

Auditoría de Sistemas

Módulo 1: Conceptos Básicos

Dra. Marcela Capobianco

Departamento de Ciencias e Ingeniería de la
Computación
Universidad Nacional del Sur

1

Copyright

.Copyright © 2016 Marcela Capobianco .

.Se asegura la libertad para copiar, distribuir y modificar este documento de acuerdo a los términos de la *GNU Free Documentation License, Version 1.2* o cualquiera posterior publicada por la *Free Software Foundation*, sin secciones invariantes ni textos de cubierta delantera o trasera.

.Una copia de esta licencia está siempre disponible en la página <http://www.gnu.org/copyleft/fdl.html>.

-2-

.Profesor: Dra. Marcela Capobianco (Lic)

.Asistente: Lic. Marcelo Endara
(mjen@cs.uns.edu.ar)

.Ayudante: Mg. Victor Ferracuti

-3-

Bibliografía

- Auditors guide to information systems auditing, R. Cascarino. 2007.
- CISA Review Manual. ISACA, 2013.
- CISA, Certified Information Systems Auditor Study Guide, Cannon, Bergmann, Pamplin. 2013.
- Information Technology Control and Audit. Frederick Gallegos, Daniel P. Manson, Sandra Allen-Senft. 2008.
- Information Systems Control and Audit, Ron Weber. Prentice Hall. 1998.

-4-

Cursado de la Materia

- Parcial con su correspondiente recuperatorio (materia corta)
 - Fechas: 28/10/2019 – 11/11/2019
- Un parcial más para Auditoría de Sistemas y Legislación / Fecha a definir
- Proyecto: a definir
- El proyecto se califica con A (aprobado sin errores), B (aprobado con observaciones), C (aprobado con errores), D (desaprobado) o E (excelente!)

-5-

Cursado de la Materia

- Existe la opción de promocionar la materia si obtienen 75 puntos o más en los parciales
- Además es necesario tener en el proyecto como una B o nota superior
- Y aprobar un examen coloquio que se rinde al final de la materia

-6-

Transparencias

- Las transparencias pueden contener errores.
- Las transparencias son una guía de los temas dados. Es conveniente (y lo recomendamos) leer la bibliografía correspondiente.
- Las transparencias se publican en la página de la materia. También los prácticos. (<https://cs.uns.edu.ar/~mc/ADS/>)

-7-

Auditoría de Sistemas

- Pero primero: ¿Qué es auditar? ¿Y auditar Sistemas?



-8-

¿Por Qué?

- Los Sistemas de Información (SI) juegan un rol clave en la organización
- Los auditores de sistemas son cada vez más demandados por las organizaciones



-9-

Qué aprendemos?

- Entender sobre gobierno corporativo de IT
- Conocer prácticas que aseguran service delivery
- Entender sobre desarrollo, adquisición, testeo de SI de acuerdo al contexto
- Brindar servicios de auditoría de acuerdo con estándares internacionales
- Protección de activos de información, business continuity, business recovery

-10-

Para qué tipo de trabajo me sirve

- Auditor de SI
- Consultor en seguridad
- Gerenciamiento de SI
- Auditor Interno
- Y varios mas...



-11-

Auditar SI



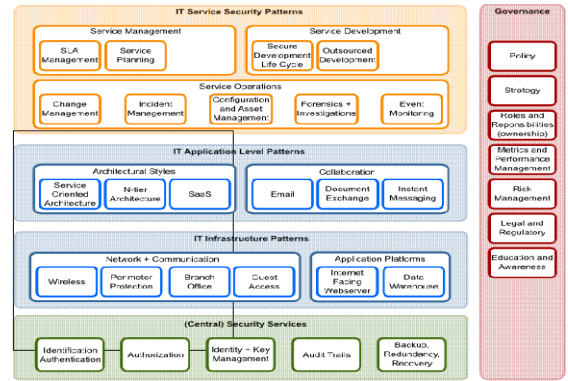
-12-

Frameworks



-13-

Razones para Controlar



-14-

Qué es Auditar...

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

-15-

Qué es Auditar...

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

-16-

Tipos de auditorias

- Financiera
- Sistemas de Información
- Operacional
- Compliance (ajustarse a una norma, como una especificación, política, norma o ley)
- Investigativa

-17-

Financiera

- Examina la confiabilidad e integridad de transacciones financieras, registros de contabilidad, estados financieros, etc

-18-

Sistemas de información

- Revisa los controles de los sistemas de información para ver si cumplen con las políticas de control interno y son efectivas en salvaguardar los assets (bienes...) de la organización

-19-

Operacional

- Se busca un uso económico y eficiente de los recursos y poder cumplir con los objetivos establecidos

-20-

Compliance (cumplimiento)

- Determinar si las entidades cumplen con las leyes aplicables, regulaciones, políticas y procedimientos

-21-

Investigativa

- Investigar incidentes de posible fraude, apropiación de assets, gastos y abusos o actividades impropias de las autoridades.

-22-

Importancia de los SI

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

-23-

Controles en los sistemas modernos

- Los sistemas computarizados son más complejos que los sistemas manuales
- Mantienen datos en formatos electrónicos, más difíciles de acceder por el auditor
- En algunos casos no existe **paper audit trail** (registros que documentan cada paso en una transacción comercial.)
- Procesan datos con muy poca intervención manual

-24-

Clasificación de controles

- **Controles generales:** los que gobiernan el ambiente en el cual el sistema es desarrollado mantenido y operado
- **Controles de aplicaciones:** los controles manuales y computarizados dentro de la aplicación de negocios que aseguran que los datos sean procesados correctamente

-25-

Clasificación de controles

- Los controles de aplicaciones dependen de los controles generales
- Si los controles generales no son adecuados la aplicación será de baja calidad y los datos no serán procesados correctamente
- En el pasado el auditor asumía confianza en los controles de aplicación (auditar "around the computer")

-26-

Clasificación de controles

- Auditar "around the computer" es una suposición fatal
- Los sistemas son cada vez más complejos y cada vez más vulnerables
- Es crítico que el auditor verifique la integridad del ambiente en que el sistema opera

-27-

Proceso de auditoría

- Planificar
- Recolectar evidencia
- Evaluar evidencia
- Comunicar los resultados

-28-

Planificar

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

-29-

Evidencia

- Recolectar ejemplos, no se puede examinar todo!
- Elegir qué actividades observar
- Revisar documentación
- Comprender los procesos de control
- Debates
- Cuestionarios
- Exámenes
- Confirmaciones
- Vouching (se refiere a la inspección de evidencia documental que respalda y confirma una transacción, por un auditor.)
- Examinar la documentación respaldatoria
- Revisiones analíticas
- Examinar relaciones y tendencias

-30-

Evaluando la evidencia

- ¿La evidencia respalda conclusiones favorables o desfavorables?
- ¿Cuán significativo es el impacto de la evidencia?
- Seguridad razonable
- **Siempre existen riesgos de que la conclusión sea incorrecta!!**

-31-

Comunicar los resultados

- Reportes escritos que resumen las recomendaciones y las conclusiones obtenidas
- Para la gerencia
- El comité de auditoría
- La junta directiva
- Otros...

-32-

Definición

La auditoría de sistemas de información es el proceso de recolectar y evaluar evidencia para determinar si:

- el sistema automático preserva los activos,
- mantiene la integridad de los datos,
- permite que los objetivos organizacionales se alcancen con eficacia,
- usa los recursos con eficiencia.

-33-

Otros Objetivos

Muchas veces la auditoría tiene otro propósito:

- asegurar que la organización cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o involuntariamente.

Ejemplos:

- Entidades financieras.
- Normas ISO
- Entidades aseguradoras

-34-

Dos tipos de auditores



-35-

Dos tipos de auditores

- **Externos:** la misión es proveer una opinión independiente de los estados financieros de la organización, u otra característica de la que deseamos tener una opinión independiente.

No son personal de la organización!!

-36-

Dos tipos de auditores

- **Interno:** trabaja en la organización. Se pregunta si:
 - Cumple la organización con su misión?
 - Revisa la confiabilidad e integridad de la información?
 - Se siguen las políticas, planes, regulaciones existentes?
 - Se promueve la eficiencia operacional?

-37-

Control interno

- Cualquier política, procedimiento o proceso diseñado para proveer una seguridad razonable para cumplir con un objetivo
- Sirven para asegurar que:
 - Los assets son protegidos
 - Las operaciones son eficientes y efectivas
 - Los reportes financieros son confiables y completos
 - Se cumple con las leyes y regulaciones

-38-

Auditor interno

- El trabajo principal de un auditor interno es verificar y reportar sobre la existencia de **controles internos** en una organización
- Se debe ver si su funcionamiento es correcto
- Algunos de estos controles se relacionan con los sistemas de información

-39-

Logro de Objetivos

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un **sistema de control interno**.

-40-

Sistema de Control Interno

- 1) separación de obligaciones,
- 2) delegación clara de autoridad y responsabilidades,
- 3) reclutamiento y entrenamiento de personal calificado,
- 4) sistema de autorizaciones,
- 5) documentos y registros adecuados,

-41-

Sistema de Control Interno

- 6) control físico y documentación sobre los activos,
- 7) chequeos independientes de performance,
- 8) comparación periódica de activos con registros contabilizados

-42-



-44-

Bibliografía

- Cascarino, Auditor's Guide to Information Systems Auditing, Wiley and sons, 2007. Capítulo 2.
- <https://www.isaca.org/pages/default.aspx>
- ¿Qué es una auditoría?: <https://www.youtube.com/watch?v=yONlxK9mjEo>