
1

## GESTIÓN DE LA FUNCIÓN DE AUDITORÍA DE SISTEMAS

ESCUELA DE COMERCIO
PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

- La función de auditoría debe ser:
  - Gestionada
  - Conducida
- Lo anterior en razón a que se cumpla el objetivo de la auditoría de sistemas.
- La optimización de los recursos y el logro de los objetivos de la empresa deben garantizarse a la alta dirección.

2

2

# ORGANIZACIÓN DE LA FUNCIÓN DE AUDITORÍA DE SISTEMAS

Auditoría **interna**
(estatuto de auditoría)

Auditoría **externa**
(contrato formal)

Alta dirección

3

3

# ORGANIZACIÓN DE LA FUNCIÓN DE AUDITORÍA DE SISTEMAS

- El estatuto de auditoría debe:
  - Establecer claramente la responsabilidad
  - Los objetivos de la gerencia para la función de auditoría
  - Delegación de autoridades
- Considerando:
  - Autoridad
  - Alcance
  - Responsabilidades

4

4

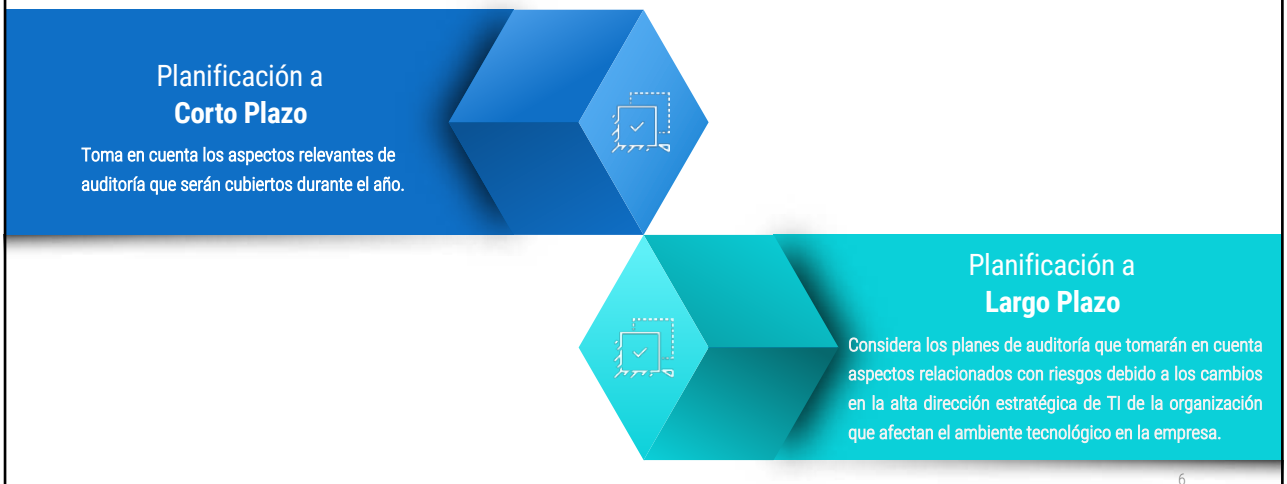
# GESTIÓN DE LOS RECURSOS DE AUDITORÍA DE SISTEMAS

- Los estándares de auditoría de SI de la Information Systems Audit and Control Association (ISACA) requieren que el auditor sea técnicamente competente y que posea las habilidades y conocimientos para diseñar y ejecutar la auditoría.
- La empresa debe contar con un plan anual detallado de capacitación basado en la dirección de la organización centrados en tocologías y riesgos.

5

5

# PLANIFICACIÓN DE LA AUDITORÍA




6

6

## RIESGOS

- Los riesgos deben medirse de forma cualitativa y cuantitativa, en base al efecto que tienen dentro de la empresa.
- La clasificación:
  - Alto: consecuencias de daño a reputación sobre 6 meses para remediar.
  - Medio: entre 3 a 6 meses
  - Bajo: Menos de 3 meses

7

7

## ASIGNACIÓN DE AUDITORÍA INDIVIDUAL

- Al auditor de sistemas de información debe entender que otras consideraciones, como por ejemplo los resultados de las evaluaciones periódicas de riesgos, los caminos en la aplicación de la tecnología, la evaluación de los aspectos de privacidad y los requerimientos regulatorios pueden afectar el enfoque general de la auditoría.

8

8

## PASOS PARA REALIZAR UNA PLANIFICACIÓN DE AUDITORÍA

- Para realizar la planificación de una auditoría, el auditor de sistemas de información debe seguir los pasos que se indican:
  - Lograr una comprensión de la misión, los objetivos y el propósito u los procesos del negocio, incluyendo los requerimientos de información y procesamiento, tales como disponibilidad, integridad, seguridad y tecnología del negocio y la confidencialidad de información.
  - Revisar los papeles de trabajo anteriores.
  - Entender los cambios en el entorno de negocios del auditado. →

9

9

## PASOS PARA REALIZAR UNA PLANIFICACIÓN DE AUDITORÍA

  - Identificar los contenidos específicos tales como políticas, estándares y directrices requeridos, procedimientos y estructura de la organización.
  - Realizar un análisis de riesgos para ayudar a diseñar el plan de auditoría.
  - Establecer el alcance y los objetivos de la auditoría.
  - Desarrollar el enfoque de la auditoría o estrategia de la auditoría.
  - Asignar recursos humanos a la auditoría.
  - Dirigir la logística del trabajo de auditoría.

10

10

## EFECTOS DE LAS LEYES Y REGULACIONES EN LA PLANIFICACIÓN DE UNA AUDITORÍA DE SISTEMAS

- Debido a la dependencia cada vez mayor de los sistemas de información, los países buscan incluir en las regulaciones:
  - Establecimiento de requerimientos regulatorios.
  - Responsabilidades asignadas a las entidades correspondientes.
  - Funciones de auditoría financiera, operativa y de TI.

11

11

## PASOS PARA DETERMINAR CUMPLIMIENTO EXTERNO

Identificar los requerimientos gubernamentales.

Documentar las leyes y regulaciones aplicables.

Determinar si la gerencia y auditoría han tomado en cuenta las leyes.

Revisar los documentos internos que consideran el cumplimiento de la ley.

Determinar los procedimientos que se ocupan del cumplimiento.

Revisar contratos externos para verificar el cumplimiento de estos requisitos.

12

12

## ESTÁNDARES Y DIRECTRICES DE AUDITORÍA Y ASEGURAMIENTO DE SISTEMAS DE ISACA

- La **Information Systems Audit and Control Association** (ISACA) define una serie de directrices para asegurar la continuidad y la correcta auditoría de sistemas de información dentro de la empresa.
- Estándar de auditoria y aseguramiento de SI 1201

13

13

## CÓDIGO DE ÉTICA PROFESIONAL DE ISACA

- Respaldar la implementación y promover el cumplimiento de los estándares, procedimientos y controles.
- Realizar sus funciones con objetividad, diligencia y celo profesional.
- Servir en beneficio de las partes interesadas de un modo legal y honesto.
- Mantener la privacidad y confidencialidad de la información obtenida.

14

14

## CÓDIGO DE ÉTICA PROFESIONAL DE ISACA

- Mantener la competencia en el campo y las responsabilidades profesionales.
- Informar a las partes los resultados de los trabajos realizados.
- Apoyar la formación para mejorar la seguridad y control de SI.
  - Código de ética profesional de ISACA

15

15

## MARCO GENERAL DE LOS ESTÁNDARES DE AUDITORÍA

- Los objetivos de los estándares de auditoría y aseguramiento de la calidad son informar:
  - A los auditores sobre el nivel mínimo requerido de desempeño aceptable para cumplir con las responsabilidades.
  - A la gerencia sobre las expectativas de la profesión.
  - Los titulares de certificación sobre la investigación de a los auditores.

16

16

## ESTÁNDARES DE AUDITORÍA

- Los estándares de auditoría y aseguramiento de sistemas de información aplicables a auditoría de sistemas son:
- General:
  - 1001 – Estatuto de la función de auditoría.
  - 1002 – Independencia organizacional.
  - 1003 – Independencia profesional.
  - 1004 – Expectativa razonable.
  - 1005 – Debido cuidado profesional

17

17

## ESTÁNDARES DE AUDITORÍA

  - 1005 – Debido cuidado profesional
  - 1006 – Competencia.
  - 1007 – Afirmaciones.
  - 1008 – Criterios.
- Desempeño:
  - 1201 – Planificación de la asignación.
  - 1202 – Evaluación de riesgo en planificación.
  - 1203 – Desempeño y supervisión.

18

18

## ESTÁNDARES DE AUDITORÍA

- 1204 – Materialidad.
- 1205 – Evidencia.
- 1206 – Uso del trabajo de otros expertos.
- 1207 – Irregularidades y actos ilegales.

• Reportes:

- 1401 – Planificación de la asignación.
- 1402 – Actividades de seguimiento.

19

19

## DIRECTRICES DE AUDITORÍA Y ASEGURAMIENTO DE SISTEMAS

• El objetivo de las directrices de auditoría y aseguramiento de sistemas de información es proporcionar información adicional sobre como cumplir con los estándares de auditoría. Para ello, el auditor deberá:

- Tenerlas en cuenta al determinar la forma de implementar los estándares.
- Usar el juicio profesional para aplicarlas a auditorías específicas.
- Poder justificar cualquier diferencia.

20

20

## PRINCIPALES DIRECTRICES (42)

- G1 – Uso del trabajo de otros auditores, 1 marzo 2008.
- G2 – Requerimientos de evidencia de auditoría, 1 mayo 2008.
- G3 – Uso de técnicas de auditoría asistidas por computador, 1 marzo 2008.
- G4 – Contratación de servicios externos de actividades de SI, 1 mayo 2008.
- G7 – Debido cuidado profesional, 1 marzo 2008.
- G8 – Documentación de la auditoría, 1 marzo 2008.
- G9 – Consideraciones de Auditoría para irregularidades y actos ilegales, 1 sept. 2008.
- G10 – Muestreo de auditoría, 1 agosto 2008

21

21

## HERRAMIENTAS Y TÉCNICAS DE AUDITORÍA

- Las herramientas provistas por Information Systems Audit and Control Association (ISACA) proveen ejemplos de procesos que un auditor de SI posiblemente podría seguir en una asignación de auditoría. Las herramient.as y técnicas se clasifican en:
  - Serie de referencia (libros)
  - Programas de auditoría/aseguramiento.
  - Libros blancos
  - Artículos de revistas

22

22

# INFORMATION TECHNOLOGY ASSUANCE FRAMEWORK (ITAF)

- ITAF™ es un modelo integral para el establecimiento de buenas prácticas que:
  - Proporciona orientación acerca del diseño, la realización y los reportes de las asignaciones de auditoría y aseguramiento de SI.
  - Define los términos y conceptos específicos para el aseguramiento de SI.
  - Establece los estándares que definen los requerimientos relacionados con los roles y las responsabilidades, conocimientos y habilidades, y diligencia, conducta y reporte de los profesionales de auditoría.
  - ITAF 3rd edition

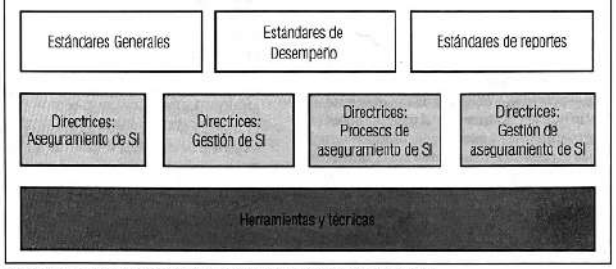
23

23

# INFORMATION TECHNOLOGY ASSUANCE FRAMEWORK (ITAF)

- ITAF™ se centra en la orientación de ISACA® y el IT Governance Institute ITGI® e instruye 3 categorías de estándares:

Figura 1.3 - La taxonomía de ITAF: ¿Cómo está ITAF organizado jerárquicamente?




Fuente: ISACA, *ITAF™: A Professional Practices Framework for IT Assurance*, USA, 2006, figura 1

24

24

# INFORMATION TECHNOLOGY ASSUANCE FRAMEWORK (ITAF)

- ITAF™ considera la inclusión de las siguientes secciones del estándar:
  - Sección 1000 – Estándares generales.
  - Sección 1200 – Estándares de desempeño.
  - Sección 1400 – Estándares sobre reportes.
  - Sección 3000 – Directrices de aseguramiento de sistemas de información.
  - Sección 3200 – Temas relacionados con la empresa.
  - Sección 3400 – Procesos de gestión de sistemas de información.
  - Sección 3600 – Procesos de auditoría y aseguramiento de sistemas de información.
  - Sección 3800 – Gestión de auditoría y aseguramiento de sistemas de información.

25

25

# ANÁLISIS DE RIESGOS

- El análisis de riesgos es parte de la planificación de auditoría y ayuda a identificar los riesgos y las vulnerabilidades para que el auditor pueda determinar los controles necesarios de mitigación.
- Al analizar los riesgos del negocio que surgen con el uso de tecnologías de la información, es importante que el auditor tenga una comprensión clara de los siguientes aspectos:
  - El propósito y la naturaleza del negocio, el entorno en el que opera el negocio y los riesgos del negocio relacionados.

→

26

26

## ANÁLISIS DE RIESGOS

- La dependencia de la tecnología para procesar y entregar información del negocio.
- Los riestos para el negocio que supone el uso de TI y cómo impactan en el logro de las metas y objetivos de la empresa.
- Una buena visión general de los procesos del negocio y del impacto de TI y los riesgos relacionados en los objetivos de los procesos de la empresa.

27

27

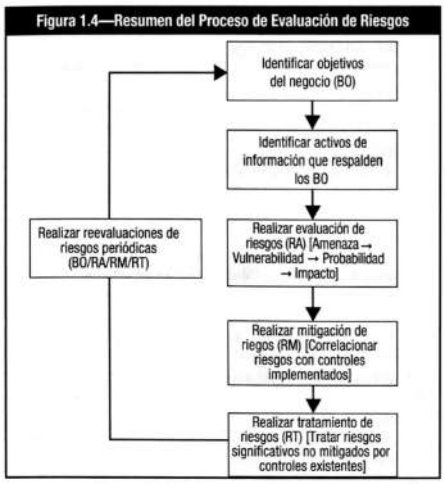
## THE RISK IT FRAMEWORK™ BY ISACA®

- Es un conjunto de principios guía y directrices de procesos de negocio y gestión de riesgo. El marco Risk IT explica el riesgo de TI y permite a los usuarios:
  - Integrar la gestión del riesgo de TI en la gestión de riesgos empresariales general de la empresa.
  - Tomar decisiones bien informados acerca de la magnitud del riesgo, la vulnerabilidad y la tolerancia al mismo.
  - Comprender como responder al riesgo.
  - Risk IT Framework

28

28

## THE RISK IT FRAMEWORK™ BY ISACA®




29

29

## CONTROLES INTERNOS

- Los controles internos están normalmente constituidos por políticas, procedimientos, prácticas y estructuras organizacionales implementadas para reducir los riesgos para la organización.
- Los elementos de control que se deberían considerar al evaluar la fortaleza de un control están clasificados como preventivos, detectivos o correctivos de acuerdo a su naturaleza.

30

30

# CLASIFICACIONES DE CONTROL

Figura 1.5—Clasificaciones de control

| Clase | Función | Ejemplos |
|---|---|---|
| Preventivos | • Detectan los problemas antes de que aparezcan.<br>• Monitorean tanto la operación como las entradas.<br>• Intentan predecir los problemas potenciales antes de que ocurran y realizan ajustes.<br>• Evitan que ocurra un error, omisión o acto malicioso. | • Emplean sólo personal calificado.<br>• Segregan funciones (factor disuasivo).<br>• Controlan el acceso a instalaciones físicas.<br>• Utilizan documentos bien diseñados (evita errores).<br>• Establecen procedimientos adecuados para la autorización de transacciones.<br>• Completan verificaciones de edición programadas.<br>• Utilizan software de control de acceso que permita que sólo el personal autorizado tenga acceso a archivos sensibles.<br>• Utilizan software de encriptación para evitar la divulgación no autorizada de datos. |
| Detectivos | • Utilizan controles que detectan e informan la ocurrencia de un error, omisión o acto fraudulento. | • Totales de comprobación (hash totals)<br>• Puntos de verificación en trabajos de producción<br>• Controles de eco en telecomunicaciones<br>• Mensajes de error en etiquetas de cintas<br>• Verificación duplicada de cálculos<br>• Reporte de rendimiento periódico con variaciones<br>• Informes de cuentas vencidas<br>• Funciones de auditoría interna<br>• Revisión de registros (logs) de actividad para detectar intentos de acceso no autorizado |
| Correctivo | • Minimizar el impacto de una amenaza.<br>• Remediar problemas descubiertos por controles detectivos.<br>• Identificar la causa de un problema.<br>• Corregir errores que surgen de un problema.<br>• Modificar los sistemas de procesamiento para minimizar futuras ocurrencias del problema. | • Planificación de contingencia<br>• Procedimientos de respaldo<br>• Procedimientos de nueva ejecución |

31

31

# OBJETIVOS DE CONTROL DE SI

- Proporcionan un conjunto completo de requisitos de alto nivel que la gerencia debe tener en cuenta para un control eficaz de cada proceso TI. Objetivos:
  - Son enunciados del resultado deseado o del propósito a ser alcanzado con la implementación de controles en torno a los procesos de sistemas de información.
  - Están compuestos de políticas, procedimientos, prácticas y estructuras organizacionales.
  - Están diseñados para brindar confianza razonable de que se alcanzarán los objetivos del negocio.

32

32

## OBJETIVOS DE CONTROL DE SI

- Los objetivos de control de SI específicos pueden incluir:
  - La salvaguardia de activos.
  - Asegurar la integridad de los entornos de sistemas operativos en general, operaciones y redes.
  - Asegurar la integridad de los entornos de sistemas sensibles y críticos.
  - Asegurar autenticación apropiada de los usuarios.
  - Aseguramiento de la eficiencia y efectividad de las operaciones.

→

33

33

## OBJETIVOS DE CONTROL DE SI

- Cumplimiento de los requerimientos de los usuarios, con las políticas y normas organizacionales.
- Aseguramiento de continuidad TI a través de planes de continuidad del negocio (BCP) y recuperación de desastres (DRP).
- Mejora de la protección de datos y sistemas mediante respuesta a incidentes.
- Aseguramiento de la integridad y confiabilidad de sistemas mediante implementación de procedimientos de gestión de cambios.

34

34

## CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT™ V5)

- COBIT™ versión 5 provee un marco completo que ayuda a las empresas a alcanzar sus objetivos de gobierno y la gestión TI de la empresa.
- En general, permite que las Tecnologías de Información se gobiernen y controlen de manera holística (como un todo) en toda la empresa, incorporando el negocio integral y las áreas funcionales de responsabilidad de TI.
  - Cobit 5.

35

35

## CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT™ V5)

**Figura 1.6—Principios de COBIT 5**


Fuente: ISACA, COBIT 5, USA, 2012, figura 2

36

36

## CONTROLES GENERALES

- Los controles generales incluyen:
  - Controles internos de contabilidad.
  - Controles operativos que se ocupan de las operaciones, funciones y actividades diarias.
  - Controles administrativos relacionados con la eficiencia operacional.
  - Políticas y procedimientos de seguridad de resguardo de activos de información.
  - Políticas generales para el diseño y uso de documentos y registros.
  - Procedimientos y prácticas para asegurar la protección adecuada en el acceso.
  - Políticas de acceso y uso de activos.

37

37

## REALIZACIÓN DE UNA AUDITORÍA DE SISTEMAS

- Las técnicas de gestión de proyectos para gestionar y administrar proyectos de auditoría, ya sea automatizados o manuales, incluyen los siguientes pasos:
  - Planificar la asignación de auditoría.
  - Elaborar el plan de auditoría.
  - Ejecutar el plan.
  - Monitorear la actividad del proyecto.

38

38

## CLASIFICACIÓN DE LAS AUDITORÍAS

- Los distintos tipos de auditoría que pueden realizarse interna o externamente:
  - Auditorías de cumplimiento.
  - Auditorías financieras.
  - Auditorías operativas.
  - Auditorías integradas.
  - Auditorías administrativas.
  - Auditorías de sistemas de información.
  - Auditorías especializadas.
  - Auditorías forenses.

39

39

## PROGRAMAS DE AUDITORÍAS

- Es un conjunto de procedimientos e instrucciones de auditoría paso a paso que debe realizarse completar una auditoría. Estos procedimientos pueden incluir:
  - Uso de software especializado de auditoría.
  - Uso de software especializado para evaluar contenidos de archivos y BD.
  - Técnicas de elaboración de diagramas de flujo para documentación.
  - Uso de registros (logs) disponibles en sistemas de control y SO.
  - Revisión de la documentación.
  - Observaciones y consultas.
  - Inspecciones y verificaciones; y, revisión de controles.

40

40

# METODOLOGÍA DE AUDITORÍA

**Figura 1.7—Fases de la auditoría**

| Fases de la auditoría | Descripción |
|---|---|
| Sujeto de la auditoría | • Identificar el área que será auditada. |
| Objetivo de auditoría | • Identificar el propósito de la auditoría. Por ejemplo, un objetivo podría ser determinar si los cambios del código fuente del programa ocurren en un ambiente bien definido y controlado. |
| Alcance de la auditoría | • Identificar los sistemas, funciones o unidades específicos de la organización que serán incluidos en la revisión. Por ejemplo, en el ejemplo de cambios de programa anterior ejemplo de cambios de programa anterior, el enunciado de alcance podría limitar la revisión a sólo un sistema de aplicación o a un período limitado. |
| Planificación de preauditoría | • Identificar habilidades y recursos técnicos necesarios.<br>• Identificar las fuentes de información para la prueba o examen, como diagramas de flujo funcionales, políticas, normas, procedimientos y papeles de trabajo anteriores a la auditoría.<br>• Identificar las localidades o instalaciones que serán auditadas. |
| Procedimientos de auditoría y pasos para recolección de datos | • Identificar y seleccionar el enfoque de auditoría para verificar y comprobar los controles.<br>• Identificar una lista de individuos que serán entrevistados.<br>• Identificar y obtener las políticas, estándares y directrices departamentales para realizar la revisión.<br>• Desarrollar herramientas y metodología de auditoría para probar y verificar el control. |
| Procedimientos para evaluar los resultados de la prueba o la revisión | Específico de la organización |
| Procedimientos para las comunicaciones con la gerencia | Específico de la organización |
| Preparación del reporte de auditoría | • Identificar los procedimientos de seguimiento de la revisión.<br>• Identificar los procedimientos para evaluar/probar la eficiencia y efectividad operacional.<br>• Identificar los procedimientos para probar los controles.<br>• Revisar y evaluar la calidad de los documentos, políticas y procedimientos. |

41

41

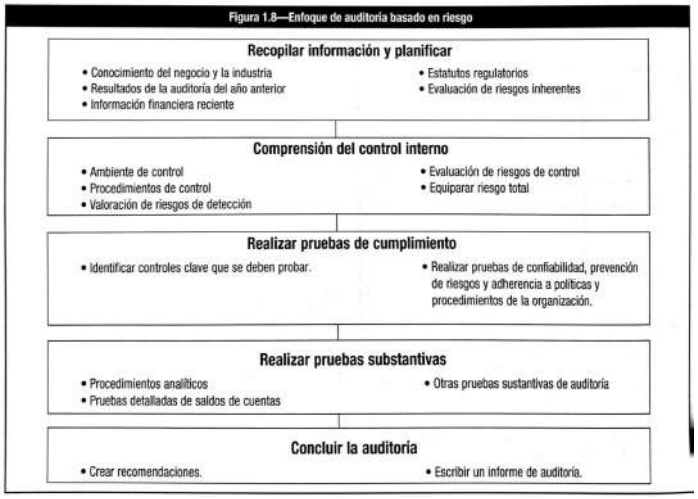
# DETECCIÓN DE FRAUDE

- El auditor de SI debe observar y ejercer el debido cuidado profesional en todos los aspectos de su trabajo (Audit Standard SI S3 by ISCACA).
- El auditor debe estar consciente de los requerimientos legales potenciales que conciernen a la implementación de procedimientos específicos de detección de fraude y el reporte correspondiente a las autoridades.
- Considerar nuevas técnicas:
  - Machine Learning
  - Inteligencia Artificial

42

42

# AUDITORÍA BASADA EN EL RIESGO




43

43

# RIESGO DE AUDITORÍA Y MATERIALIDAD

- El riesgo de auditoría está influenciado por:
  - Riesgo inherente.
  - Riesgo de control.
  - Riesgo de detección.
  - Riesgo de auditoría general.

44

44

## PRUEBAS DE CUMPLIMIENTO Y SUSTANTIVAS

- Las pruebas de cumplimiento consisten en recolectar evidencia con el propósito de probar el cumplimiento de una organización con procedimientos de control.
- La prueba sustantiva la evidencia se recoge para evaluar la integridad de transacciones individuales, datos u otra información.

45

45

## CONFIABILIDAD DE LA EVIDENCIA

- Los determinantes para evaluar la confiabilidad de la evidencia de auditoría incluyen:
  - Independencia del proveedor de la evidencia.
  - Credenciales de la persona que suministra la información o evidencia.
  - Objetividad de la evidencia.
  - Tiempo de disponibilidad de la evidencia.

46

46

## PROBLEMA PRINCIPAL DE CONFIABILIDAD

- Las personas tienen limitaciones al momento de procesar, almacenar y rescatar grandes volúmenes de datos.
- A pesar de que la estadistica ayuda a mejorar los procesos, los auditores a nivel mundial no presentan aptitudes ni desarrollo matemático.
- El software y los grandes volumenes de datos imposibilitan el trabajo manual.

47

47

## HERRAMIENTAS DE APOYO

**Recurso metodológico**

Herramientas de carácter metodológico de apoyo a la auditoría. También son conocidas como herramientas del auditor.

**Recurso de software**

Sistemas informáticos de apoyo al proceso de auditoría

48

48

## HERRAMIENTAS DEL AUDITOR

- Cuestionarios, generalmente binarios.
- Entrevistas, usados para aclaratorias.
- Checklist.
- Trazas o huellas.

49

49

## HERRAMIENTAS METODOLÓGICAS

- COBIT: Mejores prácticas de auditoría y control de SI, permitiendo a la gerencia comprender y gestionar los riesgos que conlleva el uso de tecnologías en la empresa. Controles:
  - De negocio y TI a nivel de dirección ejecutiva.
  - Controles generales de TI.
  - Controles a nivel de aplicación.

50

50

## HERRAMIENTAS METODOLÓGICAS

- ITAF (Information Technology Assurance FrameWork):
  - Es una guía para el diseño, conducción y reporte de la auditoria de TI como de revisiones de aseguramiento en donde define términos y concepto específicos para el aseguramiento de TI.
- CICLO V:
  - Identificación de procesos de la organización que son estrategicos para el negocio.
- CICLO PDCA:
  - Plan, Do, Check, Act

51

51

## TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT's)

- Conjunto de técnicas y herramientas que se usan en el desarrollo de las auditorías con el fin de mejorar la eficiencia, alcance y confiabilidad del proceso de auditoría.
- Se consideran métodos y procedimientos.
- Son técnicas básicas de un auditor moderno.

52

52

## AUDITORÍA ASISTIDA POR COMPUTADOR

- Las CAATs (Computer Assisted Audit Techniques) permiten a los auditores recopilar antecedentes de forma independiente, tanto de la organización como de la arquitectura de software y hardware.
- Las CAATs incluyen numerosos tipos de herramientas y técnicas, tales como software generalizado de auditoría (GAS), software de depuración (debugging), escaneo (scanning), pruebas y mapeo.

53

53

## AUDITORÍA ASISTIDA POR COMPUTADOR

- Estas herramientas y técnicas se pueden usar para efectuar diversos procedimientos de auditoría que incluyen:
  - Pruebas de detalles de transacciones y saldos.
  - Procedimientos de revisión analítica.
  - Pruebas de cumplimiento de controles generales y de aplicación de SI.
  - Evaluación de vulnerabilidades y penetración.
  - Pruebas de seguridad de aplicaciones y escaneo de seguridad.

54

54

## TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT's)

- Permite a un auditor obtener la suficiente evidencia confiable para sustentar sus observaciones y recomendaciones.
- El auditor debe tener capacidades especificas:
  - Conocimientos informáticos
  - Discernimiento en el uso adecuado de las TI
  - Capacidades analíticas.

55

55

## TÉCNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADOR (CAAT's)

- Auditoría asistida por computador se puede usar en:
  - Pruebas de detalles de transacciones y balances.
  - Procedimientos analíticos.
  - Pruebas de controles generales.
  - Programas de muestreo para extractar datos.
  - Pruebas de control en aplicaciones.
  - Recálculos.

56

56

# AUDITORÍA A TRAVÉS DE COMPUTADORES

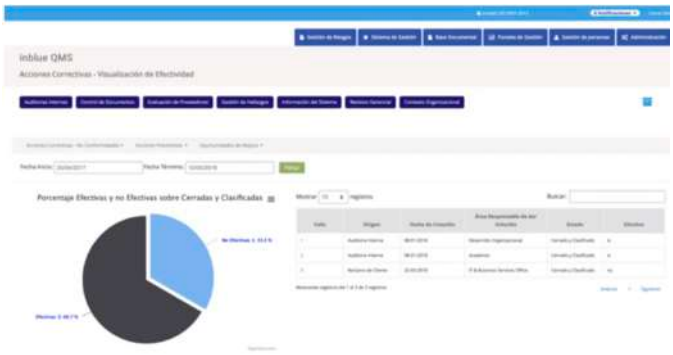
- El auditor debe seguir las pistas de auditoría a través de la fase de operaciones internas o proceso automatizado de datos.
- Los intentos de verificación de los procesos de control involucran el uso de software.
- Los enfoques primarios son:
  - Programas de testeo
  - Programas computarizados de validación.
  - Software de revisión de sistemas.

57

57

# SOFTWARE DE APOYO

- inblueQMS




58

58

# SOFTWARE DE APOYO

- AuditBrain


59

59

# SOFTWARE DE APOYO

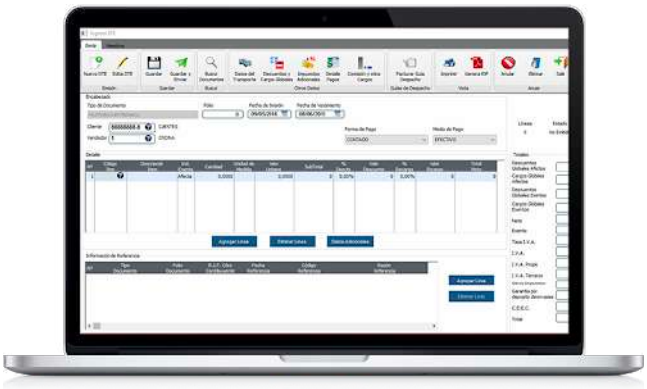
- iAuditoria

60

60

# SOFTWARE DE APOYO

- Audisoft

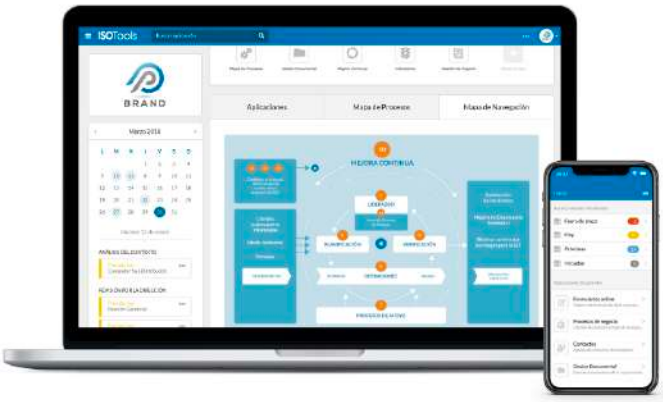


61

61

# SOFTWARE DE APOYO

- ISOTools




62

62

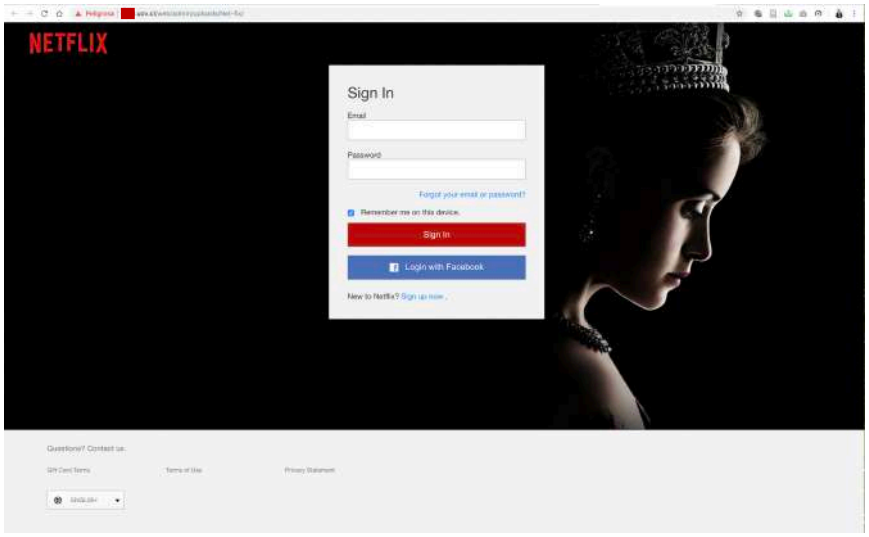
## VARIABLES A CONSIDERAR

- Tamaño
- Objetivos de la auditoría
- Costos
- Usabilidad

63

63

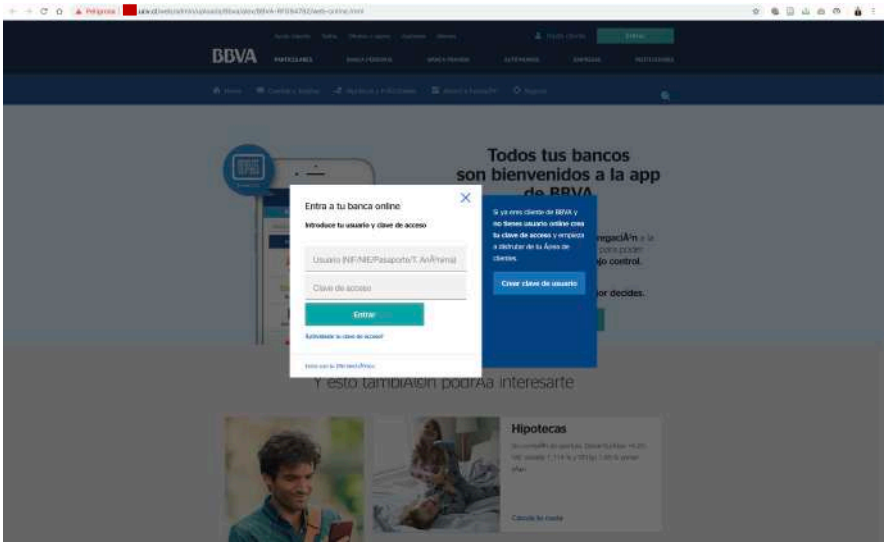
## EJEMPLOS DE VULNERABILIDAD




64

64

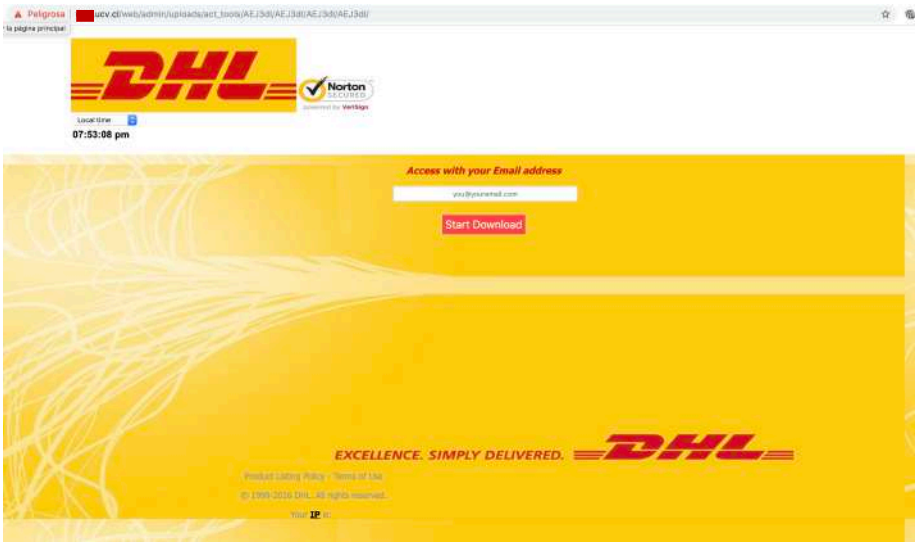
# EJEMPLOS DE VULNERABILIDAD




65

65

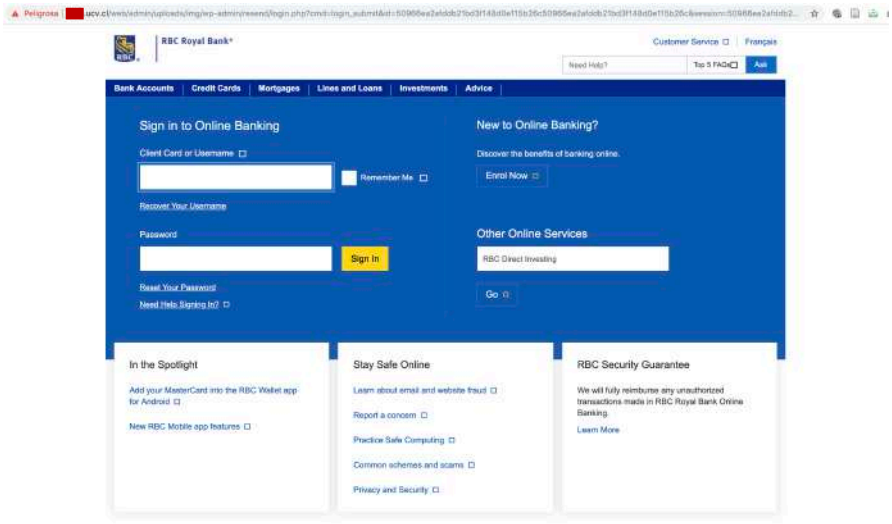
# EJEMPLOS DE VULNERABILIDAD




66

66

# EJEMPLOS DE VULNERABILIDAD




67

67

# DOCUMENTACIÓN DE AUDITORÍA

- La documentación de auditoría debe incluir como mínimo:
  - La planificación y preparación del alcance y de los objetivos de la auditoría.
  - La descripción y/o recorridos en el área de auditoría vista.
  - El programa de auditoría.
  - Los pasos de auditoría realizados y la evidencia recopilada.
  - El uso de servicios de otros auditores y expertos.
  - Los hallazgos, conclusiones y recomendaciones.
  - Informe final.

68

68

# CONCLUSIONES

- Es necesario utilizar sistemas en la auditoría:
  - Ventajas competitivas profesionales
  - Ventajas de la empresa.
- Sistemas para la toma de decisiones.

69

69

ESCUELA DE COMERCIO
PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

MÓDULO 1

## EL PROCESO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

**Prof. Mg. Rafael Mellado S.**
rafael.mellado@pucv.cl
COM5163 – Sistemas de Información 3
Escuela de Comercio

70

70