Auditoría de Sistemas

Módulo 1: Conceptos Básicos

Dra. Marcela Capobianco

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

Copyright

Presentación .....

- Profesor: Dra. Marcela Capobianco (Lic)
- Ayudante: Ing. Natalia Martinez (Lic)
- Asistente: Lic. Marcelo Endara (mjen@cs.uns.edu.ar)
- Ayudante: Mg. Victor Ferracuti

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.

Cursado de la Materia

- Parcial con su correspondiente recuperatorio (materia corta)
- Un parcial más para Auditoría de Sistemas y Legislación
- Entregas de 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!)

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

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/)

Auditoría de Sistemas

- Pero primero: ¿Qué es auditar?

¿Por Qué?

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

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

Para qué tipo de trabajo me sirve

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

Auditar SI


IS Audit Process
IT Governance
System and Infrastructure Lifecycle Management
IT Service Delivery And Support
Protection of Information Asset
Business Continuity And Disaster Recovery
IS Audit

Frameworks


CISA
Certified Information Systems Auditor®
An ISACA® Certification

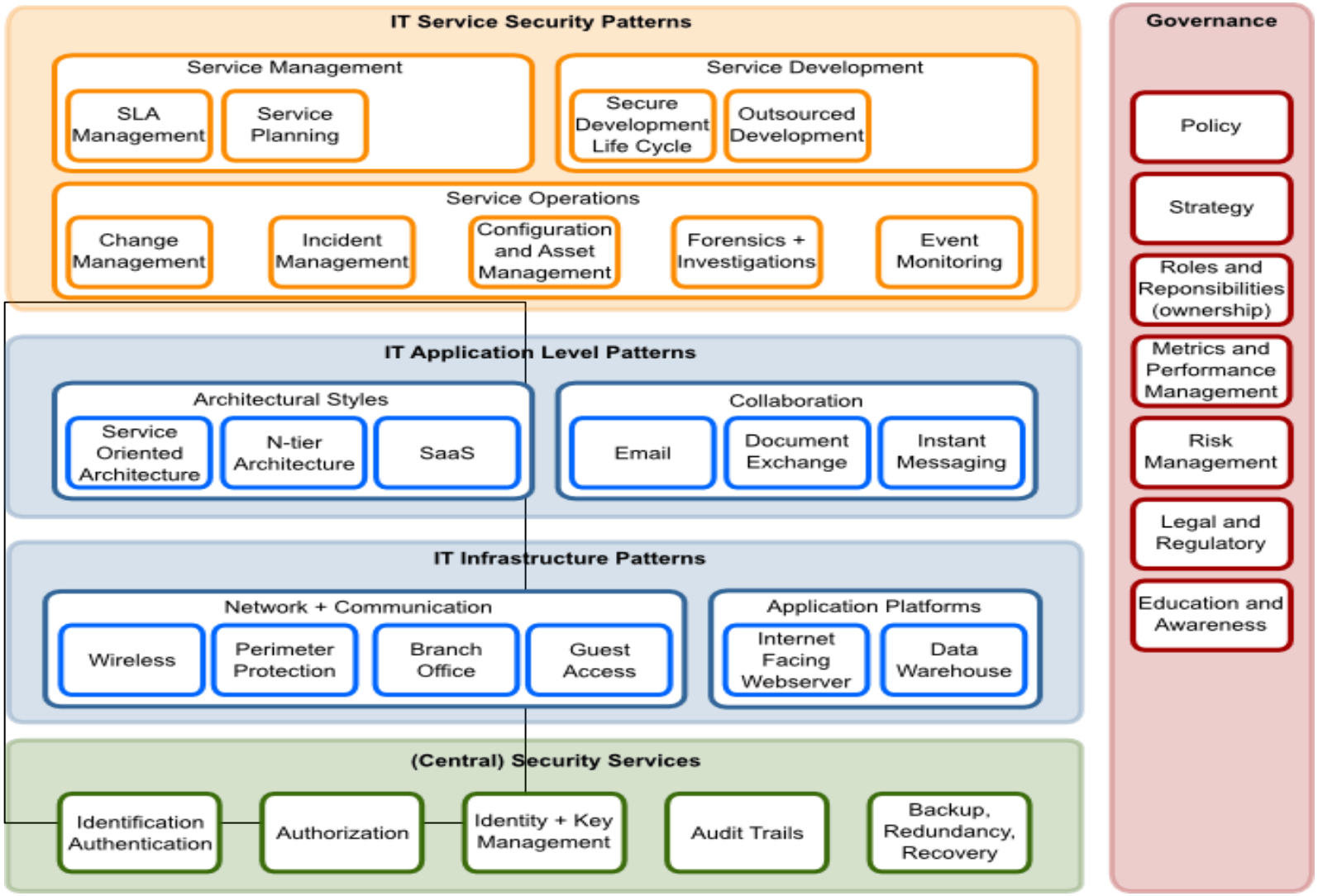

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY


ISACA®
Serving IT Governance Professionals


CISM®
CERTIFIED INFORMATION SECURITY MANAGER®


Risk IT
BASED ON COBIT®

Razones para Controlar



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

Tipos de auditorias

- Financiera
- Sistemas de Información
- Operacional
- Compliance
- Investigativa

Financiera

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

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 salvaguardas los assets de la organización

Operacional

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

Compliance

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

Investigativa

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

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

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
- Procesan datos con muy poca intervención manual

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

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”)

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

Proceso de auditoría

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

Planificar

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

Evidencia

- Recolectar ejemplos, no se puede examinar todo!
- Elegir qué actividades observar
- Revisar documentación
- Comprender los procesos de control
- Debates
- Cuestionarios
- Exámenes

- Confirmaciones
- Vouching
- Examinar la documentación respaldatoria
- Revisiones analíticas
- Examinar relaciones y tendencias

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

Comunicar los resultados

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

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.

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

Dos tipos de auditores

- Externos: la misión es proveer una opinión independiente de los estados financieros de la organización, u otra característica de a que deseamos tener una opinión independiente.
- No son personal de la organización

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?

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

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

Logro de Objetivos

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

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,

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

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

Bibliografía

- Cascarino, Auditor's Guide to Information Systems Auditing, Wiley and sons, 2007. Capítulo 2.
- Capítulos de la serie “El socio”.