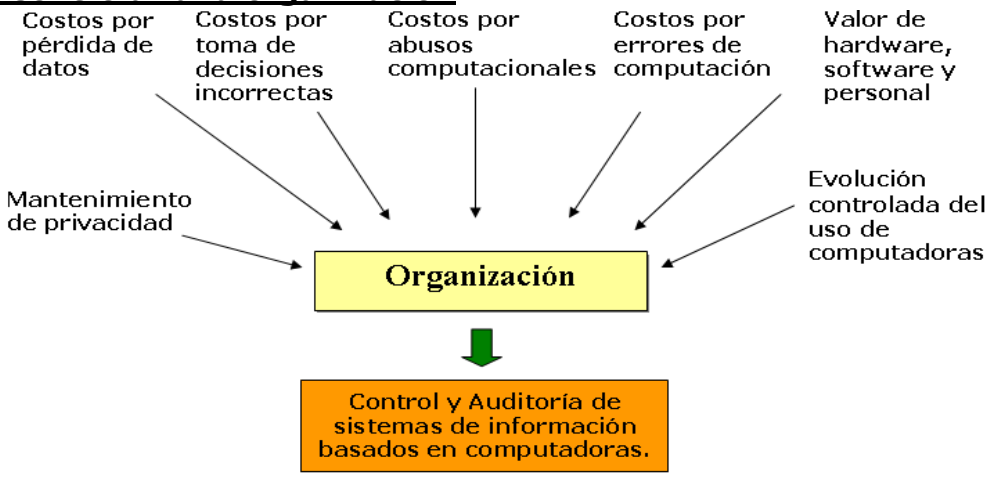
Auditoría de Sistemas
Módulo 1: Conceptos Básicos

Razones para Controlar una organización



Costos por pérdidas de Datos
Los datos proveen a la organización de una imagen de sí misma, de su entorno, de su historia, y su futuro. Si la imagen es exacta, la organización aumenta las posibilidades de adaptarse y sobrevivir a un entorno cambiante. Si la imagen es inexacta, se puede incurrir en pérdidas.

Costos por toma de decisiones incorrectas
La alta calidad en la toma de decisiones depende, en parte, de la calidad de los datos y de la calidad de las reglas de decisión que existen en los SI automatizados. La importancia de datos exactos depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
- Alta Gerencia: Planeamiento estratégico → probablemente acepten algunos errores en los datos.
- Gerencia Media: Control administrativo y operativo → requieren datos más exactos.

Las decisiones para que los datos sean correctos involucran detección, investigación y corrección de procesos fuera de control. El tener reglas de decisión exactas en un SI depende del tipo de decisiones hechas por personas que tienen algún interés en la organización. Una regla de decisión incorrecta puede tener un impacto menor (Ej.: cálculo de amortización erróneo en un bien de poco valor) o puede ser considerable (Ej.: cálculo erróneo en la cantidad de servidores en un buscador).

Costos por Abuso Computacional
Un abuso computacional es un incidente asociado con tecnología de computación, en el cual una víctima sufre o podría haber sufrido pérdida, y un perpetrador con intención logra o podría lograr ganancias. Los tipos de abuso computacional son:
- **Hacking**
  Una persona logra un acceso no autorizado a un sistema de computación para leer, modificar o borrar programas o datos, o para discontinuar un servicio.
- **Virus**
  Son programas que atacan a archivos ejecutables, áreas del sistema, o archivos de datos que contienen macros, para causar una disfunción en las operaciones computacionales o dañar datos y programas.
- **Acceso Físico Ilegal**
  Una persona logra un acceso físico no autorizado al lugar donde se encuentra la computadora. Como resultado, pueden causar daño físico al hardware o hacer copias no autorizadas de programas y datos. Ejemplo: acceso a una sala de cómputos o a un terminal.
- **Abuso de Privilegios**
  Una persona usa privilegios que le han sido asignados para propósitos no autorizados (Ej.: Hacer copias no autorizadas de datos confidenciales)

Las consecuencias pueden ser la destrucción, sustracción o modificación de activos, la violación de la privacidad, la interrupción de operaciones, el uso no autorizado de activos o el daño físico a personas.

Costos por Errores de Computación
Los costos por un error de computación pueden ser altos, en términos de pérdida de vida humana, privación de libertad o daño al medio ambiente. Ya que los sistemas pueden controlar el monitoreo de pacientes, cirugías, vuelo de misiles, o reactores nucleares.

Valor de los activos
- Datos: ¿qué pasa si la competencia obtiene información confidencial?
- Hardware: ¿qué pasa si un componente crítico deja de funcionar?
- Software: ¿qué pasa si se destruye?
- Personal: ¿qué pasa si un profesional calificado deja la empresa?

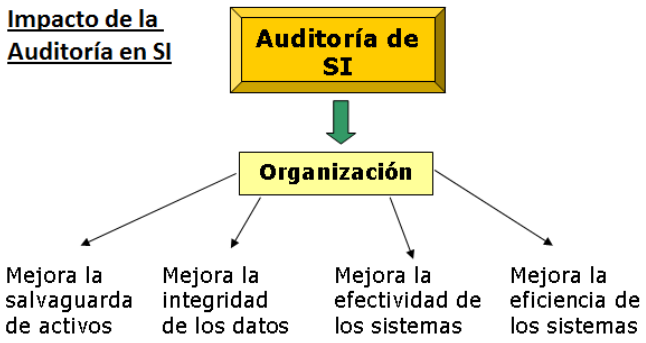
Mantenimiento de Privacidad
Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia. Con sistemas automatizados se puede integrar y buscar información que en las manos incorrectas podría utilizarse para obtener detalles de una persona y usarlos en su contra.
Evolución controlada del Uso
Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada. Las consecuencias de usar sistemas no confiables pueden ser catastróficas.

Auditar
Es el proceso sistemático de obtener y evaluar evidencia sobre las acciones económicas y eventos a fin de determinar que tan bien se corresponden con los criterios establecidos.

Tipos de auditorías
- **Financiera**
  Examina la confiabilidad e integridad de transacciones financieras, registros contables, estados financieros, etc.
- **Sistemas de Información**
  Revé los controles de los sistemas de información para ver si cumplen con las políticas de control interno y son efectivas en salvaguardar los activos de la organización.
- **Operacional**
  Se busca un uso económico y eficiente de los recursos para poder cumplir con los objetivos establecidos.
- **Cumplimiento**
  Determinar si las entidades cumplen con las leyes aplicables, regulaciones, políticas y procedimientos.
- **Investigativa**
  Investigar incidentes de posible fraude, apropiación de activos, gastos y abusos o actividades impropias de las autoridades.

Auditoría de Sistemas de Información
Proceso de recolectar y evaluar evidencia para determinar si:
- El sistema preserva los activos
- Mantiene la integridad de los datos
- Permite que los objetivos organizacionales se alcancen con eficacia
- Usa los recursos con eficiencia

Muchas veces la auditoría tiene otro propósito: asegurar que la organización cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o involuntariamente.
Ejemplos:
- Entidades financieras
- Normas ISO



Preservar activos
Los activos de los SI incluyen: hardware, software, facilidades, personas (que tienen conocimientos), archivos de datos, documentación de sistemas e insumos.
Integridad de datos
Estado que en el cuál los datos poseen ciertos atributos, como completitud, pureza, veracidad y correctitud. Si la integridad no es mantenida, la organización no posee representación de sí misma o de los eventos.
Efectividad de los sistemas
Un sistema de información es efectivo si satisface sus objetivos. Esto se puede medir:
- Durante el proceso de desarrollo garantizando que se satisfagan los requerimientos de los usuarios.
- Mediante una post-auditoría.

Para poder evaluar la efectividad de un sistema de información se deben conocer las características de los usuarios y el entorno de toma de decisiones.
Eficiencia de los sistemas
Un SI es eficiente si usa los recursos mínimos para satisfacer sus objetivos. Los recursos de un sistema de información son el tiempo de procesador, periféricos, software y el trabajo manual. Muchas veces el uso de los recursos no se puede estudiar con respecto a un sólo sistema. Generalmente, la eficiencia se estudia cuando se agotan los recursos.

Importancia de los SI (Sistemas de Información)
- Es imposible que exista una organización competitiva que no necesite SI.
- No es cierto que podamos volver a las operaciones manuales cuando algo falla.
- Para que los sistemas sirvan deben ser controlables y confiables.
- Los auditores pueden confirmar si esto es así o no.

Control Interno

Cualquier política, procedimiento o proceso diseñado para proveer una seguridad razonable para cumplir con un objetivo. Sirven para asegurar que los activos son protegidos, que las operaciones sean eficientes y efectivas, que los reportes financieros sean confiables y completos, y ver si se cumple con las leyes y regulaciones.

Logro de Objetivos

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un sistema de control interno que incluya:

- Separación de Obligaciones
  En un sistema manual, personas diferentes deben iniciar y registrar transacciones, además de prevenir errores o detectar irregularidades.
  En un sistema automatizado el programa el realiza todas las funciones, por lo que la separación de obligaciones se aplica distinto: se separa la capacidad de ejecutar el programa, de la de modificar el programa.
- Delegación
  Una delegación clara de autoridad y responsabilidad es esencial en todo tipo de sistemas. En un sistema automatizado, hacer esto de una manera no ambigua puede ser dificultoso. Ejemplo: cuando múltiples usuarios tienen acceso a los mismos datos, y la integridad es violada, no es fácil ubicar al responsable para identificar y corregir el error.
- Personal Competente y Confiable
  A las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder:
  - Un analista puede aconsejar a la gerencia sobre el equipamiento de alta tecnología y de altos costos
  - Un operador asume la responsabilidad de salvaguardar software crítico y datos realizando copias de respaldo

  El personal responsable de los sistemas automatizados tiene delegado mayor poder que los que realizan tareas manuales, y no es fácil para las organizaciones asegurar que el personal de sistemas sea competente y confiable. La alta rotación de este personal es común, por lo que la gerencia tiene poco tiempo para evaluarlo. Además algunos parecen tener poco desarrollado su sentido de ética.
- Sistema de Autorizaciones
  La gerencia establece dos tipos de autorizaciones:
  - Autorizaciones generales: las políticas que la organización debe seguir (Ej.: lista de precios).
  - Autorizaciones específicas: aplicables a transacciones individuales (Ej.: compra de activos de alto valor).

  En los sistemas automatizados las autorizaciones están embebidas dentro de los programas.
- Documentos y Registros
  Se debe asegurar que los documentos y registros sean adecuados. En un sistema automatizado no es necesario un documento para iniciar una transacción (Ej.: Un pedido telefónico o un sistema de reposición automático de stock). En un sistema bien diseñado debería haber mayores registros de auditoría que en un sistema manual. Se deben prever controles de acceso y facilidades de login para asegurar que los rastros de auditoría sean exactos y completos.
- Control de Acceso Físico
  El control de acceso físico a los activos y a los registros es crucial, tanto en sistemas manuales como automáticos.
  - Sistema manual: puede tener que acceder a varios sitios.
  - Sistema automatizado: todos los registros necesarios se pueden mantener en un solo lugar.

  La concentración de información aumenta la posibilidad de pérdida que puede surgir por abuso o desastre.
- Supervisión Gerencial Adecuada
  En sistemas manuales se facilita, ya que empleados y supervisores, suelen compartir el lugar físico.
  En sistemas automatizados, las comunicaciones permiten que los empleados estén cerca de los clientes y la supervisión se debe llevar a cabo en forma remota, construyendo controles de supervisión dentro del sistema. El gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados.
- Chequeos de Performance
  En sistemas manuales, los chequeos realizados por otra persona ayudan a detectar errores o irregularidades. En sistemas automatizados, los programas siempre ejecutan el mismo algoritmo, a excepción de que ocurra una falla de hardware o de software. Los auditores deben evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas.
- Comparación Periódica
  Se deben controlar regularmente los datos que representan los activos con los activos reales, para determinar datos incompletos o inexactos. En sistemas automatizados se deben preparar programas para que hagan esto (Ej.: control de inventarios). Estos controles deben implementarse durante el desarrollo de los sistemas.

Controles en los sistemas modernos

Los sistemas computarizados son más complejos que los sistemas manuales. Mantienen datos en formatos electrónicos, más difíciles de acceder por el auditor.

- En algunos casos no existe un paper audit trail.
- Procesan datos con muy poca intervención manual.
- Las organizaciones dependen tanto de su SI que deben de recuperarse ante su falla o destrucción.
- Se rigen con leyes y restricciones diferentes que los sistemas manuales.

- También pueden ayudar a los auditores a brindar un servicio de calidad ya que es posible analizar la información que antes estaba distribuida y era imposible de reunir.

Clasificación de controles

- Generales: los que gobiernan el ambiente en el cual el sistema es desarrollado, mantenido y operado.
- De aplicación: los controles manuales y computarizados dentro de la aplicación de negocios que aseguran que los datos sean procesados correctamente.

Los controles de aplicaciones dependen de los controles generales. Si los controles generales no son adecuados, la aplicación será de baja calidad y los datos no serán procesados correctamente.
En el pasado, el auditor asumía confianza en los controles de aplicación (auditar around the computer), lo cual es una suposición fatal, ya que los sistemas son cada vez más complejos y vulnerables.
Es crítico que el auditor verifique la integridad del ambiente en que el sistema opera.

Proceso de auditoría

Planificar

¿Quién, cómo, cuándo y por qué? El trabajo se orienta a las áreas con mayores riesgos

Recolectar evidencia

Recolectar ejemplos, no se puede examinar todo. Elegir qué actividades observar.
Revisar documentación. Comprender los procesos de control. Realizar debates, cuestionarios, exámenes y confirmaciones. Examinar la documentación de respaldo, revisiones analíticas, examinar relaciones y tendencias.

Evaluar evidencia

La evidencia, ¿Respalda conclusiones favorables o desfavorables? ¿Cuán significativo es su impacto?
Seguridad razonable: Siempre existen riesgos de que la conclusión sea incorrecta.

Comunicar los resultados

Reportes escritos para la gerencia, el comité de auditoría y la junta directiva, que resuman las recomendaciones y conclusiones obtenidas.

Tipos de Auditores

Externos

Su misión es proveer una opinión independiente de los estados financieros de la organización u otra característica de la que se desea tener una opinión independiente. No pertenecen a la organización.

Internos

Trabajan en la organización. Su trabajo principal es verificar y reportar sobre la existencia de controles dentro de la misma organización, asegurándose que su funcionamiento sea correcto. Algunos de estos controles se relacionan con los sistemas de información. Evalúan si:

- La organización cumple con su misión
- La información es confiable e íntegra
- Se siguen las políticas, planes y regulaciones existentes
- Se promueve la eficiencia operacional

Módulo 2. Normativas

Organización de la función de auditar

Una auditoría puede ser interna o externa. El rol del auditor interno debe establecerse claramente mediante un audit charter aprobado por la gerencia.
La auditoría en SI puede ser parte del departamento de auditoría o puede ser un grupo independiente, además puede estar integrada dentro de una auditoría financiera y operacional para proveer seguridad con respecto a los controles de IT. La auditoría de SI es, en este último caso, un soporte.

Audit Charter

Es un documento que tiene que estar aprobado por el máximo gerente de la empresa y establece quién es la autoridad general, el alcance y las responsabilidades del auditor. Si la auditoría la realiza una firma externa se necesita un contrato.

Que se debe asegurar

- Alcanzar los objetivos de la auditoría
- Mantener la independencia
- Contribuir a un manejo eficiente de IT
- Contribuir a que la organización alcance sus objetivos de negocio

Planificación

Existen 2 tipos de planificación: a corto y a largo plazo.

- A corto plazo: lo que puede realizarse en 1 año como máximo.
- A largo plazo: objetivos a largo plazo que toman en cuenta elementos relacionados con el riesgo respecto a cambios estratégicos en la organización con respecto a IT.

Cómo realizar una planificación

Se debe replantear al menos una vez al año. Hay que considerar cambios en los riesgos, marco regulatorio y tecnologías que deben ser aprobados por la gerencia. Se deben entender los objetivos de negocio y procesos, incluyendo la disponibilidad necesaria, la seguridad y la confidencialidad.

- Identificar contenidos clave: políticas, estándares y guías.
- Contar con procedimientos y una estructura organizativa.
- Se debe realizar un análisis de riesgos para ayudar a diseñar el plan.
- Especificar el alcance y los objetivos de la auditoría.
- Desarrollar una estrategia de auditoría.
- Asignar personal para realizar la auditoría
- Organizar la logística necesaria
- Se debe considerar el panorama tecnológico actual y la dirección futura
- Leer publicaciones industriales, planes estratégicos, reportes anuales y memorias.
- Leer informes de auditorías anteriores.
- Entrevistar gerentes.
- Asignar recursos disponibles a las tareas del plan

Importancia de la independencia profesional

El reporte debe estar libre de condicionamientos o influencias, y quien actúe como auditor debe tener un alto estándar de ética.
El término auditor proviene del latín y significa "alguien que escucha disputas y las juzga". Existe una línea muy fina entre lo ético y lo legal. Hay cosas que pueden ser legales pero no son éticamente correctas. Con el tiempo, algunas cosas que comienzan a pensarse como no éticas se convierten ilegales al introducirse legislación al respecto (ej.: la esclavitud, las drogas, peleas de perros, etc.).

Responsabilidad profesional

- Confidencialidad: Los ingenieros deben respetar la confidencialidad de sus empleados o clientes independientemente de si se firmó un contrato al respecto o no.
- Competencia: No se deben aceptar trabajos que estén fuera del área de competencia.
- Derecho de propiedad intelectual: Se deben conocer los derechos de propiedad, patentes, etc. Se debe también proteger la propiedad intelectual de los empleados y clientes.
- Uso incorrecto de las computadoras: Los ingenieros no deben usar sus habilidades técnicas para hacer un uso incorrecto de las computadoras de otras personas. Ejemplos de esto varían desde usar las computadoras para jugar hasta infectarlas con virus.

Código de ética del ACM

Sociedades profesionales de los EEUU han cooperado para producir este código que contiene 8 principios que

involucran a distintos profesionales de la rama de IT. Los miembros de estas organizaciones automáticamente se adhieren al código al ingresar.

Preámbulo

La versión corta del código resume las aspiraciones en un alto nivel de abstracción, mientras que en la versión completa se dan detalles y ejemplos. Entre las dos permiten entender el código.

Los adherentes se comprometen a realizar, del análisis, especificación, diseño, desarrollo, testeo y mantenimiento de software, una profesión respetada y beneficiosa, comprometida con la salud, seguridad y bienestar del público. Esto se logra a través de los siguientes 8 principios:

- Interés Público: Actuarán en forma consistente con el interés público.
- Cliente y empleador: Actuarán de manera que este en los mejores intereses de su empleador y su clientes, consistentemente con el interés público.
- Producto: Deben alcanzar los estándares más altos posibles.
- Juicio: Mantendrán integridad e independencia en el juicio profesional.
- Gestión: los directores de proyectos deben subscribirse a un manejo ético del desarrollo y mantenimiento de SW.
- Profesión: Harán progresar la integridad y reputación de la profesión consistentemente con el interés público.
- Colegas: Serán justos y proveerán soporte a sus colegas.
- Participarán en un aprendizaje de por vida de su profesión y promoverán un acercamiento ético a la misma.

El código de ética de ISACA

Es específico para auditores de sistemas de información.

Principios ISACA

- Favorecer la implementación y cumplimiento de estándares, procedimientos y controles apropiados para los SI.
- Realizar sus deberes con diligencia y cuidado profesional en acuerdo con los estándares y mejores prácticas.
- Servir al interés de los stakeholders en forma legal y honesta manteniendo altos estándares, con conducta y carácter.
- Mantener la privacidad y confidencialidad de la información obtenida durante el trabajo a menos que sea requerido por una autoridad legal revelar información. La información no puede ser usada para beneficio personal.
- Ser competentes en los campos de trabajo y sólo acceder a realizar aquellas actividades que pertenezcan a las áreas de competencia.
- Informar a las partes apropiadas sobre los resultados del trabajo realizado, revelando todos los hechos significativos conocidos.
- Promover la educación profesional de los participantes para mejorar su entendimiento de la seguridad y control de los SI.

Estándares ISACA

El objetivo es hacer que los auditores de SI tengan un nivel mínimo de performance para garantizar que se cumplan las expectativas de la gerencia en cuanto a la calidad del trabajo. Estos estándares definen requerimientos obligatorios para las auditorías:

S1: Audit Charter

El propósito, responsabilidad y autoridad de la función de auditar SI debe estar documentada en un audit charter o engagement letter. Se debe aprobar en un nivel adecuado de la organización.

S2: Independencia

Independencia profesional: entre el auditor y el que está siendo auditado.

Independencia organizacional: el área que hace la auditoría en SI debe ser independiente del área o actividad que está siendo revisada.

S3: Ética profesional

El auditor debe adherir al código de ética ISACA y ejercer su profesión con responsabilidad adhiriendo a las normas profesionales.

S4: Competencia

Debe tener la habilidad y el conocimiento para realizar la tarea asignada, sometiéndose a una educación continua.

S5: Planificación

Planificar para cumplir los objetivos respetando las leyes aplicables y los estándares de auditoría. Desarrollar y documentar un acercamiento basado en riesgos. Desarrollar y documentar un plan de auditoría detallando la naturaleza y objetivos, tiempos, alcance y recursos requeridos.

S6: Performance

Se debe supervisar al staff, recolectar suficiente evidencia y documentar el trabajo realizado.

S7: Reportes

Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada

S8: Seguimiento

Evaluar si se han tomado las acciones apropiadas de acuerdo a lo recomendado.

S9: Irregularidades

Concierne como lidiar con irregularidades y actos ilegales.

S10: Gobernanza

Evaluar si las políticas de IT se alinean con los objetivos de la organización, los controles y riesgos asociados.

S11: Riesgos

Usar un acercamiento basado en riesgos para la planificación, con el fin de determinar prioridades para el uso de los recursos disponibles. Al planificar revisiones individuales se debe identificar y abordar riesgos relevantes al área.

Guias ISACA

Las guías proveen información sobre cómo cumplir con los estándares. Se debe usar el juicio profesional para aplicarlas o no a una auditoría particular. Por ejemplo:
G2: Cómo obtener suficiente evidencia de manera apropiada. Se debe justificar una desviación de lo que dice la guía.
G5: Ayudar al auditor a crear el Audit Charter, especialmente en casos de auditoría interna.

Procedimientos ISACA

Provee ejemplos de procedimientos que el Auditor de Sistemas puede utilizar en una revisión. Los procedimientos ofrecen información de cómo cumplir con los estándares al realizar una auditoría de sistemas pero no especifican requerimientos.

Procedimientos

P1: Evaluación de riesgo de SI
P2: Firmas digitales
P3: Detección de intrusos
P4: Virus
P5: Autoevaluación de control de riesgos
P6: Firewalls
P7: Irregularidades y actos ilegales
P8: Evaluación de seguridad
P9: Evaluación de controles administrativos sobre métodos de encriptación.
P10: Control de cambios de aplicaciones empresariales
P11: Transferencia electrónica de fondos.

Cómo administrar la complejidad. Para administrar la complejidad, se sugiere:
1. Factorizar el sistema en subsistemas
2. Determinar la confiabilidad de cada subsistema, y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.

Módulo 3: Controles, Riesgo y Planificación

La Naturaleza de los Controles

Un **control** es un sistema que previene, detecta o corrige eventos ilegales.
Un **evento ilegal** puede surgir si se ingresan al sistema (o si al hacerlo el sistema modifica el input) datos no autorizados, inexactos, incompletos, ineficaces o ineficientes; también si se introducen datos redundantes.
Ej.:

- Inputs incorrectos en un programa interactivo
- Un programa que contiene instrucciones erróneas que resultan en una ejecución incorrecta.
- Un mecanismo de usuario/contraseña es un control sólo en el contexto de un sistema que asegure que el password se elige con seguridad, se valida correctamente, se almacena de forma segura y se hace un seguimiento de su uso indebido.

No sólo deben ayudar a alcanzar los objetivos operacionales y de negocio sino que deben abordar los eventos no deseados mediante prevención, detección y corrección.

Controles internos

Comprenden políticas, procedimientos y políticas organizacionales. Pueden ser manuales o automatizados y se implementan para detectar, prevenir, reducir y corregir los riesgos de la organización. Proveen seguridad a la gerencia de que los objetivos de negocio serán alcanzados.
Comprenden 5 componentes relacionados:

1. **Controles de entorno**
   Se evalúan los elementos que controlan sistemas y procedimientos. Ej.: Filosofía y estilo de gerenciamiento y operación, métodos para monitorear performance y formas de asignar autoridad y responsabilidad.
2. **Evaluación de riesgo**
   Se evalúan los elementos que identifican, analizan y administran los riesgos a los que la organización está expuesta. Ej.: Planificaciones de proyectos y documentos de administración de riesgos.
3. **Actividades de control**
   Se evalúan los elementos que aseguran que las transacciones son autorizadas, las responsabilidades separadas y los documentos y registros mantenidos adecuadamente. Se clasifican en:
   - Controles contables, que aseguran distintos niveles de autorizaciones y responsabilidades.
   - Controles administrativos, que aseguran eficiencia y eficacia.
4. **Información y Comunicación**
   Se evalúan los elementos que identifican, capturan e intercambian información para verificar que lo hagan en tiempo y forma. Permite asignar responsabilidades del personal adecuadamente. Ej.: notificaciones, minutas de reuniones.
5. **Monitoreo**
   Se evalúan los elementos que aseguran que los controles internos operan confiablemente en el tiempo. Ej.: monitoreo de performance, control de calidad.

Controles Internos	Implementación
Actividades de Control	Procedimiento para instalar programas en producción (control gerencial)
Controles de Entorno y Evaluación de Riesgos	Existencia de comité de seguimiento de proyectos (control gerencial)
Información y Comunicación	Procedimiento para comunicar información (control gerencial) Procedimiento para capturar, registrar y procesar transacciones (control de aplicación)
Monitoreo	Procedimiento para medir la productividad del personal (control gerencial)

Tipos de Controles

Controles Preventivos

Se acompañan de instrucciones de cómo completar el formulario (No son el control. Ocurren antes del hecho pero nunca pueden ser 100% efectivos ni confiar ciegamente en ellos). Pueden incluir controles como restricciones en los usuarios, requerimientos para passwords, separar autorizaciones de transacciones.

Controles Detectivos

Un programa que valida los datos del input, rechazando los erróneos. Detectan irregularidades luego de ocurrido el hecho, pueden ser más baratos que chequear cada transacción con un control preventivo. Pueden incluir uso efectivo de audit trails y uso de reportes de excepción.

Controles Correctivos

Un programa que detecta el ruido en comunicaciones y permite corregir datos corruptos. Asegura la corrección de los problemas identificados por los controles detectivos y normalmente requieren de intervención humana con el IS. Pueden incluir planes de recuperación de desastre y capacidades para revertir transacciones. Este tipo de controles pueden ser muy propensos a errores debido a que ocurren en circunstancias inusuales y típicamente requieren de decisiones humanas, toma de decisiones e implementación.

Class	Function	Examples
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring.	• Employ only qualified personnel. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors). • Establish suitable procedures for authorization of transactions. • Complete programmed edit checks. • Use access control software that allows only authorized personnel to access sensitive files. • Use encryption software to prevent unauthorized disclosure of data.
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.	• Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past-due account reports • Internal audit functions • Review of activity logs to detect unauthorized access attempts
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.	• Contingency planning • Backup procedures • Rerun procedures

Objetivo de la Auditoría

Reducir las pérdidas esperadas por eventos ilegales mediante controles preventivos, que reducen la probabilidad que estos eventos ocurran, y controles detectivos y correctivos que reducen la cantidad de pérdidas cuando los eventos ilegales ocurren. La tarea del auditor es determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales.

División de la Auditoría

Para administrar la complejidad, se sugiere:

1. Factorizar el sistema en subsistemas.
2. Determinar la confiabilidad de cada subsistema, y sus implicancias en el nivel de confiabilidad general.

Factorización

El primer paso para comprender un sistema complejo es particionarlo por la función que realiza. Un subsistema es una componente lógica que realiza ciertas funciones básicas para el sistema en general.

Los auditores deben identificar primero las principales funciones que el sistema realiza para cumplir sus objetivos. El proceso de factorización termina cuando se ha particionado el sistema en partes lo suficientemente pequeñas, que puedan ser entendidas y evaluadas.

Existen otras dos guías muy importantes para factorizar un sistema:

- **Acoplamiento**
  Cada subsistema debería ser relativamente independiente del resto para ser más fácil de comprender.
- **Cohesión**
  Todas las actividades realizadas por el subsistema apuntan a cumplir la función principal del subsistema.

Se debe lograr máxima cohesión y mínimo acoplamiento, o intentar otra factorización. Maximizar la cohesión es equivalente a minimizar el acoplamiento.

Confiabilidad en los subsistemas

El primer paso es determinar el menor nivel de los subsistemas, luego se evalúa la confiabilidad de los controles en cada uno.

Formas de Factorización

Funciones gerenciales

Son las funciones que se deben realizar para asegurar que el desarrollo, la implementación, operación y mantenimiento de los SI procedan de una forma planificada y controlada.

Subsistema Gerencial	Descripción
Alta Gerencia	Debe asegurar que las funciones de los SI estén bien administradas. Decisiones de políticas a largo plazo de cómo serán usados los SI.
Gerencia de Sistemas de Información	Responsabilidad general de planificar y controlar todas las actividades de los SI. Aconseja a la alta gerencia de las decisiones políticas de largo plazo y las traduce en metas y objetivos de corto plazo.
Gerencia de Desarrollo de Sistemas	Responsable del diseño, implementación y mantenimiento de los sistemas.
Gerencia de Programación	Responsable de la programación de los nuevos sistemas, mantenimiento de los viejos y soporte general.
Administración de Datos	Responsable de lograr los objetivos de planificación y control en relación al uso de los datos de la organización.
Gerencia de Aseguramiento de Calidad	Responsable de asegurar que el desarrollo, operación y mantenimiento de los sistemas es conforme a los estándares de calidad establecidos
Administración de Seguridad	Responsable por los controles de acceso y seguridad física de las funciones de los SI.
Gerencia de Operaciones	Responsable de la planificación y control de las operaciones diarias.

Funciones de aplicación

Tareas que son necesarias ejecutar de forma cíclica para realizar un procesamiento de información confiable. Los sistemas de información que soportan una organización se dividen en ciclos. Los ciclos varían de acuerdo al tipo de organización: industria, entidad financiera, etc. En general incluyen: ventas y cobranzas, administración de personal, sueldos y jornales, compras y pagos, contabilidad y producción, inventario y almacenaje. Cada ciclo es factorizado en uno o más sistemas de aplicación (Ej: Ventas puede subdividirse en: captura de pedidos y facturación).

Subsistema de Aplicación	Descripción
Limítrofe	Componentes que establecen las interfaces entre el usuario y el sistema.
Input	Componentes que capturan, preparan e ingresan comandos y datos al sistema.
Comunicaciones	Componentes que transmiten datos entre los subsistemas y sistemas.
Procesamiento	Componentes que realizan toma de decisiones, cálculos, clasificación, ordenamiento y sumarización de datos dentro del sistema.
Base de Datos	Componentes que definen, agregan, acceden, modifican o eliminan datos.
Output	Componentes que buscan y presentan los datos al usuario.

Confiabilidad en los controles

Se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema, considerando todos los eventos válidos o ilegales. Para esto, hay que considerar las principales funciones que realiza el subsistema y, sobre cada una, evaluar cómo se cumple con esa visión normativa y analizar si debería modificarse. Todos los eventos en un sistema de aplicación deben surgir de una transacción.

Para determinar si un evento es legal o ilegal deben considerarse las transacciones que pueden ocurrir como input al subsistema.

Cuando la transacción se recibe como input el sistema cambia de estado, esto también puede ocurrir a medida que el sistema procesa la transacción (Ej.: toma de pedidos). Para identificar todos los eventos que pueden ocurrir en un sistema como resultado de la transacción, se debe entender cómo el sistema la procesa.

Generalmente los auditores aplican técnicas de walk-through:

- Se considera una transacción particular.
- Se identifican todos los componentes del sistema que la procesan.
- Se trata de entender cada paso de procesamiento que ejecuta cada componente
- Se considera cualquier error o irregularidad (evento ilegal) que pueda ocurrir en el camino.

Para que este proceso no sea costoso al realizarlo para todas las transacciones:

- Se agrupan transacciones que tengan un procesamiento similar.
- Se las entiende a estas y a los eventos que puedan surgir como resultado, como a un grupo.
- Se tratan sólo aquellas transacciones que se consideran importantes para los objetivos de la auditoría.

Riesgos en una Auditoría

Para poder cumplir con los objetivos de la auditoría, se debe recolectar evidencia. Podría ocurrir que se cometan errores al tomar algún valor. El riesgo de auditoría es el riesgo de que un auditor fracase al detectar las pérdidas materiales reales, o potenciales, o los registros incorrectos.

RDA = RI * RC * RD

Dónde:

RDA: Riesgo Deseado de Auditoría; RI: Riesgo Inherente; RC: Riesgo de Control; RD: Riesgo de Detección

Riesgos

- El "Control" comprende a todos los elementos de una organización que la ayudan a alcanzar sus objetivos.
- El control es "efectivo" siempre que sea en pos de asegurar que la organización alcance sus objetivos de manera confiable.
- El liderazgo implica hacer elecciones con cierto nivel de incertidumbre.
- El "Riesgo" es la posibilidad de que uno o más individuos u organizaciones experimenten consecuencias adversas a causa de esas elecciones.

Definición (ISO/IEC)

La probabilidad de que una dada amenaza explote las vulnerabilidades de un activo o grupo de activos, causando daño a la organización.

Análisis de riesgos

Es una parte de la planificación que ayuda a identificar riesgos y vulnerabilidades para que los auditores puedan determinar los controles necesarios para mitigarlos. Para estimar el valor de un producto, proceso o negocio hay que:

- Identificar procesos
- Identificar los tipos de riesgos asociados con cada proceso
- Identificar los controles asociados con cada proceso
- Evaluar si el control es adecuado
- Determinar los controles claves asociados con cada proceso

Riesgos de IT

El uso de IT trae beneficios y también riesgos asociados. Consiste de eventos relacionados con IT que podrían impactar en el negocio negativamente y está asociado con el uso, propiedad, manejo, influencia y adopción de IT dentro de la empresa. Deben manejarse igual que otros riesgos (de mercado, crediticios, operacionales), pero suelen ser relegados por la gerencia.

Tienen frecuencia y magnitud desconocida y son un desafío cuando se quieren alcanzar metas y objetivos estratégicos. También añaden incertidumbre a la búsqueda de oportunidades.

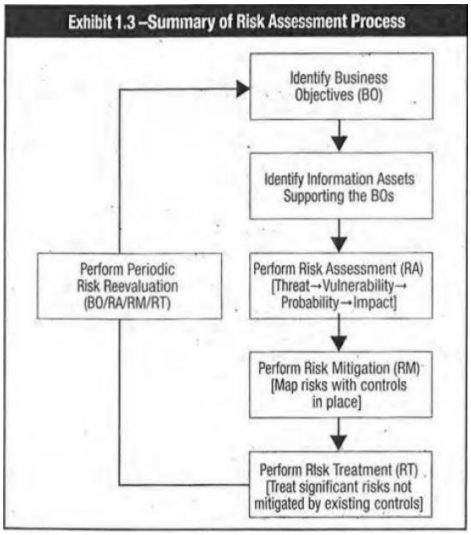
Entender los riesgos de IT

Para analizar los riesgos de IT el auditor debe entender:

- El objeto y la naturaleza del negocio.
- El ambiente en que opera.
- La dependencia de la tecnología.
- Como el riesgo de IT impacta en los riesgos del negocio y en el alcance de los objetivos del negocio.

El auditor en SI se enfoca frecuentemente en riesgos muy serios asociados con:

- La confidencialidad y disponibilidad de la información
- La integridad de la información crítica y de los procesos que la crean, guardan o manipulan
- La efectividad del manejo de riesgo que la organización usa.



Evaluación de riesgos

Los riesgos de IT son dinámicos, es estratégico para la gerencia reconocerlo y establecer un proceso de manejo de riesgos de IT que esté en concordancia con los riesgos de negocio de la organización.

Luego se identifican controles para mitigar los riesgos identificados, que deberían prevenir o reducir la probabilidad de que el evento de riesgo ocurra, detectar la ocurrencia, minimizar el impacto o transferir el riesgo.

La selección de contramedidas debe realizarse mediante un análisis costo- beneficio:

- Costo de control vs. beneficio de minimizar el riesgo.
- Cuánto es el riesgo residual que la gerencia está dispuesta a aceptar.
- Métodos preferenciales para lidiar con el riesgo.

Clasificación de los riesgos

- **Riesgo deseado**
  El riesgo que se desea correr.
- **Riesgo inherente**
  Es la probabilidad de que una pérdida significativa suceda antes de que opere algún factor reductor del riesgo. Para evaluarlo, el auditor debe considerar cuales son los tipos y naturaleza de los riesgos, tanto como los factores que indican que un riesgo existe.
- **Riesgo de control**
  Mide la probabilidad de que los procesos de control establecidos para limitar o manejar el riesgo inherente no sean efectivos. El auditor debe saber cómo medir si los controles son efectivos o no sabiendo qué controles son más efectivos que otros. Controles más fuertes reducen el riesgo pero pueden ser prohibitivos.
- **Riesgo de auditoría**
  Es el riesgo que el cubrimiento no aborde exposiciones del negocio. Se pueden desarrollar programas para reducir

este riesgo. Proveen guías sobre que controles sirven para cuales riesgos y los testeos substantivos y de compliance a ser realizados. Deben usarse con cuidado y adaptarse al contexto.

Opiniones de Auditoría: Estándares

- Excusada: en base al trabajo realizado no se puede emitir opinión.
- Adversa: el auditor determina que han ocurrido pérdidas sustanciales.
- Calificada: el auditor determina que han ocurrido pérdidas no sustanciales.
- No calificada: no han ocurrido pérdidas.

Informe de Auditoría

Un informe típico debería incluir:

- Introducción (Describe los objetivos de la auditoría)
- Enfoque general
- Conclusiones críticas (Un resumen)
- Recomendaciones (Acciones necesarias para abordar las conclusiones críticas)
- Datos (Que respalden las conclusiones críticas)

Objetivos de control de SI

Los objetivos se deben abordar de una forma que sea relevante a los procesos relacionados con los SI:

- Salvaguarda de los activos.
- Asegurar la integridad de sistemas operativos, incluyendo el manejo de redes.
- Asegurar la integridad de sistemas de aplicaciones críticos, como sistemas financieros y que manejen datos sensibles.
- Autorización de la entrada.
- Validación de la entrada.
- Correctitud de procesamiento de transacciones.
- Precisión, completitud y seguridad de la salida.
- Integridad, disponibilidad y confidencialidad de las BD.
- Asegurar una apropiada identificación y autenticación de los usuarios.
- Asegurar la eficiencia y efectividad de las operaciones.
- Cumplir con normas, políticas, regulaciones.
- Asegurar disponibilidad de los servicios de IT desarrollando BCP y DRP.

Controles generales

Proveen políticas procedimientos y prácticas establecidos por la gerencia para intentar alcanzar un objetivo específico.
Ej.:

- Change management procedures: Controls designed to ensure changes meet business requirements.
- Source code/document version control procedures: Controls designed to protect the integrity of the program code.
- Software development/life cycle standards: Controls designed to ensure the IT projects are effectively managed.
- Logical access policies, standards and processes: Controls designed to manage access based on business need.

Controles de aplicación

Son controles con fines específicos que están automatizados para el procesamiento completo y correcto de los datos, desde la entrada hasta la salida. Ej.:

- Identification: Controles de que todos los usuarios son identificados inequívocamente
- Authentication: Controles que proveen mecanismos de autenticación en sistemas de aplicación.
- Authorization: Controles que aseguran que solo determinados usuarios del negocio tienen acceso al sistema
- Input controls: Controles que aseguran la integridad de los datos almacenados en el sistema cuando se ingresan.

COBIT (Control OBjetives for Information and related Tecnology)

Su objetivo es ver si IT está alineado correctamente con los objetivos de negocio. Para esto brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, busca investigar, desarrollar, hacer público y promover un marco de control de gobierno de IT autorizado, actualizado y aceptado internacionalmente.
Se creó con las características principales de ser:

- Orientado a Negocios: relacionar objetivos de negocio con objetivos de IT.
- Orientado a Procesos: para organizar las actividades de IT.
- Basado en Controles.
- Impulsado por Mediciones: proveer métricas y modelos de madurez

Define las actividades de IT en un modelo genérico de procesos organizado en cuatro dominios:

Planear y organizar (PO)

Estrategias y tácticas. Tiene que ver con identificar la manera en que la IT puede contribuir de la mejor manera al logro de los objetivos del negocio.

- PO1 Definir un plan estratégico de TI.
- PO2 Definir la arquitectura de la información.
- PO3 Determinar la dirección tecnológica.
- PO4 Definir la organización de TI y sus relaciones.
- PO5 Administrar las inversiones en TI.

- PO6 Comunicar la dirección y aspiraciones de la gerencia

Adquirir e Implementar (AI)

Entregar y dar soporte (DS)

La entrega de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

- DS1 Definir niveles de servicio.
- DS2 Administrar servicios prestados por terceros.
- DS3 Administrar desempeño y capacidad.
- DS4 Asegurar servicio continuo.
- DS5 Asegurar la seguridad de los sistemas.
- DS6 Identificar y asignar costos.

Monitorear y evaluar (ME)

Todos los procesos de IT deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

- M1 Monitorear el proceso.
- M2 Evaluar lo adecuado del control Interno.
- M3 Obtener aseguramiento independiente.
- M4 Proporcionar auditoría independiente.

¿Cómo realizamos la auditoría?

Auditar es un proceso sistemático mediante el cual un profesional competente obtiene y evalúa evidencia sobre hipótesis sobre un proceso para poder emitir una opinión sobre el mismo.

Auditoría de SI

La auditoría de sistemas de información analiza y evalúa de los sistemas automáticos para procesar información. También de los procesos no automáticos relacionados y de las interfases entre estos dos.

Pasos

Para planificar, se debe tener en cuenta la naturaleza de los controles, la factorización, los riesgos y los tipos de procedimientos de auditoría. Algunos pasos se pueden realizar en paralelo.

- Planificación.
- Riesgos en general y en particular para las áreas y aplicaciones a auditar.
- Desarrollar un programa de auditoría que consista de objetivos y procedimientos para satisfacer los objetivos de auditoría.
- Recolectar evidencia
- Evaluar las fortalezas y debilidades basándose en la evidencia.
- Preparar un reporte que presente las áreas con debilidades de control y las recomendaciones para remediar esto.

Restricciones

Situaciones que pueden restringir la auditoria:

- No hay empleados disponibles.
- Los empleados son nuevos en el área.
- Se sobrecarga a los empleados demasiado.
- Falta de conocimiento en general.
- Falta de documentación.

Para solucionar estos problemas se deben conocer técnicas de manejo de proyectos:

- Desarrollar un plan más detallado
- Registrar la actividad realizada comparando con el plan
- Ajustar el plan y tomar acciones correctivas

Programa de auditoría

Basándose en el alcance y los objetivos, se evalúa desde diferentes perspectivas:

- Seguridad: Confidencialidad, integridad y disponibilidad
- Calidad: Efectividad y eficiencia
- Fiduciario: Cumplimiento y confiabilidad

Se elabora una estrategia y un plan de auditoría, donde se identifican el alcance, los objetivos y procedimientos necesarios para obtener la evidencia. Usualmente incluye:

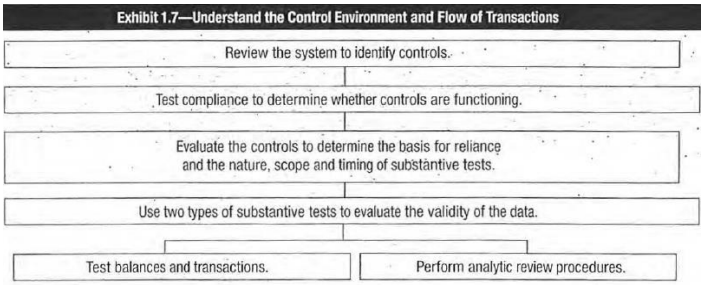
- Obtener y registrar un entendimiento del área u objeto.
- Realizar un análisis de riesgo, un plan general y un cronograma.
- Planificación detallada con descomposición de tareas y referencias temporales concretas.
- Revisión del área a auditar.
- Verificar y evaluar los controles existentes para alcanzar los objetivos.

Audit Phase	Description
Audit subject	• Identify the area to be audited.
Audit objective	• Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review such as functional flow charts; policies, standards, procedures and prior audit workpapers. • Identify locations or facilities to be audited.
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	Organization-specific
Procedures for communication with management	Organization-specific
Audit report preparation	• Identify follow-up review procedures. • Identify procedures to evaluate/test operational efficiency and effectiveness. • Identify procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

- Verificar que los controles se cumplan y apliquen consistentemente.
- Testeo sustantivo, donde se confirma la precisión de la información.
- Realizar un reporte.
- Seguimiento en caso de que sea una auditoría interna.

El auditor debe entender los siguientes puntos para planificar buenos tests:
- Uso de software general de auditoría para resumir los contenidos de archivos de datos y logs
- Cuestionarios y observación directa
- Uso de técnicas de data flow para documentar aplicaciones y procesos de negocio
- Revisión de documentación
- Guías y procedimientos
- Reperformance de controles

Fases usuales
- Sujeto de auditoría: identificar que se va a auditar.
- Objetivo: identificar para que se realiza la auditoría.
- Alcance: identificar los sistemas, funciones o unidades organizacionales que se incluirán.
- Planificación preauditoría: identificar habilidades, técnicas, información, lugares a testear y recursos necesarios.
- Procedimientos de auditoría:
  - Seleccionar el acercamiento que se usará.
  - Individuos a entrevistar
  - Obtener políticas, estándares y guías de trabajo en uso para revisar.
  - Desarrollar herramientas de auditoría y metodologías para testear los controles.
- Procedimientos específicos para evaluar los resultados
- Procedimientos específicos para comunicarse con la gerencia
- Preparar el reporte:
  - Identificar procesos de seguimiento
  - Identificar procesos para evaluar eficiencia, eficacia y para testear controles
  - Revisar documentos, políticas y procedimientos.



Objetivos de la auditoría

Se suele focalizar en verificar que existan controles internos que minimicen los riesgos de negocio y que estén funcionando. La gerencia puede darle al auditor un objetivo general, que éste deberá trasladar a objetivos de control de SI. Identificamos también controles generales y de aplicación clave para el objetivo, y se testea por compliance o se decide usar un testeo sustantivo. Si se confía en los controles existentes se minimiza el testeo sustantivo.

Compliance vs Sustantivo

El testeo por compliance (cumplimiento) reúne evidencia para verificar que una organización cumpla con los procedimientos de control, de acuerdo con sus políticas y procedimientos. En cambio, la verificación sustantiva utiliza la evidencia para evaluar la integridad de transacciones, datos u otra información individual que haya sido procesada.

Evidencia

Cualquier información usada por el auditor para sustentar las conclusiones de la auditoría: contratos, entrevistas, documentos internos, resultados de los testeos, etc.

La confiabilidad debe ser tenida en cuenta:
- Independencia de quien provee la evidencia: Si es de una fuente externa es más confiable. Contratos o acuerdos con terceros pueden ser considerados confiables si se tiene acceso al original.
- Calificación de quien provee la evidencia: Tanto para fuentes externas como internas o el mismo auditor, debe considerarse la calificación y responsabilidades de quien provee la información o de quien la analiza. Si un auditor no tiene buen entendimiento del área que controla, la información que reúna puede no ser confiable.
- Objetividad de la evidencia: Es siempre más confiable la evidencia objetiva que la que requiere la interpretación o juicio de alguien. La revisión de un inventario es objetiva, pero el análisis de eficiencia basado en la charla con el personal podría no serlo.
- Tiempo de la evidencia: Se debe considerar el tiempo durante el cual la información existe y es válida para realizar testeos de compilance y sustantivos. El contenido de una planilla podría no mantenerse estático en el tiempo si no se le realizan copias de respaldo frecuentes.

La evidencia es competente cuando es válida y relevante.

Técnicas para recolectar evidencia
- Revisar la estructura organizacional de SI
- Revisar políticas y procedimientos de SI
- Revisar estándares de SI
- Revisar documentación de SI
- Entrevistar al personal apropiado
- Observar performance de procesos y empleados.

Documentar Evidencia

No se debe invertir demasiado tiempo en esta etapa. Hay que:

- Completar cuestionarios
- Construir diagramas de flujo de alto nivel
- Construir tablas de decisión
- Redactar descripciones narrativas
- Utilizar herramientas CASE

Finalmente se debe evaluar el riesgo

Sampling

Se usa cuando tiempo y costo resultan prohibitivos para poder probar todos los eventos o transacciones. Existen dos acercamientos:

- Muestreo Estadístico

  Usa las leyes de probabilidad para:
  - Calcular el tamaño de la muestra.
  - Seleccionar los elementos de muestreo
  - Evaluar los resultados de la muestra y hacer inferencias.

  Con el muestreo estadístico, el auditor decide cuantitativamente cuan cerca debe representar la muestra a la población total y su nivel de confiabilidad. Los resultados de una muestra estadísticamente valida son matemáticamente cuantificables.

- Muestreo no estadístico

  Es un muestreo a discreción, en el cual el auditor decide subjetivamente cuales son los elementos y transacciones más riesgosos y el número de elementos a examinar.

Evaluando fortalezas y debilidades

El auditor debe analizar las fortalezas y debilidades de los controles evaluados y determinar si sirven para alcanzar los objetivos de control. Se usa una matriz con errores y controles y se asigna un valor numérico, y a partir de esto los controles pueden compensarse entre sí.

Comunicando los resultados

La entrevista final da la oportunidad al auditor de discutir los resultados. Se debe:

- Asegurar que los hechos presentados en el reporte son correctos
- Asegurar que las soluciones son realistas
- Recomendar fechas de implementación

Primero se debe hablar con quien fue auditado particularmente, para luego comunicar los resultados a la gerencia.
Si piden ayuda para implementar lo que se recomendó, recordar que un auditor no es un consultor.

Reporte

Es el producto final, no hay un formato específico, cada organización tendrá el suyo y comunica lo que se encontró a la gerencia. Un auditor entrenado sabrá cómo es más efectivo comunicar los resultados. Usualmente contiene:

- Una introducción al reporte, objetivos, alcance, acciones realizadas, fechas y restricciones.
- Problemas encontrados (Audit findings): en secciones separadas
- Conclusión general del auditor y opinión sobre los controles y los riesgos encontrados.
- Recomendaciones y qué se encontró en forma más detallada.

Al hablar sobre el reporte se deben discutir fechas para implementar las medidas correctivas.
Saber negociar, entender que puede haber otras prioridades, pero ser firmes.

Documentos a generar en una auditoría

- Planificación y preparación del alcance y los objetivos
- Descripción del área de alcance
- Programa de auditoría
- Pasos realizados y evidencia recolectada
- Uso de servicios de auditores externos
- Copia del reporte

Módulo 4: Controles Gerenciales

Desafíos de la Alta Gerencia

- Estudiar e incorporar tecnología de HW y SW permanentemente cambiante.
- Determinar el impacto de estos cambios en la organización.
- Desarrollar productos innovadores para competir.

Motivación

Un gerente se desempeña bien si logra:

- Planificar: determinar objetivos y formas de lograrlos.
- Organizar: obtener, asignar y coordinar los recursos.
- Conducir: motivar, guiar y comunicar.
- Controlar

Planificar

La alta gerencia debe elaborar un plan maestro sobre los sistemas de información, que incluya:

- Reconocer oportunidades y problemas en los cuales los SI pueden ser aplicados.
- Identificar los recursos necesarios para proveer la tecnología requerida.
- Formular estrategias y tácticas para obtener los recursos necesarios

Importancia de Planificar

La planificación de los SI es de vital importancia:

- Una planificación pobre ocasiona que no existan los recursos humanos, de HW y de SW necesarios para desarrollar correctamente la función.
- Se pierde posición competitiva.

Evaluar la Función de Planificar

La alta gerencia debe preparar dos tipos de planes:

- Plan estratégico: cubre los próximos 3 a 5 años:
  - Evaluar la información actual
  - Direcciones estratégicas
  - Estrategia de desarrollo
- Plan operacional: cubre los próximos 1 a 3 años:
  - Informes de avances
  - Iniciativas a tomar
  - Cronograma de implementación

Modelo de McFarlan

La necesidad de planificación está en función de:

- La importancia estratégica de los SI existentes actualmente
- La importancia estratégica de los SI propuestos a futuro

Identifica 4 tipos de organizaciones, con diferentes necesidades:

IMPORTANCIA		**SI Futuros**	
		Baja	Alta
SI Actuales	Baja	Soporte	Reconversión
	Alta	Industriales	Estratégicas

- Soporte: Los SI existentes y propuestos tienen poca importancia ya que son solo un soporte para la organización. Necesita poca planificación.
- Industrial: Los SI propuestos tienen poca importancia, pero los existentes son críticos. Requiere moderada planificación, especialmente a corto plazo.
- En Reconversión: Los SI existentes tienen poca importancia, pero los propuestos son críticos. Se requiere planificación de moderada a extensa, especialmente a largo plazo.
- Estratégicas: Los SI existentes y propuestos son críticos. Se requiere planificación a corto y largo plazo, de recursos y necesidades.

Modelo de Sullivan

Se focaliza en 2 dimensiones:

- Infusión: Grado de integración de los SI a las operaciones diarias.
- Difusión: Grado de dispersión de los SI en la organización.

Identifica 4 tipos de organizaciones:

GRADO		**Infusión de SI**	
		Baja	Alta
Difusión de SI	Baja	Tradicional	Medular
	Alta	Federal	Compleja

- Tradicional: Ha ocurrido poca infusión y poca difusión, por lo que su poca planificación puede ser realizada por un grupo centralizado.
- Federal: Ha ocurrido poca infusión pero existe alta difusión, por lo que se necesita planificación moderada. La planificación puede ser descentralizada y basada en necesidades de usuarios finales y divisiones. Generalmente se resisten a planificaciones a lo largo de toda la organización.
- Medular: Ha ocurrido poca difusión pero existe alta infusión, entonces necesita planificación de moderada a extensa. La planificación es centralizada, concentrándose en las necesidades de los grupos de SI.
- Compleja Ha ocurrido infusión y difusión en grado alto. Se requiere mucha planificación para considerar a todo el espectro, desde divisiones (con su correspondiente autonomía) hasta usuarios finales y la organización en su conjunto.

Estrategia de los SI

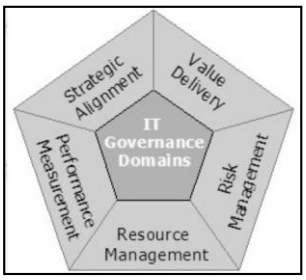
La planificación estratégica de IS se relaciona con la dirección a largo plazo que la organización quiere tener en cuanto a nivelar IT para mejorar su proceso de negocio. Lo crean el CISO (Chief Information Security Officer) junto con el comité ejecutivo y el comité estratégico. Una planificación efectiva debe considerar los requerimientos de nuevos sistemas y de actualización, junto con la capacidad de la organización para desarrollar nueva funcionalidad mediante proyectos bien gerenciados. También debe balancear los costos de mantenimiento y nuevas iniciativas.

Corporate governance

Hoy en día se debe hacer un alineamiento estratégico entre los objetivos de IT y los de negocio. Las tecnologías de la información son tan críticas que no pueden ser relegadas a especialistas en IT, debe recibir la atención también de la alta gerencia.

Frameworks

Implementar frameworks de e-governance nos brinda prácticas que favorecen al feedback en value delivery y risk management.



- Manejo de recursos de IT: mantener un inventario y abordar el manejo de riesgo.
- Mediciones de performance: que todos los procesos generen valor.
- Gestión de compliance.

IT governance frameworks

- COBIT
- ISO 27001: implementación y gestión de programas de seguridad de la información.
- IT Infrastructure Library (ITIL): Framework con información práctica sobre como alcanzar un manejo exitoso de IT.

Rol del auditor

El auditor juega un rol fundamental en la implementación de un framework, ya que está bien posicionado para influenciar en la gerencia y ayudar a mejorar y efectivizar las iniciativas implementadas. Puede asegurar concordancia con iniciativas de IT governance.

Aspectos a auditar

- Alineación de la función de IS con la misión, visión, valores, objetivos y estrategias de la organización.
- Si se alcanzan los objetivos de performance establecidos gracias a las funciones de IS.
- Requisitos legales, medioambientales, fiduciarios, de seguridad, privacidad y de calidad de información.
- Los controles de la organización.
- Los riesgos inherentes de IS.
- Gastos e inversiones de IT

Information Security governance

Dentro de IT governance, IS governance se focaliza en: confidencialidad, integridad y disponibilidad de la información, continuidad de servicios y protección de activos de información. Es una parte importante e integral de IT governance, ya que, en muchas organizaciones, la información es el negocio (Ej.: Servidores de email).

Dada la importancia y complejidad debe tener un nivel alto en el organigrama, siendo responsabilidad de la junta de directores y de la gerencia ejecutiva.

Beneficios

- Mayor confianza en la interacción con los socios y en la relación con los clientes.
- Protege la reputación de la organización.
- Permite nuevas y mejores formas de procesar transferencias electrónicas.

Roles y responsabilidades

- Junta directiva: aprobar políticas, realizar monitoreo y métricas.
- Alta gerencia: realizar una estrategia efectiva en costo.
- Comité de conducción: un representante de cada departamento involucrado es vital para un cambio cultural.
- CISO: puede ser el CIO, CEO, CFO o alguien más que se encargue de dirigir las operaciones de IT.

Comité de conducción

No debe involucrarse en operaciones rutinarias. Supervisa la función de IS y sus responsabilidades, e incluye representantes de la alta gerencia, la gerencia de usuarios y el departamento de IT. El chair debería ser un miembro de la junta que entiende las implicancias de la seguridad de la información.

- Revisa los planes a corto y largo plazo de IS.
- Adquisiciones significativas.
- Aprueba estándares y procedimientos.
- Decisiones sobre asignación de responsabilidades, centralización y descentralización.

Políticas y procedimientos

Reflejan la posición de la alta gerencia sobre los controles para IT, recursos relacionados y los procesos del departamento de seguridad de la información.

Políticas

Son documentos de alto nivel que reflejan la filosofía de la organización y el pensamiento estratégico de la alta gerencia. Es la gerencia quien las escribe, promulga, revisa y actualiza, de forma clara y concisa, para que sean efectivas. Los empleados y terceros afectados por una política deben recibir una explicación de la misma y entenderla. En el caso de terceros, deben ser ligados mediante un contrato de servicios.

Los departamentos definen las políticas de bajo nivel, usando un acercamiento top-down para facilitar la consistencia y estar alineadas con los objetivos de negocio.

Los controles se obtienen a partir de las políticas, que deben ser auditadas por compliance. Siempre se debe balancear control con la productividad, ya que el costo del control no debe exceder al beneficio esperado.

Política de Seguridad de la Información

- Declaración de la intención de la gerencia, que apoye los objetivos y principios de seguridad de la información, en línea con los objetivos de negocio.
- Framework para fijar objetivos de control y controles.
- Explicación de las políticas de seguridad, principios, estándares y requerimientos de compliance más importantes.
- Definición responsabilidades.
- Referencias a documentación de soporte.

Revisión de la política de SI

Debe ser revisada, tener un responsable que responda ante pedidos y revisiones, y debe haber un proceso para hacer cambios y registrarlos. El auditor, al revisar las políticas, debe saber:

- Base por la cual fue definida
- Contenidos
- Excepciones
- Proceso para aprobarla e implementarla
- Entrenamiento del personal
- Revisiones periódicas y actualizaciones

Procedimientos

Pasos claros y concisos para implementar políticas, que están definidos en detalle y bien documentados. Los dueños de los procesos los derivan de las políticas, pero son más dinámicos que estas. Es importante guardarlos, distribuirlos y darlos a conocer por la gente a la que afectan, sino no sirven.

Se debe realizar una revisión independiente para ver si se siguen los procedimientos. Si las prácticas operacionales no se corresponden con procedimientos, el auditor y la gerencia están en problemas, ya que es difícil identificar controles y ver si están en operación.

Gerenciamiento del riesgo

Es el proceso de identificar riesgos y amenazas a los recursos de información. Se debe decidir qué medidas tomar para reducir el riesgo a niveles aceptables para la compañía.

Involucra identificar, analizar, evaluar, tratar y comunicar el impacto del riesgo en los proyectos de IT, definiendo el nivel de seguridad con el que se protegerán estos activos. Esto impacta en todas las inversiones futuras de tecnología.

Se deben decidir las estrategias que se usarán y dejar en claro las responsabilidades de cada actor.

Dependiendo del tipo de riesgo y de su importancia para el negocio, la gerencia y la junta directiva pueden elegir realizar alguna de las siguientes acciones:

- Evitarlo: Eliminar la causa que puede provocarlo.
- Mitigarlo: Disminuir su probabilidad e impacto mediante controles.
- Transferirlo: Compartir el riesgo con terceros, como empresas aseguradoras.
- Aceptarlo: Reconocer su existencia y monitorearlo.
- Ignorarlo: La peor alternativa es rechazar su existencia.

Desarrollar un programa de manejo de riesgo

Establecer el objetivo del programa (Ej.: Reducir el número de incidentes), definiendo KPIs antes de iniciar el plan y luego usarlos para evaluar los resultados. Los responsables son la alta gerencia y la junta directiva.

Asignar responsables del programa, ya sea un individuo o equipo, que lo diseñe, implemente y asegure su adopción en la organización.

Risk IT

La organización debe establecer un proceso repetible de manejo de riesgos. Risk IT es un modelo basado en las normas COBIT con tres dominios: Governance, Evaluation y Response.

Risk Governance

El objetivo es asegurar que las prácticas de manejo de riesgos de IT están embebidas en la organización. Permite a la organización asegurar un retorno óptimo ajustado al riesgo.

- RG1 - Establecer y mantener una visión común de riesgos: Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la organización para las pérdidas relacionadas con IT y la tolerancia subjetiva de IT que posee el liderazgo.
- RG2 - Integrar con ERM: Integrar la estrategia y operaciones de IT con decisiones estratégicas del negocio.
- RG3 - Hacer decisiones de negocios basadas en riesgo: Asegurar que las decisiones de la organización consideren el rango completo de oportunidades y consecuencias que surgen de confiar en IT.

Risk response

Asegurar que los eventos de riesgo relacionados con IT son abordados en una forma efectiva en costo y en línea con las prioridades de negocio

- RR1 - Articular riesgos: Asegurar que la información sobre el verdadero estado de las exposiciones y oportunidades relacionadas con IT está disponible en tiempo y forma para la gente apropiada.
- RR2 - Gestionar riesgos: Asegurar que las medidas para aprovechar oportunidades estratégicas y reducir riesgos a un nivel aceptable son manejadas como un portfolio.
- RR3 - Reaccionar a eventos: Asegurar que las medidas para aprovechar oportunidades inmediatas o limitar la magnitud de las pérdidas de eventos relacionados con IT son efectivas y se activan en tiempo y forma.

Risk evaluation

Asegurar que todos los riesgos relacionados con IT están identificados, analizados y presentados en términos del negocio.

- RE1 - Recolectar datos: Identificar datos relevantes para permitir la efectiva identificación, análisis y reporte de los riesgos.
- RE2 - Analizar riesgos: Crear información útil para soportar decisiones de riesgo que toman en cuenta la relevancia para el negocio de los factores de riesgo.
- RE3 - Mantener un perfil de riesgos: Mantener un inventario actualizado y completo de riesgos conocidos y atributos, recursos de IT, capacidades y controles como se los entiende en el contexto de los productos, servicios y procesos del negocio.

Prácticas de gestión de IS

Reflejan las políticas y procedimientos desarrollados para varias actividades y gerenciamiento relacionadas con SI. En muchas organizaciones el departamento de SI es de soporte, es decir que ayuda a que los otros departamentos desarrollen sus operaciones diarias de forma efectiva y eficiente. Como los SI se han vuelto esenciales en las operaciones diarias, y la tendencia dicta que sean cada día más importantes, resulta crucial que esté bien dirigido.

Manejo de RRHH

Se relaciona con las políticas y procedimientos de la organización para reclutar, entrenar, seleccionar y promover el personal. Estas operaciones impactan en la calidad del personal y en el área de IT.

Selección de Personal - Control

- Control de referencias
- Selección en base a salud física y mental
- Obligación contractual para personal clave
- Doctrinas propias de la organización
- Acuerdos de confidencialidad
- Explicación de protocolos organizacionales a observar. (Ej.: confidencialidad, cuidado de equipos)
- Códigos de ética
- Acuerdos de conflictos de intereses

Riesgos de control

Si no se realizan los controles adecuadamente, puede ser que el personal no sea el adecuado para la posición en que fue contratado o que no se realicen los chequeos de referencias y no se conozca el desempeño en puestos anteriores.
Los servicios tercerizados pueden introducir riesgos que no son tenidos en cuenta, ya que no controlamos directamente sus RRHH. Esto puede llevar a que algunos empleados no consideren los acuerdos y requerimientos de confidencialidad.

Desarrollo del Personal

Se deben realizar evaluaciones periódicas al personal para identificar sus debilidades y fortalezas. A partir de esto se pueden identificar oportunidades para el crecimiento personal y profesional (promoción) de los empleados.
Los empleados deben comprender claramente las reglas de la evaluación, estar informados de la misma, tener posibilidades de discutirla con su superior y apelar la evaluación en caso de discordancia.

Finalización de Servicios

La terminación de servicios puede ser voluntaria o involuntaria. Cuando un empleado se va, la alta gerencia debe ser informada de inmediato y su supervisor debe reportar las razones que llevaron a esto.

Control

- Recuperar llaves y tarjetas de identificación
- Cancelar sus claves de acceso
- Modificar las listas de distribución
- Devolver libros, documentación, informes y cualquier equipo utilizado

Tareas

- Si el empleado no está descontento debe capacitar a su reemplazo.
- Si está descontento se lo debe separar de las áreas críticas y pedirle que abandone la organización cuanto antes.

Sourcing (abastecimiento)

Se relaciona con la forma en que la organización va a obtener las funciones de SI requeridas. Puede ser desarrollado por alguien de la empresa (In-Sourcing), por alguien externo (Out-Sourcing) o por un equipo conformado por empleados y externos.

Las funciones de SI pueden realizarse en el lugar del departamento de SI (Onsite), fuera del departamento pero en la misma área geográfica (Offsite) o en algún lugar remoto alrededor del mundo (Offshore), es una ventaja si se tienen distintas zonas horarias de disponibilidad.

Elección del tipo de sourcing

Decidirse por un tipo de servicio u otro depende de:

- Importancia de los SI en la empresa
- Si la función requiere conocimientos específicos de procesos y staff crítico para alcanzar sus objetivos
- Si la función puede realizarse en otro lugar con costo menor o igual y sin mayor riesgo
- Experiencia usando servicios de terceros

Outsourcing

Requiere que la gerencia revise el sistema de control sobre el cual puede depender, para mejorar los procesos de negocio a través de una reestructuración y así tomar ventaja sobre la competencia. En estos casos se debe:

- Definir la función de SI que será implementada.
- Describir los niveles de servicio requeridos y métricas mínimas.
- Conocer el nivel de habilidades y calidad deseadas.
- Comparar el costo in-house con lo ofrecido.
- Realizar una revisión a conciencia de los posibles proveedores.

Las razones para el outsourcing son:

- Concentrarse en actividades centrales
- Menores márgenes de ganancia
- Incremento de la competencia y menores ingresos
- Flexibilidad con respecto a la organización y la estructura

Algunos servicios que suelen realizarse mediante Outsourcing:

- Data entry
- Diseño y desarrollo de nuevos sistemas
- Mantenimiento de aplicaciones existentes
- Conversión de aplicaciones legacy
- Operación del help desk o call center

Outsourcing no sólo es una decisión en cuanto a costos, es una decisión estratégica que puede brindarle a la empresa mejor calidad del servicio, continuidad, procedimientos de control, ventaja competitiva y conocimiento técnico. Es clave elegir bien al proveedor y redactar bien el contrato y el SLA.

Service Level Agreement

Son una forma contractual de ayudar al departamento de SI a gestionar los recursos de información bajo el control de un proveedor. Comprometen al proveedor a un nivel requerido de servicio y soporte, establecen requerimientos de HW y SW, penalidades y opciones de enforcement.

Monitoreo de outsourcing

Se debe monitorear regularmente y realizar auditorías. Hay que asegurar que se cumplan las condiciones establecidas en el contrato y el SLA. También que los incidentes sean reportados y gestionados apropiadamente.

Al auditar outsourcing:

- Incorporar que se espera de la calidad del servicio (CMM, ISO, ITIL, etc)
- Reporte incumplimientos y seguimiento
- En el desarrollo asegurar que se incluyan controles de cambios y requerimientos de testeo
- Detallar parámetros específicos de performance
- Un criterio de resolución de conflictos
- Indemnización por daños
- Cláusulas sobre derechos a auditar
- Mantenimiento de CIA

Organizar la función de SI

Un departamento de SI puede ser organizado de muchas maneras, un organigrama organizacional es importante para mostrar cómo está estructurada la empresa. El auditor debe determinar si la estructura y las descripciones de cada rol son las adecuadas

Analista de Sistemas

- Detallar requerimientos de información de aplicaciones nuevas y actuales
- Diseñar la arquitectura de SI para satisfacer los requerimientos
- Facilitar la implementación de los SI
- Escribir procedimientos y documentación para usuarios finales.

Analista Programador

- Diseñar, codificar, testear, corregir y documentar programas.
- Modificar programas para remover errores,
- Mejorar la eficiencia de un programa y satisfacer nuevas necesidades.

Programador de Sistemas
- Mantiene y mejora el software operativo, el de librerías y el utilitario.
- Provee asistencia cuando ocurren fallas de sistemas no usuales.

Administrador de Datos
- Relevar los requerimientos de datos de los usuarios
- Formular políticas a seguir sobre datos
- Planificar la evolución de las bases de datos de la organización
- Mantener la documentación sobre los datos

Administrador de Base de Datos
- Responsable por la eficiencia de las Bases de Datos
- Mantener el control de accesos a las Bases de Datos
- Asistir a los usuarios a utilizar mejor las Bases de Datos

Administrador de Seguridad
- Implementar y mantener la seguridad física y lógica de los SI
- Controlar el estado de la seguridad sobre los SI
- Investigar las violaciones a la seguridad
- Asistir a los usuarios a diseñar controles
- Mantener los mecanismos de control de acceso

Administrador de Red
- Planificar, implementar y mantener las redes de datos y voz.

Especialista en Soporte a Clientes/Usuarios Finales
- Aconsejar a los usuarios finales en el análisis, diseño e implementación de sistemas
- Determinar las necesidades de herramientas de usuarios finales
- Dar soporte a usuarios finales sobre las distintas herramientas

Especialista en Aseguramiento de Calidad
- Establecer estándares para el control de la calidad en la función de los SI
- Asegurar que todos los sistemas cumplen con los requerimientos de calidad antes de ser puestos en producción

Project manager
- Responsables de planificar y organizar un proyecto.
- Tienen que manejarse con el presupuesto asignado.
- Tienen que ejecutar la visión del comité de planeamiento.

Aspectos a evaluar

Las responsabilidades, obligaciones y autoridad de cada puesto deben estar claras y las personas deben comprenderlas correctamente.

Separación de Obligaciones

Siempre se debe preservar la separación de obligaciones, es importante para prevenir y detectar actos maliciosos. Si una sola persona es responsable de diversas aplicaciones críticas, es posible que ocurran errores que no se detecten en tiempo y forma, y el daño potencial que puede producir es grande. Se deben limitar el acceso a las computadoras, programas en producción, datos y sistemas operativos.
En organizaciones descentralizadas es más difícil, ya que es el usuario quien analiza, programa, y opera, aunque no siempre cuente con el perfil de un profesional en SI.

Funciones importantes a separar
- Custodia de activos
- Registro de transacciones y autorizaciones

Combinaciones

El departamento de sistemas y el de usuarios finales siempre deben estar separados, por el riesgo que conlleva combinar funciones incompatibles.

Mecanismos de control

Para asegurar la separación de obligaciones:
- Autorización de transacciones:
  Responsabilidad del departamento de los usuarios. Se realizan chequeos periódicos buscando registros de transacciones no autorizadas.
- Custodia de activos:
  Se debe determinar y asignar apropiadamente a un departamento en particular que determinará el nivel de seguridad apropiado para protegerlos.

Las decisiones de control de acceso se basan en una política organizacional que suele ser discrecional o mandataria.
Los mecanismos de control se proveen combinando seguridad física, de aplicaciones y del sistema. No deben interrumpir el ciclo normal de trabajo ni sobrecargar a los administradores o auditores.

Compensando la falta de separación

En algunas organizaciones pequeñas puede no haber suficiente personal para separar las funciones, por lo que tenemos que implementar controles que mitiguen los riesgos.

Los audit trails permiten al auditor crear un mapa que sigue hacia atrás el flujo de la transacción para compensar la ausencia de separación de obligaciones. El auditor debe poder determinar quien inició la transacción, el tiempo y los cambios introducidos basándose en:

- Reconciliación
- Reporte de excepciones
- Logs de transacciones
- Revisión de los supervisores
- Revisiones independientes

La Ubicación de la Función de SI

El auditor debe determinar la importancia asociada a los SI y evaluar si su función está ubicada correctamente para asegurar autoridad e independencia, ya que impacta en la efectividad que tiene dentro de la organización.

- Si la organización es estratégica, debe ser un grupo independiente y ubicarse en lo alto en la jerarquía para participar en la toma de decisiones.
- Si la organización es soporte, su ubicación es menos importante ya que no participa en las decisiones estratégicas y puede no ser un sector independiente, diseminando su función en áreas usuarias y dependiendo de la gerencia más importante (Ej.: Contaduría).

Conducir

La conducción es una función gerencial compleja diseñada para influir en el comportamiento de un individuo o grupo. El proceso de conducción requiere que la gerencia motive, dirija y comunique información a sus empleados. Si no se conduce correctamente, el personal puede no comprender los objetivos generales, desmotivarse y no comunicar los resultados obtenidos.

Para el auditor es difícil evaluar esta tarea, debe comprender tres aspectos:

- Cómo motivar subordinados
- Cómo encontrar un estilo de liderazgo para las características del trabajo
- Cómo comunicarse claramente con los subordinados.

La mayoría de las teorías se basa en que no existe una mejor manera de motivar a todos.

Al asignar miembros a distintos proyectos existen dos tipos de personas:

- Los que tienen facilidad para trabajar con incertidumbre.
- Los que son más conservadores y les molesta la incertidumbre.

Los auditores no tienen los conocimientos ni la experiencia para evaluar si cada persona está motivada. Se examinan:

- Estadísticas de rotación de personal
- Fracasos frecuentes de proyectos en cuanto a satisfacer presupuestos
- Niveles de ausentismo.

Existen distintos estilos de conducción, desde democráticos a autoritarios, y ninguno es más apropiado que el otro, varía dependiendo de las personas y las tareas. Algunos requieren mayor conducción que otros y algunos son más inseguros o inexpertos que otros.

Lo ideal es buscar gerentes con estilos de conducción adaptables o capacitarlos para este fin. Al igual que con la motivación, es difícil para el auditor evaluarla. Debe analizar rotación de personal, cumplimiento de presupuestos e inasistencias.

Comunicación Efectiva

La función de SI requiere que se realicen tareas de manera precisa, por lo que la comunicación entre supervisores y subordinados es crítica. Los mensajes deben comprenderse claramente y el auditor puede evaluar canales formales e informales de comunicación.

Canales Formales

Planificación de sistemas, documentación de estándares y políticas, outputs de reuniones y memorándums enviados.

Se debe estar alerta a elementos que distorsionan la buena comunicación, como mensajes ambiguos, o con información filtrada o subjetiva.

Canales Informales

Incluye entrevistas con el personal, observar si existe un propósito en los miembros de un equipo y evaluar las tareas que se realizan. En entrevistas con la gerencia, se puede analizar cómo el gerente se dirige a los empleados.

Los problemas de comunicación pueden tener un efecto directo e inmediato, o indirectos y a largo plazo (Ej.: Pérdida de respeto a los superiores y rotación de personal). Los auditores deben poder evaluar ambos casos.

Evaluar la Función de Control

Determinar cuándo las tareas de las funciones de SI se desvían de las actividades planificadas.
Si la alta gerencia controla estas funciones surgen 2 preguntas:

- ¿Cuánto debe invertir la organización en la función de los SI?
- ¿Tiene la organización un beneficio económico por la función de los SI?

Los gerentes buscan los promedios del mercado para determinar cuánto invertir, lo cual refleja una instancia reactiva en lugar de proactiva. Esto sucede generalmente cuando la función de los SI no está ligada a la estrategia general de la organización, y la alta gerencia ve la función de SI como un gasto y no como una inversión.
Comúnmente, si es una inversión de capital, se invierte hasta que no haya pérdidas o haya beneficios. El problema de esta visión es que los SI están plagados de intangibles y se vuelven obsoletos rápidamente. Los auditores deben evaluar si la alta gerencia decide sobre cuanto invertir y controla el análisis de inversión de capital.
En cuanto al beneficio económico, no existe un método fácil de evaluación. Se puede realizar algo con post-auditoría y proyectos muy controlados. Es muy difícil en entornos distribuidos con varios proyectos simultáneos.

Bussines Continuity Planning

El BCP es responsabilidad de la alta gerencia. Su objetivo es permitir que el negocio siga ofreciendo los servicios críticos ante un problema y sobreviva a una interrupción desastrosa. El primer paso para diseñarlo es identificar los procesos de negocio de importancia estratégica, luego se hace un análisis de riesgo de los activos que soportan los procesos clave y una lista de vulnerabilidades con las probabilidades de que sucedan. El plan debe abordar todas las funciones y activos necesarios para producir un nivel reducido pero suficiente de funcionalidad, y debe incluir procedimientos para minimizar las consecuencias.
El BCP consiste en:

- Plan para la continuidad de operaciones.
- Un DRP (Disaster Recovery Plan) para recuperar o mudar una locación que se ha vuelto inoperable.
- El plan de restauración para volver a la normalidad en un lugar nuevo o recuperado.

BCP en los SI

El acercamiento es el mismo, ya que en este caso la continuidad de los SI está amenazada y tienen importancia estratégica. Debe incluirse en el BCP general o ser consistente con este, y actualizarse si la estructura de IT cambia.

Principales Amenazas

- Daño por Fuego
  Suele ser la amenaza más seria, ya que las pérdidas por el fuego pueden ser sustanciales. Algunos países tienen servicios gubernamentales que aconsejan sobre las medidas de protección contra incendios. Los administradores de seguridad deben revisar y testear las protecciones contra incendios periódicamente, y debe entrenarse al personal para su uso correcto. Se deben documentar los procedimientos a realizar por emergencias.
- Daño por Agua
  Se deben tener techos, paredes y puertas a prueba de agua cuando sea posible. Dentro de la instalación, hay que asegurar que existe un correcto sistema de drenado, colocar alarmas en lugares estratégicos, cubrir el hardware con protectores cuando no se lo usa y ubicar los bienes por encima del nivel del suelo.
- Variaciones de Energía
  Pueden ser aumento de potencia (sobrecarga), disminución o corte. Las fuentes de energía deben monitorearse para asegurar que sean adecuadas y confiables. Para proteger de aumentos temporarios, se instalan reguladores de voltaje y para aumentos sostenidos, interruptores de circuitos. Para protección contra cortes, se usan fuentes alternativas, como UPS. También se debe tener en cuenta otros objetos, como cerraduras electrónicas en puertas.
- Polución
  La polución (generalmente polvillo) puede desde dañar discos hasta causar incendios. Se debe filtrar el aire a través de los sistemas de aire acondicionado y evitar la acumulación de polvillo en techos y pisos.
- Intrusión no autorizada
  Por fuera se deben colocar cercos de protección y seguridad en puertas y ventanas. En el interior es recomendable un sistema de bloqueo electrónico de puertas y seguridad en los conductos de aire acondicionado.

Seguridad lógica

Identificar y autenticar a los usuarios es un pre-requisito necesario para determinar quién tiene autorización para acceder a cada sitio y los niveles de autoridad.

Seguridad de las comunicaciones

Los datos se deben proteger de las escuchas y manipulaciones asegurando los medios de comunicación (Ej.: Cables o fibra óptica) y encriptando y autenticando los mensajes.

Information Security Policy

Para proteger en forma efectiva los activos, la política de seguridad de la compañía debe proveer guías que determinen el valor de los recursos de información, el impacto de los eventos que podrían ocurrir y el nivel de riesgo que están dispuestos a aceptar.

Debe decir que

- La información es un recurso importante que debe ser protegido
- Para esto la organización cumplirá con todas las leyes aplicables y regulaciones
- El acceso será garantizado a los individuos que lo requieran para realizar sus funciones.
- Se mantendrá la confidencialidad.
- La información se protegerá en forma apropiada contra modificaciones no autorizadas.
- La información estará disponible para soportar las decisiones de negocio.
- Se implementarán controles que garanticen la integridad, confidencialidad y disponibilidad.

Plan de Recuperación de Desastre

A pesar de los resguardos, la función de los SI puede sufrir un desastre y quedan dos controles como último recurso, el Plan de Recuperación de Desastre y los Seguros.

Su propósito es restaurar las operaciones de la función de los SI luego de una situación de desastre.

Se deben tener planes y ensayos para cada tipo de impacto, ya sea localizado (Ej.: Daño en una BD) o generalizado (Ej.: Incendio en una instalación). Estos planes son caros y difíciles de preparar, mantener y testear.

Los auditores deben evaluar que existan, estén en su lugar y sean adecuados. Si el auditor es externo, debe constatar la habilidad del cliente de retomar sus operaciones, poniendo especial cuidado en las demandas que puedan surgir por no cumplir los contratos con terceras partes.

El plan debe proveer políticas, guías y procedimientos para todo el personal involucrado con los SI, como procedimientos de backup diarios. El plan de Recuperación de Desastre consta de cuatro partes:

Plan de Emergencia

Acciones a realizar inmediatamente luego del desastre. La gerencia debe identificar en que situaciones se invoca el plan y las acciones que se inicien en cada caso dependiendo de su naturaleza (Ej.: Irse o quedarse en el lugar).

Para cada situación incluir:

- Quién debe ser notificado inmediatamente
- Acciones a tomar por el personal, tanto para salvaguardar activos como su integridad
- Procedimientos de evacuación y retorno.

Se debe especificar el responsable para cada tarea, y el procedimiento a seguir.

Plan de Backup

Incluye los tipos de backup que se deben mantener, frecuencia de ejecución, procedimientos, ubicación de los recursos, sitio donde pueden restaurarse, operaciones para restaurar, personal responsable, prioridades para recuperar los sistemas y un cronograma que muestre cuando cada sistema puede ser recuperado.

- Controles
  El plan necesita actualización permanente, ya que el personal, hardware y software disponible va cambiando. La mayor dificultad radica en asegurar que todos los recursos críticos están resguardados.
- Recursos
  - Personal: Entrenamiento y rotación de obligaciones para facilitar reemplazos. Acuerdos con otras empresas para proveer personal.
  - Hardware: Acuerdo con otras empresas para provisión del hardware.
  - Facilidades: Acuerdo con otras empresas para provisión de facilidades.
  - Documentación: Inventario de lo que está almacenado de manera segura dentro y fuera del sitio.
  - Insumos: Inventario de insumos críticos almacenados de manera segura dentro y fuera del sitio, con listas de vendedores que los provean.
  - Datos/Información: Inventario de lo que está almacenado de manera segura dentro y fuera del sitio.
  - Software de aplicación/Sistema: Inventario de lo que está almacenado de manera segura dentro y fuera del sitio.
- Sitios
  - Cold Site: No está en línea permanentemente, pero tiene todas las facilidades para instalar los equipos necesarios. Puede ser de la misma organización o contratado. Es adecuado solo si la organización tolera un tiempo sin sistema.
  - Hot Site: Son compartidos y en ellos se guardan el software, los datos e insumos. Todo el hardware y las facilidades están disponibles en el sitio todo el tiempo, por lo que son caros de mantener.
  - Warm Site: Provee un nivel de backup intermedio. Tiene todas las facilidades del cold site, además del hardware que podría ser difícil de conseguir o instalar.
  - Acuerdo Recíproco: Dos o más organizaciones se proveen mutuamente de sitios de backup en caso de que alguna sufra un desastre. Es una alternativa barata e informal que requiere buena capacidad de procesamiento.
- Contratos
  Al usar un sitio de backup de otra empresa, los contratos deben incluir:
  - Momentos de disponibilidad del sitio.
  - Cantidad de organizaciones que simultáneamente pueden usar el sitio.
  - Prioridad que se asignará a usuarios concurrentes en el caso de un desastre común.
  - Período por el cual se puede usar el sitio.
  - Condiciones bajo las cuales se puede usar el sitio.

- Facilidades y servicios que se comprometen a proveer en el sitio.
- Controles que se implementarán en el sitio.

Plan de Recuperación

Define procedimientos para restaurar las capacidades completas de los SI, específicamente para cada tipo de desastre. También especifica un comité de recuperación y sus responsabilidades, provee guías e indica qué aplicaciones recuperar primero.

Plan de Testeo

Identifica deficiencias en los planes y en la preparación de la organización y del personal ante un desastre. Debe permitir simular desastres periódicamente, seguir los planes y especificar porque estos pueden considerarse o no satisfactorios.

- Inconvenientes: Interrumpir las operaciones diarias, o que ocurra un desastre como resultado de la simulación
- Soluciones: Probarlo mediante inspecciones formales y no en la práctica, o simular en un horario no conflictivo.

Auditando la continuidad de un negocio mediante el BCP

- Evaluar la relación del BCP con los objetivos de negocio.
- Comparar el BCP con estándares y regulaciones existentes.
- Verificar la efectividad del plan mediante testeos anteriores.
- Verificar como se transportan los datos resguardados.
- Evaluar la respuesta del personal ante emergencias.
- Evaluar que los manuales y procedimientos relacionados sean fáciles de entender.

Questions to consider include:

- Who is responsible for administration or coordination of the plan?
- Is the plan administrator/coordinator responsible for keeping the plan up-to-date?
- Where is the DRP stored?
- What critical systems are covered by the plan?
- What systems are not covered by the plan? Why not?
- What equipment is not covered by the plan? Why not?
- Does the plan operate under any assumptions? What are they?
- Does the plan identify rendezvous points for the disaster management committee or emergency management team to meet and decide if business continuity should be initiated?
- Are the documented procedures adequate for successful recovery?
- Does the plan address disasters of varying degrees?
- Are telecommunication's backups (both data and voice line backups) addressed in the plan?
- Where is the backup facility site?
- Does the plan address relocation to a new information processing facility in the event that the original center cannot be restored?
- Does the plan include procedures for merging master file data, automated tape management system data, etc., into predisaster files?
- Does the plan address loading data processed manually into an automated system?
- Are there formal procedures that specify backup procedures and responsibilities?
- What training has been given to personnel in using backup equipment and established procedures?
- Are the restoration procedures documented?
- Are regular and systematic backups of required sensitive and/or crucial applications and data files, being taken?
- Who determines the methods and frequency of data backup for critical information stored?
- What type of media is being used for backups?
- Is offsite storage used to maintain backups of critical information required for processing either onsite or offsite operations?
- Is there adequate documentation to perform a recovery in case of disaster or loss of data?
- Is there a schedule for testing and training on the plan?

Módulo 5: Desarrollo - Adquisición - Mantenimiento

Proyectos y programas

La realización de un proyecto comprende muchos factores, como costo, calidad y confiabilidad. Un programa es un grupo de proyectos que tienen un objetivo común, es por esto que se dice que son más complejos y de mayor duración. Quienes toman decisiones estratégicas intentan determinar qué proyectos pueden otorgar ventajas competitivas a la compañía

Enterprise Resource Planning - ERP

Son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y distribución de una compañía. Típicamente manejan la producción, logística, distribución, inventario, envíos, facturas y contabilidad de la compañía de forma modular. Sin embargo, también pueden intervenir en el control de ventas, entregas, pagos, producción, administración de inventarios, calidad de administración y la administración de recursos humanos.

SAP Business Suite

Es un conjunto de programas que permiten a las empresas ejecutar y optimizar distintos aspectos como los sistemas de ventas, finanzas, operaciones bancarias, compras, fabricación, inventarios y relaciones con los clientes. Ofrece la posibilidad de realizar procesos específicos de la empresa o crear módulos independientes para funcionar con otro software de SAP o de otros proveedores.

Causas de fallos

- Falta soporte de la gerencia
- Pobre actitud de los usuarios
- Objetivos de negocios poco claros
- La gente de IT no entiende las necesidades del negocio
- No se especificaron requerimientos adicionales
- Cambios en los requerimientos
- Cambios organizacionales durante el proyecto
- Conversión de archivos demasiado optimista
- Documentación pobre
- Testing inadecuado

Controles en el desarrollo

- Methodology (SDLC)
- Políticas de contratación
- Entrenamiento
- Revisiones técnicas
- Participación en las auditorías
- Testeo de los sistemas
- Revisiones post-implementación
- Documentación
- Revisiones de schedule
- Asignación de trabajos
- Monitoreos de performance
- Monitoreos y reportes de estado

Las fallas de los controles durante el desarrollo causan:

- Decisiones erradas de la gerencia
- Registros inexactos
- Interrupción del negocio
- Fraudes
- Violación de leyes
- Costos operativos excesivos
- Objetivos no alcanzados

Systems development life cicle control (SDLC)

Los objetivos de control para cada etapa del SDLC incluyen 6 etapas:

- Metodología
- Inicio del proyecto
- Estudio de factibilidad
- Diseño del sistema
- Desarrollo e implementación
- Operación del sistema

Metodología

Se sigue una metodología estructurada y formal, definiendo claramente roles y responsabilidades. Son actualizadas a medida que se avanza.

Inicio del proyecto

El departamento de usuarios está involucrado en la definición del nuevo sistema y sus modificaciones, es quien define el alcance antes de comenzar a trabajar y quien autoriza el comienzo de cada etapa. En esta etapa también se eligen equipos de trabajo adecuados.

Estudio de factibilidad

Se evalúan cursos de acción alternativos para seleccionar una solución apropiada que sea factible tecnológica y económicamente. Todos los riesgos relevantes se identifican y los costos se incluyen en el análisis de costo/beneficio. Es la gerencia quien aprueba el proyecto.

Diseño de sistemas

Los programas se especifican a partir de los estándares de la organización. La metodología a usar (prototipos, espiral, metodologías ágiles, etc.) debe ser apropiada para el tipo de sistema a construir. Se estandariza la documentación y la estructura de los archivos. Los requerimientos de validación de entrada deben ser apropiados, deben identificarse las fuentes de datos, definirse y aprobarse los requerimientos de seguridad y aprobarse los registros de auditoría.

Desarrollo e implementación

Al contratar personal de programación, deben especificarse niveles de calidad.

Deben estar disponibles descripciones actualizadas de todos los programas y documentación estandarizada. El testeo del programa tendrá en cuenta la eficiencia y será exhaustivo y efectivo.

El plan de conversión asegurará una transición suave hacia el nuevo sistema, mediante pruebas de aceptación y planes de entrenamiento para los usuarios. Los paquetes comerciales seleccionados deben ser compatibles con las políticas de operación.

Operación del Sistema

Se asegura una operación eficiente del sistema, los controles deben operar correctamente y de acuerdo al uso pretendido. Las modificaciones al sistema se permitirán sólo mediante la autorización apropiada.

Planificación del Objetivo

Se usa para estimar la cantidad de personal necesario utilizando distintos medidores, como Lines Of Code (LOC) que miden el tamaño del producto y los Puntos de Función de Albrecht que miden la funcionalidad del producto.

Puntos de Función

Primero se estima cantidad de ítems y se asigna un peso a cada ítem según una tabla. Luego se calcula la sumatoria de los pesos y se calcula un factor de ajuste dependiendo de 14 factores preestablecidos. Para cada factor se asigna un peso de 0 (irrelevante) a 5 (esencial), que estima su complejidad.

Componentes del Factor de Complejidad Técnico

F1 Confiablidad de back-up y recuperación	*F2* Comunicación de datos
F3 Funciones Distribuidas	*F4* Performance
F5 Altamente dependiente de la configuración	*F6* Entrada de datos on line
F7 Facilidad operacional	*F8* Actualización on line
F9 Interface compleja	*F10* Procesamiento complejo
F11 Reusabilidad	*F12* Facilidad de instalación
F13 Multiples sites	*F14* Facilidad de cambio

Planificación

Los auditores deben evaluar si la planificación es adecuada para el proyecto, mediante observaciones, cuestionarios y entrevistas.

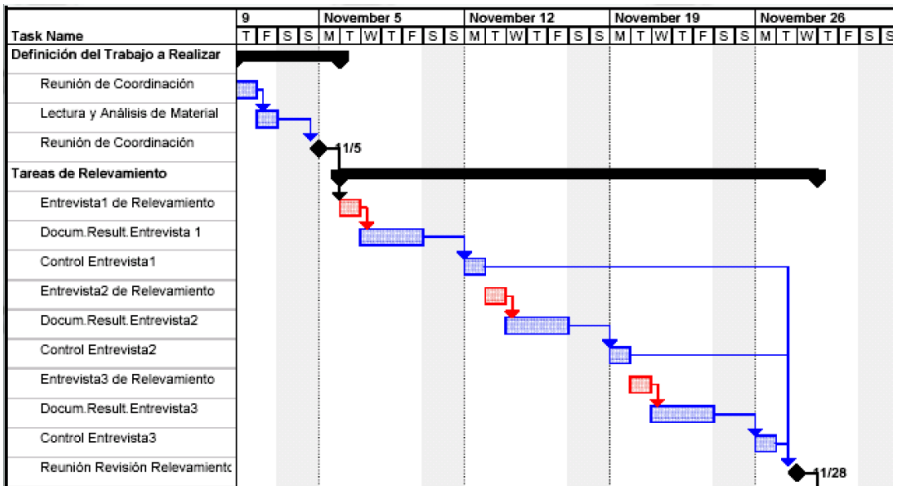
Control

La gerencia es quien establece procedimientos de revisión y control de acceso. La calidad del trabajo debe ser controlada y luego decidir si se continúa con la próxima tarea. Los controles de acceso deben ser tanto manuales como automáticos.

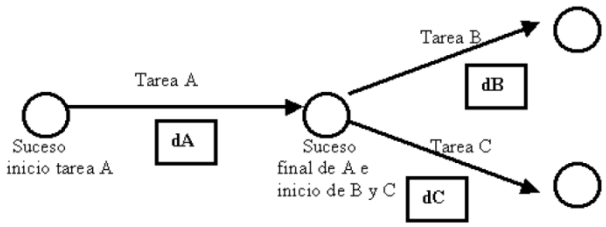
Técnicas de control

Existen tres técnicas principales para monitorear las tareas. Las dos primeras permiten determinar las consecuencias de terminar anticipadamente o con demora una tarea:

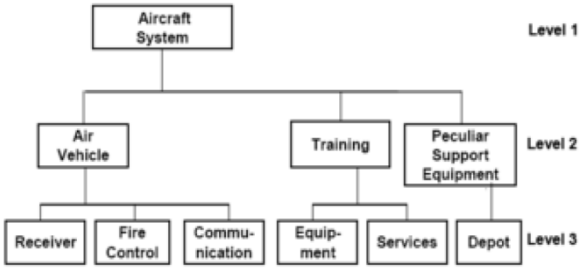
- Diagramas de Gantt



- Program Evaluation and Review Technique (PERT)



- WBS - Work Breakdown Structures



Modelos del proceso (SDLC)

La elección de la estrategia de desarrollo depende del proyecto, métodos, herramientas, controles y entregas. Intentan ordenar una actividad inherentemente caótica, exhibiendo características del "modelo del caos".

- Modelo lineal
  Es el modelo tradicional, también llamado modelo en cascada
- Modelo de prototipos
  Se usa cuando no están claros los requisitos, para que el cliente vea de antemano cómo será la aplicación final.
- Modelo DRA
  Por las limitaciones de tiempo se usa un enfoque en escalas. Enfatiza un ciclo de desarrollo corto y comprende:
  - Modelado de Gestión
  - Modelado de Datos
  - Modelado del Proceso
  - Generación de aplicaciones
  - Pruebas y entrega
- Modelos evolutivos
  Se usa en productos que evoluciona con el tiempo, ya que permiten desarrollar versiones cada vez más completas del SW. Existen distintas alternativas:
  - Modelo incremental: modelo secuencial + prototipo.
  - Modelo espiral
  - Modelo de desarrollo concurrente
- Desarrollo basado en computación
  Posibilitado por el paradigma de objetos, es evolutivo por naturaleza. Se identifican las clases candidatas, se eligen las que ya existen en la biblioteca para reutilizarlas y se desarrollan las que no están disponibles.
- Modelo de métodos formales
  Se especifica, desarrolla y verifica mediante una notación matemática formal. Se usa en sistemas de extrema seguridad, pero tiene problemas de aplicabilidad en entornos de gestión.
- Desarrollo Ágil
  Son reglas de comportamiento para mejorar el desarrollo, que se adaptan y evolucionan con cada proyecto.

Etapas comunes

Sin importar el SDLC usado nos encontraremos con las siguientes etapas:

- Estudio de factibilidad
- Diseño preliminar
- Diseño detallado
- Código, testeo e implementación
- Conversión e Instalación
- Revisión post implementación

Estudio de factibilidad

Será necesario si la junta directiva quiere un cambio en la política de negocios o mejorar algún aspecto al negocio, como efectividad o eficiencia. También puede ser que haya habido algún cambio legislativo o tecnológico.

Diseño preliminar

Se tienen en cuenta:

- La funcionalidad de negocios requerida por el sistema y los servicios que requiere.
- Acciones que van a tomar los usuarios y las responsabilidades de cada uno.

- Reglas de decisión a aplicar.

Diseño detallado

Comenzamos a trabajar con la jerga propia de la ingeniería de software, definiendo:

- Formatos de archivos y datos
- Limites operacionales
- Lógica de procesamiento
- Reglas de acceso

En esta etapa pueden surgir los siguientes problemas:

- El departamento de IT se aísla para desarrollar el sistema y, al no tener interacción con los usuarios, el producto no es el esperado.
- El personal disponible para las pruebas no tiene la autoridad o el conocimiento necesario.
- Se busca constantemente lo último en tecnología sin importar lo que verdaderamente se necesita.

Implementación

Se revisan el alcance y los objetivos para asegurar que sigan siendo válidos. Luego se planifica la implementación, asignando responsabilidades para el desarrollo de las distintas partes. Tareas:

- Programación
- Creación de prototipos
- Prueba de unidades
- Testeo de integración
- Documentación
- Instalación
- Testeo de aceptación
- Entrenamiento de los usuarios
- Conversión de archivos

Conversión e instalación

Incluye todas las actividades necesarias para poner al sistema en funcionamiento. Puede ser que no haya habido un sistema anteriormente, pero en caso contrario se hace una transición que, dependiendo de la naturaleza del sistema puede ser una etapa menor o involucrar todo un período. Típicamente comprende:

- Adquisición de datos
- Identificación de fuentes
- Desarrollo de programas de conversión
- Rectificar los datos de entrada
- Conversión de archivos

Si existe un sistema anterior, la conversión puede ocurrir de 3 maneras posibles:

- Discontinuación abrupta
  Reduce costos de conversión, pero no hay vuelta atrás
- Instalación por etapas
  Reduce costos de conversión y la transición es ordenada, pero no hay vuelta atrás y se le genera dificultades a los usuarios por tener q usar 2 sistemas.
- Instalación en paralelo
  Corren en paralelo por lo que se tienen menos riesgos, pero los usuarios deben tratar con ambos sistemas durante un tiempo y se tienen mayores costos por tener que operar en simultaneo.

En cualquier caso involucra 4 actividades:

- Entrenamiento del personal: Se capacita a usuarios principales y secundarios
- Instalación del nuevo HW/SW: Si se compró HW o SW nuevo se debe instalar y testear.
- Conversión de programas y archivos: Puede ser extenso si el sistema anterior es manual o incompatible.
- Planificación de operaciones y pruebas: Pruebas de planificaciones, coordinar entrada, procesamiento y output.

Los auditores deben prestar atención a la administración del proceso de cambio en etapas de conversión y cuáles son los riesgos si la instalación es abrupta. Se deben planificar y controlar cuidadosamente las tareas de conversión, y ajustar los controles al finalizar, ya que se relajan durante el proceso.

Revisión post implementación

En este último paso, se determina que salió bien y mal con el proceso. Se pueden mejorar las técnicas de control para próximos desarrollos. El objetivo del SDLC es controlar la generación de sistemas de calidad, de acuerdo a la especificación y dentro del presupuesto

Operación y Mantenimiento

No es parte del SDLC. Se pueden realizar 3 tipos de mantenimiento:

- Correctivo: Corrigiendo errores de lógica detectados
- Adaptativo: Cambiando al sistema para adaptarlo al entorno
- Perfectivo: Mejorando la eficiencia de procesamiento.

Rol del auditor

Evalúa si los controles son adecuados para que el sistema sea entregado tal como fue pactado y escribe reportes a la gerencia apropiada, incluyendo una estimación del progreso y las mejoras requeridas. Debe tener entendimiento del proceso de desarrollo adoptado y de la dinámica del negocio. Puede participar del proyecto o solo revisarlo.

Auditor como participante del proceso

Sirve para asegurar que los controles sean implementados en forma adecuada. Esto puede traer problemas para la independencia del auditor, ya que se vuelve parte del equipo.

Revisar los entregables del proyecto

El auditor se encarga de revisar los entregables en cada una de las etapas del proyecto, pero sin formar parte del equipo de desarrollo.

Auditoría y control de paquetes adquiridos

Conviene evaluar si el software a implementar ya está disponible en el mercado. El 60% del SW desarrollado son paquetes estándares, por lo que al terminar el diseño preliminar puede ser que comprar convenga más.

La decisión se debe tomar dependiendo de una variedad de criterios:

- Restricciones de tiempo
- Capacidad del personal
- Costos
- Soporte

Un paquete estándar puede modificarse o combinarse con interfaces escritas a medida para satisfacer las necesidades a menor costo, con menos riesgo, más rápido y utilizando menos recursos. El auditor puede asistir en la adquisición.

Pasos necesarios al adquirir:

- Revisar las necesidades y requerimientos
- Adquirir el software
- Modificar o personalizar el software
- Adquirir las interfaces
- Testeo del usuario y aceptación
- Mantenimiento y modificaciones

Request for Information (RFI)

Se emite en un estadío temprano del proceso para obtener información de los productos disponibles, pulir el análisis de producto y a partir de eso averiguar si nos interesa algún proveedor determinado. Debe incluir:

- Visión general de la organización
- Funcionalidad deseada (en general)
- Ambiente operacional actual (hardware y software)

El equipo del proyecto evalúa las respuestas y procede a desarrollar la definición de requerimientos detallada. Una vez que se pudo completar esta se desarrollar un Request for Proposal.

Request for Proposal (RFP)

Además de una definición detallada de los requerimientos, incluye información de los usuarios, el ambiente en que operará, deadlines para implementar, etc. Cuando algún paquete evaluado cumple con los requerimientos se envía un RFP a su desarrollador.

Elección

Luego de recibir las propuestas de los proveedores, se las evalúa tomando en cuenta características del producto y del proveedor, se negocia el contrato y se realiza la instalación. Se puede hacer un outsourcing de la instalación.

Licencias de Software

Contrato entre el titular del derecho de autor y el usuario del programa, que detalla las condiciones de uso.

Clasificación

- Licencia de software libre (Free Software)
  Puede ser con o sin protección heredada
- Licencia de código abierto (Open Source)
- Licencia de software propietario
  Incluye Shareware y Freeware

Software Libre

Puede ser gratis o pago.

Tiene 4 libertades:

- Libertad 00: Ejecutar el programa con cualquier fin.
- Libertad 01: Estudiar y modificar el programa.
- Libertad 10: Copiar el programa para ayudar a tus pares.
- Libertad 11: Mejorar el programa y de hacer públicas esas mejoras, para beneficio de todos.

Licencia Pública General de GNU (GNU GPL)

Se usa en un 60% del software libre. El autor conserva los derechos permitiendo su redistribución y modificación siempre que permanezca bajo licencia GNU GPL, nunca propietaria.

Licencias de tipo BSD

Se utilizan en software distribuido junto a los sistemas operativos BSD. Mantiene la protección de copyright para requerir la adecuada atribución de la autoría en trabajos derivados, pero permite redistribución y modificación.

Esto provoca que sea sensible al Embrace-Extend-Extinguish (EEE), una práctica de las grandes empresas de software que consiste en apoyar un estándar, colaborar con las organizaciones de estandarización (como el W3C o el IETF), implementar el estándar parcialmente añadiendo extensiones propietarias sólo en sus productos para otorgar beneficios extra a sus clientes y aumentar el uso de las mismas hasta que el estándar propietario se convierta en el único

relevante.

Licencias Open Source

Es filosóficamente diferente del movimiento del software libre y tiene relación con la fundación OSI. Su objetivo es darle mayor relevancia a los beneficios de compartir código fuente y captar el interés de la industria.
Cuando un programador puede leer, modificar y redistribuir el código fuente, éste evoluciona y mejora, ya que los usuarios lo adaptan a sus necesidades y corrigen sus errores más rápido de lo que se podría con un desarrollo cerrado.
La OSI sólo aprueba las licencias que se ajustan a la OSD (Open Source Definition).
Premisas del movimiento OS

- Libre redistribución: El software puede ser regalado o vendido libremente.
- Código fuente: El código fuente está incluido o se obtiene libremente.
- Trabajos derivados: La redistribución de modificaciones está permitida.
- Integridad del código fuente del autor: Pueden requerir que las modificaciones se redistribuyan como parches.
- Sin discriminación de personas o grupos: Nadie puede dejarse fuera.
- Sin discriminación de áreas de iniciativa: Los usuarios comerciales no pueden ser excluidos.
- Distribución de la licencia: Se aplican los mismos derechos a todo el que reciba el programa.
- La licencia es específica de un producto: El programa no puede licenciarse como parte de una distribución mayor.
- La licencia restringe otro software: No obliga a que otro software distribuido con software abierto deba ser abierto.
- La licencia es tecnológicamente neutral: No se requiere la aceptación de la licencia por clic de ratón u otra forma específica.

Libre vs. Open Source

Libre implica open source, pero open source no implica libre.

Software propietario

Los propietarios establecen los derechos de uso, distribución, redistribución, copia, modificación y cesión. No permiten que sea modificado, desensamblado, copiado o distribuido ilegalmente y regulan el número de copias que pueden ser instaladas e incluso los fines concretos para los cuales puede ser utilizado. Algunos limitan la responsabilidad derivada de fallos en el programa, pero suelen ofrecer soporte técnico y actualizaciones durante el tiempo de vida del producto.
Estas licencias son llamadas Contrato de Licencia para Usuario Final (CLUF) o End User License Agreement (EULA).

Modelos de comercialización del Software

Puede pensarse al software como un producto o como un servicio, ya que tiene características de ambos.

El software como producto

El software puede considerarse un producto ya que:

- Es diseñado
- Es replicado
- Es distribuido
- Es vendido generando una "cosa" tangible: la cajita
- Ventajas
  El costo se paga una vez, se cobra miles de veces y podemos elegir la licencia que más se ajuste a lo que deseamos o diseñar una propia. También permite agregar obsolescencia programada para mantener al mercado cautivo.
  Si logramos una posición monopólica podremos reducir costos de desarrollo, proteger nuestro monopolio mediante patentes que impidan o desalienten la competencia e incrementar nuestros ingresos litigando.
- Desventajas
  Es difícil contemplar las necesidades de miles de usuarios. La competencia nos puede arruinar el negocio brindando un producto similar a menor costo y, aun sin competencia, competiríamos contra nuestros productos anteriores, ya que el software no se estropea.
  El soporte técnico que brindamos genera pérdidas y, aunque podemos solo soportar a las últimas versiones, somos los responsables legales del funcionamiento del producto. Además, la piratería nos afecta seriamente.
- Aspectos poco éticos
  La ley de oferta y demanda asegura a los clientes obtener el mejor producto al menor precio pero, si bien la competencia es buena para el cliente, no lo es para el productor, por lo que se tiende a monopolizar el mercado.
- Patentes de software
  Son similares a las patentes comunes, pero en vez de patentar un objeto material, patentamos una idea. Son un capital para quien las posee pero un riesgo para el resto del mundo.
- Sistemas de protección basados en software:
  - Pueden ser crackeados
  - Pueden traer problemas de confiabilidad
- Sistemas de protección basados en hardware:
  - Un poco más seguros.
  - Molestan al usuario.
  - Pueden traer problemas de compatibilidad.

Este enfoque permite recaudar cuantiosas cantidades de dinero a empresas ya establecidas pero es complicado que una empresa recién formada pueda tener éxito siguiendo este enfoque.

El software como servicio

Presenta ciertas características que lo hacen un servicio:
- No se fabrica, se desarrolla.
- Los clientes vienen a pedirlo
- Se genera algo no tangible: el servicio brindado
- Las compañías de software no suelen vender el software, sino los permisos para usarlo.
- Ventajas
  Genera más puestos de trabajo para los empleados y es una gran oportunidad de negocio para empresarios pequeños o medianos, porque la mayoría del software sigue siendo a medida (los usuarios no suelen estar conformes con el software que usan). La reconversión de los sistemas existentes es una de las oportunidades para aprovechar, también podemos centrar nuestro servicio en torno al soporte, que junto con el mantenimiento insumen del 70% al 80% del costo del software.
  Podemos usar repositorios como punto de partida de nuestros desarrollos, o bien usar software libre como infraestructura del servicio que brindamos.
  El desarrollo que ha tenido internet brinda espacio para los servicios web, que puede depender de servicios de terceros. Ya existen empresas que apuestan por esta nueva visión proveyendo herramientas necesarias (Ej.: .NET, Applets, Servlets, AJAX, etc.).
  Se encuentra protegido por licencias del tipo copyleft, que lo hacen ser imposible de piratear.
- Desventajas
  No se gana nada con mantener una posición monopólica, ya que es imposible mantener cautivo al mercado, y las patentes constituyen un inconveniente cuando basamos nuestro servicio en software libre. El software como servicio implica cambio, que siempre es resistido.
- Brinda alternativas que no han sido exploradas:
  - Software libre como punto de partida.
  - Software libre como infraestructura.
  - Servicios webs y la web semántica
- Situación ideal para empresas recién formadas o en formación.
- El software como servicio ha encontrado dos nuevos aliados:
  - Gran cantidad de software libre de calidad.
  - El interés en torno a los servicios web.

Un modelo híbrido
También es posible ensayar un modelo híbrido, en el que brindamos el servicio de obtener de forma gratuita los productos que desarrollemos a lo largo de un cierto período. Esto goza y sufre de algunas de las ventajas y desventajas de ambos acercamientos.

Mantenimiento de los SI

Es el proceso de ordenar los cambios de los sistemas para mantener la integridad del código y los ejecutables.

Proceso de gestión de cambios
Debe existir una metodología para priorizar y aprobar cambios. Comienza cuando se aprueba un cambio, y puede iniciarse por distintos actores. Los usuarios deben proponer cambios usando algún tipo de comunicación formal y se debe poder hacer un seguimiento a cada requerimiento de cambio, asignándole un número a cada uno e ingresándolo en algún sistema. Esta información debe ser mantenida por el staff encargado del mantenimiento, en registros manuales o automáticos, incluyendo mínimamente: ID del programador, fecha y hora, nro. de requerimiento, cambio en las líneas de código.
En caso de sistemas adquiridos el vendedor puede distribuir parches, que deben ser revisados por la gerencia de usuarios y del sistema.

Cuando hay poco personal
Se requieren controles compensatorios por la falta de separación de obligaciones. Si la persona que crea el programa es también quien lo opera se debe tener especial cuidado, se requiere que se aprueben los cambios por la gerencia de usuarios antes de ponerlos en producción (Puede tener un SW de control de cambios para automatizar esta tarea).

Separación de obligaciones
Los programadores no deben tener acceso para modificar, escribir o borrar datos en producción, en algunos casos tampoco podrán leer los datos almacenados.

Aprobación
Después de que el usuario final esté conforme, se debe obtener la aprobación de la gerencia de usuarios en algún documento que el staff de mantenimiento almacene como evidencia.

A tener en cuenta
Debe actualizarse la documentación existente (en la empresa y offsite) para reflejar los cambios.

Probar los cambios
Los programas cambiados deben ser testeados con la misma disciplina que los nuevos para asegurarse de que funcionan según lo esperado.

Testear
Al hacer las pruebas es importante comprobar que la funcionalidad existente no fue dañada, que no se degradó la performance y que no se lo expuso a problemas de seguridad.

Auditar el proceso de cambio
Se debe asegurar que se protege a los programas de cambios no autorizados cumpliendo con los siguientes objetivos:
- Restringir el acceso a las librerías

- Realizar supervisiones
- RFC aprobados y documentados
- Un formulario para Solicitud de Cambios (RFC) con especificación del cambio, costo, fecha de lanzamiento, firmas de quien propone y quien autoriza, y equipo asignado
- Seleccionar un subconjunto de cambios para revisar su proceso
- Si un grupo independiente actualiza los programas en producción, verificar que se posea el RFC

Cambios de emergencia

En los manuales debe estar especificado que hacer si se requieren cambios urgentes para que el SI siga operando. Estos deben aplicar los procesos de manejo de cambio de forma retroactiva y se mantienen en una librería de emergencia hasta que se completa el proceso normal.
Se usan IDs monitoreadas que permiten que el programador tenga acceso al ambiente de producción

Deployment de los cambios

Una vez que la gerencia de usuarios aprueba los cambios, un grupo independiente encargado de la calidad pone en producción las modificaciones. Se deben implementar restricciones de acceso a través del SO o algún paquete externo
En SDs se deben cambiar todos los nodos con tiempo para asegurar que:

- Se realicen controles sobre la conversión de los datos
- Se entrene al personal
- Se reduzca el riesgo de cambiar todos los nodos a la vez

Causas de los cambios no autorizados

- El programador tiene acceso a las librerías en producción
- El usuario responsable de la aplicación no sabe del cambio
- No están establecidos los RFC estándares ni los procedimientos
- No firmaron para autorizar la realización del cambio
- El responsable no autorizó el cambio en producción
- El programador puso código extra para beneficio personal
- Los parches no fueron testeados
- El vendedor tiene acceso a cargar los cambios en el sistema en producción

Control de versiones

A todo desarrollo le conviene tener archivada su historia, ya que si colaboran varias personas, es necesario registrar el cambio de cada autor por si alguna modificación produjo un error oculto. Se monitorean los cambios al código, documentación y archivos de configuración para volver atrás cuando se llega a un dead end.
A veces se mantiene una versión estable y una experimental.

Gestión de fuentes

Un sistema de gestión de fuentes registra la historia como un conjunto de diferencias (con los meta-datos necesarios) sobre el patrón más reciente. Debe permitir la colaboración y el trabajo concurrente.

Gestión de versiones

El control puede ser pesimista u optimista. El pesimista bloquea los archivos y provoca retrasos, el optimista deja avanzar pero nos informa cuando se producen conflictos.

Conceptos básicos

Un repositorio está compuesto por el código fuente en un punto del tiempo y su historia asociada, un conjunto ordenado de cambios llamado changeset. A cada changeset le podemos asociar información adicional, como autor y fecha.
La operación más básica es el branch, que produce una working copy sobre la que se pueden elaborar cambios de forma concurrente. Luego se deben combinar los cambios con un merge y se actualiza el repositorio con un commit, creando una versión diferente del archivo.
Un export es similar a un commit, pero produce una versión sin metadata.
Una versión aprobada de un documento se denomina baseline.

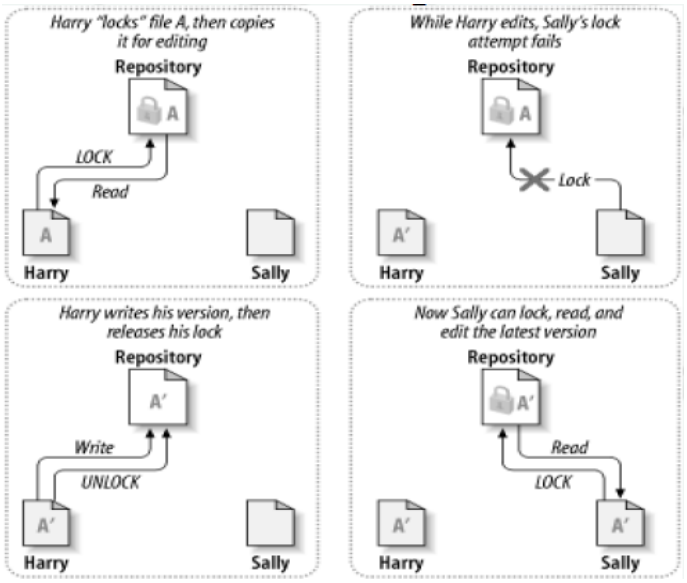
Paradigmas

Existen dos paradigmas de funcionamiento:

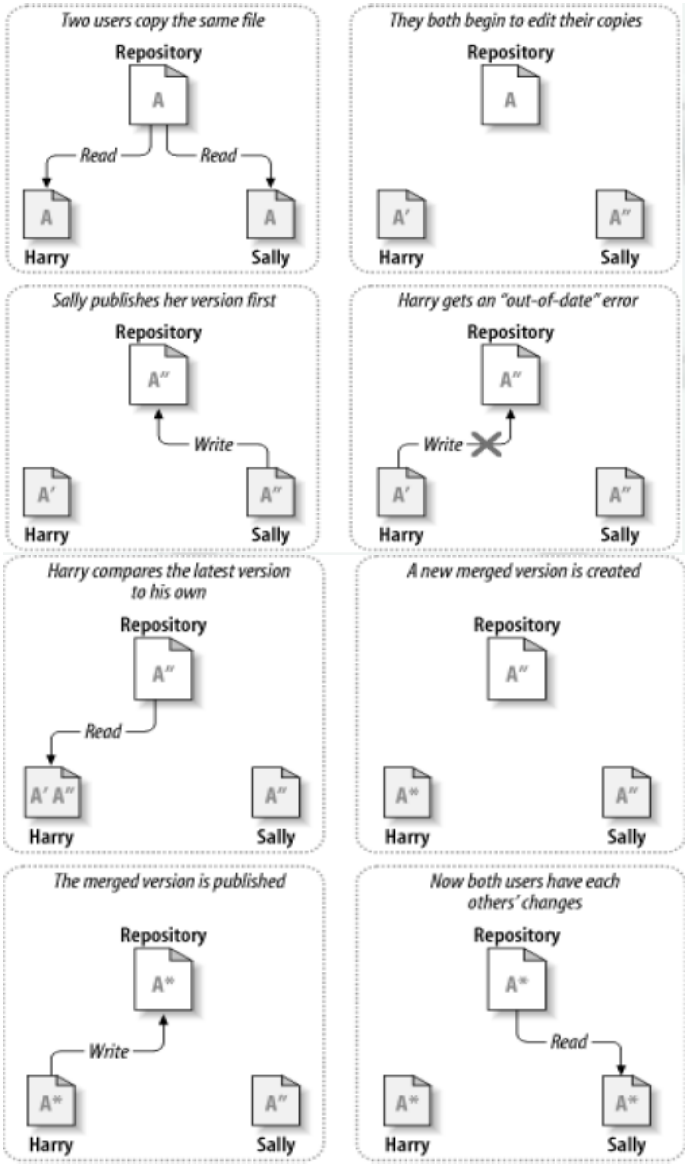
- Centralizado
  Tiene una arquitectura centralizada tipo cliente servidor
- Distribuido
  No existe un punto central, los nodos son pares

Problema
Cuando dos o más personas trabajan editando el mismo archivo concurrentemente, puede ser que los cambios de uno sean sobrescritos por otro. Los Sistemas de Gestión de Versiones (SGV) poseen algoritmos de detección y resolución de conflictos, y solo informan al usuario si no puede resolverlo automáticamente. Soluciones:

- Lock-Modify-Unlock



- Copy-Modify-Merge



SGVs Centralizados

Un repositorio único global al que todos los desarrolladores se conectan, en el que se guardan todos los changesets y se crean todos los branches. En el modelo básico se debe trabajar online
Hay dos tipos de SGV centralizados:
- Los que usan Lock-Modify-Unlock
  Antiguo, simple y limitado
- Los que usan Copy-Modify-Merge
  Se hace una copia del estado del repositorio, se modifica y se aplica el changeset con un merge.

SGVs Distribuidos

No existe un punto central, los repositorios se distribuyen en diversas máquinas, aunque cada desarrollador tiene un repositorio sobre el cual trabaja independientemente. No existen niveles de acceso, todos tienen control completo.
Periódicamente se consolidan los trabajos de todos en algún repositorio convenido mediante una generalización del merge, que se realiza frecuentemente y es imprescindible para el funcionamiento del sistema.

Concurrent Versioning System (CVS)

Es un sistema de gestión de fuentes optimista, creado a fines de los 80 y muy usado en los proyectos de Software libre. Trabaja con un repositorio central que se accede con un esquema cliente/servidor.
El administrador decide quien tiene acceso a cada parte del repositorio y puede ver quienes editan cada cosa, ya que varios clientes pueden trabajar en paralelo.
Puede permitirse un acceso anónimo de solo lectura, fundamental para entregar versiones frecuentemente al público.
Al comenzar a trabajar se hace un check out (o branch) del proyecto o de una rama ya creada, luego, cuando se realiza el check-in (o commit) de los cambios, se intenta un merge. Si falla, el usuario debe resolver el conflicto, sino se incrementa el número de versión y se etiqueta al changeset con los datos del usuario para saber quién hizo cada cambio en particular.
Los clientes pueden mantener distintos branches del sistema. Una versión released pude formar un branch para arreglar bugs, mientras que una versión bajo desarrollo para agregar funcionalidad puede formar otro.
Para almacenar las distintas versiones eficientemente, CVS usa delta compresión.

Inconvenientes de CVS:
- No soporta renombramientos ni cambios de directorio
- Es complicado el uso de ramas y mezclas
- Necesita conexión con el servidor siempre
- No posee atomic commits para grupos de archivos (Si A hace commit de 10 archivos y B hace un commit del archivo 8, solo los primeros 7 se aceptan y el repositorio queda inconsistente)
- El commit no se puede revertir
- No permite usar otras herramientas para mezclar ficheros que han dado lugar a conflictos
- No posee una interfaz gráfica nativa
- No genera un changelog de forma nativa

Subversion

Se pensó como reemplazo a CVS y soluciona gran parte de sus problemas
Usa el modelo Copy-Modify-Merge, haciendo todas las operaciones posibles sin conexión y enviando al servidor sólo los cambios.
Para solucionar el problema de CVS en donde se perdía la historia del archivo, el modelo es de un filesystem versionado por lo que, al copiar un archivo A a un archivo B, no se copia el archivo sino que se bifurca a B la línea de tiempo de A. Maneja versiones por repositorio, no por archivo como CVS.
Los repositorios subversion tienen una interface web gratis.
Conclusiones
Estos sistemas, que han revolucionado la comunicación entre desarrolladores, deben acompañar y ajustarse a la manera en la que concebimos y desarrollamos software. También se pueden utilizar en otras disciplinas, por ejemplo, para administrar versiones de documentos CAD.

Controles de aplicación

Se realizan sobre las entradas y salidas de datos y procesamiento de transacciones de cada programa de aplicación. Su objetivo es asegurar la completitud, precisión y valides de los registros, permitiendo asegurar la confiabilidad e integridad de los datos y el sistema. Para esto, controlan que:
- Sólo se ingresen datos completos, válidos y precisos
- El procesamiento realice la tarea correcta
- Los resultados alcancen las expectativas
- Los datos sean mantenidos correctamente

Metodología

El auditor debe testear que los controles realicen:
- Edit tests
- Totalizaciones
- Reconciliaciones
- Identificaciones
- Reportes de datos incorrectos o excepcionales
- Es bueno combinar procedimientos manuales con automatizados

Tareas del auditor
- Entender el funcionamiento de la aplicación

- Desarrollar una estrategia de testeo
- Identificar las fortalezas en los controles
- Identificar las debilidades y donde impactan
- Testear los controles para asegurar que funcionen y sean efectivos

Controles de entrada

Debe asegurar que cada transacción es ingresada, procesada solo una vez y registrada en forma precisa y completa. La información ingresada debe ser válida.

Documentos fuente

Son la base física sobre la cual se registra una transacción y contienen:

- Descripción del business transaction
- Fecha
- Monto
- Firma / autorización

Hay leyes que regulan cuanto tiempo deben guardarse como evidencia para los auditores, junto con las cintas de la caja registradora, los recibos de las tarjetas, las órdenes de venta y las facturas. Sus objetivos son:

- Reducir la probabilidad de errores
- Controlar el flujo de trabajo
- Facilitar la entrada de datos al sistema
- Incrementar la velocidad y precisión de lectura de datos
- Facilitar los chequeos posteriores

Autorización de la entrada

Todos los documentos fuentes deben ser controlados en forma apropiada y todas las transacciones que lo necesiten deben ser aprobadas y autorizadas de alguna de las siguientes formas:

- Firmas en documentos fuente
- Controles de acceso online
- Contraseñas únicas
- Identificación de las terminales
- Uso de documentos fuente

Controles batch y balances

Los controles batch agrupan transacciones de entrada para realizar controles. Pueden usarse formularios preimpresos con números correlativos que permitan verificar más fácilmente. Los tipos de controles pueden ser:

- Total monetario
- Items totales
- Total de documentos

Se deben combinar con otros procedimientos de seguimiento:

- Asegurar que cada transacción genera un documento de entrada
- Que todos los batch fueron procesados
- Que existan formas de solucionar las diferencias

Reporte y gestión de errores

El procesamiento de la entrada requiere identificar los errores para solo aceptar datos correctos. Existen distintas formas de reaccionar ante un batch con errores:

- Rechazar las transacciones con errores
- Rechazar el batch completo
- Poner el batch en suspenso
- Aceptar el batch y marcar las transacciones erróneas

Técnicas de control de entrada

- Logs de transacciones, mantenido manual o automáticamente.
- Reconciliación de los datos, controlando si los datos se procesaron y registraron correctamente.
- Documentar con evidencia escrita.
- Procedimientos de corrección, creando archivos de errores, identificando correcciones en suspenso y aprobando las correcciones hechas.

Controles de proceso

- Aumentan la confiabilidad mediante la validación de datos y los controles de procesamiento
- Cálculos manuales
- Chequeos de edición
- Controles programados
- Chequeos de límites
- Los datos se pueden clasificar en:
  - Parámetros de control del sistema
  - Datos que no cambian regularmente
  - Datos maestros
  - Archivos de transacciones

Controles de salida

Controla que los datos sean presentados, formateados y enviados en una manera consistente y segura:

- Almacenando los documentos críticos en lugares seguros

- Generando instrumentos negociables, formularios, etc.
- Distribuyendo reportes
- Gestionando errores

Pasos al auditar los controles de aplicación

- Identificar los componentes de la aplicación y el flujo de información
  - Revisar documentación
  - Entrevistar personal clave
- Identificar fortalezas y debilidades
- Revisar la documentación:
  - System development methodology documents
  - Cambios en el programa
  - Manuales del usuario
  - Documentación técnica
- Revisar el flujo de transacciones en el sistema
- Usar un modelo de análisis de riesgo:
  - Tiempo desde la última auditoría
  - Complejidad de las operaciones
  - Cambios en el ambiente de operaciones
  - Cambios en posiciones clave
  - Competencia y activos en riesgo
  - Auditorías anteriores
- Observar los procedimientos diarios de los usuarios para analizar su performance
  - Autorizaciones
  - Balances
  - Control de errores
  - Distribución de reportes
- Probar la integridad de los datos
- Probar los sistemas de aplicación

Auditoría continua

Permite recolectar evidencia mientras se desarrollan las operaciones normales sin entorpecerlas. Son muy importantes en sistemas complejos que no dejan paper trail, ya que reducen tiempos y costos, y permiten responder en tiempo y forma, lo cual aumenta la confianza en el sistema. Si no se encuentra nada importante sólo se guarda.

Técnicas

- Systems Controf Audit Review File and Embedded Audit Modules (SCARF/ EAM)
  Software para monitoreo dentro de la aplicación
- Integrated Test Facility (ITF)
  Se introducen entidades dummy para realizar pruebas
- Snapshots
  Se toma una especie de instantánea del camino que sigue una transacción, desde el principio hasta el fin
- Continuous and Interpreted Simulation (CIS)
  Un programa decide que si una transacción sigue un criterio y de ser así la auditar
- Ganchos de auditoría
  Se integran ganchos que funcionan como banderas rojas para evitar irregularidades

Exhibit 3.33—Concurrent Audit Tools—Advantages and Disadvantages

	SCARF/EAM	ITF	Snapshots	CIS	Audit Hooks
Complexity	Very high	High	Medium	Medium	Low
Useful when:	Regular processing cannot be interrupted.	It is not beneficial to use test data.	An audit trail is required.	Transactions meeting certain criteria need to be examined.	Only select transactions or processes need to be examined.

Auditar el desarrollo, adquisición y mantenimiento

Primero, el auditor debe reunirse con los desarrolladores para identificar que areas requieren controles, rankear los riesgos, discutir implementaciones de controles y evaluar los controles disponibles y el proceso de desarrollo.
Luego debe participar en revisiones post implementación, analizar el proceso de mantenimiento e identificar y testear los controles implementados.

Auditar el Desarrollo

- Niveles de supervisión de la junta directiva
- Métodos de manejo de riesgo dentro del proyecto
- Gestión de incidentes

- Gestión de costos
- Procesos de planificación
- Procesos para reportar a la alta gerencia
- Procesos de gestión de cambios
- Gestión de la participación de los distintos actores
- Proceso de aprobación y firmas

Estudio de factibilidad
- Ver que sea razonable la propuesta y la relación costo-beneficio
- Determinar cuan crítica es la necesidad y si hay que implementar algo nuevo

Requerimientos
- Revisar el documento de definición de requerimientos, mediante entrevistas con usuarios clave
- Verificar la aprobación del proyecto y su costo
- Revisar la especificación del User Acceptance Testing (UAT)

Auditar la Adquisición
- Analizar el estudio de factibilidad y determinar si la decisión de adquirir es la adecuada
- Revisar el RFP y determinar si el proveedor elegido coincide
- Asegurar que el contrato haya sido revisado legalmente antes de firmarlo y que incluya los items listados.

RFP = Request For Proposal

Diseño y Desarrollo
- Revisar que los flujos de datos adhieran al diseño general y que los controles de entrada, procesamiento y salida sean íntegros.
- Entrevistar a los usuarios para verificar si comprenden la operación del sistema y las interfaces
- Determinar si los registros de auditoría proveen correcto seguimiento de las transacciones del sistema
- Revisar los resultados de los QA para los programas desarrollados

Testing

Durante el testeo se comprueba:
- Si el sistema valida los requerimientos
- El comportamiento del sistema
- Los controles

El auditor debe comprobar también:
- Si el plan de testeo es completo
- Si los usuarios participaron en diseños de test y/o firma de los resultados
- Los reportes de error, para determinar errores en los datos y resolución de errores
- Reconciliar controles sobre los datos convertidos
- Si la documentación del sistema y del usuario final coincide con el testeo
- La seguridad del sistema mediante pruebas de penetración
- Si se planearon pruebas de controles en los testeos unitarios y del sistema
- Los procedimientos que registran y realizan el seguimiento de los reportes de error
- La aceptación del usuario
- Que el software haya sido enviado al equipo de implantación

Implantación

Debe hacerse de acuerdo a los procedimientos de control de cambios de la organización, incorporando los cambios del testing en la documentación y revisando que los datos se hayan convertido correctamente.

Revisión post-implementación

Cuando el sistema se estabilizo en producción:
- Determinar si se alcanzaron los objetivos, los requerimientos y los costos/beneficios del estudio de factibilidad
- Revisar los cambios requeridos para el nuevo sistema
- Revisar los controles de entrada y salida implementados, y los logs de errores de operaciones para buscar errores

Procedimientos de cambios en el sistema

Luego de la implementación y estabilización, el sistema entra en la etapa de mantenimiento. Hay que considerar:
- El uso de una metodología formal para autorizar, priorizar y controlar los cambios
- Si los procedimientos para cambios de emergencia están en el manual
- Satisfacción de los usuarios con el tiempo y costo que llevo realizar los cambios
- Restricciones de acceso sobre los fuentes en producción y ejecutables

Revisar los cambios

Para un subconjunto de los cambios hechos:
- Determinar si fueron realizados como se esperaba y si se cambió la documentación
- Evaluar si los procesos para realizarlos son adecuados
- Revisar si se respetaron los procedimientos
- Revisar los procedimientos para asegurar la integridad de ejecutables y código
- Revisar los ejecutables en producción y asegurar que sólo haya una versión del código

Archivos útiles en las auditorias

Master File

El Archivo Maestro contiene registros de datos permanentes que fueron creados cuando comenzó el negocio.

Los registros pueden haber comenzado a mantenerse en papel y al pasar del sistema manual a uno automático se los convierte en bases de datos. Contienen información que va desde datos de empleados y clientes, hasta ventas anuales hasta la fecha. Se los suele indexar por sus campos clave.

Archivo de transacciones

Es una colección de registros de transacciones que sirven para actualizar los archivos maestros. Sirven también como registros de auditoría y parte de la historia de la organización. Antes se los transfería a un almacenamiento offline periódicamente, pero cada vez más se mantienen online para realizar distintos análisis.

Módulo 6: Controles de entorno

HASTA ACA INCLUSIVE

El subsistema de entorno establece la interfaz entre el usuario y el sistema. Los controles en él tienen tres propósitos:
- Identificar y autenticar a los usuarios potenciales de un sistema
- Identificar y autenticar los recursos que intentan usar los usuarios
- Restringir las acciones de los usuarios que han obtenido recursos

Debido al e-commerce, son de los controles más importantes. Se dividen en dos tipos:
- Criptográficos
- De acceso

Controles criptográficos

Se diseñaron para proteger la privacidad y las modificaciones no autorizadas de datos. Son utilizados en muchos subsistemas, en forma de passwords, PIN y firmas digitales. Deben asegurar:
- Confidencialidad
- Autenticidad
- Integridad

La criptografía es la práctica y el estudio de técnicas para la comunicación segura en presencia de adversarios (terceros). Se encarga de construir y analizar protocolos que superen la influencia de los adversarios. Sus componentes principales son:
- Encriptación: La práctica de escribir mensajes de forma tal que sólo puedan ser leídos por sus destinatarios
- Autenticación: Asegura que los usuarios son quienes dicen ser y que un mensaje no ha sido alterado sin permiso.

Encriptación/Desencriptación

La función y llave usadas pueden ser iguales o diferentes en cada proceso:
- Encriptación
  Un mensaje plano es transformado en texto cifrado. Se usa una función matemática y una clave.
- Desencriptación
  Es el proceso inverso.

Algoritmos y llaves

Los algoritmos están estandarizados y publicados, pero se ocultan las llaves, que son parte de la entrada del algoritmo.
Si se usa la misma llave para encriptar y desencriptar el algoritmo es simétrico, sino es asimétrico.
Los simétricos tienen una llave privada y los asimétricos un par de llaves publica/privada, en los que, cuando una encripta la otra desencripta y viceversa. Si encripto con mi llave privada, firmo y si me quieren enviar un mensaje encriptan con mi llave pública.

Algoritmos simétricos

Asume que los participantes acordaron una clave común y pueden intercambiarla en forma segura. Los más populares son:
- Data Encription Standard (DES)
  Es un sistema cifrado desarrollado por IBM, tiene una llave de 64 bits (56+8) y convierte un bloque pasándolo a través de 16 rondas de cifrado.
  En Unix se usaba para cifrar el password, pero hoy en día es vulnerable a los ataques por fuerza bruta debido al tamaño pequeño de su clave. Para proporcionar mejor seguridad se lo utiliza en la forma Triple DES.
- Advanced Encription Standard
  La evolución de DES es AES, creado en el 2001. Su proceso de estandarización tomó 5 años y hoy es el algoritmo simétrico más popular.

Pueden mezclarse con algoritmos asimétricos para obtener eficiencia y seguridad.

Algoritmos asimétricos

Usan un par de llaves, los mensajes codificados con la llave pública del receptor sólo pueden ser desencriptados cuando el receptor usa su llave privada. La ventaja es que cada entidad genera un par de llaves y publica su llave pública sin necesidad de requerir una transmisión secreta o acordar una clave común. También pueden garantizar integridad y autenticación, no sólo privacidad. Los más populares son:
- RSA
  Es el más usado actualmente. Las llaves públicas y privadas son intercambiables, se utilizan de tamaños variables de 512, 1024, o 2048 bits.
- El Gamal
  Menos común que RSA, usado en PGP, GNU PG. Tiene tamaños variables de clave de 512 o 1024 bits.

Su mayor defecto es no ser eficientes.
Para comprobar integridad utilizan funciones Hash:
- El emisor calcula el hash, lo codifica con el mensaje usando la clave pública del receptor y lo envía.
- El receptor recibe el mensaje y lo decodifica con su clave privada
- El receptor recalcula el hash del mensaje y lo compara con el hash recibido para verificar integridad.

Si se requiere mayor seguridad, pueden utilizar Firmas Digitales:
- El emisor calcula el hash, que se encripta con la clave privada del emisor para crear la firma digital.
- Se procede como en el caso anterior, pero junto con el mensaje encriptado se envía la firma digital.
- El receptor procede como en el caso anterior al recibir el mensaje, y además procesa la firma digital.
- El receptor obtiene el certificado digital del emisor y usa la clave pública que contiene para obtener el código hash codificado en la firma digital, el cual compara con el código hash recibido en el mensaje.

- El receptor compara la clave pública de la firma digital con la del certificado digital para evitar impostores.

Administración de las llaves

La administración de llaves involucra:

- Generar la llave
  Una sola llave criptográfica para toda la plataforma otorga simplicidad, pero no protege los datos contra usuarios internos no autorizados ya que mucha gente tendrá acceso al texto limpio descifrado. Siempre conviene tener varias llaves para distintos tipos de acceso.
  La longitud de una llave involucra hacer un balance entre el overhead y la seguridad. Si la seguridad es un problema, para RSA se deben usar 2048 bits.
- Distribuir la llave.
  Algunas llaves deben ser distribuidas a diferentes destinos. Para mayor seguridad, la llave puede fragmentarse y transportarse por diferentes medios.
  Una llave también puede ser distribuida electrónicamente. Los criptosistemas de llave pública también proveen medios importantes para distribuir llaves de manera segura.
- Instalar la llave
  Si una llave no es generada en una facilidad criptográfica debe ser instalada desde una fuente externa. El método usado depende de la arquitectura del sistema donde se instalará la llave. Podría ser ingresada seteando switches, por un teclado o transmitida por alguna línea de comunicación. También existen dispositivos que pueden ser usados para generar e instalar llaves. La llave es generada por el dispositivo y guardada en una memoria segura. El proceso debe ser seguro y no debe dejarse lugar a posibles intercepciones.

Para el auditor, evaluar la administración de las llaves es muy importante para juzgar si un criptosistema es confiable.

Controles de acceso

Son el tipo de control más común en el subsistema de entorno. Restringen el uso del sistema a usuarios autorizados, limitando las acciones que puedan realizar y aseguran que los usuarios obtienen recursos auténticos.
Cuando sólo una persona utiliza los recursos, los controles son directos y pueden utilizarse barreras físicas para este fin. Aunque cara, esta estrategia está justificada si los recursos son lo suficientemente críticos.

Mecanismo de Control de Acceso (MCA)

Los controles se implementan mediante un MCA, que asocia los usuarios a los recursos a los que tienen permitido acceder y con qué privilegios. Generalmente es implementado como parte del S.O.
Procesa requerimientos de recursos de la siguiente manera:

- Los usuarios se identifican ante el mecanismo e indican su intención de requerir recursos.
- Los usuarios se autentican y el mecanismo también lo hace.
- El mecanismo reconoce que es un usuario válido.
- Los usuarios detallan los recursos que requieren y las acciones que van a realizar.
- El mecanismo accede a información de los usuarios y los privilegios que tienen para cada recurso

Identificación y autenticación

Los privilegios asignados a un usuario dependen de su nivel de autoridad y del tipo de recurso requerido. Un usuario puede autenticarse de las siguientes formas:

- Información recordada: Nombre, fecha de nacimiento, cuenta, password, PIN.
- Objetos poseídos: Tarjeta plástica, llave, identificación.
- Características personales: Huella digital, voz, tamaño de la mano, firma, retina, preferencias personales. Son casi imposibles de falsificar.

Problemas con información recordada

- Información recordada
  Puede ser olvidada por lo que suelen elegir información fácil de adivinar o escribirla en algún lugar no seguro.
- Objetos poseídos
  Pueden ser perdidos o robados. Se debe confiar en que el usuario avise que no posee más el objeto.
- Características personales
  Los dispositivos necesarios son más costosos.

Durante el proceso de autenticación los usuarios deben estar seguros que están interactuando con un mecanismo de control de acceso auténtico. Una tercero no autorizado podría escribir un programa que simule ser el mecanismo de control de acceso del sistema para capturar un password del usuario mediante "phishing". También podría darse un ataque de tipo "man in the middle", donde el atacante se encuentra entre el usuario y el mecanismo de autenticación capturando datos.

Políticas de control de acceso

Un MCA se usa para hacer cumplir una política de control de acceso. Existen dos tipos:

- Discrecional
- Mandatorias

Políticas Discrecionales

Los usuarios especifican al MCA quién puede acceder a sus recursos mediante una matriz de autorización, donde las filas son los usuarios, las columnas los recursos y el contenido de la celda el privilegio del usuario para ese recurso.
Ellos pueden agregar filas que representen recursos que han creado, pero sólo el administrador podrá borrar filas y columnas de la matriz.

Políticas Mandatorias

Provee menor flexibilidad. A usuarios y recursos se les asignan atributos de seguridad fijos que solo el administrador puede cambiar.

Módulo 7: Operaciones y Soporte

Las expectativas de servicio de una organización se derivan de sus objetivos. El delivery de servicios de IT incluye operaciones de SI, servicios de IT y gerenciamiento de SI. Incluyendo:

- Manejo de operaciones, software, arquitectura, infraestructura de red y hardware.
- Entender SL management, IT financial management, continuidad del servicio, gestión de seguridad de la información
- Manejo de incidentes
- Tecnologías wireless, seguridad
- Servicios en Internet
- Tecnologías Cliente-Servidor
- Pasos clave al realizar la revisión de las operaciones, bases de datos e infraestructura de red
- Conocer controles más efectivos

Service Level Agreement

El departamento de sistemas es de servicio para los usuarios finales. El SLA es un acuerdo entre la organización de IT y los clientes. Sirve para evaluar y ajustar los servicios que pueden brindarse interna o externamente. Considerar:

- Precisión
- Completitud
- Tiempo y forma
- Seguridad

Controles del sistema

Al efectuar controles sobre el sistema y brindar soporte integral para el mismo hay varios aspectos a tener en cuenta.

Herramientas a utilizar

Existen muchas herramientas para medir la efectividad y eficiencia de los servicios de IT:

- Reportes de excepción
- Logs de aplicaciones y del sistema
- Reportes de problemas sufridos por los operadores
- Cronogramas de los trabajadores

Operaciones de infraestructura

- Ejecutar y monitorear trabajos
- Facilitar backups
- Monitorear accesos y usos de datos sensibles
- Monitorear la adherencia a procesos de IT establecidos
- Participar en testeo de DRPs
- Monitorear la performance, disponibilidad y falla de recursos de información
- Facilitar la resolución de problemas y el manejo de incidentes.

Monitoreo del uso de los recursos

- Procesos de manejo de incidentes
- Gestión de problemas
- Detección, documentación y control de condiciones anormales
- Los errores típicos que se loguean son de aplicación, sistema, operaciones, redes y hardware.

Mesa de ayuda

Primero se documentan los incidentes y se inicia el proceso de resolución priorizando los incidentes y enviándolos al personal de IT apropiado. Se debe realizar un seguimiento de los reportes y clausurarlos cuando se resuelven.

Manejo del proceso de cambios

Documentar formalmente el proceso de solicitar, autorizar, testear, implementar y comunicar cambios.

Tipos de releases

Dependiendo de los cambios que se le hagan a las nuevas versiones, cambia la denominación:

- Major: Un cambio significativo o agregado de funcionalidad
- Minor: Mejoras y arreglos de errores. Integran en ellas a los arreglos de emergencia.
- Emergency releases: Actualizaciones puntuales que arreglan problemas urgentes

Arquitectura y software

- Sistema Operativo
- Bases de Datos y DBMS
- Manejo de Licencias

Controles de acceso

Los dueños especifican, en la política de seguridad de cada subsistema, quien puede acceder a cada dato y con qué privilegios. En los DBMS previenen accesos no autorizados.

Control de acceso discrecional

Estos privilegios se les dan a usuarios que son designados como propietarios y pueden variar entre SMBDs. Entre las distintas posibilidades, un usuario podría ser autorizado para:

- Crear esquemas
- Crear, modificar, o eliminar vistas asociadas al esquema
- Crear, modificar, o eliminar relaciones asociadas al esquema.

- Crear, modificar, o eliminar tuplas en las relaciones asociadas con el esquema.

Los usuarios no propietarios del dato pueden ser sujetos a 4 tipos de restricciones de acceso implementadas por vistas:

- Dependientes del nombre
  Privilegios que tiene un usuario sobre un recurso de cierto nombre. Estos tipos de acceso de control son también conocidos como control de acceso independiente de contenido.
- Dependientes del contenido
  Los privilegios que tiene un usuario sobre un recurso dependen del contenido de ese recurso. Permite bloquear el acceso si el valor del recurso es confidencial. Ej.: Acceder a leer "sueldo", solo si sueldo < $ 5.000.
- Dependientes del contexto
  Los privilegios que tiene un usuario sobre un recurso dependen del contexto bajo el cual quieren acceder. Ej.: Acceder a leer "sueldo" para emitir un informe estadístico, pero no para ver un caso puntual.
- Dependientes de la historia
  Los privilegios sobre un recurso dependen de los accesos y acciones anteriores. Podrían no autorizarse sucesiones de consultas que permitan averiguar datos y luego cruzarlos para averiguar otros. Ej.: Si no se permite la consulta (Nombre, Sueldo) pero un empleado obtiene (Sueldo, Dirección), no debería poder hacer la consulta (Dirección Nombre) a continuación.

Una forma de implementar estos 4 tipos de restricciones es mediante vistas que presenten sólo un subconjunto de la DB. Los datos presentados pueden estar filtrados por uno o más tipos de restricciones de acceso.
Los privilegios pueden propagarse si un usuario otorga sus privilegios, o algún subconjunto de ellos, a otro.
Para prevenir la extensión de la propagación, se requiere:

- Control de propagación horizontal
- Control de propagación vertical
- Revocación de privilegios

Control de acceso obligatorio

Es una política de seguridad en la que los recursos se clasifican en niveles, y a cada usuario se le asigna un nivel que lo habilita a acceder a recursos que estén a su nivel o menor.
Los SBD asignan un nivel para cada atributo, ítem de dato o registro de una relación, por lo que para cada nivel se presenta una vista distinta de la BD. Hay dos aproximaciones para crear estas vistas:

- Implementar vistas por filtrado de datos en una tupla o instancia de registro en una relación, almacenando una única tupla y aplicando las condiciones al presentar los datos al usuario.
- Crear múltiples tuplas que satisfacen las reglas de cada nivel (Poliinstanciación).

Implementación del control

Un factor que afecta la confiabilidad de los mecanismos de control de acceso es donde se implementan:

- Enfoque 1 - Dentro del kernel del sistema operativo.
  (+) La confiabilidad de los mecanismos se incrementa
  (+) Las reglas son más consistentes si se ejecutan por un único componente.
  (-) Mayor tamaño y complejidad del kernel.
  (-) Dificultad al mantener la seguridad e integridad del kernel.
- Enfoque 2 - Embebida en los componentes de administración de BD y SO.
  (+) Las reglas en un SBD suelen ser ejecutadas por los componentes del sistema de administración de BD (acceso a datos) como también del SO (acceso a SMBD). Los usuarios tendrían que identificarse y autenticarse.
  (-) En una BD distribuida, es más difícil asegurar la seguridad e integridad de los controles de acceso. Debe existir un conjunto completo y consistente de reglas que consideren accesos múltiples y soporten replicación.
  (-) En BD replicadas se deben imponer reglas para asegurar el control de acceso a cada sitio.
  (-) En BD particionadas los requerimientos de los usuarios deben estar controlados en forma consistente y completa.

Controles de integridad

Los tipos de restricciones provistos por el sistema dependerán del modelo conceptual y del modelado de datos que soporte. Para ilustrar la naturaleza de los controles de integridad posibles, proveemos una visión de los mismos asociados con:

- Modelo entidad-relación
- Modelo de datos relacional
- Modelo de datos de objetos

Modelo Entidad-Relación

Las construcciones del modelo son: entidades, relaciones y atributos.

- Restricciones sobre Entidades
  Son tipos básicos o clases de objetos del mundo real que se modelan. Se les aplican las siguientes restricciones:

Restricción de Integridad	Descripción
Unicidad	Cada instancia de una entidad debe ser única
Cardinalidad máxima	Especifica el número máximo de instancias de una entidad que puede existir en la base de datos
Cardinalidad mínima	Especifica el número mínimo de instancias de una entidad que puede existir en la BD

Restricción de integridad	Descripción
Tipo de valor de un atributo	Especifica los tipos de valores permitidos para un atributo (real, alfanumérico)
Conjunto de valores de un atributo	Especifica el conjunto permitido de valores para un atributo
Leyes de transición	Especifica las relaciones entre valores previos de atributos y sus nuevos valores

Restricción de integridad	Descripción
Identificador de entidad	Especifica los atributos cuyos valores únicos identifican cada instancia de una entidad.
Tipo de valor de un identificador	Especifica los tipos de valores permitidos para los atributos que comprenden un identificador de entidad (ej: número real, entero, string alfanumérico).
Conjunto de valores de un identificador	Especifica el conjunto permitido de valores para los atributos que comprenden el identificador de una entidad

- Restricciones sobre Relaciones

Una restricción de integridad que se aplica a las relaciones es la cardinalidad, que especifica el número máximo o mínimo de instancias de una entidad que puede asociarse con una instancia de otra. También pueden aplicarse:

Restricción de integridad	Descripción
Referencias	Son establecidos para mantener consistencia sobre tuplas de la relación. Si una tupla en la relación refiere a un dato en otra tupla de la relación o a una tupla de otra relación, este control asegura que la tupla referenciada debe existir.

Restricción de integridad	Descripción
Llaves o Claves	Especifica las llaves candidatas de una relación. Estos valores deben identificar únicamente cada tupla de la relación
Entidad	Se establecen para asegurar que las claves primarias nunca tienen valores nulos.

Modelo de datos de Objetos

Los constructores fundamentales en este modelo son los objetos y sus relaciones. Los objetos poseen:

- Propiedades estructurales, que reflejan características estáticas del objeto. (Atributos)
- Propiedades dinámicas, que reflejan como un objeto cambia de estado. (Métodos)

Para cada tipo de propiedades existen distintas restricciones

- Restricciones sobre Propiedades Estructurales

Restrición	Descripción
Identificador único	Cada objeto debe ser único. El sistema de BD puede generar un identificador de objeto que lo identifica a través de su vida.
Llave o clave única	Las claves de objetos son distintas de los identificadores de objetos. Diferentes restricciones podrían aplicarse. Por ej: las llaves podrían ser únicas dentro de un tipo de objeto o dentro de todos los subtipos de un tipo.
Tipos de valores de atributos	Especifica los tipos de valores permitidos para un atributo de un objeto (número real, string alfanumérico, lista, etc)

Restricción	Descripción
Conjunto de valores de un atributo	Especifica el conjunto de valores permitido para un atributo de un objeto. Podrían ser definidos proceduralmente (a través de un método) como una función de los valores de otros atributos de objetos
Tipos y herencia	Aseguran que un objeto de un subtipo comparte todas las restricciones de integridad asociados con su super-tipo.

- Restricciones sobre Propiedades Dinamicas
  Los controles sobre las propiedades dinámicas se reflejan mediante los procedimientos y métodos públicos que operan sobre los objetos ocultando la estructura del objeto.
- Restricciones sobre Relaciones
  En el modelo de datos de objetos, las relaciones indican:
  - Que los valores de al menos uno de los objetos dependen de los valores de otros objetos en la relación
  - Que un objeto es una componente de otro objeto por agregación o composición.

Restricción	Descripción
Referencial	Si un objeto hace referencia a otro objeto, éste debe existir y ser del tipo correcto
Compo-sición	Especifica las acciones que deben entenderse sobre la inserción y eliminación de objetos que participan en relaciones. Ejemplo, si una clase es eliminada desde la base de datos, todas sus subclases también deben ser eliminadas.
Cardinalidad	Especifica el número mínimo o máximo de objetos de una clase particular que puede participar en una relación.

Controles del SW de aplicación

La integridad del SBD también depende de los controles en los programas de aplicación que usan la BD. Veremos distintos protocolos de actualización y reporte a implementarse en una aplicación para proteger la integridad de la BD. Estos protocolos de buscan que los cambios en la BD reflejen los cambios de las entidades y sus asociaciones en el mundo real. Los más importantes consideran:

- La secuencia de los archivos de transacciones y maestro
- Que todos los registros de un archivo sean procesados
- Procesar en orden correcto múltiples transacciones para un único registro
- Mantenimiento de cuentas transitorias

Controles criptográficos

Son utilizados para proteger la integridad de datos almacenados. Existen dos tipos de encriptación:

- Bloque
  Opera sobre bloques de datos individuales y debería usarse cuando los usuarios requieren acceso a sólo una parte de un archivo.
- Stream
  Los valores criptográficos de un bloque de datos dependen de los valores de otros bloques de datos. Esto es útil para transferir archivos enteros entre dos usuarios.

Hace más complejo el manejo de BD distribuidas, ya que se debe decidir si se mantendrán las mismas llaves en cada copia cuando la BD se replica:

- Si se decide mantener las mismas llaves.
  (+) Si una réplica se pierde se puede obtener una copia o derivar la transacción para otro sitio. También se puede balancear la carga del sistema si un sitio esta sobrecargado.
  (!) Las llaves deberían ser distribuidas de una forma segura.
  (-) Como residen en más sitios, crece el riesgo.
- Cada sitio con su propia llave
  (+) Las llaves serán más seguras
  (-) Es más difícil usar réplicas como back-up y procesar transacciones en sitios distintos de donde se inicia la transacción.

Controles de manejo de archivos

Son políticas para manejar dispositivos físicos y archivos, algunos incluyen sistemas de gestión de versiones. Con el advenimiento de los DBMS, los controles han dejado de hacerse en las aplicaciones para hacerse en estos, lo cual provee descentralización. El auditor debe:

- Listar todos los tipos de registros, analizando sus descripciones y nombres
- Identificar que cada registro tenga una clave única
- Estudiar relaciones y sets, evaluando su fortaleza
- Verificar que el diseño sea consistente con las necesidades del negocio
- Revisar las funciones de monitoreo y control
- Monitorear las revisiones y diseños que ha realizado el Administrador de la DB

- Monitorear la calidad de los datos y la performance
- Examinar los roles que requieren segregación (Administradores, usuarios, programadores, auditores internos)

Controles de operación

Asegurar la existencia y efectividad de los controles contra accesos no autorizados, controles para asegurar completitud y precisión. También controles de recuperación y reinicio (técnicas y herrramientas).

Módulo 8: Aspectos legales Auditoría de Sistemas y Legislación

1) Ramas del derecho
2) Dominios en Internet
3) Privacidad de la Información
4) Ley de Habeas Data
5) Teletrabajo
6) Delitos Informáticos
7) Ley de Propiedad Intelectual del Software
8) Consejo Profesional de Ciencias Informáticas – Pcia. Buenos Aires

Derecho

Es el conjunto de normas que regulan la convivencia social y permiten resolver los conflictos interpersonales. El derecho público prevé la intervención del Estado ya que existe un interés estatal comprometido. El derecho privado comprende las normas en que las relaciones entre particulares son tratadas con igualdad.

Ramas del derecho

El derecho público comprende:

- Derecho constitucional
  Organización del Estado, como normas e instituciones básicas del funcionamiento estatal, y forma de gobierno.
- Derecho penal
  Trata la pretensión penal de derecho público, surgida en la relación Estado–Autor, que comúnmente puede extinguirse a través de la pena. Su función es proteger contra lesiones a la convivencia humana y valores jurídicos importantes.
- Derecho administrativo
  Conjunto de normas y principios que regulan y rigen el ejercicio de función la administrativa del poder.
- Derecho internacional público
  Conjunto de normas que rigen las de los Estados entre si y con ciertas entidades que poseen personalidad jurídica internacional. Toca temas como nacionalidad, extradiciones, mar territorial, hostilidades armadas, etc.
- Derecho procesal
  El conjunto de actos mediante los que se constituye, desarrolla y determina la relación jurídica establecida entre el juzgador y las partes. Tiene como finalidad dar solución al litigio a través de una decisión del juzgador basada en el derecho aplicable y los hechos afirmados y probados.

La informática es regulada por el derecho privado. Cada rama tiene distintas incumbencias, excepto la rama agraria:

- Derecho civil
  El tronco común del cual se han separado las otras ramas. Rige a las personas físicas y jurídicas sin tomar en cuenta la actividad que desarrollan, nacionalidad y situación patrimonial, que si determinan la aplicación de otras ramas. El contenido es de carácter residual, ya que abarca las relaciones jurídicas que no son alcanzadas por otra rama.
  En informática se relaciona con la Firma electrónica, digitalización de actos jurídicos, sistema de nombres de dominios, propiedad intelectual, sociedad sin papeles y publicidad por correo electrónico
- Derecho comercial
  Se relaciona con las marcas y patentes por la gran cantidad de conflictos entre usuarios de nombres de dominio y titulares de marcas registradas.
- Derecho Penal
  Toma relevancia con la aparición de nuevos delitos no tipificados para evitar daños al comercio y a la población frente al ataque de hackers y crackers, la propagación de virus y abuso de líneas telefónicas por phreackers.
- Derecho Constitucional
  Abarca la privacidad de datos personales, la autodeterminación informativa y los mercados de venta de datos.
- Derecho Laboral
  A partir de la aparición del teletrabajo o modalidades de trabajo de similares características.

Nombres de Dominio

El trámite de solicitud de dominio se realiza totalmente en línea en www.nic.com para dominios internacionales o en www.nic.ar para dominios nacionales. NIC – Argentina identifica al Ministerio de Relaciones Exteriores, Comercio Internacional y Culto en su carácter de administrador del Dominio Argentina en Internet.

Reglas del registro

El registro de un nombre se otorga a la persona física o jurídica que primero lo solicite:

- Cuando el registrante completa el formulario manifiesta conocer y aceptar las reglas, procedimientos e instrucciones vigentes. La información suministrada a través del mismo tiene carácter de declaración jurada.
- Se debe suministrar: DNI, CUIT o CUIL.
- El registro del nombre tiene validez de un año a partir de la fecha de inscripción y es renovable durante el último mes de vigencia. Si no se renueva en ese periodo, se producirá la baja automática.
- Se deben proporcionar los datos de una persona responsable que sirva de contacto.

- Las denominaciones que contengan palabras, letras, o nombres distintivos que use o deba usar la Nación, las provincias o los municipios, sólo podrán registrarse por las entidades públicas correspondientes.
- Las denominaciones "gov.ar" se reservan para dependencias estatales.

Conflictos de Nombres de Dominio

Se habla de la doble naturaleza del nombre de dominio ya que sirve como dirección y marca. Casos de *ciberocupación* han sido realizados por personas que se anticiparon a registrar como propios nombres de empresas o marcas. La World Intellectual Property Organization (WIPO) dictó estas *recomendaciones*:

- Protección del nombre de dominio
- Aplicación de la normativa existente de marcas y competencia
- Acciones para promover la cesación del uso del nombre de dominio robado e indemnizaciones por daños y perjuicios
- Adopción de medidas cautelares
- La WIPO presiona para que los registros nacionales adopten estas normativas y recomienda aumentar el control de datos suministrados por los solicitantes.
- Hacer una declaración jurada obligatoria indicando que no se conoce la existencia de un derecho prioritario, que se hace de buena fe y lícitamente.

Privacidad

Se deben arbitrar los medios jurídicos para la protección de la privacidad. Hoy en día es posible capturar datos precisos de distintas personas, relacionarlos y mostrar un perfil estudiado del individuo sin que la persona lo sepa.

Propiedad de la Información

Los pioneros en el tema fueron:

- 1973
  Data Privacy Act - Suecia
- 1974
  Privacy Act - EEUU
- 1986
  Electronic Comunication Privacy Act - EEUU
- 1988
  Computer Matching and Privacy Protection - EEUU

El titular debe tener derecho de acceso a sus datos registrados en bases de datos públicas o privadas. El administrador debe dar a los datos el destino para el que se recabaron y solo podrá darle otro uso si tiene la autorización del titular.

Clasificación de los Datos

Son públicos aquellos que tienen menor importancia y se encuentran a disposición de todos (Ej.: nombre, domicilio, teléfono, documento). Los privados son aquellos que constituyen la información sensible.

Protección Datos Personales

Estos principios, han sido reconocidos a nivel internacional por las Directivas de la Unión Europea (1995), las Actas norteamericanas anteriormente citadas, la Declaración de Humahuaca (1999) y la Carta de Venecia (2000):

- Limitación
  Deben ser recabados con fines lícitos y leales. Si son sensibles solo con consentimiento del titular.
- Buena Fe
  No podrán ser obtenidos por medio de engaños.
- Calidad
  Deberán ser exactos, completos, actualizados, para evitar errores a quienes los solicitan ni perjudicar a los titulares.
- Finalidad
  Deben especificar y respetar el fin preciso para el cual son recabados.
- Restricción de Uso
  Su uso debe limitarse a fines lícitos informando al destinatario de la información.
- Justificación Social
  Que sean relevantes y necesarios para la sociedad.
- Confidencialidad
  Los administradores deberán tomar las medidas necesarias para que no lleguen a manos de terceros.
- Garantía de seguridad
  El control del estado es necesario para una adecuada política de seguridad.
- Limitación temporal
  No deben ser conservados más allá del tiempo previsto.
- Transparencia
  Debe ser fácil acceder a la información de quienes son los responsables de los bancos de datos, sus domicilios y el carácter de los datos que poseen.
- Participación
  El individuo debe ser educado en la política de manejo de datos y conocer sus derechos para hacerlos valer. El banco de datos no debe entorpecer el ejercicio de esos derechos.
- Consentimiento
  Cuando se trata de datos sensibles, el banco debe contar con el consentimiento del titular.

- Acceso
  El titular debe tener acceso a los datos para controlar o verificar que sean exactos. Debe poder hacerlo a intervalos regulares, limitados en el tiempo.

Clases de Bancos de Datos

- Información crediticia y solvencia (Veraz)
- Datos genéticos
- Archivos de seguridad (Policiales o militares)
- Salud
- Abonados a servicios
- Investigaciones de mercado
- Censo

Hábeas Data

Todos tenemos el derecho de acceder a nuestros datos personales registrados en bancos de datos. Si el acceso es negado o no se brinda de conformidad, el Habeas Data es el recurso legal para conseguirlos. Proviene del latín y significa "tener el dato". Surge en Europa para combatir la proliferación irrestricta de datos computarizados y, mediante una acción judicial, conocer los datos existentes en los bancos públicos o privados y cuál es su finalidad.
Ante su falsedad, inexactitud, desactualización, error o discriminación, se podrá exigir su rectificación, supresión, confidencialidad o actualización. Las partes del recurso son:

- Sujeto Activo
  Persona física o jurídica que se sienta afectada, sus tutores o curadores, y sus sucesores hasta 2do grado
- Sujeto Pasivo
  Los responsables o usuarios de bancos de datos destinados a proveer informes.
- Objeto
  El objeto de la acción es que las personas tomen conocimiento de sus datos, que encuentren contenidos y exigir su modificación.
- Bien Jurídico Protegido
  Va desde el derecho a la intimidad hasta el derecho al honor, pasando por el de identidad, imagen y reputación.

Teletrabajo

Es la realización de tareas fuera del lugar habitual de trabajo por medios telemáticos. Se introdujo como telecommuting en un sistema de comunicaciones para la NASA, refiriéndose al trabajo realizado fuera del lugar habitual y con una presencia virtual del trabajador. Puede ser de tiempo completo o parcial, dando lugar a las siguientes categorías:

- Teleempleado
- Freelance
- Combinado o mixto.

Cuando el trabajo se realiza online, los directivos pueden enviar indicaciones y monitorear lo que hace el trabajador.

Ventajas para el trabajador

- Mayor flexibilidad horaria, disponibilidad y aprovechamiento del tiempo
- Evitar traslados, ahorrando tiempo y dinero
- Reorganización familiar
- Realización de tareas según su objetivo
- Facilidad para discapacitados motores

Ventajas para la empresa

- Reducción de costos fijos, de infraestructura y viáticos
- Personal más especializado y productivo
- Reducción del ausentismo
- Inexistencia de conflictos por convivencia
- Posibilidad de ampliar horarios de trabajo

Ventajas para la sociedad

- Menos contaminación y trafico
- Empleo para discapacitados y mujeres embarazadas y en post parto
- Desarrollo de zonas alejadas, descongestionando las grandes áreas pobladas

Desventajas para el trabajador

- Aislamiento y cambio en sus relaciones sociales
- Falta de diferenciación entre el ámbito laboral y familiar
- Pérdida de algunas garantías laborales

Desventajas para la empresa

- Pierde control sobre el empleado
- Requiere mayor coordinación de tareas y de motivación para el empleado
- Posible competencia desleal del empleado
- Posible uso de los medios de la empresa para fines personales

Recomendaciones de la Organización Internacional del Trabajo

La OIT especifica ciertos requerimientos para las empresas que quieren adoptar esta modalidad:
- Reconocer como asalariado a los trabajadores que trabajan regularmente para un mismo empleador
- Los trabajadores a distancia deben tener los mismos regímenes de prestaciones sociales que los empleados internos
- El sistema de retribución debe ser idéntico a lo que sería para un trabajador interno
- Tener una referencia horaria clara para que el empleador no extienda el tiempo de trabajo unilateralmente.
- Garantizar las condiciones para su participación en las actividades sindicales en los centros de trabajo.
- Los gastos e inversiones para la realización del trabajo deberían ser abonados por las empresas, considerando materiales, instalaciones y costes energéticos estimados.
- Establecer sistemas de contacto periódico con el resto de los trabajadores para limitar la sensación de aislamiento
- Ofrecer capacitaciones permanentes e información actualizada sobre cambios y requerimientos de los trabajadores.
- Las posibilidades de promoción deben ser iguales a las de los trabajadores internos
- El paso de trabajador interno a teletrabajador será de carácter voluntario.
- Los lugares de teletrabajo deberán reunir todos los requerimientos de seguridad y salud laboral
- Deben facilitarse los medios para que los representantes sindicales puedan comunicarse con los trabajadores

Lugares apropiados para el Teletrabajo
- En casa, creando las condiciones necesarias
- Oficinas satélites de la empresa en las cercanías de los hogares de los empleados.
- Lugares compartidos por varias empresas para abaratar costos (Telecentros)
- Entorno Móvil utilizando PC e impresoras portátiles y sistemas de telefonía celular

Delitos Informáticos

Cualquier acto ilegal en el cual el conocimiento de informática sea esencial para su cometerlo, investigarlo y perseguirlo. Pueden clasificarse en delitos CONTRA o MEDIANTE el sistema, dependiendo de cómo sean utilizadas las computadoras. Existen distintas figuras y modalidades:
- Hackers
  Acceden a un sistema informático sin autorización
- Crackers
  Inutilizan sistemas de protección mediante programas creados con ese fin
- Phreacker
  Utilizan técnicas de fraude en telefonía
- Introducción de virus

Todos requieren una tipificación legal en el daño que provocan, la información que roban o los impedimentos a los sistemas que producen.

Marco Legal Existente

En nuestra Constitución se contemplan y protegen derechos fundamentales:
- Art.18: Privacidad del domicilio y papeles privados
- Art.19: Privacidad del individuo
- Art.43: Garantía de Hábeas data

La Ley Penal Tributaria incorpora la alteración dolosa de registros que puede ser realizada por el contribuyente, un agente del órgano fiscal o un tercero. Se encuentra dentro de los delitos fiscales comunes, es doloso y comprende: sustraer, suprimir, ocultar, adulterar, modificar o inutilizar registros. La pena es de dos a seis años y se aplica aunque el objetivo no se haya logrado.

La Ley 24.073 de la AFIP obliga a los contribuyentes a mantener por dos años, desde la fecha del cierre del ejercicio económico, los soportes magnéticos con datos de la materia imponible.

La reciente ley de protección de datos modifica el Código Penal, creando sanciones penales:
- Tendrá prisión de un mes a dos años el que inserte o haga insertar a consciencia datos falsos a un archivo de datos personales.
- La pena será de seis meses a tres años para quien, a sabiendas, proporcione a un tercero información falsa contenida en un archivo de datos personales.
- Aumenta la pena cuando del hecho se derive perjuicio a alguna persona.
- Cuando el responsable sea un funcionario público en ejercicio, se lo inhabilitará para el desempeño del cargo público por el doble del tiempo que el de la condena.

Se incorpora como art.157bis del Código Penal:
- Tendrá la pena de prisión de un mes a dos años quien, violando sistemas de confidencialidad o seguridad de datos, acceda a un banco de datos personales. También cuando revele a un tercero la información registrada en un banco de datos personales cuyo secreto esté obligado a preservar.
- Si el autor es funcionario público sufrirá pena de inhabilitación de 1 a 4 años.

Derechos de autor

Modifica la ley 11.723 y protege los derechos de autor de obras científicas, literarias, artísticas, comprendiendo escritos de toda naturaleza, incluso programas de computación (fuente y objeto). Protege la expresión de la idea y no la idea en sí misma.

En cuanto al software, se puede reproducir una única copia de backup que esté identificada debidamente.

Historia en Argentina

- Se aplica la ley universal para derechos de autor
- La DPNI rechaza la protección por patentes
- Se realiza una segunda modificación de la ley de derechos de autor para poder registrar Software
- Una vez registrado se puede licenciarlo porque se poseen derechos de autor sobre el mismo

Derechos de autor y licencias

Existen distintos tipos de licencias con las que se puede licenciar un SW dado:

- Software Libre
  No implica renunciar a los derechos de autor.
- Software Propietario
- Shareware
- Open Source

Protección del Software en el código penal

Las penas se extienden a quien edite, venda o reproduzca el software ilegalmente. La copia privada para fines personales no se encuentra contemplada.
Se otorga a la parte empleadora la titularidad sobre los derechos de autor cuando el programa es realizado por un empleado suyo contratado con ese fin.

Patentes

Los derechos de autor son universales, pero las patentes de invención cambian en cada país. Se otorgan por un período limitado a cambio de que se publique la invención, es decir, no se pueden patentar ideas, conceptos abstractos o conocimiento. Los permisos dependen de la persona que obtiene la licencia y pude requerir un pago.
La discusión sobre si tiene o no sentido patentar software depende de cómo se defina a un programa (Ej.: en Europa no se puede patentar un programa).
Algunas patentes que hoy son de uso general:

- Ventas en un clic por internet
- Creación de múltiples archivos a partir de uno solo (Descompresión)
- Uso de "popup notes" cuando se mueve el puntero sobre un objeto de la pantalla.
- Al instalar software en un sistema, cuando se copia más de un archivo y algunos ya existen, se sobrescriben.

Consejo Profesional

En el país es el Consejo Profesional de la Provincia de Buenos Aires matricula a profesionales y auxiliares.

Requisitos

Poseer un título en carreras de Ciencias Informáticas, encuadrándose en:

- Título superior expedido por una universidad Argentina.
- Título de post grado expedido por una universidad Argentina
- Título expedido por universidad o institución profesional extranjera y validado por una universidad Argentina.