Auditoría Informática: Resumen de teoría

Victor Franco Matzkin

Basado en una selección de resúmenes[1], apuntes tomados en clase y capítulos[2] del libro: Auditoría Informática, un enfoque práctico (Piattini).

Índice

[1] Resúmenes de Cesar Castillo, Cristian Escudero, Gabriel Dalmolín, Carlos Gentile, Mario Rosales, Franco Santellán, Facundo Salmerón y Guido Ghisolfi.

[2] Capítulos 2,3,4,5,8,9,10,11,12,14,15 y 18.

1. Introducción

1.1. Control interno y Auditoría

El *Control Interno* es cualquier actividad o acción realizada manual y/o automáticamente para prevenir, detectar y/o corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

En un principio, en las empresas el control interno se limitaba a los controles contables internos, ya que el área financiera era la más importante y ésta podía ser auditada externamente. Al no hacer controles sobre otras actividades de la organización (como las actividades operativas), muchas veces los riesgos no se podían anticipar y los problemas no se podían controlar.

Estos problemas, sumados a los grandes cambios que se produjeron en las organizaciones (como la reestructuración de los procesos, la gestión de calidad total, la contratación externa y la descentralización) y de una forma más general, ante la globalización, la diversificación de las actividades, la eliminación de ramas de negocio no rentables, la introducción de nuevos productos en respuesta a la competencia, y la formación de alianzas y fusiones de empresas, los directivos buscan *evitar fallos* significativos y actuar de manera *proactiva* antes de que surjan los problemas, de manera que se pueda asegurar la *integridad* y *continuidad de la organización*.

En el sector terciario, el sector de informática es vital ya que soporta los sistemas de información del negocio, por el volumen de recursos, presupuestos que maneja, entre otras cosas, lo que da lugar al *control interno informático* y la *auditoría informática*.

Una *Auditoría*, por otro lado, es una actividad que tiene como objetivo *emitir una opinión profesional*. Esta actividad se realiza sobre determinados objetos. La opinión profesional tiene como objetivo ver si el objeto analizado cumple con objetivos que le fueron prescriptos.

Existen varios tipos de auditoría (financiera -sobre estados contables-, de gestión -basada en la administración de los recursos-, de cumplimiento -ver si los procedimientos se adecuan a las normas-, informática, entre otras.

Tipos de controles:

- **Preventivos:** Controles que se realizan antes de que las cosas funcionen, para prever problemas. Ej: *software* que impida los accesos no autorizados al sistema.
- **Detectivos:** Descubre una desviación, y cuando ésta ocurre trata de corregirla. Ej: registro de intentos no autorizados.
- **Correctivos:** Existe un problema y hay que recuperarse del hecho. Ej: recuperación de un archivo dañado a partir de sus copias de seguridad.

Los límites del **control** los brindará el costo/beneficio de la empresa en cuestión, ya que es una actividad diaria para la misma. Es responsabilidad de la Dirección plantear una estrategia de inversiones en recursos informáticos así como implantar sistemas de controles internos de manera que se garanticen unos grados de eficiencia y seguridad suficientes de los activos informáticos.

1.1.1. Control Interno Informático

El *Control Interno Informático* (CII) es un control *diario* de todas las actividades informáticas, para verificar que éstas se realizan cumpliendo procedimientos, estándares y normas fijados por la Dirección de la Organización o la Dirección de Informática, así como los requerimientos legales. Los recursos humanos que colaboran en el CII pueden (o deben) colaborar en un proceso de Auditoría Informática.

1.1.2. Auditoría Informática

La *Auditoría Informática* (AI) es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De esta forma, la auditoría informática busca cumplir con los *objetivos tradicionales de auditoría*, que son la protección de activos e integridad de los datos y objetivos de gestión que abarcan eficacia y eficiencia.

En una AI pueden analizarse los sistemas de aplicación, recursos informáticos, planes de contingencia, verificar cumplimiento de normas y estándares, economicidad, entre otras cosas.

Entre los objetivos del auditor informático, están: detectar errores, falencias o fraudes (cualquier error puede perjudicar los activos, y en fraudes se debe trabajar con prudencia, ya que se puede terminar en un proceso judicial), y diseñar pruebas anti-fraude a partir de un *Análisis de Riesgos* (permiten saber a qué estamos expuestos).

Control Interno Informático vs Auditoría Informática:

- Similitudes:
  - Son realizados por expertos informáticos.
  - Verifican el cumplimiento de controles internos, normas impuestas y procedimientos.

- Diferencias:
  - El CII funciona *diariamente*, mientras que una AI se realiza de manera *eventual*.
  - El CII responde al *gerente de Área de Informática*, mientras que la AI responde al *gerente general*.
  - El CII es realizado por *personal interno*, mientras que la AI se realiza mediante la *colaboración* de personal externo con interno.
  - El CII se realiza sobre actividades del *departamento de informática*, mientras que una AI trabaja además de ésta, en *áreas externas* que hacen uso de ella.

1.2. Metodologías de Control Interno, Seguridad y Auditoría Informática

Según la definición, un *método* es el *modo de decir o hacer con orden una cosa*. A su vez, *metodología* se define como *conjunto de métodos que se siguen en una investigación científica o exposición doctrinal*. Esto quiere decir que un proceso científico debe estar sujeto a una metodología definida anteriormente.

La informática crea riesgos de los que hay que protegerse y preservar la entidad con una serie de contramedidas y la calidad y eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos. Ésta es una de las funciones de los auditores informáticos.

1.2.1. La metodología de la Auditoría Informática

El contexto al que se enfrenta el auditor involucra una alta dependencia de los sistemas de información, la tecnología es un motor de cambio social acelerado, las TICs poseen un ciclo de vida corto (se realizan cambios frecuentes) y se necesitan expertos eficientes en AI (poseer criterio de trabajo), por lo que todo análisis deberá tener en cuenta este entorno.

La metodología de la Auditoría Informática se formaliza en el *Plan del Auditor Informático*, el cual determina si se realizará o no la auditoría. Los distintos puntos que definen la metodología son:

- Definición del objeto de la auditoría: ¿A qué/quién se le va a realizar la Auditoría?
- Toma de contacto:
  - Conocer la organización.
  - Ubicación de las TICs en el organigrama: ¿Quién depende de quién? ¿El sector informático es lo suficientemente independiente?.
  - Segregación de las funciones informáticas (especialización de las funciones -redes, desarrollo, Bases de Datos-) y del Control Interno Informático.
  - Descripción de la organización interna del área o departamento: Dentro de cada área, ver la subdivisión de las tareas (por ejemplo, en *desarrollo*, están *análisis de requerimientos, testing*, etc).
  - Descripción de las funciones de cada sector: Escribir las funciones, responsabilidades y tareas que debe cumplir cada sector (misiones y funciones de cada puesto de trabajo).
- Procedimientos: Son las distintas tareas que se realizan en la auditoría: Apertura (comunicar a las áreas el comienzo de la auditoría), entrega y discusión de debilidades, redacción de informes, cierre de auditoría (informar que hay conclusiones de la auditoría), entrega del informe final y presentación de las conclusiones (debate).
- Tipos de AI:
  - Completa: Se realiza sobre todo el área.
  - Limitada a un aspecto determinado del área (Ej: evaluar la red, una aplicación).
  - Comprobación de acciones correctivas de auditorías anteriores (ya hubo una auditoría previamente y se quiere ver si ésta dio resultados.
- Sistema de evaluación y aspectos a considerar: Informe de Auditoría, fecha para realizar una futura. auditoría.

1.3. Perfil del Auditor Informático

Se deberán contemplar las siguientes características para mantener un profesional adecuado y actualizado:

1. Conocimientos básicos en:
   - Desarrollo informático, gestión de proyectos y ciclos de vida de proyectos de desarrollo tecnológico.
   - Gestión del departamento de tecnología.
   - Análisis de riesgos en un entorno informático.
   - Sistemas operativos.
   - Telecomunicaciones.
   - Gestión de Bases de Datos.
   - Redes locales.
   - Seguridad física.
   - Gestión de la seguridad y continuidad del negocio.

- Gestión de problemas y cambios.
- Administración de datos.
- Ofimática.
- Comercio electrónico.
- Encriptación de datos.

2. Técnicas de gestión empresarial y conocimientos financieros del negocio.
3. Conocimiento del concepto de *Calidad Total*.

Legalidad y C omportamiento: La AI sirve para delegar o implicar responsabilidades, ya que puede ser usada en procesos legales. Tener en cuenta:

- Interdependencia de criterios, actitud mental objetiva.
- Responsabilidad, idoneidad y corrección.
- Disciplina y confidencialidad.
- Función de asesoramiento en todo momento.
- Seleccionar los procedimientos de auditoría (alcance, oportunidad).
- Considerar aspectos de integridad del patrimonio.
- Obtener elementos de juicio válidos, pertinentes y suficientes sobre los objetivos examinados.
- Elaborar actas e informes con los requisitos o características que correspondan a toda información
- Realizar observaciones claras.

1.4. Funciones a desarrollar por la Auditoría Informática

La función *Auditoría Informática* debe mantener en la medida de lo posible los objetivos de revisión que le demande la organización, abarcando en lo posible:

- Verificación del control interno, tanto de las aplicaciones como de los sistemas informáticos, centrales y periféricos.
- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de la gestión.
- Análisis de la integridad, fiabilidad y certeza de la información a través del análisis de las aplicaciones.
- Auditoría del riesgo operativo de los circuitos de información.
- Análisis de la gestión de los riesgos de la información y de la seguridad implícita.
- Verificación del nivel de continuidad de las operaciones.
- Análisis del Estado del Arte tecnológico de la instalación revisada y de las consecuencias empresariales que un desfase tecnológico puede acarrear.
- Diagnóstico sobre el grado de cobertura que dan las aplicaciones a las necesidades estratégicas y operativas de información de la organización.

El **auditor informático** es responsable para establecer los *objetivos de control* que reduzcan o eliminen la exposición al riesgo de control interno. El auditor deberá revisar los controles y evaluar resultados de su revisión para determinar correcciones y mejoras. Tiene además la obligación de proveer procedimientos y observaciones para mejorar la efectividad, eficacia y medición del riesgo empresarial.

1.4.1. Aspectos a tener en cuenta en la auditoría

- Normas
- Evidencias: La opinión debe estar basada en evidencias justificadas.
- Irregularidades: Como fraudes y errores.
- Documentación: Información utilizada y pruebas que permitan formar una opinión. Incluye:
  - El contrato Cliente-Auditor.
  - Declaraciones de la Dirección
  - Contratos que afecten el Sistema de Información.
  - Informe sobre terceros vinculados.
  - Conocimiento de la actividad del cliente.

1.4.2. Informe de Auditoría

El *Informe de Auditoría* es la comunicación formal al cliente de alcances, resultados y conclusiones de la Auditoría llevada a cabo. Contiene además de las falencias encontradas, un plan de acciones[3] que permite revertir la situación teniendo en cuenta aspectos económicos de los Recursos Humanos, cumplimiento de normas y una evaluación global de toda la Auditoría. Se compone de:

[3] El plan de acción se debe basar en la realidad de la empresa (debe poder ser realizable).

- Identificación del informe.
- Identificación del cliente.
- Identificación de la empresa a auditar.
- Objetivos de la auditoría.
- Normativas aplicadas y excepciones.
- Alcance de la auditoría.
- Conclusiones.
- Resultados.
- Informes previos.
- Fecha del informe.
- Identificación y firma del auditor.
- Distribución del informe.

2. Auditoría de la dirección informática

2.1. El área informática

En un principio el área de las tecnologías de información no poseía tanta relevancia dentro de las empresas, por lo que su tamaño fue siempre menor al de otras tales como RR.HH, administración, logística, finanzas, producción o marketing. En las últimas décadas, al cambiar el paradigma, este sector adquiere una importancia vital, apoyando ahora a todas las demás áreas y relacionándose con *clientes externos* lo cual se traduce en una alta dependencia empresarial, y un sector al que hay que dedicarle importantes recursos económicos (cada vez más), por lo que más aún debe ser analizado.

2.2. Actividades de la dirección informática

La dirección informática es un área que si bien es responsable de las tareas informáticas que se realizan, no realiza tareas técnicas. Las actividades principales son planificar, organizar y coordinar y controlar.

2.2.1. Planificar

Esta etapa consiste en prever la utilización de la tecnología, a través de la observación del entorno, condiciones económicas, nuevas tendencias tecnológicas, fallas de la tecnología actual, obsolescencia, etc.

1. **Plan Estratégico de los Sistemas de Información:** Impulsado por el *responsable*[4] (gerente, director) debe asegurar el alineamiento de los Sistemas de Información con los objetivos de la empresa.
   Este plan debe ser aprobado por toda la organización, ya que incumbe a otros estamentos de la empresa, desde el *Comité de Informática* hasta la *Dirección General*. El plazo del plan está determinado por el entorno de la empresa (aunque generalmente se piensa de 3 a 5 años).
2. **Plan operativo anual:** En éstos, se planifica qué actividades se van a desarrollar en cada año (desarrollo, cambios previstos, recursos, plazos) dentro del *Plan Estratégico*.
3. **Plan de recuperación ante desastres:** La dirección prevee la posibilidad de que una instalación informática se vea afectada por desastres de variada naturaleza, y planifica para hacerle frente.

Tareas del auditor al examinar el proceso de planificación:

1. Evaluar si razonablemente cumple con los objetivos.
2. Evaluar si las tareas y actividades en el plan tienen la correspondiente y adecuada asignación de recursos para poder llevarse a cabo.
3. Revisar actas confeccionadas dedicadas a la planificación estratégica.

2.2.2. Organizar y Coordinar

Consiste en estructurar los recursos, flujos de información y controles para cumplir con los objetivos planificados.

- **Comité de informática:** La comunicación y el entendimiento entre la dirección informática y las áreas usuarias es *dificultoso*, por lo que para evitarlo se puede crear un comité, que propone un lugar de encuentro entre las partes para debatir ideas y que los usuarios puedan conocer las necesidades del conjunto de la organización y participar en la fijación de prioridades. En esta reunión se busca evitar que algunos sectores se vean más favorecidos que otros respecto a la utilización de los recursos. Las funciones que cumple el comité son:
  - Aprobar el Plan Estratégico y sus inversiones asociadas.
  - Fijar prioridades de los proyectos.
  - Ser un vehículo de discusión entre el departamento de informática y los usuarios.
  - Vigilar la actividad del departamento de informática.

  Frente a un comité existente, el auditor informático debe:

[4] El responsable es quien debe impulsar el plan, ya que éste lo va a conducir.

- Asegurarse de que el comité existe y cumple su papel.
- Conocer sus funciones.
- Entrevistar a miembros destacados.
- Entrevistar a representantes de los usuarios.
- Elaborar un juicio sobre validez, adecuación y actuación del comité.

- **Posición del área de tecnología en la empresa:** Es importante poseer *autoridad* frente a otras áreas, lo cual se materializa mediante una *jerarquía*. El auditor deberá ver dónde se ubica el departamento y analizar su independencia.
- **Descripción de funciones y responsabilidades del departamento:** El auditor deberá ver si esos límites están explicitados.
- **Estándares:** Los fomenta la gerencia/dirección del área y deben ser conocidos por los usuarios.
- **Gestión de Recursos Humanos:** Si los RR.HH. están calificados, se obtienen buenos resultados. Los responsables deben intervenir en la selección, preparación, evaluación de desempeño, promoción y finalización, tratando de minimizar los inconvenientes.
- **Comunicación entre el Gerente y las áreas:** La calidad depende de la comunicación.
- **Gestión económica:** Presupuestación, adquisición de bienes y servicios, medición de reparto de costo.
- **Seguros:** Poseer coberturas para los sistemas informáticos.

2.2.3. Controlar

Efectuar un seguimiento permanente de las distintas actividades del Departamento de Tecnología, y que esté asegurado el cumplimiento de la normativa legal. Es muy importante la opinión del auditor acerca de la dirección.

3. Auditoría de la Seguridad Física

Con la parte física se hace referencia a los bienes tangibles que proporcionan un continente, medio o vehículo para el software. Esto es todo aquello que rodea y se incluye en el computador. La *seguridad física* garantiza la integridad de los activos humanos, lógicos y materiales de un Centro de Procesamiento de Datos, a través del análisis de riesgos. La seguridad física debe ser auditada para asegurar que el servicio se pueda seguir dando y se haga de una manera segura.

El auditor tiene en cuenta varios aspectos y proporciona evidencia de la seguridad física en el ámbito en el que se lleva a cabo la labor profesional. Hace hincapié en la Funcionalidad, Racionalidad y Seguridad de los medios físicos.

3.1. Análisis de de Riesgos:

El análisis de riesgos comprende una serie de acciones que permiten disminuir problemas y determina el nivel de seguridad a aplicar. Se deben tomar medidas:

1. **Antes:** para obtener y mantener un determinado nivel de seguridad. Son acciones que permiten evitar el fallo y disminuir consecuencias. Las personas deben realizar un uso profesional de los entornos físicos. Ejemplos:
   - Selección del personal.
   - Medidas de protección generales.
   - Potencia eléctrica.
   - Sistema contra incendios.
   - Control de acceso.
   - Ubicación del centro de cómputos.
   - Ubicación del edificio.
   - Elementos de construcción.
2. **Durante:** a través de medidas de contingencia. Ante un desastre (cualquier evento que cuando ocurre tiene la capacidad de interrumpir el normal proceso de una empresa) existe un *Plan de Contingencia* que permita afrontarlo.

   El Plan de Contingencia se compone de un *Plan de Recuperación Ante Desastres* más un *Centro Alternativo de Procesamiento de Datos*. El Plan de Recuperación debe:
   - Realizar un análisis de riesgos de los sistemas críticos.
   - Establecer un *período crítico* de recuperación.
   - Realizar un análisis de *aplicaciones críticas*, priorizando procesos.
   - Determinar las prioridades de procesos por día y por su orden.
   - Establecer objetivos de recuperación.
   - Asegurar capacidad de comunicaciones y servicios de copias de seguridad.
3. **Después:** mediante planes de seguros, que compensan las pérdidas, gastos y/o responsabilidades que puedan surgir una vez detectado y corregido el fallo. Tipos de seguros:

- Del centro de procesamiento.
- De los medios de Software.
- Gastos del plan de contingencias.
- Gastos por la pérdida del negocio.

3.2. Áreas de la Seguridad Física

No existe un sector exclusivo que se encargue de la seguridad física. Ésta, está repartida en quienes conducen, administradores y/o responsables de seguridad/normas. Las áreas que deben reforzar la seguridad son:

- **Centro de procesamiento de datos e instalaciones:** Cámara acorazada, oficinas, almacenes, servidores, sala de host, ubicación del CPD, instalaciones eléctricas, aires acondicionados.
- **Equipos y comunicaciones:** Se debe inspeccionar ubicación y acceso de: las computadoras, host, impresoras, medios de telecomunicaciones.
- **Seguridad física del personal:** Accesos y egresos, rutas de evacuación, normas relativas al uso de instalaciones bien distribuidas.

3.3. Fuentes de la Auditoría Física

Un Centro de Cómputos sigue un modelo *estándar* según características económicas, físicas, y actitudinales de la empresa. Para determinar la seguridad, el auditor debe recolectar información de:

- Políticas, normas y planes de seguridad emitidos y distribuidos.
- Auditorías anteriores relacionadas a la Seguridad Física.
- Contratos de Seguros, Proveedores y Mantenimiento.
- Actas e informes de técnicos y consultores (sobre edificio, electricidad, aire, etc).
- Informes de accesos y visitas.
- Informes sobre pruebas de evacuación.
- Políticas del personal.
- Proceso de cancelación de contratos y despidos.
- Rotación en el trabajo.
- Contratos fijos y temporales.
- Inventarios de soporte.
- Entrevistas con personal deseado.

Tener en cuenta que el Auditor es espectador y actor al mismo tiempo, ya que puede evaluar el correcto funcionamiento de los sistemas de seguridad utilizándolos (ej: tratar de acceder a una sección no autorizada). Se deben realizar entrevistas (no interrogatorias), y también consultar a técnicos y peritos (ajenos o no a la empresa). Se puede acordar el uso de grabadoras de audio/video, o en su defecto tomar notas.

3.4. Buenas prácticas de la seguridad física

- Los edificios de procesamiento de datos deben ser discretos y ofrecer mínimo señalamiento.
- Ubicar las instalaciones en lugares que no sean de fácil acceso para el público.
- Ubicar adecuadamente equipos de soporte en lugares donde se reduzca el riesgo (limitar acceso a impresoras).
- Aislar equipamiento que requiera protección especial.
- Escritorios/pantallas limpios (no dejar programas abiertos).
- Documentos bajo llave.
- Información sensible en cajas fuertes o bóvedas.
- No dejar PCs encendidas y desatendidas.
- Proteger puntos de recepción de correo. Bloquear fotocopiadoras.
- No retirar nada de la organización sin autorización.

4. Delitos informáticos

4.1. Delito informático

Un delito informático es un hecho ilícito que se comete mediante medios o sistemas informáticos. Los delitos ya tipificados (robos, hurtos, etc) pueden efectuarse o favorecerse a través de medios informáticos, esto es, debido al avance de la tecnología y la aparición de Internet, surgen nuevas formas de establecer relaciones, medios comisivos de delitos, perjuicios, impunidad, por lo que se necesita *legislación* y *controles* hacia estas nuevas formas de relación.

Saber quiénes cometen delitos implica la creación de áreas específicas que se avoquen de lleno en la temática, ya que existe una alta necesidad de actualización. Desde un punto de vista social, el uso de la tecnología requiere *responsabilidad*: necesidad de generar conciencia, promover reformas legislativas, cooperación internacional, generar capacitación, etc.

Dentro de los delitos tipificados, se encuentran aquellos relacionados a la pornografía infantil, acceso a Bases de Datos no autorizados, SPAM, estafas, daño de sistemas informáticos, falsificación de datos, entre otros, que se detallan en la ley a continuación.

4.2. Ley de Delitos Informáticos (26388)

La Ley 26388 "Delitos Informáticos"propone modificar/sustituir/incorporar tipos penales al *código penal*. Mantiene el esquema de márgenes punitivos de los delitos ya previstos (no modifica las penas). Incorpora a las nuevas tecnologías como forma de cometer delitos. También establece penas más severas si quien comete el delito es un funcionario público.

4.2.1. Art. 77: Terminología

Incorpora los siguientes términos:

- Documento: Cualquier representación de actos o hechos (comprende al documento electrónico).
- Independencia del soporte: Papel, audio, disco, video, etc.
- Objetivo: Escritura, almacenamiento, transmisión, archivo.
- Firma: Incorpora la firma digital, que es el resultado de la aplicación de un procedimiento criptográfico seguro a un documento digital que permite garantizar su *integridad*.
- Firma electrónica: Uso de un usuario/contraseña. Es equivalente a una firma manuscrita.

4.2.2. Art. 128: Pornografía infantil

Este artículo es relativo a la producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación y distribución por cualquier medio de pornografía infantil (menor de 18 años), y la suministración de material pornográfico a menores de 14 años.

4.2.3. Art. 153 y 155: Comunicaciones electrónicas

Este artículo está referido a las comunicaciones electrónicas, específicamente al acceso, manipulación, intercepción o publicación de una comunicación electrónica o revelación de datos secretos.

4.2.4. Art. 153 bis: Hacking

Establece penas para cuando se da el acceso sin autorización a un sistema informático, o se excede la autorización existente. La pena es mayor si se trata de un organismo público o financiero.

4.2.5. Art. 157 bis: Bases de Datos

Relacionado con el acceso a un Banco de Datos personales a través de cualquier medio, la revelación de los datos de una BD, o su modificación sin la debida autorización.

4.2.6. Art. 173 inciso 16: Estafa Informática

Relacionado a la defraudación (perjuicio económico) mediante técnicas de manipulación informática que altere el funcionamiento de un sistema informático o la transmisión de datos.

4.2.7. Art. 183: Daño y Sabotaje

Relativo a la alteración, destrucción e inutilización de datos, documentos o sistemas así como la venta, distribución e introducción de un programa destinado a causar daño (virus, troyanos, gusanos).

Si se realiza sabotaje en sistemas informáticos esenciales (servicios de salud, telecomunicaciones, energía, medios de transporte, etc), la condena es mayor.

4.2.8. Art. 197: Interrupción de Telecomunicaciones

Regula las penas para cuando se interrumpe o entorpecen comunicaciones telegráficas, telefónicas, etc, o bien se resiste al restablecimiento de la comunicación interrumpida.

4.2.9. Art. 255: Supresión o alteración de Pruebas Digitales

Relativo a la sustracción, alteración, ocultamiento, destrucción o inutilización de todo o una parte de objetos que estén destinados a servir de prueba ante una autoridad.

5. Auditoría del Desarrollo

5.1. Ingeniería de Software y Auditoría del Desarrollo

Una de las áreas pertenecientes al departamento de informática es el área de desarrollo. Ésta abarca todas las fases que se deben seguir desde la necesidad de un sistema de información hasta su construcción e implantación. La auditoría del desarrollo tratará de verificar la existencia y aplicación de procedimientos de control adecuados que permitan garantizar el desarrollo de sistemas de información según los principios de la ingeniería de software, ya que mediante éstos se busca obtener un software económico, fiable, que cumpla los requisitos establecidos y funcione de manera eficiente sobre máquinas reales[5].

5.2. Funciones de las Áreas de Desarrollo

- **Planificación:** Planificación del área y participación en la elaboración del Plan Estratégico Informático de la organización.
- **Desarrollo de sistemas:** Análisis, diseño, construcción e implantación.
- **Estudio e Investigación:** Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. relacionadas con el desarrollo y su adopción.
- **Formación:** Establecer un plan de formación para el personal del área.
- **Normas y estándares:** Establecer normas y controles para las actividades del área y comprobar su observancia.

5.3. Tipos de Auditoría

Existen dos tipos de Auditoría del Desarrollo:

- Auditoría de la organización y del área de desarrollo: Es una interiorización hacia el área (entrevistas, observación, etc). Entre los objetivos de control se encuentran:
  - El Área de Desarrollo debe tener objetivos asignados dentro del departamento y una organización que permita el cumplimiento de los mismos.
  - El personal debe contar con la formación adecuada y estar motivado para el trabajo.
  - Si existe un plan de sistemas, los proyectos deben basarse en éste y lo mantendrán actualizado.
  - La propuesta y aprobación de nuevos proyectos deben realizarse de forma reglada.
  - La asignación de recursos a los proyectos debe hacerse de forma reglada.
  - El desarrollo de sistemas debe hacerse aplicando principios de Ingeniería del Software ampliamente aceptados.
  - Las relaciones con el exterior del departamento tienen que producirse de acuerdo a un procedimiento.
  - La organización del área debe estar siempre adaptada a las necesidades de cada momento.
- Auditoría orientada a un proyecto puntual del área: Cada desarrollo de un nuevo sistema de información es un proyecto con entidad propia, donde el proyecto tiene objetivos marcados y afecta a determinadas unidades de la organización. Al auditar un proyecto, se deben analizar la documentación del proyecto, sectores afectados, responsables, riesgos. Puede analizarse cuando está siendo construido (de esta forma, la opinión del auditor puede afectar el desarrollo -aunque esta opinión no sea vinculante-) o puede hacerse a algo que esté ya construido.

6. Protección de Datos Personales

6.1. El uso de los datos

La información fue un bien valioso en todas las épocas, pero en ninguna alcanzó la importancia que tiene en la actualidad, en donde informaciones parciales y dispersas pueden ser convertidas en informaciones en masa y organizadas. Por lo tanto, el estado debe garantizar en algunos casos, la limitación del uso de la informática para garantizar el honor, la intimidad personal y familiar de sus ciudadanos y el legítimo ejercicio de sus derechos.

Los *Datos Personales* son información de cualquier tipo referida a Personas Físicas o Ideales determinados (nombre, DNI, fecha de nacimiento, etc) o determinables (perfil psicológico, físico, fisiológico, etc). Por otro lado, se consideran *Datos Excluidos* a aquellos que son de uso interno, fuentes periodísticas, o artículos periodísticos disociados de datos personales. Se considera titular a la persona física o jurídica con domicilio legal en el país cuyos datos sean objeto del tratamiento, y usuarios de datos a cualquier persona que realice tratamiento de datos.

En la actualidad, proporcionamos datos relacionados a la actitud, personalidad, comportamiento y hábitos que terminan en manos de terceros. Estos datos representan *poder* y *valor*, que se concentran en la *industria del dato*. En la esfera privada puede ser útil para aumentar las ventas, mientras que en la pública permite brindar servicios (gobierno electrónico).

[5] *Fritz Bauer*

6.2. Legislación Argentina

Particularmente en Argentina, para limitar el avance de la tecnología sobre los derechos de las personas, existen varias normas, entre ellas:

- Normas sectoriales: Cada uno de estos sectores establece normas de acuerdo a sus realidades particulares.
  - Sector Financiero.
  - Sector Asistencial.
  - Censos poblacional y de vivienda.
- Art. 43 de la Constitución Nacional (reforma de 1994): Incorpora a los ciudadanos la posibilidad de interponer la acción de amparo *Habeas Data*, para que pueda tomar conocimiento de sus datos personales que consten en registros o bancos de datos públicos o privados, conocer la finalidad para las cuales se los emplean y en caso de falsedad o discriminación poder exigir la supresión, rectificación, confidencialidad o actualización.
- Ley 25.326 Protección de Datos Personales.
- Decreto 1558 2001: Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Creación de la Dirección Nacional de Protección de Datos Personales (organismo de control).

6.3. Ley de Protección de Datos Personales (25.326)

Esta ley brinda Protección Integral (garantizar el derecho al honor e intimidad de las personas y el acceso a la información que sobre las mismas se registre) de los Datos Personales asentados en archivos, registros, bancos de datos, etc ya sean públicos y privados y que estén destinados a dar informes.

Según esta ley, un *archivo* es un conjunto de Datos Personales, que sean objeto de tratamiento o procesamiento, electrónicos o no, sin importar la modalidad de formación, organización, etc. El titular de un archivo es el *Responsable de archivo*.

Las *operaciones* del *Tratamiento de Datos* contemplan la recolección, conservación, ordenación, modificación, etc así como la cesión de los datos a terceros a través de comunicaciones, consultas, etc.

El *consentimiento* debe ser libre, expreso e informado, el titular debe prestar su consentimiento. Para ello, el titular debe conocer:

- Finalidad y quienes pueden ser sus destinatarios.
- Existencia del banco de datos, electrónico o no y la identidad y domicilio del responsable.
- Carácter facultativo u obligatorio de las respuestas al cuestionario que se proponga.
- Las consecuencias de proporcionar los datos, negativa a hacerlo o inexactitud de los mismos.
- Posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

No es necesario el consentimiento cuando:

- Datos Obtenidos por Fuentes de Acceso Público e Irrestricto.
- Recabados por el ejercicio de funciones propias de los Poderes del Estado o en virtud de una obligación legal.
- Listados limitados a: Nombre, DNI, Identificación Tributaria o Previsional, Ocupación, Fecha Nacimiento, Domicilio.
- Derivados de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.

6.3.1. Archivos de Datos

La agrupación de Datos Personales es posible sí y solo sí el organismo se encuentra inscrito en la Dirección Nacional de Protección de Datos Personales. Los datos deben cumplir las siguientes condiciones:

- Ser ciertos, adecuados, pertinentes y no excesivos.
- No utilizar medios desleales y fraudulentos.
- No pueden utilizarse para otras finalidades distintas a las que motivaron su obtención.
- Datos exactos y actualizados o deben suprimirse.
- Almacenados de forma que permitan el derecho al acceso de su titular.
- Destruirlos cuando dejen de ser necesarios o pertinentes.

6.3.2. Datos sensibles y medidas de seguridad

Los *Datos Sensibles* son aquellos que revelan origen racial o étnico, opiniones políticas, religión, sindicatos, salud, vida sexual, etc. Ninguna persona puede ser obligada a proporcionarlos, sólo pueden ser recolectados por razones de interés general autorizadas por ley, o con finalidad estadística o científica siempre y cuando no se identifiquen sus titulares, y está prohibido formar archivos, bases o registros con datos sensibles.

Los usuarios de archivos deben adoptar medidas técnicas y organizativas, garantizar la seguridad y confidencialidad de los datos personales, evitar la adulteración, pérdida consulta o tratamiento no autorizado y detectar desviaciones de información. Además, está prohibido reunir datos personales sin implementar medidas técnicas de Integridad y Seguridad, y transferir Datos Personales a países y organismos internacionales que no proporcionen los niveles de protección adecuados.

7. Auditoría de las Bases de Datos

La auditoría de Bases de Datos es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a los datos almacenados en las Bases de Datos, incluyendo la capacidad de determinar: quien accede a los datos, cuando se accedió a los datos, desde que tipo de dispositivo, desde que ubicación en la red, cuál fue la sentencia SQL ejecutada, y cuál fue el efecto del acceso a la Bases de Datos. La selección del administrador de Bases de Datos (DBA) es un desafío ya que deben considerarse todos los riegos asociados al uso de las BD.

7.1. Objetivos de la Auditoría de las Bases de Datos

Entre los objetivos generales de la Auditoría de las Bases de Datos, se encuentran:

- Mitigar los riesgos asociados con el manejo inadecuado de los datos.
- Apoyar el cumplimiento regulatorio.
- Satisfacer los requerimientos de los usuarios.
- Evitar acciones criminales.
- Evitar multas por incumplimientos.

Estos objetivos se obtienen evaluando la definición de estructuras físicas y lógicas de las Bases de Datos, control de carga y mantenimiento de las Bases de Datos, integridad de los datos y protección de accesos, estándares para análisis y programación en el uso de Bases de Datos.

7.2. Importancia de los Controles Internos

- Toda la información de la organización reside en las Bases de Datos y deben existir controles relacionados con el acceso a las mismas.
- Se debe poder demostrar la integridad de la información almacenada en la Bases de Datos.
- Las organizaciones deben mitigar los riesgos asociados a la perdida de datos y a la fuga de información.
- La información confidencial es responsabilidad de las organizaciones.
- Los datos convertidos en información a través de las Bases de Datos y procesos representan el negocio de la organización.
- Las organizaciones deben tomar medidas mucho más allá de asegurar sus datos (legalidad).
- Deben monitorearse perfectamente a fin de conocer quién o qué les hizo, cuándo y cómo.

7.3. Riesgos producto de la utilización de las Bases de Datos

- Incremento de la dependencia del servicio informático debido a la concentración de datos.
- Mayores posibilidades de acceso en la figura del administrador de Bases de Datos.
- Incompatibilidad entre sistemas de seguridad de acceso propias del sistema de gestores de Bases de Datos y el sistema general de instalación.
- Mayor impacto de los errores en datos o programas que en los sistemas tradicionales que no usan Bases de Datos.
- Rupturas de enlaces o cadenas por fallos del software o de los programas de aplicación.
- Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de Bases de Datos (administradores, programadores, etc.).

7.4. Ciclo de Vida de las Bases de Datos

1. **Estudio previo y plan de trabajo:** Consiste en evaluar el Plan Estratégico y aprobar la Estructura Orgánica de los Proyectos, con la participación del Sector de Gestión y Control de las Bases de Datos. Las responsabilidades se dividen según el tipo de administrador:

Administrador de Datos: Planifica, organiza y controla los activos de datos en la organización. Se encarga de realizar el diseño conceptual y lógico de la Bases de Datos, asesorar al personal de sistemas durante el desarrollo de aplicaciones, establecer estándares de diseño de Bases de Datos, desarrollo y contenido del diccionario de datos, desarrollar planes estratégicos y tácticos para la manipulación de datos, controlar integridad y seguridad de datos, proporcionar controles de seguridad.

Administrador de las Bases de Datos: Administra el entorno/funcionalidades de las Bases de Datos. Se encarga de realizar el diseño físico de la Bases de Datos, asesorar en la adquisición de hardware y software, resolver problemas del sistema de Bases de Datos y del software asociado, monitorear el sistema de Bases de Datos, asegurar la integridad de datos, asegurar seguridad y confidencialidad, etc.

En esta etapa se realiza un análisis del estudio tecnológico de viabilidad (costo/beneficio), se lleva a cabo el proyecto, se desarrolla o compra y se informa a la gerencia para la toma de decisiones.

2. **Concepción de la Bases de Datos y selección del equipo:**
   - Comienzo del diseño de la Bases de Datos, mediante la utilización de modelos y técnicas de diseño conceptual, especificación de documentos fuentes, mecanismos de control.
   - Definir la arquitectura de la información, mediante el modelo de arquitectura de información y su actualización, datos y diccionarios de datos corporativos.
   - Seleccionar equipamiento de acuerdo al impacto del nuevo software y su nivel de seguridad.
3. **Diseño y carga**:
   - Realizar diseños lógicos y físicos de la Bases de Datos (definición de tablas, vistas, índices, aprobación del usuario y administrador de Bases de Datos).
   - Carga de datos (manual, migraciones, pruebas en paralelo, controles de integridad).
4. **Explotación y mantenimiento:**
   - Pruebas de aceptación con participación de los usuarios.
   - Sistema puesto en explotación (uso), mediante definición de procedimientos de explotación y mantenimiento, como verificación de exactitud, complejidad y autorización, manejo de errores en entrada de datos, distribución de salidas, etc, y rendimiento del sistema (tuning).
5. **Revisión post-implantación:** Plan para evaluar logros de resultados esperados, de satisfacción y necesidades de los usuarios, costos y beneficios obtenidos, formación de los usuarios.

7.5. Auditoría y Control Interno de un Entorno de Bases de Datos

Cuando el auditor se encuentra el sistema de gestión de base datos deberá estudiarlo éste y su entorno. Entre los componentes del SGBD se encuentran el núcleo y el catálogo, componente fundamental que permite asegurar el funcionamiento y la seguridad de la base de datos. El entorno se compone de:

- **Software de auditoría:** Paquetes que facilitan la labor del auditor en cuanto a extracción de datos de la base de datos, el seguimiento de las transacciones, etc. Hay también productos que permiten realizar auditoría del dato.
- **Sistema de monitorización y ajuste:** Complementan facilidades ofrecidas por el propio sistema de gestión de bases de datos, ofreciendo mayor información para optimizar el sistema (sistemas expertos).
- **Sistema operativo:** Es una pieza clave del entorno. El SGBD se apoya en menor o mayor medida en los servicios que el sistema operativo le ofrezca como control de memoria, gestión de áreas de almacenamiento intermedio (buffers), manejo de errores, mecanismos de bloqueos.
- **Monitor de transacciones:** Puede incluirse dentro del propio SGBD o considerarse un elemento más del entorno con responsabilidades de confidencialidad y rendimiento.
- **Protocolos y sistemas distribuidos:** Los sistemas distribuidos exigen una función de administrados de base de datos centralizada que establezca estándares generales para la distribución de datos a través de las aplicaciones. Deben existir buenas pistas de auditoría para todas las transacciones. Deben existir controles para prevenir interferencias de actualización sobre las bases de datos. Deben realizarse análisis adecuados de costos y beneficios en el diseño de entornos distribuidos. Los sistemas distribuidos exigen una función de administrados de datos centralizada que establezca estándares generales.
- **Paquetes de seguridad:** Productos disponibles en el mercado que permiten la implantación efectiva de una política de seguridad.
- **Diccionario de datos:** Bases de datos de *metadatos*. Como daños pueden causar perdida de integridad de los procesos.
- **Herramientas CASE:** Herramientas de soporte de diseño y concepción de sistemas de información. Herramientas claves de auditoría para revisar el diseño de las bases de datos, comprobar el empleo correcto de la metodología y asegurar un nivel mínimo de calidad.
- **Lenguaje de cuarta generación L4G:** Amplia gama de generadores de aplicaciones de formularios de informes, etc., que actúan sobre la base de datos. Pueden ocasionar problemas si sobre los mismos no se establecen los controles correspondientes. Pueden ser

ineficientes, consumir grandes recursos, limitados en el uso de alguna metodología.

- **Facilidades de usuarios:** Interfaces gráficas fáciles de usar que permiten al usuario final acceder a los datos sin tener que conocer las sintaxis de los lenguajes de SGBD. Verificar medidas de seguridad de dichas herramientas y bajo qué condiciones han sido instaladas.

8. Auditoría de la Ofimática

8.1. Ofimática

La *Ofimática* es todo sistema informatizado que Genera, Procesa, Almacena, Recupera, Comunica y Presenta Datos[6] relacionados con el funcionamiento de las Oficinas. Incluye:

- Aplicaciones específicas para la Gestión de Tareas
  - Procesadores de textos.
  - Hojas de cálculo.
  - Bases de datos personales.
- Herramientas para la Gestión de Documentos
  - Control de expedientes.
  - Sistemas de almacenamiento óptico de la información.
  - Agendas de contactos.
- Sistema de Trabajo en Grupo
  - Correo electrónico.
  - Control de flujo de trabajo (procesos automatizados).

Características Particulares de los Entornos Ofimáticos

- Las aplicaciones se encuentran distribuidas por los diferentes Departamentos de la Organización en lugar de encontrarse en una única ubicación centralizada.
- Se produce un traslado de la responsabilidad sobre ciertos controles de los Sistemas de Información a Usuarios finales NO dedicados profesionalmente a la informática, que pueden NO comprender de un modo adecuado la importancia de los mismos y la forma de realizarlos.

Estas particularidades tienen como *consecuencia*:

- Adquisiciones poco planificadas.
- Desarrollos ineficaces e ineficientes.
- Falta de conciencia de los usuarios acerca de la Seguridad de la Información.
- Deficientes Copias de Seguridad.
- Escasa Formación del Personal.
- Ausencia de Documentación.

8.2. Controles de los Entornos Ofimáticos

8.2.1. Economía, Eficacia y Eficiencia

1. Determinar si el **Inventario Ofimático** refleja *con exactitud* los Equipos y Aplicaciones existentes en la Organización, caso contrario el inventario *no es fiable*.
2. Determinar y evaluar el **Procedimiento de Adquisición de Equipos y Aplicaciones**. Pueden darse adquisiciones *centralizadas* y *descentralizadas* del departamento.
3. Determinar y evaluar las **Políticas de Mantenimiento** definidas en la Organización. La existencia de Procesos *descentralizados* propician la adquisición de equipos NO incluidos en Inventario ni Contratos de Mantenimiento. Es conveniente:
   - Comprobar la existencia de garantías de equipos adquiridos y pagos innecesarios así como conocimiento del estado de dichas garantías por parte de los usuarios finales.
   - Constatar disponibilidad de Contratos de Mantenimiento vigentes con Empresas Externas e identificación de los que hayan caducado.
   - Verificar existencia de Registro de Incidentes.
   - Evaluar la respuesta de proveedores ante requerimientos.

[6] Los datos que manejan estas aplicaciones están desperdigados en muchas oficinas, sin poder ser alcanzados por los SGBD, o las medidas de seguridad que éstos proporcionan.

4. Evaluar la **Calidad de las Aplicaciones** del entorno Ofimático desarrolladas por Personal de la propia organización. Verificar la existencia de un Departamento responsable de controlar el desarrollo de aplicaciones o bien si los departamentos han desarrollado Aplicaciones de uso Interno, bajo su propio criterio, sin control. Implica Determinar la Metodología empleada y el proceso de Testeo.
5. Evaluar la corrección del procedimiento existente para la realización de los **Cambios de Versiones y Aplicaciones**. Implica:
   - Verificar la existencia de Procedimientos Formales para Autorización, Aprobación, Adquisición de Nuevas Aplicaciones y Cambios de Versiones.
   - Verificar análisis de Problemas de integración e incompatibilidades de los nuevos productos previo a su implantación.
   - Verificar que los usuarios se hayan capacitado en su utilización y que los encargados de mantenerlos hayan adquirido los conocimientos suficientes.
6. Determinar si los usuarios cuentan con suficiente **formación** y con la **documentación de apoyo** necesaria para desarrollar sus tareas de un modo eficaz y eficiente. En este sentido la falta de formación, la existencia de conocimientos deficientes y las capacidades no aprovechadas tienen como consecuencia la pérdida de eficacia y eficiencia. Aquí es necesario:
   - Verificar existencia de Plan de Formación.
   - Verificar entrega de documentación sobre operativa del Producto.
7. Determinar si el **equipamiento** existente se ajusta a las *necesidades reales* de la organización. Los equipos obsoletos subutilizados repercuten en el funcionamiento correcto de la organización. Se debe verificar existencia de subutilización o necesidad de actualización o ampliación de equipos.

8.2.2. Seguridad y Condicionantes Legales

1. Determinar si existen garantías suficientes para **proteger los accesos no autorizados** a la *información reservada* de la empresa y la *integridad* de la misma en estos entornos. Implica tener:
   - Agendas de Contactos.
   - Informes sobre temas confidenciales.
   - Estadísticas obtenidas con Información extraída de las Bases de Bases de Datos Corporativa.
2. Determinar si el **Procedimiento de Generación de las Copias de respaldo** es fiable y garantiza la *recuperación* de la Información en caso de necesidad. Implica:
   - Periodicidad.
   - Asignación de responsabilidades.
   - Adecuado Almacenamiento de los Soportes.
   - Eficacia en el procedimiento de recuperación.
3. Determinar si está garantizado el **funcionamiento ininterrumpido** de aquellas aplicaciones cuya caída podría suponer *pérdidas de integridad* de la información y aplicaciones. Se deben prever *cortes de energía* y *caídas de tensión*.
4. Determinar el grado de exposición ante la posibilidad de intromisión de **Virus**. La materialización de este tipo de intromisión podría ocasionar:
   - Pérdida de Información.
   - Empleo de recursos y tiempo para restablecer el sistema.
   - Paralización temporaria de las actividades o algún proceso de la empresa.

9. Propiedad Intelectual

En Argentina existen varias leyes que regulan la *Propiedad Intelectual*, inicialmente la Ley 11.723 y posteriormente la ley 25.036 que modifica a la anterior para incluir los programas de computación.

9.1. Ley 11.723 de Propiedad Intelectual

9.1.1. Objetivo

El objetivo de esta ley es proteger las obras[7] científicas, literarias y artísticas sea cual fuere el procedimiento de reproducción, creadas por las personas, registrándolas y otorgándoles un *derecho de propiedad*, que les da la facultad de disponer la obra, publicarla, ejecutarla, representarla, y exponerla en público, enajenarla, traducirla, adaptarla o de autorizar su traducción y de reproducirla en cualquier forma.

9.1.2. Titulares

Son titulares de la obra:

- El Autor de la Obra
- Los Herederos o Derecho-habientes
- Los que con permiso del Autor: Traducen, Adaptan o Modifican
- Las Personas Físicas o Jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido éste en el desempeño de sus funciones laborales, salvo estipulación contraria.

Esta titularidad se ejerce durante la vida del autor y hasta 70 años a partir del año siguiente de la muerte de éste.

9.1.3. Obras de Software

Respecto a las obras de Software, quien haya recibido de los autores de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo. Dicha copia deberá estar debidamente identificada y ésta no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

9.2. Decreto 165/94

Este decreto proporciona un marco legal de protección para las diferentes expresiones de las obras de software y base de datos, así como sus diversos medios de reproducción, considerando:

- Obras de Software:
  - Diseños, generales y detallados, del flujo lógico de los datos en un sistema de computación.
  - Programas de computación, tanto en su versión *Fuente* (lector humano) como su versión *Objeto* (destinada a ser ejecutada por el computador).
  - La documentación Técnica, cuyos fines sean la explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.
- Obras de Bases de Datos[8]:
  - Producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.

9.3. Dirección Nacional de Derecho de Autor

La *Dirección Nacional del Derecho de Autor* es un organismo dependiente del Ministerio de Justicia que tiene como principal objetivo proteger al autor desde que crea su obra.

9.3.1. Funciones

La DNDA posee como funciones:

- Custodiar las obras inéditas (aquellas que no han sido editadas, publicadas o exhibidas)
- Registrar las obras publicadas, las publicaciones periódicas y los contratos.
- Asesorar a organismos públicos, entidades privadas y/o particulares con respecto a la interpretación de las normas vigentes en materia de derecho de autor.

[7] programas de computación fuente y objeto, compilaciones de datos o de otros materiales, obras dramáticas, composiciones musicales, dramático-musicales, cinematográficas, coreográficas y pantomímicas, obras de dibujo, pintura, escultura, arquitectura, modelos y obras de arte o ciencia aplicadas al comercio o a la industria, impresos, planos y mapas, plásticos, fotografías, grabados y fonogramas.

[8] Se incluyen como obras literarias

10. Network Information Center Argentina

El *Network Information Center* es un organismo que administra el Registro de nombres de dominio y asegura el funcionamiento del DNS (Sistema de Nombres de Dominio) para el Dominio de Nivel Superior Geográfico *.ar* y sus subdominios (*com, org, net, tur, int, gob, mil, edu*).

10.1. Funciones

NIC se encarga de:

- Administrar el Dominio Argentina de Internet.
- Efectuar el Registro de Nombres de Dominio solicitados.

El registro de los Dominios posee una validez de 1 año y es renovable. Además, para cada registro se requiere una *Persona de Contacto*, que será el responsable para efectuar modificaciones de la delegación o renovación.

Es de destacar tambien que NIC Argentina no interviene en conflictos entre entidades registrantes, solicitantes o terceros relativos al registro o uso de un nombre de dominio; y carece de competencia respecto a los contenidos de las páginas web que puedan construirse bajo los nombres de dominio que integran su registro.

11. Auditoría de Redes

Todos los sistemas de comunicación, desde el punto de vista de la auditoría, presentan una problemática común: La información transita por lugares físicamente alejados de las personas responsables, lo cual presupone un compromiso en la seguridad, ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información.

11.1. Elementos sometidos a control

En una Auditoría de la Red, se deben revisar:

- Diseño de la Red.
- Cableado.
- Instalaciones eléctricas.
- Tráfico de redes.
- Climatización de servidores.
- Procedimientos de respaldo.
- Licencias de software.
- Inventarios de equipos.

11.2. Auditoría de la Gerencia de Comunicaciones

La gerencia de comunicaciones es responsable de las siguientes áreas:

- Gestión de Red, inventario de equipamiento y normativas de conectividad.
- Monitorización de las comunicaciones, registro y resolución de problemas
- Revisión de costos y asignación formal a proveedores y servicios de transporte.
- Creación y aplicabilidad de estándares.
- Evaluación de las necesidades de comunicaciones.
- Balanceo de tráfico entre rutas.
- Selección de equipamiento.

11.2.1. Objetivos de Control

- Tener una gerencia con plena autoridad de *voto y acción*.
- Llevar un registro actualizador de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- Mantener una vigilancia constante sobre cualquier acción en la red.
- Registrar un coste de comunicaciones y reparto a encargados.
- Mejorar el rendimiento y la resolución de problemas presentados en la red.

11.3. Auditoría de la Red Física

La Red Física se audita para saber hasta qué punto las *Instalaciones físicas* del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes.

11.3.1. Consideraciones

Se debe comprobar o tener en cuenta:

- El registro de los accesos físicos provenientes desde el exterior.
- El cableado no pueda ser interceptado físicamente desde el interior del edificio.
- Qué parte del cableado podrá estar en condiciones de funcionar ante la presencia de un desastre.

- La red física es un punto de contacto entre la *gerencia de comunicaciones* y la *gerencia de mantenimiento* quien aporta personal para el tendido de cables y su mantenimiento.

11.4. Auditoría de la Red Lógica

A través de métodos lógicos es posible el envío indiscriminado de mensajes lo cual puede bloquear la red y por lo tanto a los equipos de la instalación. Por lo tanto, es necesario:

- Monitorizar la red.
- Revisar los errores o situaciones anómalas que se producen, para evitar un daño interno.
- Tener implementados procedimientos para detectar y aislar equipos.

11.4.1. Objetivos de Control

Verificar la existencia de:

- Contraseñas de acceso y procedimientos que limitan o detectan accesos no autorizados.
- Control de errores de transmisión.
- Registros de la actividad de la Red.
- Encriptación de la información sensible.
- Controles para evitar la importación y exportación de datos a otros sistemas informáticos.

11.4.2. Controles

Se debe comprobar si el sistema:

- Solicita usuario y contraseña para cada sesión.
- No permite acceso a ningún programa sin identificar ni autenticar.
- Inhabilita al usuario después de n intentos fallidos.
- Exige cambios periódicos de claves por parte de los usuarios.
- Enmascara las claves en la pantalla.
- Informa al usuario cuál es su última conexión.

11.5. Procedimientos de Gestión de Redes y Comunicaciones

- Procedimiento Formal de registración de Usuarios:
  - Usar IDs de usuario únicos.
  - Usar IDs grupales sólo cuando son convenientes para el trabajo a desarrollar.
  - Obtener autorización del propietario del sistema.
  - Otorgar nivel e acceso para el propósito del negocio.
  - Entregar a los usuarios un detalle escrito de sus derechos de acceso.
  - Mantener un registro formal de todas las personas autorizadas.
  - Cancelar los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la empresa.
  - Limitar y controlar la asignación y uso de privilegios.
- Administración de contraseñas: controlar a través de un procedimiento de administración formal:
  - Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas en secreto y las de los grupos exclusivamente entre los miembros.
  - Garantizar que los usuarios cambien de inmediato su primer contraseña.
  - Las contraseñas nunca deben ser almacenadas en medios sin protección.
  - Considerar el uso de otras tecnologías de identificación (Biometría).
  - Llevar a cabo un proceso formal a intervalos regulares a fin de revisar los derechos de acceso de los usuarios (cada 6 meses) y los privilegios especiales.
- Responsabilidad del usuario:
  - Mantener contraseñas en secreto.
  - Evitar registros en papel de las contraseñas.
  - Cambiar las contraseñas siempre que existan indicios de compromiso del sistema.
  - Seleccionar contraseñas de calidad.
  - Cambiar regularmente y evitar reciclar contraseñas.
  - No incluir contraseñas en procesos automatizados de inicio de sesión.
- Control de acceso a la red:
  - Identificar y verificar la identidad y la terminal o ubicación de cada usuario autorizado.
  - Registrar los accesos exitosos y fallidos del sistema.
  - Limitar el número de intentos de conexión no exitosos permitidos.
  - Limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión.

    - Las terminales inactivas en ubicaciones de alto riesgo deben apagarse después del período definido de actividad.

- Monitoreo: Detectar desviaciones y registrar eventos, estos últimos relacionados a:
    - Accesos no autorizados (usuarios existentes).
    - Aplicaciones con privilegios.
    - Intentos de acceso no autorizados.
    - Alertas o fallas del sistema.

Preguntas de Examen

1. Explique en qué consiste la actividad de controlar llevada a cabo por la dirección informática.
2. Dé ocho ejemplos de Control Interno Informático que considere vitales de implementar. Ordenarlos según su orden de prioridad.
3. ¿Cuál es el objeto de la Ley 25326 de Protección de Datos Personales?
4. ¿Cuáles son las normas aplicables en nuestro país para la protección de Datos Personales?
5. ¿En qué consisten los Datos Personales y cómo deben ser los mismos?
6. ¿Qué derechos tengo como titular de los Datos Personales?
7. ¿Cómo debe ser el consentimiento al dar Datos Personales? ¿En qué casos no es necesario?
8. ¿Cuál es la autoridad de aplicación de la Ley y cuáles son sus funciones?
9. ¿Se pueden ceder los Datos Personales?
10. ¿Qué es la ofimática? ¿Qué características poseen los entornos ofimáticos y cuáles las consecuencias que posibilitan la Auditoría sobre los mismos?
11. Enunciar controles recomendables en entornos ofimáticos y fundamentar su aplicación.
12. ¿Cuál es el objetivo de una Auditoría de la Seguridad Física? Identificar Áreas de Seguridad Física y Fuentes de su Auditoría.
13. Describa qué es y cuál es el contenido de un Informe de Auditoría.
14. ¿Con qué elementos hay que trabajar para realizar el Informe de Auditoría?
15. ¿Qué es el Plan de Contingencia y qué aspectos se deben tener en cuenta para su preparación?
16. ¿Qué aspectos debe considerar el auditor al evaluar como la dirección o gerencia de informática organiza y coordina las actividades de sus sectores o áreas?
17. De su opinión sobre quién o quienes deben realizar cada una de las actividades (organizar y coordinar).
18. Diferencias y similitudes entre Control Interno Informático y Auditoría Informática.
19. Emita una opinión sobre como justifica la inversión necesaria en CII y AI.
20. ¿Qué aspectos se deben tener en cuenta al auditar un desarrollo de software?
21. ¿Cómo motivaría al personal del área de desarrollo?
22. Detalle la metodología de la Auditoría Informática.
23. ¿Qué son los delitos informáticos?
24. ¿En qué consiste una Auditoría de las Bases de Datos?
25. ¿Quiénes son los titulares del derecho de propiedad intelectual?
26. ¿Que son las obras de software y base de datos?