
		clientes, entre otros.	Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	Evalúe el cumplimiento de políticas y normas de seguridad.	Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.
15.3	Consideraciones de las auditorías de los sistemas de	Verifique si se han implementado oportunamente las observaciones y recomendaciones señaladas en las	Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o

Ref.	Objetivo	Aspectos a evaluar	Posibles métricas
	información	auditorías realizadas a los recursos de TI.	bajo). Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.

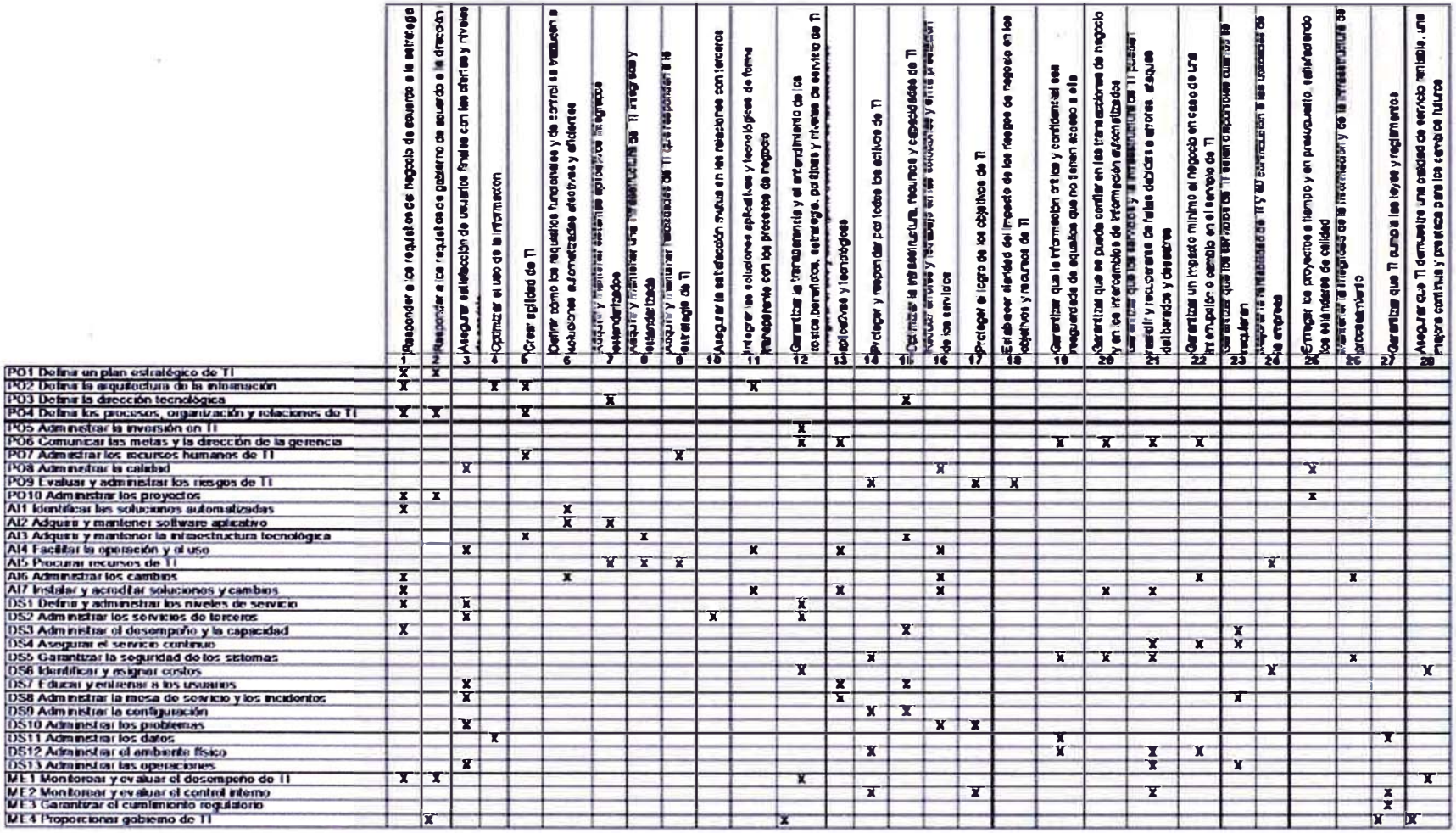
ANEXO 4

ESQUEMAS DE PROCESOS Y METAS DE NEGOCIO, PROCESOS, CONTROLES Y METAS DE TI, SEGÚN COBIT

DOMINIOS Y PROCESOS DE TI



PROCESOS Y METAS DE TI SEGÚN COBIT



Equivalencia entre los procesos de TI y las áreas focales del gobierno de TI, COSO, los recursos TI de COBIT y los criterios de información de COBIT

		Áreas focales de gobierno de TI					COSO					Recursos TI de COBIT				Criterios de información de COBIT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Administración de recursos	Administración de riesgos	Medición del desempeño	Medio ambiente de control	Evaluación de riesgos	Actividades de control	comunicación	Vigilancia	Personas	Información	Aplicación	Infraestructura	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y organizar																						
PO1 Definir un plan estratégico de TI	A	P		S	S			P		S	S	X	X	X	X	P	S					
PO2 Definir la arquitectura de la información	B	P	S	P	S				P	P			X	X		S	P	S	P			
PO3 Definir la dirección tecnológica	M	S	S	P	S			S	P	S				X	X	P	P					
PO4 Definir los procesos, organización y relaciones de TI	B	S		P	P		P			S	S	X				P	P					
PO5 Administrar la inversión en TI	M	S	P	S		S		S	P			X		X	X	P	P					S
PO6 Comunicar las metas y la dirección de la gerencia	M	P			P		P			P		X	X			P					S	
PO7 Administrar los recursos humanos de TI	B	P		P	S	S	P			S		X				P	P					
PO8 Administrar la calidad	M	P	S		S		P		P	S	P	X	X	X	X	P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	A	P			P			P				X	X	X	X	S	S	P	P	P	S	S
PO10 Administrar los proyectos	A	P	S	S	S	S	S	S	P		S	X		X	X	P	P					
Adquirir e implantar																						
AI1 Identificar las soluciones automatizadas	M	P	P	S	S				P					X	X	P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P					X		P	P		S			S
AI3 Adquirir y mantener la infraestructura tecnológica	B			P					P						X	S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S		X		X	X	P	P		S	S	S	S
AI5 Procurar recursos de TI	M		S	P					P			X	X	X	X	S	P				S	
AI6 Administrar los cambios	A		P	S				S	P		S	X	X	X	X	P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S	X	X	X	X	P	S		S	S		
Entregar y dar soporte																						
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S	X	X	X	X	P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S	X	X	X	X	P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S			X	X	P	P			S		
DS4 Asegurar el servicio continuo	M	S	P	S	P	S	S		P	S		X	X	X	X	P	S			P		
DS5 Garantizar la seguridad de los sistemas	A			P					P	S	S	X	X	X	X			P	P	S	S	S
DS6 Identificar y asignar costos	B		S	P		S			P			X	X	X	X		P					P
DS7 Educar y entrenar a los usuarios	B	S	P		S		P			S		X				P	S					
DS8 Administrar la mesa de servicio y los incidentes	B	S	P			S	S			P	P	X		X		P	P					
DS9 Administrar la configuración	M		P		S				P				X	X	X	P	S			S		S
DS10 Administrar los problemas	M		P		S				P	S	S	X	X	X	X	P	P			S		
DS11 Administrar los datos	A		P	P	P				P				X						P			P
DS12 Administrar el ambiente físico	B			S	P			S	P						X				P	P		
DS13 Administrar las operaciones	B			P					P	S		X	X	X	X	P	P		S	S		
Monitorear y evaluar																						
ME1 Monitorear y evaluar el desempeño de TI	A					P				S	P	X	X	X	X	P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P	X	X	X	X	P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S	X	X	X	X						P	S
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P	P	S		S	P	X	X	X	X	P	P	S	S	S	S	S

Nota: La equivalencia con COSO se basa en el marco de trabajo original de COSO. La equivalencia también aplica en lo general, al subsiguiente *COSO Marco de trabajo integrado – Administración de riesgos empresariales*, el cual profundiza en el control interno, brindando un foco más robusto y extenso en el tema más amplio de administración de riesgos empresariales. Aunque no se pretende que reemplace al marco de trabajo de control interno del COSO original, sino que incorpore al marco de trabajo de control interno dentro de él, los usuarios de COBIT pueden optar por referirse a este marco de administración de riesgos empresariales tanto para satisfacer sus necesidades de control interno, como para migrar hacia un proceso de administración de riesgos más completo.

UNION DE LAS METAS DEL NEGOCIO CON LAS METAS DE TI

		Metas de negocio	Metas de TI									Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Perspectiva financiera	1	Expandir el porcentaje de mercado	25	28								X	X					
	2	Aumentar el ingreso	25	28								X	X					
	3	Retorno sobre la inversión	24										X					
	4	Optimizar el uso de recursos	14									X	X					
	5	Administrar los riesgos del negocio	2	14	17	18	19	20	21	22				X	X	X		
Perspectiva del cliente	6	Mejorar la orientación y el servicio al cliente	3	23								X						
	7	Ofrecer productos y servicios competitivos	5	24								X	X					
	8	Disponibilidad del servicio	10	16	22	23						X				X		
	9	Agilidad para responder a los requisitos cambiantes (tiempo para comercializar)	1	5	25							X	X					
	10	Optimización del costo de prestación del servicio	7	8	10	24							X					
Perspectiva interna	11	Automatizar e integrar la cadena de valor empresarial	6	7	8	11						X	X					
	12	Mejorar y mantener la funcionalidad del proceso de negocios	6	7	11							X	X					
	13	Disminuir los costos de los procesos	7	8	13	15	24						X					
	14	Cumplimiento de leyes y reglamentos externos	2	19	20	21	22	6	27					X			X	
	15	Transparencia	2	18														X
	16	Cumplimiento de políticas internas	7	13										X			X	
	17	Mejorar y mantener la productividad operativa y del equipo de trabajo	7	8	11	13						X	X					
Perspectiva de aprendizaje y crecimiento	18	Innovación del producto/negocio	5	25	28							X	X					
	19	Obtener información confiable y útil para la toma de decisiones estratégicas	2	4	12	20	26					X			X			X
	20	Adquirir y mantener personal capacitado y motivado	9									X	X					

Modelo de Madurez para Control Interno

Nivel de madurez	Estatus del ambiente de control interno	Establecimiento de controles internos
0 No existente O INEXISTENTE	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.	No existe la intención de evaluar la necesidad del control interno. Los incidentes se manejan conforme van surgiendo.
1 Inicial / ad hoc	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están conscientes de sus responsabilidades.	No existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI. Cuando se llevan a cabo, son solamente de forma ad hoc, a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente.
2 Repetible pero intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados pueden no estar conscientes de sus responsabilidades.	La evaluación de la necesidad de control sucede sólo cuando se necesita para ciertos procesos seleccionados de TI para determinar el nivel actual de madurez del control, el nivel meta que debe ser alcanzado, y las brechas existentes. Se utiliza un enfoque de taller informal, que involucra a los gerentes de TI y al equipo participante en el proceso, para definir un enfoque adecuado hacia el control para los procesos, y para generar un plan de acción acordado.
3 Proceso definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están conscientes de sus responsabilidades de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.	Los procesos críticos de TI se identifican con base en impulsores de valor y de riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además de facilitar talleres, se usan herramientas y se realizan entrevistas para apoyar el análisis y garantizar que los propietarios de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora.
4 Administrado y medible	Se define de forma periódica qué tan críticos son los procesos de TI con el apoyo y acuerdo completo por parte de los propietarios de los procesos correspondientes. La evaluación de los requisitos de control se basa en las políticas y en la madurez real de estos procesos, siguiendo un análisis meticuloso y medido, involucrando a los participantes clave. La rendición de cuentas sobre estas evaluaciones es clara y está reforzada. Las estrategias de mejora están apoyadas en casos de negocio. El desempeño para lograr los resultados deseados se supervisa de forma periódica. Se organizan de forma ocasional revisiones externas de control.	
5 Optimizado	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en auto-evaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.	Los cambios en el negocio toman en cuenta que tan críticos son los procesos de TI, y cubren cualquier necesidad de re-evaluar la capacidad del control de los procesos. Los propietarios de los procesos realizan auto-evaluaciones de forma periódica para confirmar que los controles se encuentran en el nivel correcto de madurez para satisfacer las necesidades del negocio, y toman en cuenta los atributos de madurez para encontrar maneras de hacer que los controles sean mas eficientes y efectivos. La organización evalúa por comparación con las mejores prácticas externas y busca asesoría externa sobre la efectividad de los controles internos. Para procesos críticos, se realizan evaluaciones independientes para proporcionar seguridad de que los controles se encuentran al nivel deseado de madurez y funcionan como fue planeado.