Resumen unidad 4 y 5

Unidad 4-Proyectos de software (continuación de la unidad)

Normas y modelos de calidad

Estándares

➢ Documentos, recomendaciones, reglas producidas por organizaciones reconocidas.

➢ Su adopción es opcional aunque puede ser impuesta por reglamentaciones o por pedido de un cliente.

➢ Asegurar el cumplimiento de normas o estándares requiere de procesos de auditoría y/o certificación.

ISO

❖ International Organization for Standardization.

❖ ISO 9000

- ➢ Familia de estándares relacionados con la administración de la calidad en los sistemas.
- ➢ Provee guías y herramientas para organizaciones que quieran asegurar la calidad de sus productos y servicios.

❖ ISO 9001

- ➢ Establecer un sistema de administración de calidad.

Principios de administración de calidad

ISO Series 9000:2015

1) Foco en el cliente
2) Liderazgo
3) Participación de la gente
4) Método de procesos
5) Decisiones basadas en evidencia
6) Mejora continua
7) Gestión de relaciones

Familia ISO/IEC 25000

★ Conocida como SQuaRE (System and Software Quality Requirements and Evaluation)

★ Evolución de otras normas:

- ○ ISO/IEC 9126 - modelo de calidad del producto software
- ○ ISO/IEC 14598 - proceso de evaluación de productos

ISO/IEC 2500n – División de Gestión de Calidad Definen todos los modelos, términos y definiciones comunes referenciados por todas las otras normas de la familia 25000.	*ISO/IEC 25000 - Guide to SQuaRE* Modelo de la arquitectura de SQuaRE, la terminología de la familia, un resumen de las partes, los usuarios previstos y las partes asociadas, así como los modelos de referencia.	*ISO/IEC 25001 - Planning and Management* Requisitos y orientaciones para gestionar la evaluación y especificación de los requisitos del producto software.
ISO/IEC 2501n – División de Modelo de Calidad Modelos de calidad detallados	*ISO/IEC 25010 - System and software quality models* Modelo de calidad para el producto	*ISO/IEC 25012 - Data Quality model:* Modelo general para la calidad

incluyendo características para calidad interna, externa y en uso del producto software.	software y para la calidad en uso. Esta Norma presenta las características y subcaracterísticas de calidad frente a las cuales evaluar el producto software.	de los datos, aplicable a aquellos datos que se encuentran almacenados de manera estructurada y forman parte de un Sistema de Información.
ISO/IEC 2502n – División de Medición de Calidad Modelo de referencia de la medición de la calidad del producto, definiciones de medidas de calidad (interna, externa y en uso) y guías prácticas para su aplicación.	*ISO/IEC 25020 - Measurement reference model and guide* Explicación introductoria y un modelo de referencia común a los elementos de medición de la calidad. También proporciona una guía para que los usuarios seleccionen o desarrollen y apliquen medidas propuestas por normas ISO.	*ISO/IEC 25021 - Quality measure elements* Conjunto recomendado de métricas base y derivadas que puedan ser usadas a lo largo de todo el ciclo de vida del desarrollo software.
ISO/IEC 2502n – División de Medición de Calidad *ISO/IEC 25022 - Measurement of quality in use* Métricas para realizar la medición de la calidad en uso del producto.	*ISO/IEC 25023 - Measurement of system and software product quality* Métricas para realizar la medición de la calidad de productos y sistemas software.	*ISO/IEC 25024 - Measurement of data quality* Métricas para realizar la medición de la calidad de datos.
ISO/IEC 2503n – División de Requisitos de Calidad Especificar requisitos de calidad que pueden ser utilizados en el proceso de elicitación de requisitos de calidad del producto software a desarrollar o como entrada del proceso de evaluación.	*ISO/IEC 25030 - Quality requirements* Conjunto de recomendaciones para realizar la especificación de los requisitos de calidad del producto software.	
ISO/IEC 2504n – División de Evaluación de Calidad Requisitos, recomendaciones y guías para llevar a cabo el proceso de evaluación del producto software.	*ISO/IEC 25040 - Evaluation reference model and guide* Modelo de referencia general para la evaluación, que considera las entradas al proceso de evaluación, las restricciones y los recursos necesarios para obtener las correspondientes salidas.	*ISO/IEC 25041 - Evaluation guide for developers, acquirers and independent evaluators* Requisitos y recomendaciones para la implementación práctica de la evaluación del producto software desde el punto de vista de los desarrolladores, de los adquirentes y de los evaluadores independientes.
ISO/IEC 2504n – División de	*ISO/IEC 25042 - Evaluation*	*ISO/IEC 25045 - Evaluation*

Evaluación de Calidad	*modules*	*module for recoverability*
Requisitos, recomendaciones y guías para llevar a cabo el proceso de evaluación del producto software.	Módulo de evaluación y la documentación, estructura y contenido que se debe utilizar a la hora de definir uno de estos módulos.	Módulo para la evaluación de la sub-característica Recuperabilidad

CMM / CMMI

CMM

★ CMM: Capability Maturity Model (Modelo de madurez de capacidad). SEI: Instituto de Ingeniería del Software - Universidad Carnegie Mellon

★ Enfoque de mejoramiento de procesos.

★ Define los elementos claves de un proceso efectivo.

★ Describe un camino de mejora evolutivo.

★ Cinco niveles de madurez:

1) Inicial
2) Repetible
3) Definido
4) Dirigido
5) Optimizado

★ Cada nivel de madurez se compone de **áreas de proceso claves**.

★ Cada área de proceso clave se organiza en cinco secciones de **características comunes.**

CMMI

➢ CMMI: Capability Maturity Model Integration (Integración del modelo de madurez de las capacidades).

ISACA: Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información.

5 componentes:

1. Modelo:

-Una vía clara para mejorar el rendimiento

-Simplificado para una adopción acelerada

2. Guías de adopción:

-Orientación para nuevos adoptantes empezar con CMMI V2.0

-Guía para la transición de CMMI V1.3 a CMMI V2.0

3. Herramientas y sistemas:

-Sistema rediseñado para acceder a modelos y recursos en línea.

4. Entrenamiento y certificación:

-Componentes modulares de formación.

-Centrarse en los objetivos del alumno.

-Opciones virtuales y presenciales.

5. Método de valoración:

-Nuevo método de evaluación para aumentar fiabilidad y reducir costes

CMMI v2.0

Un modelo con vistas personalizadas. CMMI:

- Desarrollo

El Desarrollo CMMI es un conjunto integrado de mejores prácticas que mejora la capacidad de una organización para desarrollar productos y servicios de calidad que satisfagan las necesidades de los clientes y usuarios finales.

Beneficios claves:

-*Mejore el tiempo de comercialización:* asegúrese de que los productos y servicios se entreguen de manera rápida y eficiente con poca o ninguna reelaboración.

-*Aumente la calidad:* mejore la calidad y la coherencia del desarrollo de productos para reducir los defectos.

-*Reduzca los costos:* reduzca los costos mediante procesos mejorados de planificación, programación y presupuestación.

-*Mejore la gestión del ciclo de vida del producto:* cumpla con las expectativas de los clientes durante todo el ciclo de vida del producto, desde la entrega hasta el mantenimiento y las operaciones.

-*Obtenga agilidad organizacional:* aproveche las oportunidades de mejora de ingresos y reducción de costos para ofrecer productos y servicios de manera rápida, efectiva y consistente.

- Servicios

Los Servicios CMMI son un conjunto integrado de mejores prácticas que mejora la capacidad de una organización para ofrecer de manera eficiente y efectiva ofertas de servicios de calidad que satisfagan las necesidades del mercado y de los clientes.

Beneficios claves:

-*Gane la lealtad del cliente:* supere las expectativas y la experiencia del cliente, fortalezca los puntos de contacto débiles con el cliente.

-*Desarrolle resiliencia:* reduzca el impacto de las interrupciones del servicio con un proceso para identificar y abordar incidentes potenciales y evitar que vuelvan a ocurrir.

-*Mejore el tiempo de comercialización:* asegúrese de que los servicios se entreguen de manera rápida, eficiente y de acuerdo con los acuerdos establecidos.

-*Aumente la calidad:* proporcione el nivel más alto posible de calidad de servicio.

-*Reduzca los costos:* reduzca los costos mediante una mejor planificación y una reducción de la repetición del trabajo.

- Administración de proveedores

La gestión de proveedores CMMI es un conjunto integrado de mejores prácticas que mejora la capacidad de una organización para identificar y gestionar proveedores de una manera que maximice la eficiencia de la cadena de suministro y reduzca el riesgo.

Beneficios claves:

-*Satisfaga las demandas del crecimiento:* desarrolle las capacidades necesarias para la gestión del crecimiento con una asignación eficaz de capacidad y recursos.

-*Mantenga el ritmo de las demandas de los productos:* gestione rápida y eficazmente los cambios y la complejidad en toda la cadena de suministro.

-*Reduzca el riesgo de la cadena de suministro:* aproveche las mejores prácticas repetibles para mitigar el riesgo y obtenga una comprensión compartida de la responsabilidad.

- Personas

La gente CMMI es un conjunto integrado de mejores prácticas que ayudan a identificar brechas de habilidades, eliminar cuellos de botella en el flujo de trabajo y capacitar a los miembros del equipo para desarrollar habilidades que ayudarán a que la organización tenga éxito.

Beneficios claves:

-*Impulsar el crecimiento:* Impulsa el crecimiento organizacional mediante el desarrollo de habilidades y la gestión del desempeño.

-*Mejore la eficiencia:* mejora la eficiencia identificando y mitigando los cuellos de botella.

-*Retener talento:* compita y retenga a los mejores talentos desarrollando, motivando y organizando a las personas de manera efectiva.

-*Garantice la agilidad:* garantice la agilidad para responder a los cambios continuos en la tecnología y las condiciones comerciales.

- Datos

Los Datos CMMI son un conjunto integrado de mejores prácticas para ayudar a las organizaciones a construir, mejorar y medir su función y personal de gestión de datos empresariales.

Beneficios claves:

-*Mejore la toma de decisiones:* aproveche los datos para mejorar la toma de decisiones y reducir el riesgo.

-*Reduzca los costos:* mejora la eficiencia operativa y reduce los costos mediante la arquitectura y la administración del ciclo de vida de los datos.

-*Mejore la confianza en los datos:* reduzca la amenaza de sanciones regulatorias y aumente la confianza del cliente mejorando la confianza en los datos.

-*Aumente la eficacia:* aumente la eficacia de los programas de gobernanza de datos.

- Protección (Security)

La seguridad CMMI es un conjunto integrado de mejores prácticas que mejora el proceso y el desempeño de una organización para proteger todo el ecosistema de la organización, incluido el personal, los recursos y la información.

Beneficios claves:

-*Aumente la confianza del cliente:* garantice la confianza del cliente con soluciones de productos seguras.

-*Desarrollar resiliencia:* reduzca el impacto de las interrupciones de amenazas con un proceso para identificar y abordar incidentes potenciales y evitar que vuelvan a ocurrir.

-*Mejore la moral y la rotación de los empleados:* cree una base para la aplicación consistente de la seguridad en todos los esfuerzos para incorporar fácilmente a nuevos empleados y retener a los mejores talentos.

-*Integre fácilmente:* integre de manera integral estándares y requisitos populares, como CMMC, ISO y más, en los procesos de seguridad de su organización.

- Seguridad (Safety)

La protección CMMI es un conjunto integrado de mejores prácticas que mejora la capacidad de una organización para facilitar y gestionar las actividades de seguridad.

Beneficios claves:

-*Aumente la calidad:* Proporciona el nivel más posible de seguridad del producto, ganando la lealtad y la confianza del cliente.

-*Reduzca el riesgo:* proteja y defienda contra los riesgos de seguridad siguiendo las mejores prácticas durante todo el ciclo de vida del producto.

-*Mejore la moral y la rotación de los empleados:* brindar un ambiente de trabajo seguro promueve el bienestar de sus empleados, aumentando así su deseo de trabajar.

-*Desarrolle resiliencia:* reduzca el impacto de las fallas con un proceso para prevenir y responder a incidentes de seguridad.

- Virtual

El CMMI Virtual es un conjunto integrado de mejores prácticas para ayudar a las organizaciones a desarrollar las habilidades necesarias para comprender las mejores prácticas, herramientas y técnicas para entornos comerciales virtuales para maximizar la efectividad y la eficiencia.

Beneficios claves:

-*Disminuir las vulnerabilidades:* identifique y reduzca la exposición a las vulnerabilidades asociadas con la entrega de soluciones virtualmente y/o el trabajo virtual.

-*Planifique con anticipación:* planifique las interrupciones operativas causadas por eventos globales o impactos ambientales.

-*Mejore la eficiencia:* mejora la eficiencia operativa garantizando una fuerza laboral virtual eficaz.

Certificaciones

- ❖ Las organizaciones deben certificar el cumplimiento de las normas o modelos.
- ❖ Hay empresas que realizan las evaluaciones y otorgan (o no) la certificación.
- ❖ Son procesos costosos pero otorgan beneficios a las organizaciones
  - ➢ Se mejoran los procesos: más eficiencia, competitividad, calidad,etc.
  - ➢ Se gana imagen frente a los clientes.

Métricas para productos de software

¿Qué medir?

Basadas en funciones

Métrica basada en funciones

- ❖ La intención es predecir el “tamaño” del sistema que resultará.
- ❖ El motivo es que el tamaño puede ser un indicador:
  - ➢ de la complejidad del diseño
  - ➢ del esfuerzo de codificación
  - ➢ del esfuerzo de integración
  - ➢ del esfuerzo necesario para las pruebas

Puntos de función (PF)

- ★ La métrica de puntos de función se utiliza para predecir la funcionalidad de un sistema.
- ★ Utiliza datos para:

- Estimar el costo o esfuerzo requerido para diseñar, codificar y probar el software.
- Predecir el número de errores que se encontrarán durante las pruebas.
- Prever el número de componentes y/o de líneas de código del sistema a implementar

Puntos de función (PF) - Ejemplo

Cálculo de puntos de función

Valor de dominio de información	Conteo		Factor ponderado Simple	Promedio	Complejo		
Entradas externas (EE)		×	3	4	6	=	
Salidas externas (SE)		×	4	5	7	=	
Consultas externas (CE)		×	3	4	6	=	
Archivos lógicos internos (ALI)		×	7	10	15	=	
Archivos de interfaz externos (AIE)		×	5	7	10	=	
Conteo total							

-**Número de entradas externas (EE):** . Cada entrada externa se origina de un usuario o se transmite desde otra aplicación, y proporciona distintos datos orientados a aplicación o información de control. Con frecuencia, las entradas se usan para actualizar archivos lógicos internos (ALI). Las entradas deben distinguirse de las consultas, que se cuentan por separado.

-**Número de salidas externas (SE):** Cada salida externa es datos derivados dentro de la aplicación que ofrecen información al usuario. En este contexto, la salida externa se refiere a reportes, pantallas, mensajes de error, etc. Los ítems de datos individuales dentro de un reporte no se cuentan por separado.

-**Número de consultas externas (CE):** Una consulta externa se define como una entrada en línea que da como resultado la generación de alguna respuesta de software inmediata en la forma de una salida en línea (con frecuencia recuperada de un ALI).

-**Número de archivos lógicos internos (ALI):** Cada archivo lógico interno es un agrupamiento lógico de datos que reside dentro de la frontera de la aplicación y se mantiene mediante entradas externas.

-**Número de archivos de interfaz externos (AIE):** Cada archivo de interfaz externo es un agrupamiento lógico de datos que reside fuera de la aplicación, pero que proporciona información que puede usar la aplicación.

★ Se evalúan 14 factores de ajuste.
★ El conteo total se modifica de acuerdo al peso aportado por los factores de ajuste.
★ Los PF se traducen en costo, esfuerzo, errores, líneas de código, de acuerdo a datos históricos.

Para calidad de especificación

★ Sugieren representar las características mediante una o más métricas.

Métricas del diseño arquitectónico

★ Se enfocan en características de la arquitectura del programa con énfasis en la estructura arquitectónica y en la efectividad de los módulos o componentes dentro de la arquitectura.
★ Son de “caja negra” porque no requieren conocimiento sobre el funcionamiento interior de los componentes.

★ Si la complejidad arquitectónica aumenta, aumenta la complejidad del sistema. Es probable que aumenten:

- Esfuerzo de integración
- Esfuerzo de pruebas

Tres medidas de complejidad propuestas: (Card y Glass):

➔ Complejidad estructural de un módulo i:
  - S(i)= f 2 out(i)

➔ Complejidad de datos
  - D(i) =v(i)/f out(i) 1

➔ Complejidad del sistema
  - Es la suma de las complejidades estructurales y de datos
  - C(i)= S(i)+D(i)

Del diseño orientado a objetos

Características medibles de un diseño OO

❖ *Tamaño:* El tamaño se define en función de cuatro visiones: población, volumen, longitud y funcionalidad. La población se mide al realizar un conteo estático de entidades OO, tales como clases u operaciones. Las medidas de volumen son idénticas a las medidas de población, pero se recolectan de manera dinámica: en un instante de tiempo determinado. La longitud es una medida de una cadena de elementos de diseño interconectados (por ejemplo, la profundidad de un árbol de herencia es una medida de longitud). Las métricas de funcionalidad proporcionan un indicio indirecto del valor entregado al cliente por una aplicación OO.

❖ *Complejidad:* Como el tamaño, existen muchas visiones diferentes de la complejidad del software. Whitmire ve la complejidad en términos de características estructurales al examinar cómo se relacionan mutuamente las clases de un diseño OO.

❖ *Acoplamiento:* . Las conexiones físicas entre elementos del diseño OO representan el acoplamiento dentro de un sistema OO.

❖ *Suficiencia:* Whitmire define suficiencia como "el grado en el que una abstracción posee las características requeridas de él o en el que un componente de diseño posee características en su abstracción, desde el punto de vista de la aplicación actual". En esencia, un componente de diseño (por ejemplo, una clase) es suficiente si refleja por completo todas las propiedades del objeto de dominio de aplicación que se modela, es decir, si la abstracción (clase) posee sus características requeridas.

❖ *Completitud:* La única diferencia entre completitud y suficiencia es "el conjunto de características contra las cuales se compara la abstracción o el componente de diseño". La suficiencia compara la abstracción desde el punto de vista de la aplicación actual. La completitud considera múltiples puntos de vista. Puesto que el criterio para la completitud considera diferentes puntos de vista, tiene una implicación indirecta en el grado en el que puede reutilizarse la abstracción o el componente de diseño.

❖ *Cohesión:* La cohesividad de una clase se determina al examinar el grado en el que el conjunto de propiedades que posee es parte del problema o dominio de diseño.

❖ *Primitivismo:* Una característica que es similar a la simplicidad, el primitivismo (aplicado tanto a operaciones como a clases), es el grado en el que una operación es atómica, es decir, la

operación no puede construirse a partir de una secuencia de otras operaciones contenidas dentro de una clase. Una clase que muestra un alto grado de primitivismo encapsula sólo operaciones primitivas.

❖ *Similitud:* El grado en el que dos o más clases son similares en términos de su estructura, función, comportamiento o propósito se indica mediante esta medida.

❖ *Volatilidad:* La volatilidad de un componente de diseño OO mide la probabilidad de que ocurra un cambio.

Tres grupos de métricas orientadas a objetos

-Métricas orientadas a la clase (CK)

-Métricas orientadas a la clase (MOOD)

-Métricas de Lorenz y Kidd

Métricas CK

Suite de métricas de Chidamber y Kemerer

1. Métodos ponderados por clase (MPC)
   - ★ Métodos ponderados por clase
     - Clase con *n* métodos, de complejidad *c1,..,cn*
     - La complejidad se mide con alguna métrica elegida
     - MPC = $\sum_{i=1}^{n}$ ci
   - ★ Más métodos, más complejos:
     - Más esfuerzo de implementación y pruebas
     - Más complejo el árbol de herencia
     - Más específica es la aplicación
     - Más limitada la reutilización
2. Profundidad del árbol de herencia (PAH)
3. Número de hijos (NDH)
4. Acoplamiento entre clases de objetos (ACO)
5. Respuesta para una clase (RPC)
6. Falta de cohesión en métodos (FCOM)

De la interfaz del usuario

➢ Se necesita evaluar: calidad y usabilidad

➢ Características como:
   - Cantidad de palabras
   - Gráficos
   - Colores
   - Tipografías

Para el código

➔ LOC = Lines Of Code = Líneas de Código

➔ Medidas de Halstead
   - ◆ n1 y n2= nro de *operadores* distintos que aparecen en un programa
   - ◆ N1= nro total de ocurrencias del operador
   - ◆ N2= nro total de ocurrencias del operando

➔ Usa las medidas para:
- Expresiones de longitud del programa, N=n1 log2(n1)+ n2 log2(n2)
- Volúmen de información V=N log2(n1+n2)
- Nivel del programa, nivel del lenguaje,etc

Para las pruebas

★ La mayor parte se enfoca en el proceso de las pruebas, no en las características técnicas de las pruebas en sí.

★ Métricas de Halstead
- Estimar esfuerzo de prueba mediante métricas derivadas de las de Halstead

★ Métricas para pruebas orientadas a objetos
- Consideran aspectos de encapsulación y herencia

Para el mantenimiento

❖ Pueden usarse todas las ya definidas, se proponen métricas nuevas, diseñadas explícitamente para actividades de mantenimiento.

❖ Índice de madurez de software
- ➢ Mt= nro de módulos en la versión actual
- ➢ Fc= nro de módulos con cambios en la versión actual
- ➢ Fa= nro de módulos que se agregaron
- ➢ Fd= nro de módulos de la versión anterior borrados en el actual
- ➢ IMS= Mt-(Fc+Fa+Fd)/Mt

Métricas de proceso y proyecto

- El objetivo es proporcionar indicadores para mejorar el proceso a largo plazo.
- Se recopilan durante mucho tiempo.
- Las métricas del proyecto permiten:
  - Valorar el estado de un proyecto en marcha
  - Rastrear riesgos potenciales
  - Descubrir áreas problemas antes que se vuelvan críticas
  - Ajustar el flujo de trabajo o las tareas
  - Evaluar la habilidad del equipo del proyecto para controlar la cantidad de los productos

Métricas del proceso

-Distintos usos para las métricas: privados y públicos

-Usos privados

+Tasa de defectos por individuo

+Tasa de defecto por componente

+Errores encontrados durante el desarrollo

-Las métricas privadas deben manejarse con cuidado: utilizarlas como motor para la mejora.

-Uso públicos

+Tasas de defectos en esfuerzo, tiempo calendario, datos relacionados recopilados,etc.

-Utilizarlas para mejorar el desempeño del proceso

Métricas del proyecto

-Son útiles durante la estimación. Resultados anteriores se usan como base de las estimaciones actuales.

+Minimizar calendario de desarrollo: ajustes para evitar demoras, mitigar potenciales problemas (riesgos)

+Valorar la cantidad del producto en marcha

+Modificar el enfoque técnico para mejorar la calidad

Métricas del proyecto OO

★ Lorenz y Kidd
- Número de guiones de escenario
- Número de clases clave
- Número de clases de apoyo
- Número promedio de clases de apoyo por clase clave
- Número de subsistemas

★ Métricas orientadas a casos de uso
- Los CUs describen las funciones y características visibles al usuario
- Directamente proporcional a los LOC y casos de prueba

Proceso de medición

➔ Puede caracterizarse mediante cinco actividades:
- *Formulación:* Derivación de medidas y métricas apropiadas.
- *Recolección:* Mecanismo para acumular los datos requeridos para obtener las métricas formuladas.
- *Análisis:* Cálculo de métricas y aplicación de herramientas matemáticas.
- *Interpretación:* Conocimiento ganado a partir de la representación usada.
- *Retroalimentación:* Recomendaciones derivadas de la interpretación y análisis de los resultados.

Unidad 5- Computación y sociedad

Computación y sociedad. Impacto.

Impacto personal y social

★ Beneficios: aumento de ganancias, bienes y servicios, mejora en la calidad de vida, facilidades para la comunicación, etc.

★ Nacen problemas:

Desperdicio y errores

El desperdicio y los errores relacionados con las computadoras son causas principales de problemas de cómputo que contribuyen a generar costos innecesariamente elevados y pérdida de ganancias. El desperdicio involucra el uso inadecuado de la tecnología y los recursos computacionales. Los errores se refieren a desaciertos, fallas y otros problemas que hacen que la salida de la computadora sea incorrecta o inútil, ocasionada principalmente por equivocaciones humanas. Esta sección explora el daño que se puede causar como resultado del desperdicio y los errores de cómputo.

-*Desperdicios:*

❖ Desechos tecnológicos

- Hardware
- Software

Aún cuando todavía tienen valor.

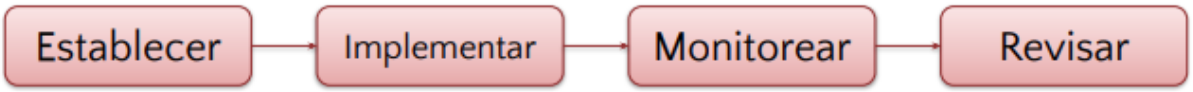
- Gasto de recursos innecesario
  - Construcción
  - Mantenimiento
- Desperdicio
  - Tiempo
  - Dinero

-Errores:

- Procedimientos inadecuados
- Falta de retroalimentación
  - En entrada o captura de datos
  - Mal manejo de archivos
  - Mal manejo de la salida del sistema
  - Planificación y control inadecuados
  - Capacidad de cómputo inadecuada
  - Fallas de acceso a información adecuada

-Errores= Prevención=

- Políticas y procedimientos
  - Adquisición y uso efectivo de sistemas y equipos
    - Justificación, definición de plataformas, proveedores
  - Eliminación de sistemas y dispositivos
  - Programas de capacitación y manuales
  - Aprobación previa a la implementación
  - Uso y administración del tiempo y los recursos



Crímenes

Poder de cómputo, velocidad, conexiones

- Como herramienta
  - Ciberataques: Un ciberterrorista es alguien que intimida u obliga a un gobierno u organización a promover sus objetivos políticos o sociales al lanzar ataques basados en computadora contra computadoras o redes y la información almacenada en ellas.
  - Robo de identidad: El robo de identidad es un crimen en el que un impostor obtiene piezas clave de identificación personal, como números de Seguro Social o licencia de conducir, para suplantar a alguien.
  - Juegos de azar
- Como objeto
  - Acceso y uso ilegal
  - Virus, spyware
  - Robo de información

- ➢ Violaciones de patentes y derechos de autor
- ➢ Estafas

-*Crímenes=Prevención=*

- ❖ Hardware y software especializado para proteger datos y sistemas.
  - ➢ Ej: encriptación de datos
- ❖ Esquemas de privilegios de acceso
- ❖ Servidores dedicados para distintas aplicaciones
- ❖ Auditorías periódicas
- ❖ Respaldos de datos

Conflictos de privacidad

- ❖ Constantemente se generan, recolectan y almacenan datos de las personas
  - ➢ ¿Quién posee esta información?
  - ➢ ¿Quién es responsable por ella?
- ❖ Privacidad en el trabajo. Monitoreo
  - ➢ Del correo electrónico
  - ➢ De mensajería instantánea
  - ➢ De uso de equipos
- ❖ Privacidad de internet
  - ➢ Manejo de la información personal en aplicaciones y sitios
  - ➢ Información de la redes sociales
  - ➢ Cookies

Huella digital

Es el rastro que dejamos al navegar en internet.

- ❖ *Datos públicos:* obra social, CUIT o CUIL, declaraciones de impuestos, domicilios declarados, cargos, becas, resultados de sorteos, resoluciones judiciales.
- ❖ *Datos publicados por otros:* fotos, posteos de amigos, familiares, clubes o espacios de pertenencia en redes sociales.
- ❖ *Datos que generás vos:* Posteos, comentarios, fotos en redes sociales y foros. Formularios que completaste, contenidos que compartiste en plataformas como tu currículum, perfiles en redes de contactos u otros contenidos como listas de reproducción y videos favoritos.

Adicciones

Impacto en el ambiente laboral

Problemas en el ambiente laboral

+Nuevos tipos de negocios y mercados

+Mayor productividad y facilidad de desarrollo de tareas que se benefician de la tecnología.

–Los empleos requieren cada vez más conocimiento de tecnologías.

–Personas temen ser reemplazadas o removidas por la incorporación de Sls y nuevas tecnologías que reforman los procesos.

- ➔ Sanitarios
  - ◆ Estrés ocupacional
  - ◆ Sedentarismo: deriva en problemas de salud serios y variados

- ◆ Riesgos relacionados con el equipamiento: Emisiones de impresoras, pantallas, radiofrecuencias
- ◆ Sindrome de tunel carpiano
- ◆ RSI (Lesión por estrés repetitivo)

Prevención

➔ Pantallas,cuidar:
- ◆ Reflejos
- ◆ Brillo
- ◆ Contraste

➔ Ergonomía
- ◆ Escritorios
- ◆ Sillas
- ◆ Teclados

➔ Flexibilidad: monitores y teclados

Ética y responsabilidad profesional

Conflictos éticos

★ Impacto de la información y las tecnologías en la sociedad.

★ Surgen conflictos éticos.

★ La demanda de centros de datos y procesamiento muy grandes genera consumos de energía muy grandes para operar y para refrigerarse.
- ○ Usar sistemas de administración de energía
- ○ Apagar equipos cuando no se utilizan
- ○ Diseño especial para edificios que alberguen centros de datos

★ Resguardo de la información recopilada de clientes
- ○ Uniones de redes
- ○ Intercambio de información con proveedores
- ○ Buscadores y aplicaciones basadas en internet que reciben nuestra información personal: datos de salud, laborales, económicos, etc.

★ Se contratan empresas que se encargan de la seguridad de los datos.

★ Neutralidad de la red
- ○ Formateo de paquetes
- ○ Filtrado de sitios
- ○ Identificación de IPs de origen

● Uso de tecnologías para las elecciones

Voto electrónico: Incorporación de *recursos informáticos* en *cualquier parte* del *proceso electoral,*ya sea en el registro de ciudadanos, la confección de mapas de distrito, la lógica electoral, el ejercicio del voto en sí mismo, el escrutinio y la transmisión de resultados.

➢ Comúnmente se interpreta:
- ○ Sistema informatizado para el acto de emitir y contar los votos en la mesa de votación, donde los y las ciudadanas entran en contacto directo con los dispositivos electrónicos.
- ○ Uso de computadoras, urnas electrónicas o dispositivos similares para la emisión y recuento automatizado del sufragio.

- Mecanismos de implementación (habituales)
  - Sistemas de recuento automático de votos mediante reconocimiento óptico de marcas hechas por ciudadanos en boleta.
  - Sistemas de registro electrónico directo: kioscos de votación, urnas electrónicas.
  - Sistemas de votación a distancia a través de internet.

Sistemas de recuento automático

-Marcas directas o indirectas

+Deben auditarse manualmente los resultados: maquinas *usadas,* seleccionadas al *azar, luego* del acto eleccionario

+Marcas indirectas: pierde muchas de sus ventajas

-Doble trabajo

-Susceptible de ataques

-Riesgo de pérdida de anonimato

Sistemas de registro electrónico directo

- Registran y tabulan el voto en simultáneo y mediante dispositivo informático.
- Operado por el votante mediante teclado, botonera o pantalla táctil.
- Registro: en memoria del dispositivo.
- Permite corregir y voto blanco.
- No permite: errores o invalidaciones.
- Ahorra trabajo:
  - Sin boletas a custodiar
  - Recuento inmediato y sin diferencias en repetición
- El resultado será siempre el mismo. Independientemente de que refleje la voluntad de los votantes o no.
- Intereses opuestos: ciudadanos votantes vs quienes conducen la elección

Sistemas de votación a través de internet

- Mecanismos que permiten emitir sufragio desde computadoras comunes conectadas a internet desde cualquier lugar del mundo.
- La identificación es imprescindible: para evitar que alguien vote dos veces, o en nombre de otro, o que vote quien no está habilitado.
- Es muy simple violar anonimato.

- Transparencia
  - ¿Cómo verificar el estado de la urna?
  - ¿Cómo comprender el proceso?
- Clientelismo
  - Mecanismos alternativos
- Velocidad de conteo
  - ¿Impacto de los errores?
- Economía
  - Refutado
- Participación ciudadana

- ¿Facilidad de uso?
- ¿Quiénes pueden auditar?
- ¿Cómo validar para avalar su opinión?
- ¿Impacto sobre los resultados?

➔ Otros

- Empresas privadas como proveedores
- ¿Mecanismos y permisos para auditar?

Códigos de ética

Conflictos éticos

➢ Diferentes profesionales definen códigos de ética y conducta profesional.

➢ Ej: CPCI (Consejo profesional en ciencias informáticas) Ciudad de Buenos Aires

➢ Ej: ACM (association for computing machinery)

- Define un código de ética para sus miembros
- Incluye: reglas morales generales, responsabilidades profesionales específicas, reglas para los líderes.
- Actualizado en Junio 2018

Código de ética - ACM

-Cuatro secciones

1. Consideraciones éticas fundamentales
2. Consideraciones más específicas de la conducta de un profesional
3. Individuos con rol de liderazgo
4. Principios sobre cumplimiento del código

-Principios generales:

1. ***Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la informática:*** Este principio, que concierne a la calidad de vida de todas las personas, afirma la obligación de los profesionales de la informática, tanto individual como colectivamente, de utilizar sus habilidades en beneficio de la sociedad, sus miembros y el entorno que los rodea. Esta obligación incluye promover los derechos humanos fundamentales y proteger el derecho de cada individuo a la autonomía. Un objetivo esencial de los profesionales de la informática es minimizar las consecuencias negativas de la informática, incluidas las amenazas a la salud, la seguridad, la seguridad personal y la privacidad. Cuando los intereses de múltiples grupos entran en conflicto, se debe prestar mayor atención y prioridad a las necesidades de los menos favorecidos. Los profesionales de la informática deben considerar si los resultados de sus esfuerzos respetarán la diversidad, se utilizarán de manera socialmente responsable, satisfarán las necesidades sociales y serán ampliamente accesibles. Se les anima a contribuir activamente a la sociedad participando en trabajos voluntarios o pro bono que beneficien el bien público. Además de un entorno social seguro, el bienestar humano requiere un entorno natural seguro. Por lo tanto, los profesionales de la informática deben promover la sostenibilidad ambiental tanto a nivel local como global.

2. ***Evitar el daño:*** El "daño" significa consecuencias negativas, especialmente cuando esas consecuencias son significativas e injustas. Las acciones bien intencionadas, incluidas aquellas que cumplen con las tareas asignadas, pueden provocar daños. Cuando ese daño no es intencionado, los

responsables están obligados a deshacerlo o mitigarlo en la medida de lo posible. Evitar daños comienza con una cuidadosa consideración de los posibles impactos en todos aquellos afectados por las decisiones. Cuando el daño es una parte intencional del sistema, los responsables están obligados a garantizar que el daño está éticamente justificado. En cualquier caso, asegúrese de minimizar todos los daños. Para minimizar la posibilidad de dañar a otros de forma indirecta o involuntaria, los profesionales de la informática deben seguir las mejores prácticas generalmente aceptadas, a menos que exista una razón ética convincente para hacer lo contrario. Además, se deben analizar cuidadosamente las consecuencias de la agregación de datos y las propiedades emergentes de los sistemas.

3. Ser honesto y confiable: La honestidad es un componente esencial de la confiabilidad. Un profesional de la informática debe ser transparente y proporcionar una divulgación completa de todas las capacidades, limitaciones y problemas potenciales pertinentes del sistema a las partes correspondientes. Hacer afirmaciones deliberadamente falsas o engañosas, fabricar o falsificar datos, ofrecer o aceptar sobornos y otras conductas deshonestas son violaciones del Código. Los profesionales de la informática deben ser honestos acerca de sus calificaciones y acerca de cualquier limitación en su competencia para completar una tarea. Los profesionales de la informática deben ser francos sobre cualquier circunstancia que pueda dar lugar a conflictos de intereses reales o percibidos o que tiendan a socavar la independencia de su juicio. Además, los compromisos deben cumplirse. Los profesionales de la informática no deben tergiversar las políticas o procedimientos de una organización y no deben hablar en nombre de una organización a menos que estén autorizados para hacerlo.

4. Ser justo y tomar medidas para no discriminar: Los valores de igualdad, tolerancia, respeto por los demás y justicia rigen este principio. La equidad requiere que incluso los procesos de decisión cuidadosos proporcionen alguna vía para reparar los agravios. Los profesionales de la informática deben fomentar la participación justa de todas las personas, incluidas las de los grupos subrepresentados. La discriminación perjudicial por motivos de edad, color, discapacidad, origen étnico, situación familiar, identidad de género, afiliación sindical, situación militar, nacionalidad, raza, religión o creencias, sexo, orientación sexual o cualquier otro factor inapropiado es una violación explícita de el código. El acoso, incluido el acoso sexual, la intimidación y otros abusos de poder y autoridad, es una forma de discriminación que, entre otros daños, limita el acceso justo a los espacios virtuales y físicos donde se produce dicho acoso. El uso de la información y la tecnología puede causar nuevas desigualdades o aumentar las existentes. Las tecnologías y prácticas deben ser lo más inclusivas y accesibles posible y los profesionales de la informática deben tomar medidas para evitar la creación de sistemas o tecnologías que priven de derechos u opriman a las personas. No diseñar para la inclusión y la accesibilidad puede constituir una discriminación injusta.

5. Respetar el trabajo requerido para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos: El desarrollo de nuevas ideas, invenciones, trabajos creativos y artefactos informáticos crea valor para la sociedad, y quienes realizan este esfuerzo deben esperar obtener valor de su trabajo. Por lo tanto, los profesionales de la informática deben dar crédito a los creadores de ideas, invenciones, trabajos y artefactos, y respetar los derechos de autor, las patentes, los secretos comerciales, los acuerdos de licencia y otros métodos para proteger las obras de los

autores. Tanto la costumbre como la ley reconocen que algunas excepciones al control de una obra por parte del creador son necesarias para el bien público. Los profesionales de la informática no deben oponerse indebidamente a los usos razonables de sus obras intelectuales. Los esfuerzos por ayudar a los demás aportando tiempo y energía a proyectos que ayudan a la sociedad ilustran un aspecto positivo de este principio. Dichos esfuerzos incluyen software gratuito y de código abierto y trabajos puestos en el dominio público. Los profesionales de la informática no deberían reclamar la propiedad privada de trabajos que ellos u otros hayan compartido como recursos públicos.

6. Respetar la privacidad: La responsabilidad de respetar la privacidad se aplica a los profesionales de la informática de una manera particularmente profunda. La tecnología permite recopilar, monitorear e intercambiar información personal de manera rápida, económica y, a menudo, sin el conocimiento de las personas afectadas. Por lo tanto, un profesional de la informática debe familiarizarse con las diversas definiciones y formas de privacidad y debe comprender los derechos y responsabilidades asociados con la recopilación y el uso de información personal. Los profesionales de la informática sólo deben utilizar la información personal para fines legítimos y sin vulnerar los derechos de individuos y grupos. Esto requiere tomar precauciones para evitar la reidentificación de datos anónimos o la recopilación de datos no autorizados, garantizar la exactitud de los datos, comprender su procedencia y protegerlos del acceso no autorizado y la divulgación accidental. Los profesionales de la informática deben establecer políticas y procedimientos transparentes que permitan a las personas comprender qué datos se recopilan y cómo se utilizan, dar consentimiento informado para la recopilación automática de datos y revisar, obtener, corregir inexactitudes y eliminar sus datos personales. Sólo se debe recopilar en un sistema la cantidad mínima de información personal necesaria. Los períodos de conservación y eliminación de esa información deben definirse, aplicarse y comunicarse claramente a los interesados. La información personal recopilada para un propósito específico no debe usarse para otros fines sin el consentimiento de la persona. Las colecciones de datos fusionadas pueden comprometer las características de privacidad presentes en las colecciones originales. Por lo tanto, los profesionales de la informática deben tener especial cuidado con la privacidad al fusionar recopilaciones de datos.

7. Respetar la confidencialidad: A los profesionales de la informática a menudo se les confía información confidencial, como secretos comerciales, datos de clientes, estrategias comerciales no públicas, información financiera, datos de investigación, artículos académicos previos a la publicación y solicitudes de patentes. Los profesionales de la informática deben proteger la confidencialidad excepto en los casos en que sea evidencia de la violación de la ley, de los reglamentos organizacionales o del Código. En estos casos, la naturaleza o el contenido de esa información no deben revelarse excepto a las autoridades correspondientes. Un profesional de la informática debe considerar cuidadosamente si dichas divulgaciones son consistentes con el Código.

-Responsabilidad profesionales

1) Esforzarse por alcanzar una alta calidad tanto en los procesos como en los productos del trabajo profesional: Los profesionales de la informática deberían insistir y apoyar un trabajo de alta calidad, tanto de ellos mismos como de sus colegas. Durante todo el proceso se debe respetar la dignidad de los empleadores, empleados, compañeros, clientes, usuarios y cualquier otra persona afectada directa o indirectamente por el trabajo. Los profesionales de la informática deben respetar

el derecho de los implicados a una comunicación transparente sobre el proyecto. Los profesionales deben ser conscientes de cualquier consecuencia negativa grave que afecte a cualquier parte interesada y que pueda resultar de un trabajo de mala calidad y deben resistir los incentivos para descuidar esta responsabilidad.

2) Mantener altos estándares de competencia profesional, conducta y práctica ética: La informática de alta calidad depende de individuos y equipos que asuman la responsabilidad personal y grupal de adquirir y mantener la competencia profesional. La competencia profesional comienza con el conocimiento técnico y con la conciencia del contexto social en el que se puede desarrollar su trabajo. La competencia profesional también requiere habilidad en comunicación, análisis reflexivo y reconocimiento y gestión de desafíos éticos. La mejora de las habilidades debe ser un proceso continuo y puede incluir estudio independiente, asistencia a conferencias o seminarios y otros tipos de educación formal o informal. Las organizaciones profesionales y los empleadores deberían fomentar y facilitar estas actividades.

3) Conocer y respetar las normas vigentes en materia de trabajo profesional: Las "reglas" aquí incluyen leyes y regulaciones locales, regionales, nacionales e internacionales, así como cualquier política y procedimiento de las organizaciones a las que pertenece el profesional. Los profesionales de la informática deben respetar estas reglas a menos que exista una justificación ética convincente para hacer lo contrario. Las normas que se consideren poco éticas deben cuestionarse. Una norma puede ser poco ética cuando tiene una base moral inadecuada o causa un daño reconocible. Un profesional de la informática debería considerar desafiar la regla a través de los canales existentes antes de violarla. Un profesional de la informática que decide violar una regla porque no es ética, o por cualquier otro motivo, debe considerar las posibles consecuencias y aceptar la responsabilidad de esa acción.

4) Aceptar y proporcionar una revisión profesional adecuada: El trabajo profesional de alta calidad en informática depende de la revisión profesional en todas las etapas. Siempre que sea apropiado, los profesionales de la informática deben buscar y utilizar la revisión de pares y partes interesadas. Los profesionales de la informática también deberían proporcionar revisiones constructivas y críticas del trabajo de otros.

5) Realizar evaluaciones integrales y exhaustivas de los sistemas informáticos y sus impactos, incluyendo análisis de posibles riesgos: Los profesionales de la informática se encuentran en una posición de confianza y, por lo tanto, tienen la responsabilidad especial de proporcionar evaluaciones y testimonios objetivos y creíbles a empleadores, empleados, clientes, usuarios y al público. Los profesionales de la informática deben esforzarse por ser perspicaces, minuciosos y objetivos al evaluar, recomendar y presentar descripciones y alternativas de sistemas. Se debe tener especial cuidado para identificar y mitigar los riesgos potenciales en los sistemas de aprendizaje automático. Un sistema para el cual los riesgos futuros no se pueden predecir de manera confiable requiere una reevaluación frecuente del riesgo a medida que el sistema evoluciona en su uso, o no debería implementarse. Cualquier problema que pueda generar un riesgo importante debe informarse a las partes correspondientes.

6) Realizar trabajos únicamente en áreas de competencia: Un profesional de la informática es responsable de evaluar posibles asignaciones de trabajo. Esto incluye evaluar la viabilidad y conveniencia del trabajo y emitir un juicio sobre si la asignación de trabajo está dentro de las áreas

de competencia del profesional. Si en cualquier momento antes o durante la asignación de trabajo el profesional identifica una falta de experiencia necesaria, debe informar al empleador o cliente. El cliente o empleador puede decidir realizar la tarea con el profesional después de un tiempo adicional para adquirir las competencias necesarias, realizar la tarea con otra persona que tenga la experiencia requerida o renunciar a la tarea. El juicio ético de un profesional de la informática debe ser la guía final para decidir si trabajar en la tarea.

7) Fomentar la conciencia pública y la comprensión de la informática, las tecnologías relacionadas y sus consecuencias: Según sea apropiado para el contexto y las habilidades de cada uno, los profesionales de la informática deben compartir conocimientos técnicos con el público, fomentar la conciencia sobre la informática y fomentar la comprensión de la informática. Estas comunicaciones con el público deben ser claras, respetuosas y acogedoras. Entre las cuestiones importantes se incluyen los impactos de los sistemas informáticos, sus limitaciones, sus vulnerabilidades y las oportunidades que presentan. Además, un profesional de la informática debe abordar con respeto la información inexacta o engañosa relacionada con la informática.

8) Acceder a recursos informáticos y de comunicación sólo cuando esté autorizado o cuando sea obligado por el bien público: Las personas y las organizaciones tienen derecho a restringir el acceso a sus sistemas y datos siempre que las restricciones sean coherentes con otros principios del Código. En consecuencia, los profesionales de la informática no deben acceder al sistema informático, software o datos de otra persona sin una creencia razonable de que dicha acción estaría autorizada o una creencia convincente de que es consistente con el bien público. Que un sistema sea de acceso público no es motivo suficiente por sí solo para implicar autorización. En circunstancias excepcionales, un profesional de la informática puede utilizar el acceso no autorizado para interrumpir o inhibir el funcionamiento de sistemas maliciosos; En estos casos se deben tomar precauciones extraordinarias para evitar daños a otros.

9) Diseñar e implementar sistemas que sean robustos y usablemente seguros: Las violaciones de la seguridad informática causan daños. Una seguridad sólida debe ser una consideración primordial al diseñar e implementar sistemas. Los profesionales de la informática deben realizar la debida diligencia para garantizar que el sistema funcione según lo previsto y tomar las medidas adecuadas para proteger los recursos contra el mal uso, modificación y denegación de servicio accidentales e intencionales. Como las amenazas pueden surgir y cambiar después de implementar un sistema, los profesionales de la informática deben integrar técnicas y políticas de mitigación, como monitoreo, parches e informes de vulnerabilidad. Los profesionales de la informática también deben tomar medidas para garantizar que las partes afectadas por las violaciones de datos sean notificadas de manera oportuna y clara, brindándoles orientación y remediación adecuadas. Para garantizar que el sistema logre su propósito previsto, las funciones de seguridad deben diseñarse para que sean lo más intuitivas y fáciles de usar posible. Los profesionales de la informática deben desalentar las precauciones de seguridad que sean demasiado confusas, inapropiadas para la situación o que de otro modo inhiban el uso legítimo. En los casos en que el mal uso o el daño sean predecibles o inevitables, la mejor opción puede ser no implementar el sistema.

★ Derecho civil - Ejs: Digitalización de documentos y actos. Nombres de dominio. Propiedad intelectual. Contratos. Correo electrónico.
★ Derecho comercial-Ejs: Marcas y patentes
★ Derecho penal- Nuevos delitos
★ Derecho constitucional- Datos personales. Manipulación y privacidad.
★ Derecho laboral- Nuevas modalidades de trabajo.

Propiedad intelectual

➔ Ley 11.723 - Régimen legal de la propiedad intelectual (1933)
➔ Ley 25.036 - Propiedad intelectual (1998)
- ◆ Se modifican los artículos 1º, 4º, 9º y 57º
- ◆ Se incorpora el artículo 55 bis

Artículo 1º:

-(…) las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, *entre ellos los programas de computación fuente y objeto*; las compilaciones de datos o de otros materiales; (…) en fin, toda producción científica, literaria, artística o didáctica, *sea cual fuere el procedimiento de reproducción.*

-La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.

Artículo 4º:

-Son titulares del derecho de propiedad intelectual:

A. El autor de la obra
B. Sus herederos o derechohabientes
C. Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.
D. Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

Artículo 9º:

-Nadie tiene derecho a publicar, sin **permiso de los autores** o de sus derechohabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición públicas o privadas.

-Quien haya recibido de los autores o de sus derecho-habientes 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**, con indicación del **licenciado que realizó la copia y la fecha de la misma.** La copia de salvaguardia **no podrá ser utilizada para otra finalidad** que la de reemplazar el ejemplo original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

Artículo 55º bis:

-55 bis: La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencias para su uso o reproducción.

Artículo 57º:

-En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el artículo 1°, tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de cien ejemplares, bastará con depositar un ejemplar. (…). Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación.

Penas

a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes

b) El que falsifique obras intelectuales (…)

c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto

d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados.

¿Por qué registrar software?

➔ **Seguridad:** Certeza de su existencia en determinada fecha

➔ **Prueba de Autoría:** Presunción de autoría otorgada por el Estado, con fecha cierta

➔ **Elemento de comparación:** En supuestos de plagio y piratería. En esos supuestos, la obra es remitida al Poder Judicial para su valoración.

➔ **Protección del Usuario de buena fe:** Se presume autor de la Obra el que figura como tal en el certificado de registro, salvo prueba en contrario.

➔ **Publicidad de las obras y contratos registrados:** Función primordial de un registro es dar a conocer su contenido.

-Tres formas de registrar software en Propiedad intelectual:

+Obras inéditas: autores o titulares utilizan solamente en forma personal o dentro de una empresa

+Obra publicada: puesta en conocimiento público (venta, regalo, donación, distribución gratuita)

+Contratos de software: licencias de uso y otros

Obras inéditas

Para llevar adelante el trámite se deberá:

1. Completar los Datos del Trámite.
2. Subir la siguiente documentación obligatoria:
   -Comprobante de Pago del Trámite (Valor: $ 900).
3. Subir la siguiente documentación complementaria:
   -Si es autor fallecido, certificado de defunción.
   -Si el autor es menor de edad, documentación que acredite vínculo con el solicitante y constancia de CUIL o CDI (en caso de ser extranjero) del menor.
   -Si el solicitante no es participante de la obra, deberá estar apoderado a través de la plataforma TAD.

Obras publicadas

Puede realizarlo el autor, el titular o quienes ellos designen. Para llevar adelante el trámite se deberá:

1. Completar los Datos del Trámite

2. Subir la siguiente documentación obligatoria:

-Comprobante de Pago del trámite (Valor del trámite $ 2500).

-Comprobante de pago de Tasa (0.2% del costo del ejemplar con un mínimo de 4,11).

Si optó por presentación física, al finalizar, se otorgará un número de Expediente Electrónico (carátula del expediente), el cual deberá presentarse junto con una copia de la obra (CÓDIGO EJECUTABLE) en la Dirección Nacional del Derecho de Autor. Si optó por la opción digital, una vez iniciado el expediente recibirá una comunicación en la cual se detallará el procedimiento para la carga digital de la obra. (...) el solicitante podrá presentar el código fuente de las obras publicadas de software de modo cifrado o encriptado, siendo responsable el titular de proveer las herramientas necesarias en caso que dicho código tenga que ser descifrado o desencriptado, a requerimiento de cualquier autoridad legitimada.

Inscripción de contratos

Para iniciar el trámite resulta necesario:

1. Completar el formulario.
2. Agregar al trámite (subir) la siguiente documentación:
   a. Contrato a inscribirse.
   b. Comprobante de pago del trámite.

   (...) el pago del trámite deberá efectuarse del siguiente modo:

   IV) Contratos cuyo objeto se vincule a obras multimedia, páginas web, software y videojuegos. Efectuar el depósito o transferencia en la cuenta del FONDO COOPERADOR (LEY 23.412) DNDA-CESSI (...) por la suma de pesos tres mil ($3000.-).

   c. Comprobante de pago de la tasa legal mediante depósito o transferencia bancaria a la cuenta del FONDO NACIONAL DE LAS ARTES (...) El cálculo del monto a pagar se efectúa del siguiente modo:

   I) Contratos con monto determinado o determinable: Se abona el uno por ciento (1%) del monto, con una tasa mínima de cuatro pesos con once centavos ($4,11).

   II) Contratos con monto indeterminado: Se abona una tasa fija de seis pesos con diecisiete centavos ($6,17).

   III) Contratos con monto en parte indeterminada y en parte determinada o determinable: Se abona el uno por ciento (1%) del monto de la parte determinada o determinable, con una tasa mínima de cuatro pesos con once centavos ($4,11).

   IV) Contratos gratuitos: Se abona una tasa fija de seis pesos con diecisiete centavos ($6,17).

   d. En caso de corresponder, copia de la documentación que acredite la personería invocada por apoderados o autorizados que actúen en representación de una persona humana o jurídica, o copia de la constancia de haber presentado la mencionada documentación ante el Registro Único de Apoderados de la D.N.D.A.

   El trámite se realiza íntegramente en línea, no siendo necesaria su concurrencia a la DNDA. Por ello, una vez presentada en debida forma la documentación indicada y luego de efectuadas las verificaciones administrativas del caso, se le remitirá la constancia de inscripción del contrato y de ese modo finaliza el trámite.

Protección de datos personales

➢ Ley 25.326 - Protección de los datos personales (2000).

➢ Modificada y/o complementada por numerosas normas y decretos.

Protección de los datos personales

★ Artículo 43, Constitución Nacional. -(Habeas data)

1. Toda persona puede interponer acción expedita y rápida de amparo, (...) contra todo acto u omisión de autoridades públicas o de particulares, que (…) lesione, restrinja, altere o amenace, (…) derechos y garantías (…).

3. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en (…) y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

★ Artículo 1 (Objeto) - La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

★ Artículo 2 (Definiciones)

- **Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- **Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- **Archivo, registro, base o banco de datos:** Designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
- **Tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- **Responsable de archivo, registro, base o banco de datos:** Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, (…).
- **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
- **Titular de los datos:** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
- **Usuario de datos:** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- **Disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

★ Artículo 5 (Consentimiento) - El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

★ Artículo 6 (Información a los titulares)- Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a. La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.

b. La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.

c. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente.

d. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.

e. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

★ Artículo 8 (Datos relativos a la salud y religiosos): Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

★ Artículo 9 (Seguridad de los datos):

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

★ Artículo 10 (Deber de confidencialidad):

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

★ La acción de protección de los datos personales o de hábeas data procederá:

a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos

b) En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

Firma digital

➔ Ley 25.506 (2001): "Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control."

➔ La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma

➔ Artículo 9- Validez.

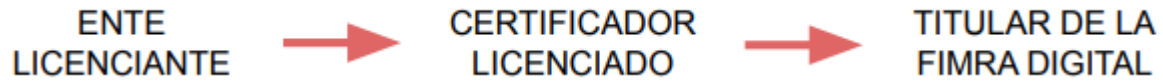
Es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante.

b) Ser debidamente verificada la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente.

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

➔ Artículo 17 - Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.



¿Cómo se obtiene?

➔ Se inicia trámite de registro mediante el certificador

Ejs: afip – anses - box custodia de archivos s.a. -digilogix s.a. - encode s.a. - lakaut s.a. - oficina nacional de tecnologías de información (onti) -tecnología de valores s.a. - ministerio de modernización

➔ Se presenta físicamente ante el certificador licenciado para constatar identidad

Delitos informáticos

❖ Ley 26.388 – Código penal (2008)

❖ Delitos informáticos contra:

- ➢ La integridad sexual.
- ➢ La libertad
- ➢ La propiedad
- ➢ La seguridad pública
- ➢ La administración pública

❖ Artículo 1 - Incorpórase como últimos párrafos del artículo 77 del Código Penal, los siguientes:

- ➢ El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- ➢ Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- ➢ Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

- Artículo 131 (2013)
  - Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.
  - Sanciona las siguientes conductas:
    - Producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir cualquier representación de una persona menor de 18 años dedicada a actividades sexuales explícitas o de sus partes genitales.
    - Tener representaciones de personas menores de edad de actividades sexuales explícitas o de sus partes genitales para distribuirlas o comercializarlas.
- Artículo 153
  - Será reprimido con prisión de 15 días a 6 meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, (…) aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
- Artículo 153 bis
  - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
  - La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
- Artículo 173 - se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
  - Inciso 15: El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.
  - Inciso 16: El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
- Artículo 183:
  - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.

➢ (Se agrega) En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujera en un sistema informático, cualquier programa destinado a causar daños.

Aspectos legales - Teletrabajo

- Resolución 1552/2012 - Teletrabajo. Definición. Condiciones.
  - "Una manera de organizar y realizar el trabajo a distancia con el uso de la tecnologías de la información y comunicación (TICS) en el domicilio del trabajador o en un lugar o establecimiento ajeno al empleador"
  - Notificar ART
  - Proveer elementos: silla, extintor, botiquín, manual
- Resolución 595/2013 – Programa de promoción del empleo en teletrabajo (PROPET)
  - Proyecto de ley 2007 + Resolución 2012

Teletrabajo – A favor

- Mejora la calidad de vida.
- Ahorra dinero y tiempo de traslado.
- Facilita la inserción de grupos vulnerables.
- Mayor tiempo para otras actividades extra laborales.
- Opción para evitar la excedencia y acompañar a la mujer durante la lactancia. Y para padres con hijos pequeños o personas que deben estar más tiempo en sus hogares.
- Alternativa ante situaciones de catástrofes naturales o pandemias.

- A nivel urbano. Aspectos positivos:
  - Cuidado del medio ambiente
  - Facilita la disminución del tránsito vehicular generando un ahorro de combustible
  - Incide en la reducción de los accidentes vehiculares

Teletrabajo – En contra

- Precariza
- Aísla: dificulta y limita relaciones interpersonales
- Provoca mayor estrés
- Extiende el tiempo de trabajo
- Ocasiona mayores gastos al trabajador
- Disminuye la productividad del trabajo
- Patrimonio exclusivo del Sector Privado

Resolución 21/2020

★ Artículo 1º – Establécese que los empleadores que habiliten a sus trabajadores a realizar su prestación laboral desde su domicilio particular en el marco de la emergencia sanitaria (…) deberán denunciar a la (…) (A.R.T.) a la que estuvieran afiliados, el siguiente detalle:

- Nómina de trabajadores afectados (Apellido, Nombre y C.U.I.L.).
- Domicilio donde se desempeñará la tarea y frecuencia de la misma (cantidad de días y horas por semana).
- El domicilio denunciado será considerado como ámbito laboral a todos los efectos de la Ley N° 24.557 sobre Riesgos del Trabajo.

★ Artículo 2º – Establécese que la Resolución (…) N° 1.552 (...) 2012 no resulta aplicable a los supuestos de excepción previstos en el artículo 1° de la presente.

Ley 27555 - año 2020

Régimen legal del contrato de teletrabajo

- ➢ Igualdad de derechos
- ➢ Combinación presencialidad / teletrabajo
- ➢ Jornada laboral
  - ○ Establecida por escrito
  - ○ Plataformas de control
  - ○ Derechos a la desconexión digital
- ➢ Tareas de cuidado
- ➢ Voluntariedad + Reversibilidad
- ➢ Elementos de trabajo
- ➢ Compensación de gastos
- ➢ Capacitación
- ➢ Sistemas de control y derechos a la intimidad. Protección de la información laboral

Entrada en vigencia: luego de 90 días contados a partir de que se determina la finalización del período de vigencia del aislamiento social, preventivo y obligatorio.

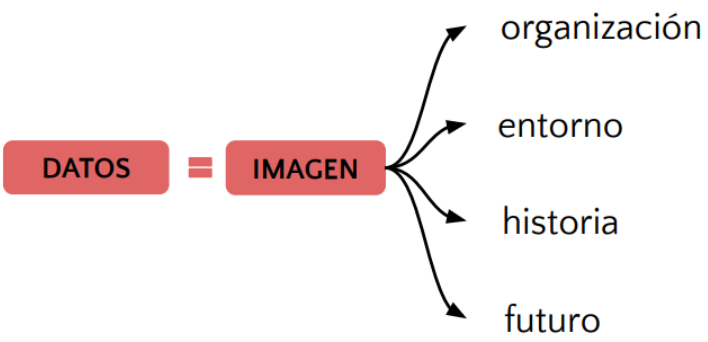
Auditoría de sistemas de información

Razones para auditar

Organizaciones: Una organización debe controlar y auditar los sistemas de información basados en ordenadores porque los costes de los errores e irregularidades que surgen en estos sistemas pueden ser elevados. La capacidad de supervivencia de una organización puede verse gravemente socavada por la corrupción o destrucción de su base de datos; los errores en la toma de decisiones causados por sistemas de información de mala calidad; las pérdidas ocasionadas por el uso indebido de los ordenadores; la pérdida de valiosos equipos y programas informáticos y de personal; los elevados costes de algunos tipos de errores informáticos, la falta de mantenimiento de la privacidad de las personas individuales y la falta de control sobre la forma en que se utilizan los ordenadores dentro de la organización.

Costos por pérdida de datos

Los datos constituyen un recurso crítico necesario para la continuidad de las operaciones de una organización. En este sentido, Everest (1985) propone que los datos proporcionan a la organización una imagen de sí misma, de su entorno, de su historia y de su futuro. Si esta imagen es precisa, la organización aumenta sus capacidades para adaptarse y sobrevivir en un entorno cambiante. Si esta imagen es inexacta o se pierde, la organización puede incurrir en pérdidas sustanciales. Estas pérdidas pueden producirse cuando los controles existentes sobre los ordenadores son laxos. Por ejemplo, la dirección puede no hacer copias de seguridad adecuadas de los archivos informáticos. Así, la pérdida de un archivo por un error del programa informático, sabotaje o desastre natural significa que el archivo no puede recuperarse y, por lo tanto, la continuidad de las operaciones de la organización se ve perjudicada.



Errores en toma de decisiones

La toma de decisiones de alta calidad depende en parte de la calidad de los datos y de la calidad de las reglas de decisión que existen en los sistemas de información informatizados. Veamos la importancia de ambos aspectos.

La importancia de disponer de datos precisos en un sistema informático depende de los tipos de decisiones que toman las personas que tienen algún interés en una organización. Por ejemplo, si los directivos toman decisiones de planificación estratégica, probablemente tolerarán algunos errores en los datos, dada la naturaleza a largo plazo de las decisiones de planificación estratégica y la incertidumbre inherente a este tipo de decisiones. Sin embargo, si los directivos toman decisiones de control de gestión y de control operativo, probablemente exigirán datos muy precisos. Este tipo de decisiones implican la detección, investigación y corrección de procesos fuera de control. Por lo tanto, los datos inexactos pueden hacer que se emprendan investigaciones costosas e innecesarias o que no se detecten procesos fuera de control. Además de la gestión, los datos incorrectos también pueden repercutir en otras partes interesadas en una organización.

La importancia de contar con reglas de decisión precisas en un sistema informático también depende de los tipos de decisiones que tomen las personas que tienen algún interés en una organización. En algunos casos, una regla de decisión incorrecta puede tener consecuencias menores. Por ejemplo, puede ocurrir un pequeño error sin consecuencias en el cálculo de la depreciación de un activo de poco valor. En otros casos, sin embargo, las consecuencias pueden ser importantes. Por ejemplo, si el algoritmo que determina el tipo de interés que debe pagarse a los clientes de un banco es incorrecto, el banco podría realizar importantes pagos en exceso a sus clientes. Podría no ser capaz de recuperar este dinero sin pérdidas sustanciales de fondo de comercio. Del mismo modo, si una regla de decisión de un sistema experto de apoyo al diagnóstico

médico es incorrecta, los médicos podrían prescribir tratamientos inadecuados a los pacientes, algunos de los cuales podrían ser mortales.

Costos por abusos computacionales

Cualquier incidente asociado con tecnología de computadoras en el que una **víctima** sufre o puede haber sufrido una **pérdida** y que un **perpetrador** con intención obtuvo o puede haber obtenido una **ganancia.**

- ★ Tipos de abuso:
  - Hackeo
  - Virus
  - Acceso físico ilegal
  - Abuso de privilegios

El abuso informático puede acarrear los siguientes tipos de consecuencias:

- ★ Destrucción
- ★ Hurto
- ★ Modificación
- ★ Violaciones de privacidad
- ★ Daño físico al personal
- ★ Uso no autorizado
- ★ Interrupción de operaciones

Valor del HW, SW y el personal

- ➢ Recursos de la organización
  - Hardware - Grandes inversiones
  - Software - Destrucción, corrupción, robo (al igual que el hw)
    - Impedir funcionamiento
    - Generar pérdidas
    - Exponer datos confidenciales
  - Personal - Recurso muy valioso de la organización

Costos de errores computacionales

- ❖ Control y automatización de múltiples tareas
  - ➢ Daños ambientales
  - ➢ Pérdidas de vidas
  - ➢ Pérdidas financieras
  - ➢ Conflictos en transporte
  - ➢ Fallas en producción
  - ➢ Etc.

Mantenimiento de la privacidad

- Acumulación de información
- Poder de procesamiento de datos
  - Integración
  - Consulta
- Preocupaciones
  - Interconexión de bases de datos y motores de búsqueda

- Bancos de datos genéticos

Evolución controlada del uso

★ Utilización de computadoras:
- Controlando armas
- Efectos en la salud mental y física
- Para realizar trabajos originalmente “humanos”

Auditoría de SI

La auditoría de sistemas de información es el proceso de recopilación y evaluación de evidencia para determinar si un sistema informático salvaguarda los activos, mantiene la integridad de los datos, permite alcanzar los objetivos organizacionales de manera efectiva y utiliza los recursos de manera eficiente. Por lo tanto, la auditoría de sistemas de información apoya los objetivos de auditoría tradicionales: objetivos de certificación (los del auditor externo) que se centran en la salvaguardia de los activos y la integridad de los datos, y objetivos de gestión (los del auditor interno) que abarcan no solo objetivos de certificación sino también objetivos de eficacia y eficiencia. A veces, la auditoría de sistemas de información tiene otro objetivo, es decir, garantizar que una organización cumpla con alguna regulación, regla o condición.

Salvaguarda de activos

Los activos del sistema de información de una organización incluyen hardware, software, instalaciones, personas (conocimiento), archivos de datos, documentación del sistema y suministros. Como todos los activos, deben estar protegidos por un sistema de control interno. El hardware puede dañarse de forma maliciosa. Software propietario y concentrado en una o una pequeña cantidad de ubicaciones, como un solo disco. Como resultado, la salvaguardia de activos se convierte en un objetivo especialmente importante que muchas organizaciones deben alcanzar.

Integridad de los datos

La integridad de los datos es un concepto fundamental en la auditoría de sistemas de información. Es un estado que implica que los datos tienen ciertos atributos: integridad, solidez, pureza y veracidad. Si no se mantiene la integridad de los datos, una organización ya no tiene una verdadera representación de sí misma o de sus eventos. Además, si la integridad de los datos de una organización es baja, podría sufrir una pérdida de ventaja competitiva. Sin embargo, mantener la integridad de los datos sólo puede lograrse a un costo. Los beneficios obtenidos deberían superar los costos de los procedimientos de control necesarios. Tres factores principales afectan el valor de un elemento de datos para una organización y, por lo tanto, la importancia de mantener la integridad de ese elemento de datos:

1. *El valor del contenido informativo de un elemento de datos para los tomadores de decisiones individuales:* El contenido informativo de un elemento de datos depende de su capacidad para cambiar el nivel de incertidumbre que rodea una decisión y, como resultado, de cambiar los beneficios esperados de la misma. decisiones que pudieran tomarse. Estas nociones han sido bien desarrolladas dentro de la teoría de la decisión estadística.

2. *El grado en que los datos se comparten entre los tomadores de decisiones:* si los datos se comparten, la corrupción de la integridad de los datos afecta no sólo a un usuario sino a muchos. El valor de un elemento de datos es una función agregada del valor del elemento de datos para los usuarios individuales del elemento de datos. Por tanto, el mantenimiento de la integridad de los datos se vuelve más crítico en un entorno de datos compartidos.
3. *El valor del dato para los competidores:* si un dato es valioso para un competidor, su pérdida podría socavar la posición de una organización en el mercado. Los competidores podrían explotar el contenido informativo del dato para reducir la rentabilidad de la organización y provocar la quiebra, liquidación, adquisición o fusión.

Efectividad del sistema

Un sistema de información eficaz logra sus objetivos. Evaluar la eficacia implica conocer las necesidades de los usuarios. Para evaluar si un sistema reporta información de una manera que facilite la toma de decisiones por parte de sus usuarios, los auditores deben conocer las características de los usuarios y el entorno de toma de decisiones. La auditoría de eficacia suele ocurrir después de que un sistema ha estado funcionando durante algún tiempo. La gerencia solicita una auditoría posterior para determinar si el sistema está logrando los objetivos establecidos. Esta evaluación proporciona información para la decisión sobre si desechar el sistema, continuar ejecutándolo o modificarlo de alguna manera. La auditoría de eficacia también se puede realizar durante las etapas de diseño de un sistema. Los usuarios suelen tener dificultades para identificar o ponerse de acuerdo sobre sus necesidades. Además, a menudo se producen importantes problemas de comunicación entre los diseñadores de sistemas y los usuarios. Si un sistema es complejo y costoso de implementar, la gerencia podría querer que los auditores realicen una evaluación independiente para determinar si es probable que el diseño satisfaga las necesidades del usuario.

Un sistema de información eficiente utiliza recursos mínimos para lograr los objetivos requeridos. Los sistemas de información consumen diversos recursos: tiempo de máquina, periféricos, software del sistema y mano de obra. Estos recursos son escasos y diferentes sistemas de aplicación suelen competir por su uso. La pregunta de si un sistema de información es eficiente a menudo no tiene una respuesta clara. La eficiencia de cualquier sistema en particular no puede considerarse aislada de otros sistemas. Los problemas de suboptimización ocurren si un sistema se "optimiza" a expensas de otros sistemas. La eficiencia del sistema se vuelve especialmente importante cuando una computadora ya no tiene exceso de capacidad. El rendimiento de los sistemas de aplicaciones individuales se degrada y los usuarios pueden sentirse cada vez más frustrados. Luego, la gerencia debe decidir si se puede mejorar la eficiencia o se deben comprar recursos adicionales. Debido a que el hardware y el software adicionales son una cuestión de costos, la administración necesita saber si la capacidad disponible se ha agotado porque los sistemas de aplicaciones individuales son ineficientes o porque las asignaciones existentes de recursos informáticos están causando cuellos de botella. Debido a que se percibe que los auditores son independientes, la gerencia podría pedirles que ayuden o incluso realicen esta evaluación.

Controles internos

Para conseguir objetivos se establece sistema de controles internos:

1) Separación de tareas

- ★ Iniciar y registrar transacciones, custodiar activos

- Previene errores
- Detecta errores e irregularidades

★ En sistema

- Determinar correctitud de funcionamiento
- Separar funciones: ejecutar software y realizarle cambios

2) *Delegación de autoridad y responsabilidades*

★ Delegar

- Autoridad
- Responsabilidades

★ Se dificulta cuando el objetivo es compartir para evitar redundancias. Ej: bases de datos.

3) *Reclutamiento y entrenamiento de personal*

★ Poder y responsabilidad depositados en personal responsable de los sistemas se incrementa

★ Dificultades

- Evaluar
- Conservar
- Conseguir personal capacitado

4) *Sistema de autorizaciones*

★ Autorizaciones para procedimientos se automatizan

- Evaluar trabajo de empleados
- Evaluar procesamiento del sistema

★ Se debe controlar si el nivel de permisos otorgado es consistente con la autoridad que se desea asignar

5) *Documentos y registros adecuados*

★ Garantizar traza de actividades

- Mínimamente equivalente a la que habría en papel o sistema manual
- En sistemas bien diseñados suele ser aún mayor

★ Registro de actividades: bitácora o "log"

6) *Control físico sobre los recursos*

★ La centralización de datos lo hace más complejo: acceso al sistema brinda mayor acceso a datos

★ Consecuencias de la pérdidas son mayores frente a cualquier eventualidad

7) *Supervisión gerencial*

★ Empleados más cerca de los clientes. más lejos de los supervisores

★ Manos visibilidad y mayores dificultades para ejercer controles

- Embeber controles en los sistemas

8) *Chequeos independientes de performance*

★ Olvidos

★ Errores

★ Descuidos

★ Intencionalidad

★ Al automatizar procesos el chequeo independiente pierde sentido.

★ Controlar correctitud de código, controles para el desarrollo. modificación, operación y mantenimiento.

9) Comparar registros con activos

★ Datos y activos que los datos supuestamente representan deben contrastarse
  - Inexactitudes
  - Incompletitudes

★ Se debe controlar el código y los procesos para manipularlo

Cambios en la auditoría

❖ Recolección de evidencia
  - ➢ Confiabilidad del sistema manual vs computacional
  - ➢ Evolución de las tecnologías

❖ Evaluación de evidencia
  - ➢ Dificultad para la trazabilidad de errores
  - ➢ Errores estocásticos vs dererministicos