

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

No. 6 - 2008

Contenido Cerrar Imprimir Página anterior Página siguiente



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 

Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

- ▶ Introducción
- ▶ La Normativa de TI de la SUDEBAN y lo que deben hacer los entes supervisados
- ▶ Componentes de la Normativa
 - ▶ Título I: Disposiciones generales
 - ▶ Título II: Planeación estratégica y organización de los recursos de información
 - ▶ Título III: Operaciones de los Sistemas de Información
 - ▶ Título IV: Contratación de proveedores externos
 - ▶ Título V: Seguridad de la información
 - ▶ Título VI: Plan de contingencia tecnológica
 - ▶ Título VII: Mantenimiento e implantación de los sistemas de información
 - ▶ Título VIII: Redes
 - ▶ Título IX: Infraestructura de las telecomunicaciones
 - ▶ Título X: Banca Virtual
 - ▶ Título XI: Disposiciones finales
- ▶ Impacto de la normativa
- ▶ Créditos / Suscribirse

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Introducción

Hoy en día las organizaciones son altamente dependientes de la tecnología de información (TI), y a medida que se incorpora como un elemento de apoyo, los riesgos se incrementan, por lo cual se hace necesario contar con un conjunto de controles engranados que permitan mantener la continuidad operacional. Por otro lado, las grandes pérdidas sufridas a nivel mundial por fallas operacionales en las Instituciones Financieras durante los últimos años, ha traído consigo una mayor concientización de la importancia de controles en el contexto de TI y un interés por la mejora de los sistemas de control interno.

Todo esto ha movido a los organismos reguladores a considerar explícitamente el riesgo derivado del uso de la TI, entre sus criterios de vigilancia. En Venezuela, la Superintendencia de Bancos y Otras Instituciones Financieras

(SUDEBAN) ha emitido recientemente la “Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea”, cuyo objetivo principal es regular la implantación y uso de la tecnología de información de los entes bajo la supervisión del referido Organismo.

El objetivo de este boletín es presentar los aspectos más relevantes de la Normativa, y su relación con las mejores prácticas y disposiciones nacionales e internacionales. Asimismo, se analizarán las fechas y plazos relacionados, y el impacto para las instituciones financieras y entes supervisados, que se deriva de su cumplimiento.

La Normativa de TI de la SUDEBAN y lo que deben hacer los entes supervisados

La Normativa tiene como objetivo y alcance “regular la implantación y uso de la Tecnología de Información de los sujetos sometidos a la supervisión, control y regulación de la SUDEBAN...”¹.

Como una de las disposiciones iniciales, las instituciones financieras debían presentar un Plan de Acción en cuarenta y cinco (45) días continuos a partir de la fecha de recepción de la Normativa, contenido de los proyectos a ejecutar, así como los tiempos y recursos para dar cumplimiento a lo allí establecido.

¹ Artículo N° 1. Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN)

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Sin embargo, unas de las actividades primarias que deben realizar las instituciones financieras con relación a este tema, es prepararse para acometer el cumplimiento de la Normativa, así como hacer un diagnóstico de la situación actual. Por tal motivo, y tomando en cuenta lo que estas actividades implican, el día 26 de marzo de 2008, se otorgó una prórroga de 30 días continuos para la entrega de este plan.

Ahora bien, los elementos de control que se establecen en la Normativa, no son nuevos, y por el contrario, se puede observar que ésta, es el producto de una combinación de estándares internacionales de seguridad y tecnología, así como disposiciones nacionales e internacionales, relacionadas con seguridad y tecnología de la información, tal como se muestra en la Figura N° 1.

Entre los estándares, se tienen:

- CobiT (Control Objectives for Information and related Technology), el cual reúne los elementos de control de la tecnología, agrupados en cuatro (4) dominios: Planificación y Organización (PO); Adquisición e Implantación (AI); Entrega y Soporte (ES); y Monitoreo y Evaluación (ME).
- ITIL (Information Technology Infrastructure Library), el cual gobierna las mejores prácticas para le gestión del servicio de TI.

- ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements), como estándar internacional para la seguridad de la información.

Entre las disposiciones nacionales e internacionales relacionadas con seguridad de la información, podemos mencionar PCI DSS (Payment Card Industry Data Security Standard), el cual es un conjunto de normativas de seguridad para la industria de tarjetas de pago que aplica a toda organización que procese información de tarjetas de crédito o débito; así como en la circular emitida por el Consejo Bancario Nacional en Junio de 2007, en donde se indican las normas de seguridad para el manejo de información electrónica en cajeros automáticos y puntos de venta.

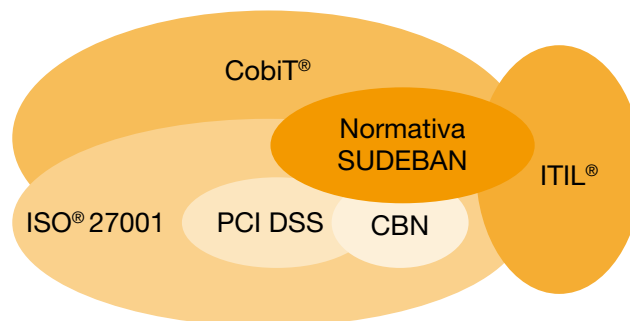


Figura N° 1. Estándares y disposiciones de seguridad y tecnología presentes en la Normativa de la SUDEBAN. ▶

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Analicemos entonces los aspectos más importantes de la Normativa, en contraste con las mejores prácticas:

Componentes de la Normativa

Título I: Disposiciones generales

En este título se establecen el objetivo principal de la Normativa, su ámbito de aplicación, los conceptos de los términos empleados, así como las definiciones de los criterios básicos de la calidad de la información, y que se encuentran definidos en CobiT (ver Figura N° 2).

Fiduciarios	<ul style="list-style-type: none">• Efectividad• Confiabilidad	<ul style="list-style-type: none">• Eficiencia• Cumplimiento
Seguridad	<ul style="list-style-type: none">• Confiabilidad• Disponibilidad	<ul style="list-style-type: none">• Integridad

Figura N° 2. Criterios de la información.

Título II: Planeación estratégica y organización de los recursos de información

- Independencia funcional de TI, políticas y procedimientos de TI:

Uno de los elementos fundamentales que se establece en los primeros artículos de la Normativa, es la independencia funcional que debe tener Tecnología de Información, con respecto a las áreas usuarias. De igual forma, la Normativa establece en su Artículo N° 7, que las políticas de TI deben estar formalmente documentadas, y que éstas deben ser de conocimiento de los usuarios, además de incluir las actualizaciones que se consideren según los cambios que hayan ocurrido en los procesos, infraestructura o personal de TI.

- Planificación estratégica de TI y Comité de Dirección y Planificación de los Servicios de Tecnología

El Artículo N° 9 de la Normativa plantea que se debe “establecer un proceso de planificación de Tecnología de la Información acorde con los objetivos del negocio”, tomando como punto de partida las iniciativas de negocio, el seguimiento continuo de las tendencias tecnológicas y las regulaciones emitidas por la SUDEBAN. Adicionalmente, se debe documentar, aprobar y monitorear un Plan Estratégico de Tecnología con los proyectos a corto plazo, cuya duración sea de un (1) año, y los proyectos a largo plazo, de duración mayor a un (1) año.

Otro aspecto fundamental que se establece en este Título, se refiere a la conformación de un Comité de Dirección y Planificación de los Servicios de Tecnología, con miembros de las áreas de Tecnología, Administración Integral de

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Riesgo, Auditoría de Sistemas y Gerentes de las unidades usuarias (Artículo N° 8). Es de hacer notar, que deberá documentarse las funciones, miembros, frecuencia de reunión, entre otros aspectos del referido Comité, y las decisiones que se acuerden en las reuniones, deberán mantenerse archivadas durante un período no menor a dos (2) años.

- Recursos Humanos

En ocasiones el personal de reciente ingreso, desconoce cuáles son sus funciones o no maneja la información necesaria para ejecutarlas; lo cual también puede ocurrir con personal con experiencia dentro de la organización, debido a que nunca se le explicó cuáles eran sus responsabilidades. En los Artículos N° 14 y N° 15 de la Normativa, se plantea que las áreas de TI y Recursos Humanos deben identificar, capacitar a los usuarios finales para brindar un uso adecuado de los recursos tecnológicos,

desarrollando una descripción detallada de roles y responsabilidades.

¿Qué dicen las mejores prácticas?

CobiT:

Si revisamos lo relacionado con la Planificación Estratégica de TI y Comité de Dirección y Planificación de los Servicios de Tecnología, en el Dominio “Planificar y Organizar” (PO), encontramos los objetivos de control que se muestran en la Tabla N° 1:



Para visualizar la tabla haga click en el icono.

Adicionalmente, en el marco de referencia CobiT se establecen varios objetivos de control detallados en el Dominio “Entregar y Dar soporte” (DS), asociados a la gestión de recursos humanos, los cuales se presentan en la Tabla N° 2.



Para visualizar la tabla haga click en el icono.

ISO/IEC 27001:

El estándar ISO/IEC 27001 por su parte, plantea los siguientes controles relacionado con el recurso humano, desde el punto de vista de seguridad:

- Definición clara de roles y responsabilidades de la seguridad de la información con base en la política de seguridad (A.6.1.3; A.8.1.1; A.8.2.1).
- Capacitación del personal para la ejecución de sus actividades y concientización sobre las políticas (A.8.2.2).

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Título III: Operaciones de los Sistemas de Información

Operaciones y procesamiento de la información

La planificación y ejecución automática de tareas, disminuye la carga de trabajo de los operadores en actividades cuya ejecución puede ser programada. Sin embargo, esta planificación automatizada de operaciones del computador, debe ser realizada bajo un entorno confiable a fin de evitar inconvenientes de seguridad ocasionados por una gestión inapropiada de estas actividades, como por ejemplo, inclusión y ejecución de tareas erróneas o no autorizadas.

Este capítulo está compuesto por seis (6) artículos, del N° 17 al N° 22, en los cuales se destacan los siguientes aspectos con relación a las operaciones de TI, a saber:

Documentación de los procesos que se realizan en el centro de procesamiento de datos, indicando:

- Comandos e instrucciones que ejecutan los operadores en el ambiente de producción.
- Registros automáticos de la ejecución de los cronogramas de trabajos, excepciones y trazas de auditoría.
- Mantenimiento y monitoreo sobre los registros automatizados de las operaciones.
- Funcionalidad y procesos que componen los cronogramas de trabajo automatizados (en línea o en lote).
- Controles que garantizan la ejecución adecuada de los cronogramas planificados.
- Mecanismos para verificar los cierres contables y distribución de información a los usuarios.
- Mecanismos de escalamiento de problemas.
 - Registro cronológico y trimestral de los procesos ejecutados.

- Revisión trimestral de las estrategias de procesamiento de la información, o cada vez que surjan cambios en la plataforma tecnológica de misión crítica².

Respaldos y resguardo de la información

La información es un activo que cada vez cobra mayor importancia dentro de la organización, ya que de ésta dependen los resultados de muchas actividades operativas críticas. En este sentido, la información debe ser respaldada y resguardada para garantizar su disponibilidad cuando sea requerida.

² En el Artículo N° 3 de la Normativa, se define Misión Crítica como: “aquellas aplicaciones, sistemas, procesos, operaciones, equipos y cableado que en caso de falla o paralización parcial o total pueden ocasionar pérdidas incalculables o severas que afecten la continuidad operativa del negocio”.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras



Este capítulo está conformado por seis (6) artículos, del N° 23 al N° 28, estableciendo lineamientos con relación al respaldo y la restauración, entre los cuales se destacan:

- Ejecución de respaldos diario, semanal y mensual, tanto de la información, como del sistema operativo, y todo software necesario para el adecuado funcionamiento de los equipos y sistemas de misión crítica.
- Pruebas periódicas de los medios de respaldo.
- Protección física y ambiental adecuada de los medios de respaldo.
- Documentación de procedimientos de respaldo y restauración.
- Ejecución de al menos dos (2) pruebas anuales de restauración.
- Identificación de los medios de respaldo, incluyendo: fecha de generación, nombre de la aplicación, tipo de información y período que se está respaldando, entre otros datos.

- Resguardo de los medios de respaldo en un mobiliario especializado.
- Disponer de centros de resguardo internos y externos, siendo este último en una ubicación remota.
- Bitácora y controles de seguridad para el traslado de medios de respaldo a locaciones externas.
- Retención de al menos diez (10) ciclos de la información de misión crítica, en el centro alterno.

¿Qué dicen las mejores prácticas?

CobiT:

Con relación a Operaciones, el objetivo de alto nivel DS13 “Administración de operaciones”, se establecen los objetivos de control detallados (ver Tabla N° 3).



Para visualizar la tabla haga click en el icono.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Asimismo, para el tema de respaldo y recuperación, el objetivo de alto nivel de CobiT, DS11 “Administración de datos”, se establecen tres (3) objetivos de control detallados que ayudan al cumplimiento de los aspectos mencionados en la Normativa, los cuales se presentan en la Tabla N° 4.



Para visualizar la tabla haga click en el icono.

ISO/IEC 27001:

Si hacemos la analogía con ISO/IEC 27001, en este estándar se establecen controles de seguridad para el proceso de respaldo y recuperación, como se especifica a continuación:

- Realización de respaldos periódicos de la información comercial y software esencial, así como la prueba de los mismos (A.10.5.1).

- Protección de los medios que contienen información crítica (A.10.7.3; A.10.8.3).

Título IV: Contratación de proveedores externos

Proveedores externos

Las organizaciones se han visto en la necesidad de tercerizar algunas de sus actividades, como estrategia de reducción de costos, y de igual forma, se hace necesario contratar los productos o servicios de tecnología de información, como parte de las estrategias y funcionamiento de equipos y aplicaciones. Algunos ejemplos son: call center (o atención a cliente), soporte técnico o help desk, impresión, mantenimiento y desarrollo de sistemas, entre otros. Sin embargo, deben establecerse “reglas de juego” para recibir el producto o servicio requerido por la organización.

En este sentido, en este título se establecen lineamientos a seguir para la gestión de proveedores, mediante nueve (9) artículos (del N° 29 al N° 37), que incluyen el proceso y criterios de selección de los proveedores de TI, consideraciones del contrato de servicios, control y seguimiento continuo y manejo de la tercerización de servicios. Adicionalmente, se establece que la SUDEBAN podrá visitar a los proveedores de servicios de tecnología de información, para realizar inspecciones, a fin de verificar el cumplimiento de los aspectos contemplados en la Normativa.

Se incluyen aspectos de selección de proveedores, tales como: estabilidad financiera y trayectoria del proveedor, costos y capacidad para brindar el servicio; y para los contratos de servicios, se establecen: acuerdos de confidencialidad, tiempos de ejecución, sanciones por incumplimiento, infraestructura tecnológica a utilizar, entre otros aspectos.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

¿Qué dicen las mejores prácticas?

CobiT:

En CobiT, específicamente en el objetivo de alto nivel DS1 “Definir y administrar los niveles de servicio”, se establecen seis (6) objetivos de control específicos con relación a la gestión de proveedores, que permiten contar con un marco de referencia en las relaciones con los proveedores, así como permite establecer los mecanismos para garantizar que se están recibiendo los servicios acordados. Los objetivos de control se enumeran a continuación:

- DS1.1 Marco de trabajo de la administración de niveles de servicio.
- DS1.2 Definición de servicios.
- DS1.3 Acuerdos de niveles de servicio.
- DS1.4 Acuerdos de niveles de operación.
- DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio.

- DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos.

ISO/IEC 27001:

Estos lineamientos se encuentran también descritos en el estándar ISO/IEC 27001, debido a que se plantea que se debe asegurar que los terceros laboren bajo los controles de seguridad, definiciones de servicio y niveles de entrega establecidos en el contrato; así como también se establece, que los servicios, reportes y registros generados por los proveedores, deben ser monitoreados y revisados periódicamente (A.10.2.1 – A.10.2.3).

ITIL:

Adicionalmente, en libro “Diseño del Servicio” (ITIL v3), específicamente en el proceso “Administración de niveles de servicio”, se contemplan los aspectos mencionados en este capítulo, y se incluyen las siguientes actividades:

- Monitorear y medir el desempeño del servicio en función de lo establecido en los contratos.
- Medir y mejorar la satisfacción del cliente.
- Diseñar y actualizar periódicamente estándares y formatos de contratos y acuerdos de servicios.

Título V: Seguridad de la información

Independencia funcional de la Función de Seguridad de la Información y políticas de seguridad:

El diseño de una administración de seguridad consistente en una organización, requiere desarrollar e implantar un conjunto de políticas de seguridad, así como procedimientos específicos que permitan el cumplimiento de las políticas, y a su vez, establezcan las actividades a ser realizadas por el personal con inherencia en la seguridad de la información.

En este sentido, en esta normativa se establecen dos (2) artículos, Artículo N° 38 y N° 39, donde

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

se establecen que se debe implementar y revisar periódicamente las políticas de seguridad de los activos informáticos de la organización, con énfasis en la administración de accesos, utilización del correo electrónico, Internet y canales electrónicos. En este sentido, se debe tomar en cuenta los siguientes aspectos:

- Se deben administrar los accesos a nivel de sistema operativo, aplicación, red y bases de datos.
- La política de seguridad de la organización establece los lineamientos para la administración y control de los accesos.

Otro aspecto importante que se plantea es la independencia funcional de Seguridad de la Información, la cual debe ser independiente de TI, Auditoría de Sistemas y Riesgo. Esto sin duda, es uno de los aspectos de impacto en la estructura organizativa de las Instituciones Financieras, ya que ocasiona que se debe analizar el reporte directo que tendrá la Función de Seguridad de la Información.

Confidencialidad de la información y auditoría

Con relación a la auditoría y confidencialidad de la información, se plantean nueve (9) artículos, del N° 40 al N° 48, en los cuales se especifican lineamientos de seguridad para equipos de red, auditoría, clasificación de la información y restricciones de acceso al ambiente productivo. En resumen, la Normativa establece aspectos como que deben existir acuerdos de confidencialidad y no divulgación definidos, y que estos acuerdos deben ser firmados por los empleados, personal temporal, contratados y usuarios externos a quienes se les provea el acceso a la información.

Asimismo, se debe establecer un esquema de clasificación de la información, que permita identificar el nivel de criticidad de un activo de información, y que adicionalmente, permita otorgar el acceso a los sistemas, aplicaciones o base de datos, de acuerdo con los perfiles de usuarios definidos y formalmente documentados.

En cuanto a logs o trazas de auditoría, la Normativa establece que deben almacenarse por al menos un (1) año, además de la existencia de un esquema de revisión y la generación de informes de las revisiones de logs realizadas.

Seguridad física

Los equipos y la adecuación de los centros de cómputos son una inversión importante que realizan las organizaciones, cuyo valor aumenta al momento que son incorporados al entorno productivo para apoyar los procesos de negocio y almacenamiento de información sensible. En este sentido, se han establecido catorce (14) artículos, desde el N° 50 al N° 63, que conforman este capítulo.

Algunos de los elementos de control que la Normativa establece a este respecto, son:

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

- Los principales equipos de cómputo y telecomunicaciones deben estar asegurados.
- Los materiales de construcción del centro de cómputos, no deben ser combustibles.
- Instalación de un sistema de detección y extinción de incendios, control de humedad y temperatura, así como la redundancia de los equipos de aire acondicionado.
- Mantenimiento adecuado de los detectores y sistemas de alarma contra incendio, salidas de emergencia, paneles de distribución eléctrica y de potencia, UPS, entre otros.
- Existencia de un sistema de seguridad eléctrica que proteja el computador central y sus periféricos, de variaciones de voltaje.
- Establecimiento de perímetros físicos para el centro de cómputo y telecomunicaciones, así como para los principales sitios alternos.
- Procedimiento para destruir los reportes generados, cuando no sean requeridos.

¿Qué dicen las mejores prácticas?

CobiT:

En CobiT se establecen varios objetivos de control detallados relacionados con la política de seguridad de la información, los cuales se presentan en la Tabla N° 5.



Para visualizar la tabla haga click en el icono.

Asimismo, el objetivo de control de alto nivel DS12 “Administración del ambiente físico”, establece cinco (5) objetivos de control detallados, relacionados con los aspectos de seguridad física contemplados en la Normativa, los cuales son:

- DS12.1 Selección y diseño del centro de datos.
- DS12.2 Medidas de seguridad física.
- DS12.3 Acceso físico.
- DS12.4 Protección contra factores ambientales.
- DS12.5 Administración de instalaciones físicas.

ISO/IEC 27001:

En relación con la independencia funcional de la Función de Seguridad en la Información, ISO/IEC 27001 establece en la sección A.6 “Organización de la Seguridad de la Información”, los controles A.6.1.1 hasta el A.6.1.3, relacionados con: 1) el compromiso de la gerencia con la seguridad de la información; 2) coordinación de la seguridad de la información; y 3) la asignación de responsabilidades de esta área.

Asimismo, si contrastamos la Normativa con el estándar ISO/IEC 27001, con respecto a la confidencialidad de la información y auditoría, se tiene lo siguiente:

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

- En el Artículo N° 40, se establece que los empleados y contratados “deben firmar de acuerdo de confidencialidad y la no divulgación de la información, como parte de sus términos y condiciones iniciales de empleo”; lo cual está contemplado en el estándar ISO/IEC 27001 en el control A.6.1.5 “Acuerdos de confidencialidad”, donde además se establece que este acuerdo debe ser revisado regularmente.
- El esquema de categorización de la información según su nivel de sensibilidad (por ejemplo: pública, confidencial, etc.), está estipulado en el control A.7.2.1 “Lineamientos de clasificación” de ISO/IEC 27001.
- La ejecución de estudios de penetración (internos y externos) con una frecuencia no mayor a un (1) año, a fin de verificar que se ha restringido el tráfico de datos entrante y saliente adecuadamente, está relacionado con los controles A.10.6.1; A.10.6.2 y A.11.4.7 del estándar ISO/IEC 27001.

- La definición, documentación y aplicación de perfiles en los sistemas, bases de datos y aplicaciones acorde con las especificaciones del cargo y actividades a realizar; así como, la restricción de acceso a los utilitarios sensitivos del sistema y de los operadores al ambiente de producción (Artículos N° 42, N° 43 y N° 47), está contemplado en el estándar ISO/IEC 27001 en los controles A.11.2.1; A.11.5.4 y A.11.6.1. Sin embargo, ISO/IEC 27001 extiende el control de la administración de acceso por parte de los usuarios, en el control A.11.2.4 “Revisión de los derechos de acceso”, en el cual se plantea la revisión periódica de los accesos otorgados a los usuarios (re-certificación de usuarios).
- La activación de los registros de auditoría para los sistemas de misión crítica, y retención de estos logs por un (1) año (Artículos N° 48 y N° 49), está en concordancia con el control A.10.10.1 “Registro de auditoría” de ISO/IEC 27001.

Con respecto a la seguridad física, a continuación se presentan los aspectos más resaltantes de la Normativa y su relación con el estándar ISO/IEC 27001:

- Instalación de un sistema de supresión de fuego de contacto seco, donde se encuentra el computador central y la cintoteca, así como mecanismos de detección y extinción de incendios, control de humedad y temperatura, y redundancia de los equipos de aire acondicionado, relacionado con el control A.9.1.4 “Protección contra amenazas externas y ambientales”.
- Realización de simulacros sobre los posibles eventos de contingencia en el centro de cómputos principal y en los centros alternos, en concordancia con el control A.14.1.5 “Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales”.
- Implementar controles de acceso físico: mecanismos de autenticación, bitácora de

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

visitantes, revisión periódica de los accesos otorgados, relacionado con los controles A.9.1.2; A.9.1.5 y A.9.1.6.

Título VI: Plan de contingencia tecnológica

Uno de los objetivos principales de un Plan de Contingencias, está asociado a la identificación de los procesos y recursos que son críticos, para sostener un desempeño aceptable en momentos de contingencia. En este sentido, la Normativa incluye cuatro (4) artículos en dos (2) capítulos diferentes, sobre el Plan de Contingencia Tecnológica, destacándose los siguientes aspectos:

- Artículo N° 64: “Existencia de un plan de contingencias tecnológicas aprobado, formalizado, actualizado, implementado y probado”, el cual debe ser revisado y actualizado periódicamente.
- Se deben generar como mínimo dos (2) copias de respaldo: una para almacenamiento in-site y otro

para el almacenamiento off-site.

- Incluir en el plan de contingencia tecnológica, el objetivo y alcance, metodología empleada, procesos críticos, clasificación de activos, prioridad y estrategia de recuperación, procedimientos detallados y tiempos de recuperación, localización de los medios de respaldo, personal contacto, niveles de escalamiento y contratos con terceros que apoyen el proceso de recuperación.
- Ejecución de simulacros al menos una (1) vez al año, según el cronograma que entregue a la Superintendencia, con participación del Auditor Interno. Los resultados obtenidos deben ser documentados y disponibles para futuras revisiones.
- Definición de procedimientos de respaldo y recuperación en las instalaciones distintas al centro de procesamiento, indicando la frecuencia, lugares de almacenamiento de los medios internos y externos, inventarios detallados, responsables y administración de los medios magnéticos.

¿Qué dicen las mejores prácticas?

CobiT:

Con relación a este tema, CobiT en su control de alto nivel DS4 “Garantizar la continuidad de los servicios”, describe la necesidad del desarrollo, mantenimiento y pruebas de los planes de continuidad de TI; almacenamiento de respaldos off-site y entrenamiento a los usuarios de forma periódica, a fin de minimizar la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos críticos del negocio. Los controles detallados, se muestran a continuación:

- DS4.1 Marco de trabajo de continuidad.
- DS4.2 Planes de continuidad de TI.
- DS4.3 Recursos críticos de TI.
- DS4.4 Mantenimiento del plan de continuidad de TI.
- DS4.5 Pruebas del plan de continuidad de TI.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

- DS4.6 Entrenamiento del plan de continuidad de TI.
- DS4.7 Distribución del plan de continuidad de TI.
- DS4.8 Recuperación y reanudación de los servicios de TI.
- DS4.9 Almacenamiento de respaldos fuera de las instalaciones.
- DS4.19 Revisión post-reanudación.

ISO/IEC 27001:

La sección A.14 “Gestión de la continuidad comercial” de este estándar establece los siguientes controles relacionados con el plan de contingencia:

- A.14.1.3 Desarrollar e implementar planes de continuidad del negocio incluyendo seguridad de la información
- A.14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio

ITIL:

Finalmente, en el libro “Diseño del Servicio” de ITIL v3 se define el proceso “Administración de la continuidad del servicio”, donde se aborda este tema, complementando con los siguientes aspectos:

- Realización del Análisis de Impacto en el Negocio (Business Impact Analysis – BIA) para cuantificar el impacto de la interrupción del servicio de TI sobre el negocio.
- Realización de Análisis de Riesgo (Risk Analysis – RA), para identificar los riesgos presentes, las amenazas asociadas y la probabilidad de materialización de los mismos, tomando en cuenta la rentabilidad de mitigar cada riesgo.
- Integración del Plan de Continuidad de TI con el resto de los planes de la organización.

Título VII: Mantenimiento e implantación de los sistemas de información

Las organizaciones deben seguir un proceso estructurado para el desarrollo y mantenimiento de sistemas, ya sea interno o externo, con la finalidad de garantizar el cumplimiento adecuado de los lineamientos establecidos por la Gerencia y la obtención de mejores resultados. Asimismo, algunas veces no se consideran de manera temprana, los mecanismos de seguridad que garanticen el acceso y la calidad de la información manejada. Esta temática está contemplada dentro de la Normativa en los Artículos N° 70 al N° 96, tratando lo siguiente:

Metodología e inclusión de la seguridad

Con relación a estos aspectos, se establece lo siguiente:

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

- Implementar una metodología de ciclo de vida del desarrollo de sistemas de información, que incluya el análisis de factibilidad.
- Procedimientos de control de cambios a programas, incluyendo el tratamiento de emergencias.
- Segregar los ambientes de desarrollo, calidad y producción, implementando los mecanismos de control de acceso correspondientes.
- El pase a producción debe ser realizado por personal que no esté relacionado con el área de desarrollo y mantenimiento.
- Definición e implantación de procedimientos automatizados que garanticen que el ejecutable corresponda a la última versión desarrollada.
- Establecimiento de estándares de pruebas, documentación y resguardo de resultados.
- Mantenimiento de la documentación técnica de los sistemas, incluyendo: objetivos, alcance, diagrama del sistema, registro de modificaciones, lenguaje de programación, manejador de bases de datos empleados,

- descripción del hardware y software, su interrelación, interconexión, descripción de las pantallas.
- Establecer formalmente los acuerdos para los desarrollos externos, considerando:
 - Uso de licencias.
 - Propiedad y custodia del código fuente durante el desarrollo.
 - Pruebas y certificación de la calidad del desarrollo.
 - Documentación del diagrama de entidad-relación, manuales técnico, de usuario y de instalación.
- Existencia de un Comité Técnico que supervise las actividades y garantice el cumplimiento de los lineamientos establecidos para el desarrollo y mantenimiento de sistemas (comité de Control de Cambios), el cual debe estar conformado como mínimo por los líderes de las áreas de Desarrollo/Mantenimiento, Planificación y Producción, Auditoría y Seguridad de la Información, con las siguientes funciones:

- Garantizar el cumplimiento de los lineamientos establecidos para todas las solicitudes recibidas.
- Evaluar las solicitudes de cambio (factibilidad, clasificación, prioridad).
- Coordinar las ventanas de tiempo para la implantación de los cambios solicitados.
- Aprobación de los cambios a efectuarse sobre las bases de datos, por parte del Administrador de Base de Datos junto con el Comité Técnico.
- Realización y documentación de pruebas unitarias e integrales, con participación del personal usuario y del Comité Técnico (las cuales deben ser firmadas).

Arquitectura de la información

Con relación a este tema, se establece lo siguiente:

- Creación de un modelo de arquitectura de información, incluyendo los modelos de datos corporativos y los sistemas de información

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras



- asociados; el cual debe ser consistente con el plan a largo plazo definido como cumplimiento del Artículo N° 9 de la Normativa.
- Creación y actualización continua del diccionario de datos corporativo, contemplando las reglas de sintaxis de datos.
 - Restricción de acceso al ambiente productivo al proveedor y a los desarrolladores.
 - Ejecución de cambios del sistema manejador de bases de datos, sólo por el Administrador de Datos.
 - Existencia de controles para garantizar la integridad de base de datos.
 - Registro de las transacciones de acceso y cambios en los repositorios donde se almacenen los programas fuentes.

¿Qué dicen las mejores prácticas?

CobiT:

CobiT en los Dominios “Planificar y Organizar”

(PO), y en el Dominio “Adquirir e Implantar” (AI), define controles relacionados a estos Artículos (ver Tabla N° 6).



Para visualizar la tabla haga click en el icono.

ISO/IEC 27001:

Asimismo, al contrastar el contenido de estos Artículos con las mejores prácticas, en el estándar ISO 27001/IEC se establecen los controles asociados, presentados en la Tabla N° 7.



Para visualizar la tabla haga click en el icono.

Título VIII: Redes

La Normativa aborda el tema de la infraestructura de redes y su administración en nueve (9) artículos, del N° 102 al N° 110, contemplando lo siguiente:

- La responsabilidad operativa de los dispositivos de red no puede ser asignada al personal responsable de las operaciones del computador central.
- Procedimientos para la administración de equipos remotos, incluyendo lineamientos para la gestión de usuarios como:
 - No se pueden utilizar claves genéricas.
 - Autorización de acceso.
 - Formalizar la entrega del usuario y de la contraseña.
 - Eliminación oportuna de cuentas redundantes y aquellas correspondientes a usuarios egresados.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

- Procedimientos para implantar mecanismos para restringir el acceso de los puertos de diagnóstico remoto.
- Protección de la información mediante mecanismos de cifrado.
- Monitoreo de eventos en los equipos de red.
- Restricción de los privilegios de acceso a los usuarios, y registro de las actividades realizadas.
- Control en la asignación y uso de privilegios especiales que permita que un usuario pueda evadir los controles de seguridad de los sistemas.

¿Qué dicen las mejores prácticas?

CobiT:

De igual forma, las mejores prácticas abarcan este tópico. En el caso de CobiT se plantean los objetivos de control específicos presentados en la Tabla N° 8, los cuales pertenecen al Dominio “Entregar y Dar soporte” (DS).



Para visualizar la tabla haga click en el icono.

Título IX: Infraestructura de las telecomunicaciones

La infraestructura de las telecomunicaciones está contemplada en doce (12) artículos, del N° 111 al N° 122, planteando:

- Cumplimiento de la norma ANSI/EIA/TIA-606 con respecto al cableado estructurado, en la cual se establece diversos colores para los cables según su función, algunos de los cuales se muestran en la Figura N° 3.






	Terminación central de oficina
	Conexión de red/circuito auxiliar
	Conexión mayor/circuito de datos
	Terminación de cable IC a MC
	Sistema telefónico

Figura N° 3. Identificación de los cables de telecomunicaciones.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Contenido Cerrar Imprimir Página anterior Página siguiente



- Empleo de mecanismos adecuados de seguridad física en el cuarto de telecomunicaciones.
- Utilización de racks para los equipos de red activos.
- Documentación técnica de la infraestructura, contemplando:
 - Diagrama lógico de red.
 - Descripción de los elementos de cableado.
 - Planos de trayectoria del cableado y ubicación de los puntos de salida.
 - Diagrama del sistema de patcheo.
 - Informe de certificación y diagrama del cableado estructurado, según lo establecido en las normas TIA/EIA/568B.

Título X: Banca Virtual

Este título está conformado por nueve (9) artículos, del N° 123 al N° 130, sobre la administración y control del servicio de banca virtual, destacándose los siguientes aspectos:

- Aprobación de la SUDEBAN para brindar servicios como historial de transacciones, pagos y transferencias.
- Identificación, medición, monitoreo y administración de los riesgos asociados a este canal.
- Auditoría de Sistemas debe realizar seguimiento continuo al funcionamiento de la Banca Virtual.
- Informar al usuario sobre las condiciones y costos del uso de la Banca Virtual, así como de la necesidad de proteger su información.

- Mantener una bitácora de acceso y de uso del servicio de la Banca Virtual, donde se almacene las transacciones y autenticaciones, por un período no menor a cinco (5) años (a partir de la fecha de la transacción).
- Mecanismos de control que permitan alertar las fallas y minimizar las vulnerabilidades técnicas presentes en la plataforma tecnológica que apoya el servicio de Banca virtual.

¿Qué dicen las mejores prácticas?

ISO 27001/IEC:

En ISO 27001/IEC este tema es tratado en los controles A.10.9.1 “Comercio electrónico”; A.10.9.2 “Transacciones en-línea”; y A.10.9.3 “Información disponible públicamente”, estableciendo que se deben implementar mecanismos de seguridad a la información sensible que se transmite a través de redes públicas.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Título XI Disposiciones finales

Los Artículos N° 132, N° 133 y N° 134 establecen el cumplimiento obligatorio de esta Normativa, en conformidad con el Artículo 251 de la Ley General de Bancos y Otras Instituciones Financieras, así como fomentar el desarrollo del talento humano y el uso obligatorio de Sistemas de Reclamos para monitorear y controlar los canales electrónicos.

Impacto de la Normativa

El cumplimiento de esta Normativa tiene un impacto significativo en los entes supervisados, en su planificación y en sus actividades diarias con respecto al uso de la tecnología, si se considera que:

- Los entes supervisados deben realizar inversiones para adaptar su infraestructura tecnológica a los requerimientos establecidos.
- La ejecución de proyectos que habían sido planificados, deberá ser postergada como consecuencia de la ejecución del plan de acción para el cumplimiento de esta Normativa, lo cual deberá realizarse en un lapso de ocho (8) meses.
- Esfuerzo y dedicación del personal fijo y proveedores para dar cumplimiento en los lapsos establecidos, pudiendo afectar las actividades cotidianas del personal.

- Con relación a los roles y responsabilidades que no habían sido contemplados, deben ser asignados a personal existente, e incluso se prevé que se pudieran crear nuevos puestos de empleo.
- Pueden existir contratos y acuerdos, cuyas cláusulas deban ser negociados nuevamente con los proveedores.
- Adaptación de la infraestructura tecnológica y adecuaciones.
- Se deberá considerar la coexistencia con la potencial exigencia del cumplimiento del estándar PCI-DSS (Payment Card Industry - Data Security Standard) y la circular del Consejo Bancario Nacional relacionada con las normas de normas de seguridad para el manejo de información electrónica en cajeros automáticos y puntos de venta.

Boletín de Asesoría Gerencial*

Normativa de Tecnología de Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y En Línea: un nuevo reto para las Instituciones Financieras

Contenido Cerrar Imprimir Página anterior Página siguiente

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado mensualmente por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666



© 2008. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3

Tabla N° 1.: Objetivos de control detallados asociados a la planificación estratégica.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
PO1.2 Alineación de TI con el negocio	<ul style="list-style-type: none">- Comunicar a los ejecutivos las oportunidades que ofrece TI.- Asegurar el entendimiento del rumbo del negocio, para saber cómo dirigir a TI.- Las estrategias de TI deben estar alineadas con el negocio, relacionando las metas y reconocer las oportunidades y limitaciones en la capacidad actual.
PO1.3 Evaluación del desempeño actual	<ul style="list-style-type: none">- Evaluar la contribución de los recursos de TI y su desempeño en el plan.
PO1.4 Plan estratégico de TI	<ul style="list-style-type: none">- Crear un plan estratégico de TI para indicar cómo TI contribuirá con las demás unidades de negocio, cómo se cumplirán los objetivos, presupuesto de inversión, estrategias de adquisición, requerimientos legales y reguladores, entre otros.
PO1.5 Planes tácticos de TI	<ul style="list-style-type: none">- Crear un portafolio de planes tácticos que se deriven del plan estratégico, describiendo las iniciativas y los requerimientos de recursos requeridos por TI, entre otros.
PO3.1 Planeación de la dirección tecnológica	<ul style="list-style-type: none">- Analizar las tecnologías existentes y emergentes.- Planificar la dirección estratégica apropiada para materializar la estrategia de TI y la arquitectura de sistemas de negocio.- El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de infraestructura.
PO3.3 Monitoreo de tendencias y regulaciones futuras	<ul style="list-style-type: none">- Establecer un proceso para monitorear las tendencias tecnológicas, de infraestructura, legales y regulatorias.
PO4.2 Comité estratégico	<ul style="list-style-type: none">- Establecer un comité estratégico de TI a nivel de consejo directivo, como parte del Gobierno Corporativo, para asesorar sobre la dirección estratégica

Tabla N° 2. Objetivos de control detallados de CobiT® asociados a la gestión de recursos humanos.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
DS7.1 Identificación de necesidades de entrenamiento y educación	<p>-Establecer y cumplir un programa de entrenamiento para los grupos de empleados, tomando en cuenta los siguientes aspectos:</p> <ul style="list-style-type: none">- Estrategias y requerimientos actuales y futuros del negocio- Valores corporativos (ej: cultura del control y seguridad)- Implementación de nuevo software e infraestructura de TI- Habilidades necesarias- Métodos de impartición y material de apoyo
DS7.2 Impartición de entrenamiento y educación	Identificar cómo se agruparan los empleados, mecanismos de entrenamiento, personal (instructores y participantes), evaluaciones de desempeño.
DS7.3 Evaluación del entrenamiento recibido	Al final el entrenamiento, se evaluarán los resultados del entrenamiento para ayudar en la planificación de futuros cursos.

Tabla N° 3. Objetivos de control detallados de CobiT asociados a la planificación y monitoreo de operaciones.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
DS13.1 Procedimientos e instrucciones de operación	Definir, implantar, mantener y divulgar procedimientos para operaciones de TI, tomando en cuenta aspectos como la entrega de turnos, estatus, actualizaciones, escalamiento, reportes, entre otros.
DS13.2 Programación de tareas	Optimizar la programación de trabajos, procesos y tareas en la secuencia más eficiente. La versión inicial y los cambios posteriores deben ser aprobados.

Tabla N° 4: Objetivos de control detallados de CobiT® asociados al proceso de respaldo y restauración.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
DS11.2 Acuerdos de almacenamiento y conservación	Procedimientos para almacenar los datos, considerando requerimientos de recuperación y seguridad, rentabilidad e integridad continua.
DS11.5 Respaldo y restauración	Procedimientos de respaldo y restauración de los sistemas, configuración e información que estén alineados con los requerimientos del negocio y con el BCP. Adicionalmente, los medios de respaldos deben ser probados periódicamente.
DS11.6 Requerimientos de seguridad para la administración de datos	Establecer mecanismos para identificar y aplicar requerimientos de seguridad de los medios de respaldo almacenados en el exterior de la organización.

Tabla N° 5. Objetivos de control detallados de CobiT® asociados a la política de seguridad.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
DS5.2 Plan de seguridad de TI	<ul style="list-style-type: none">- El plan de seguridad de TI se implementa con políticas y procedimientos de seguridad en conjunto con las inversiones en servicios, personal, software y hardware; tomando en cuenta las necesidades de la organización.
DS5.3 Administración de identidad	<ul style="list-style-type: none">- Todos los usuarios y sus actividades dentro de TI deben ser identificables. Los privilegios de acceso de los usuarios deben definirse con base a las necesidades del negocio y con requerimientos de trabajo.- Las identidades de los usuarios y sus derechos deben ser almacenados centralizadamente.
DS5.4 Administración de cuentas de usuario	<ul style="list-style-type: none">- Las acciones sobre las cuentas de usuarios deben ser realizadas por una sola área. Adicionalmente, se deben documentar los procedimientos para realizar estas tareas.- Los accesos otorgados deben ser revisados periódicamente en conformidad con la política de seguridad.

Tabla N° 6. Objetivos de control detallados de CobiT® asociados al mantenimiento de sistemas.

[Regresar al boletín](#) [Aumentar](#) [Imprimir](#)



Objetivo de control	Descripción
PO2.1 Modelo de arquitectura de información empresarial	Establecer y mantener un modelo de arquitectura que facilite el desarrollo de aplicaciones y la toma de decisiones.
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	Mantener un diccionario empresarial que incluya las reglas de sintaxis de datos, facilitando que las aplicaciones y los sistemas compartan los elementos de datos.
PO8.3 Estándares de desarrollo y adquisición	Adoptar y mantener estándares de desarrollo homogéneamente.
AI2 Adquirir y mantener	Las aplicaciones deben estar disponibles con base a los requerimientos del negocio, a través del diseño, inclusión de funcionalidades y mecanismos de seguridad, desarrollo y la configuración de acuerdo a los estándares.
AI4 Facilitar la operación y el uso	Entrenamiento del personal, incluyendo la documentación del sistema, para garantizar el uso adecuado de las aplicaciones y los sistemas.
AI6 Administrar cambios	Satisfacer los requerimientos del negocio que originaron el cambio, evitando errores y repeticiones de trabajo en la entrega de soluciones y servicios.
AI7 Instalar y acreditar soluciones y cambios	Una vez que los sistemas están desarrollados, deben ser probados en un ambiente separado, aceptados, liberados y monitoreados.

Tabla N° 7. Controles en ISO 27001/IEC asociados al mantenimiento de sistemas.

Regresar al boletín Aumentar Imprimir



Controles

A.6.1.3 Asignación de responsabilidades de la seguridad de la información

A.10.1.3 Segregación de funciones

A.10.1.4 Separación de los medios de desarrollo y operacionales

A.10.2.2 Monitoreo y revisión de los servicios de terceros

A.10.2.3 Manejar los cambios en los servicios a terceros

A.10.3.2 Aceptación del sistema

A.10.10.4 Registros del administrador y operador

A.11.5.4 Uso de utilidades del sistema

A.12.5.1 Procedimientos de control de cambio

A.12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo

Tabla N° 8: Objetivos de control detallados de CobiT® asociados a las redes.

Regresar al boletín Aumentar Imprimir



Objetivo de control	Descripción
DS5.3 Administración de identidad	Todos los usuarios y sus actividades dentro de TI deben ser identificables. Los privilegios de acceso de los usuarios deben definirse con base a las necesidades del negocio y con requerimientos de trabajo. Las identidades de los usuarios y sus derechos deben ser almacenados centralizadamente.
DS5.10 Seguridad de la red	Técnicas y procedimientos de administración para proteger la información sensible y controlar el flujo de información desde y hacia la red interna.
DS13.3 Monitoreo de la infraestructura de TI	Definir e implantar procedimientos para el monitoreo de la infraestructura de TI. Garantizar la disponibilidad de las trazas de auditoría.