Sesión #

COBIT SECURITY BASELINE

un 'kit' de supervivencia para la seguridad de información

Juan de Dios Bel, CISM, CISA
RUSENAS, Auditores y Consultores
Socio

Agenda

- COBIT Security Baseline: ¿Porqué?
- COBIT cómo fundamento para buenas prácticas de seguridad
- La Seguridad no es un esfuerzo de única vez
- Seguridad de la Información Definida
- Riesgos actuales - ¿Porqué es importante la seguridad de la información?
- COBIT Security Baseline: 39 pasos hacia la Seguridad
- 6 'Kits' de supervivencia en Seguridad de Información

COBIT Security Baseline: ¿Porqué?

National Strategy to Secure Cyberspace

- Priority III: A National Cyberspace Security Awareness and Training Program
  - Promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace
    - **Home Users and Small Business**
      - » Can help the Nation secure cyberspace by securing their own connections to it. Installing firewall software and updating it regularly, maintaining current antivirus software, and regularly updating operating systems and major applications with security enhancements are actions that individuals and enterprise operators can take to help secure cyberspace. To facilitate such actions…other organizations can make it easier for home users and small businesses to secure their systems. (A/R 3-3)
    - **Large Enterprises**
      - » Encouraged to evaluate the security of their networks that impact the security of the Nation's critical infrastructures. Such evaluations might include: (1) conducting audits to ensure effectiveness and use of best practices; (2) developing continuity plans which consider offsite staff and equipment; and, (3) participating in industry-wide information sharing and best practice dissemination. (A/R 3-4)

Control Objectives for Information and Related Technology (CobiT)

- Drafted by COBIT Quickstart (SMEs)
- Security Practitioners Updates
- Revised Edition Published

COBIT Security Baseline

- COBIT como fundamento para 'Buenas Prácticas' de Seguridad
  - COBIT proporciona directrices sobre la adopción de un estándar de gobierno y control de TI; cubre la seguridad y otros riesgos que se producen en los ambientes de TI.
  - El usuario doméstico, el usuario de pequeñas y medianas empresas, y los ejecutivos/miembros de la junta directiva de organizaciones más grandes deben ser conscientes de su papel, minimizando el riesgo y creando un nivel eficaz de seguridad.

COBIT Security Baseline

- La Seguridad no es un esfuerzo de única vez
  - Se debe administrar el esfuerzo aplicado a proteger el ambiente de trabajo sobre la base de las consecuencias de un impacto de un problema de seguridad
  - Deben usarse productos probados y expertos sobre una base de constante y continua.
  - La buena seguridad mejorará la reputación, la confidencialidad y la confianza de otros con quienes se dirige el negocio; puede ahorrar tiempo y dinero.

COBIT Security Baseline:
Estructura del Documento

COBIT Security Baseline: Estructura					
Introducción					
Seguridad de Información: su definición					
Seguridad: ¿Porqué es Importante?					
COBIT Security Baseline: 39 pasos hacia la Seguridad					
Kit de supervivencia Nº 1	Kit de supervivencia Nº 2	Kit de supervivencia Nº 3	Kit de supervivencia Nº 4	Kit de supervivencia Nº 5	Kit de supervivencia Nº 6
Usuarios Domésticos	Usuarios Profesionales	Gerentes	Ejecutivos	Alta Gerencia	Junta Directiva
Riesgos Técnicos de Seguridad Actuales					
Referencias y Antecedentes					

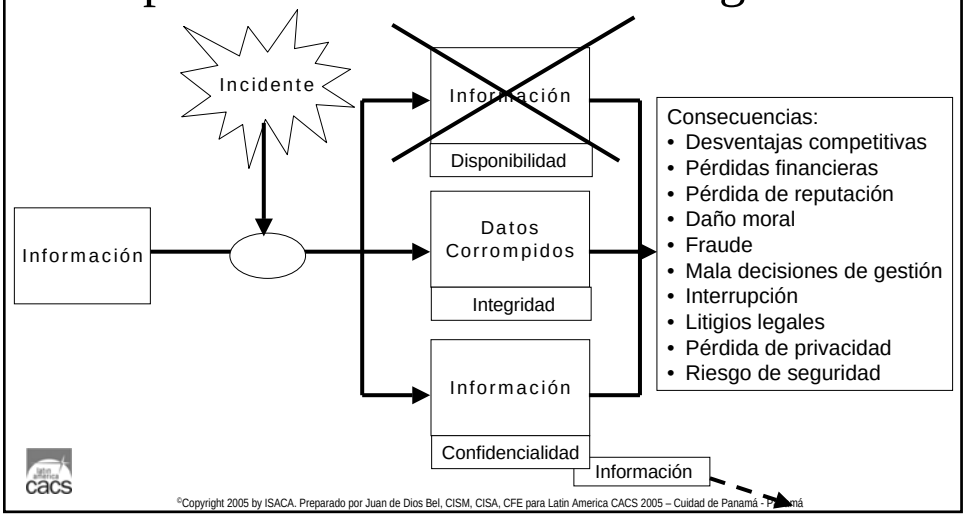
COBIT Security Baseline:

- Seguridad de Información: su definición
  - El objetivo de la seguridad de información es proteger los intereses de aquéllos que confían en la información, y en los sistemas y comunicaciones que la entregan, del daño resultante de fracasos de:
    - Disponibilidad: los sistemas están disponibles y utilizables cuando se los requiere
    - Confidencialidad: la información se revela sólo a aquéllos que tienen derecho para conocerla
    - Integridad: la información es protegida contra la modificación no autorizada
    - Autenticidad y No repudio: puede confiarse en el intercambio de transacciones e información
  - La protección se logra a través de los resguardos técnicos y no-técnicos, que varían según los tipos de usuarios.
  - La seguridad debe seguir el paso de los cambios tecnológicos

COBIT Security Baseline

- Los riesgos actuales: ¿Por qué la Seguridad de Información es importante?
  - las nuevas tecnologías introducen nuevas funcionalidades, así como nuevos y complejos riesgos.
  - Aumenta la dependencia de TI y significa un impacto más grave cuando hay una falla de seguridad.
  - Deben protegerse los datos personales y empresariales como parte de la expansión del comercio electrónico.
  - Las mejoras a la seguridad de información, puede llevar a obtener una mejora en la ventaja competitiva, puede generar la confianza y puede reforzar la 'performance' comercial.

¿Mito o Realidad?
Impacto de un incidente de seguridad



COBIT Security Baseline

- **Los riesgos técnicos de seguridad:** *Riesgos de seguridad de abuso de las computadoras*
  - Trojan Horse programs
  - Back door and remote administration programs
  - Denial-of-Service attacks
  - Being an intermediary for another attack
  - Unprotected Windows networking shares
  - Mobile Code (Java/JavaScript/ActiveX)
  - Cross-Site scripting
  - E-mail spoofing
  - E-mail-borne viruses

COBIT Security Baseline

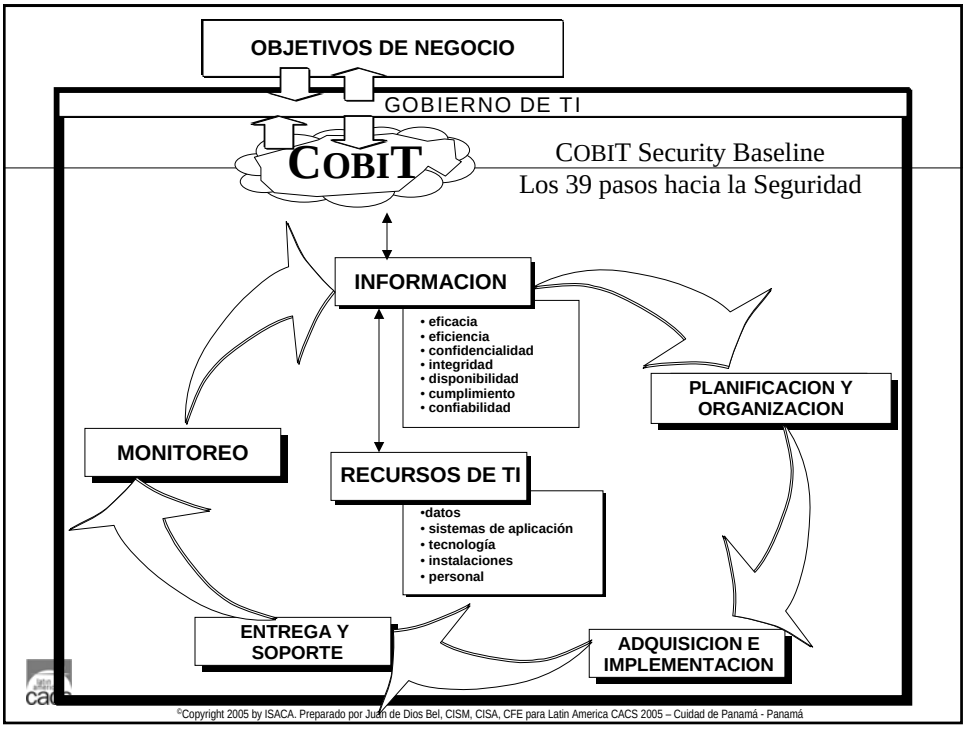
- **Los riesgos técnicos de seguridad:** *Riesgos de seguridad de abuso de las computadoras*
  - Hidden file extensions
  - Chat clients
  - Packet sniffing
  - Identity theft
  - Tunneling
  - Zombies
  - Spyware

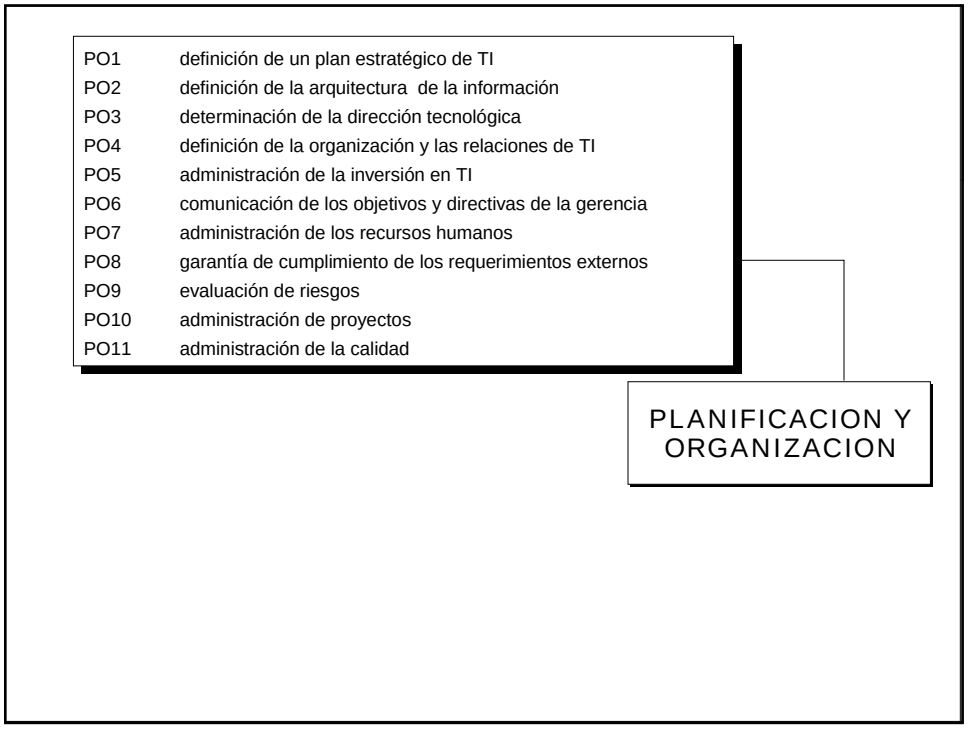
COBIT Security Baseline

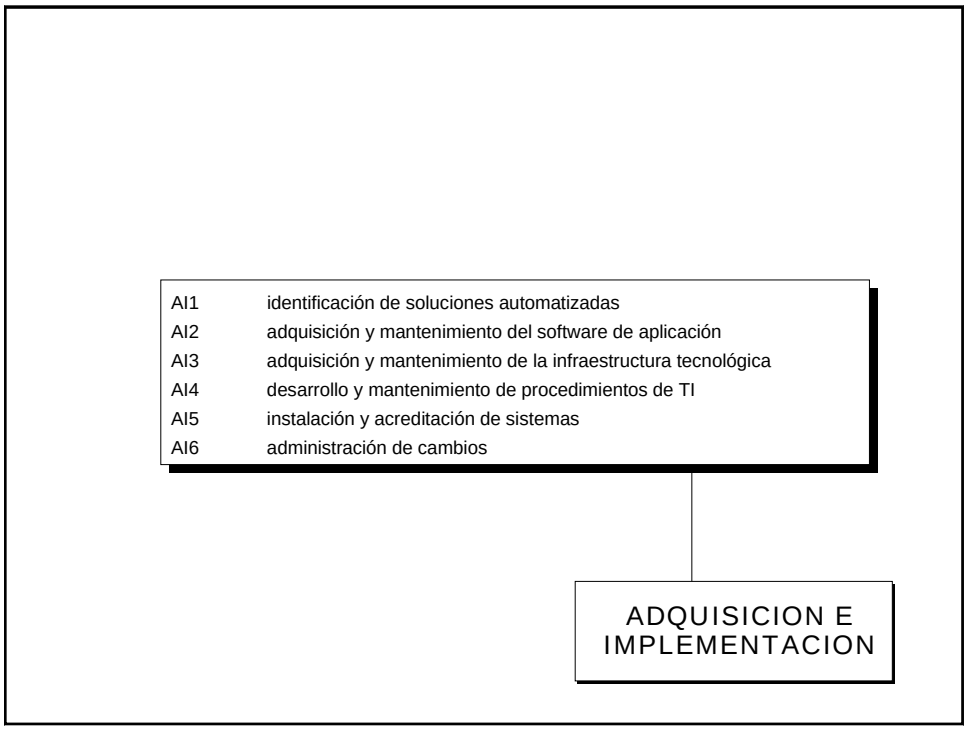
- **Los riesgos técnicos de seguridad:** *Violaciones de leyes y regulaciones*
  - Propiedad intelectual
  - Uso decente de Internet
  - Espionaje Industrial
  - Leyes y regulaciones

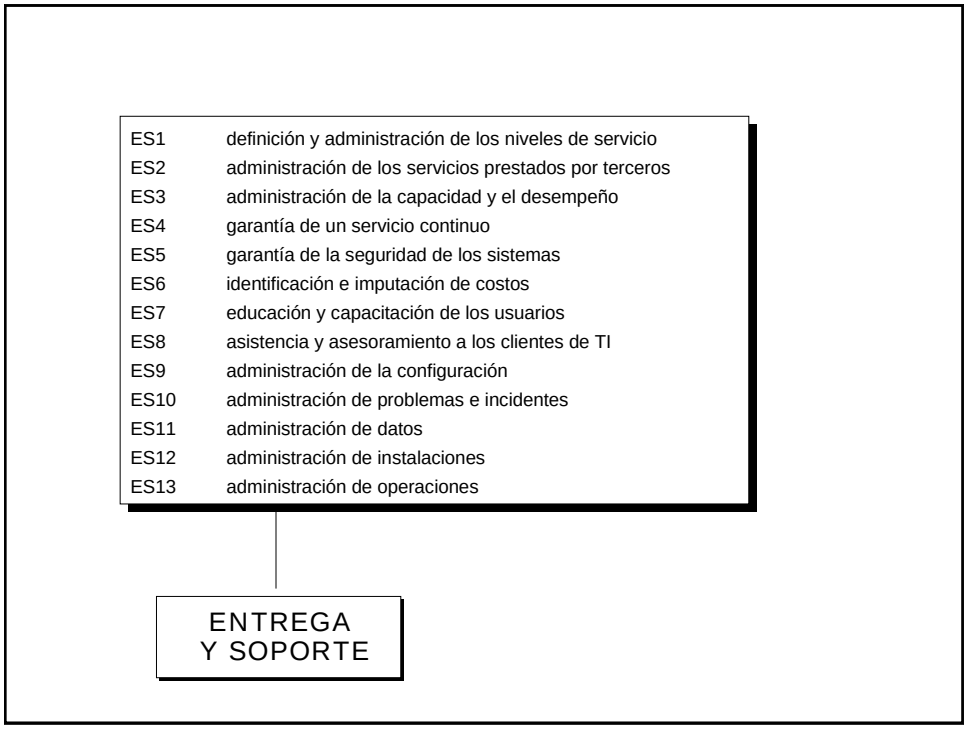
COBIT Security Baseline

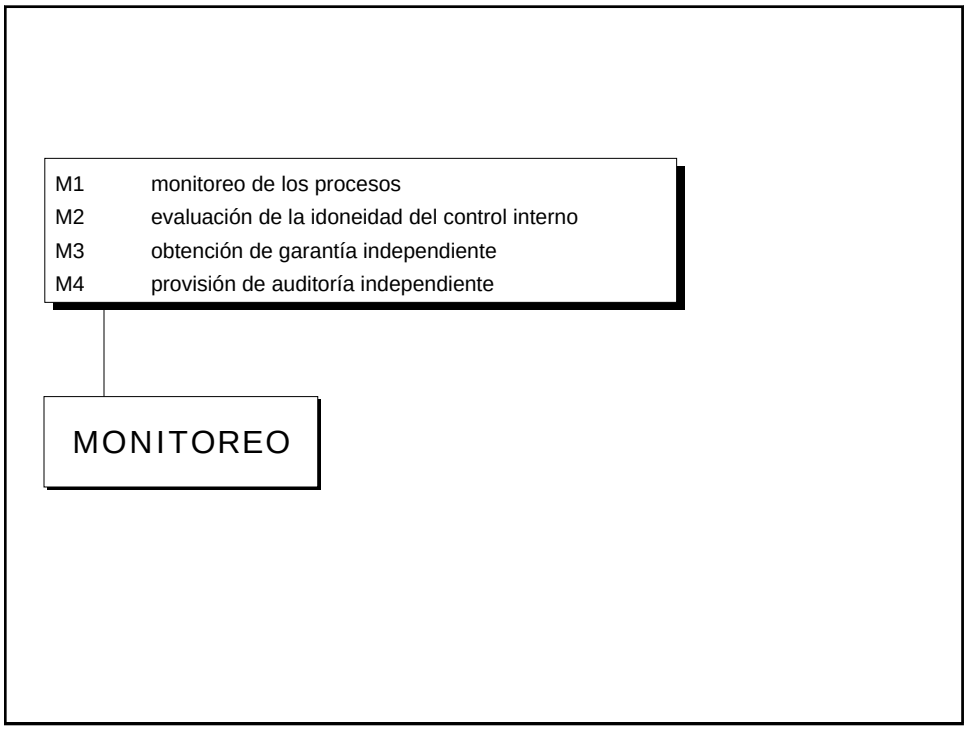
- **Los riesgos técnicos de seguridad:** *Accidentes*
  - Fallas de disco
  - Fallas y sobrecarga de energía
  - Robo físico
  - Problemas de programas




PO1 definición de un plan estratégico de TI
PO2 definición de la arquitectura de la información
PO3 determinación de la dirección tecnológica
PO4 definición de la organización y las relaciones de TI
PO5 administración de la inversión en TI
PO6 comunicación de los objetivos y directivas de la gerencia
PO7 administración de los recursos humanos
PO8 garantía de cumplimiento de los requerimientos externos
PO9 evaluación de riesgos
PO10 administración de proyectos
PO11 administración de la calidad
PLANIFICACION Y ORGANIZACION


AI1 identificación de soluciones automatizadas
AI2 adquisición y mantenimiento del software de aplicación
AI3 adquisición y mantenimiento de la infraestructura tecnológica
AI4 desarrollo y mantenimiento de procedimientos de TI
AI5 instalación y acreditación de sistemas
AI6 administración de cambios
ADQUISICION E IMPLEMENTACION


ES1 definición y administración de los niveles de servicio
ES2 administración de los servicios prestados por terceros
ES3 administración de la capacidad y el desempeño
ES4 garantía de un servicio continuo
ES5 garantía de la seguridad de los sistemas
ES6 identificación e imputación de costos
ES7 educación y capacitación de los usuarios
ES8 asistencia y asesoramiento a los clientes de TI
ES9 administración de la configuración
ES10 administración de problemas e incidentes
ES11 administración de datos
ES12 administración de instalaciones
ES13 administración de operaciones
ENTREGA Y SOPORTE


M1 monitoreo de los procesos
M2 evaluación de la idoneidad del control interno
M3 obtención de garantía independiente
M4 provisión de auditoría independiente
MONITOREO

COBIT Security Baseline

- **Planificación y Organización**

Definir un plan estratégico de TI — Definir la arquitectura tecnológica

1. Basándose en el impacto de negocio, los datos no deben ser mal utilizados, los servicios deben estar disponibles y las transacciones deben se confiables

Definir la organización y relaciones de TI

2. Definir las responsabilidades específicas por la gestión de seguridad

Comunicar los objetivos y directivas de la gerencia

3. Comunicar periódicamente las reglas para la implementación la seguridad

Administración de recursos humanos

4. Al contratar, verificar las referencias
5. Obtener, a través de contratación o entrenamiento, las habilidades necesarias para dar soporte a seguridad
6. Asegurar que ninguna tarea de seguridad importante es extremamente dependiente en un solo recurso

Asegurar el cumplimiento con los requisitos externos

7. Identificar lo que necesita ser hecho para cumplir los requisitos, los derechos de propiedad intelectual y otros requisitos

Evaluación de riesgos

8. Discutir con el personal clave lo que puede salir mal con la seguridad de TI y cómo podría impactar significativamente los objetivos de negocio
9. Establecer el entendimiento del personal de la sensibilidad y consideración de la relación costo-eficacia de los recursos necesaria para administrar los riesgos de seguridad identificados

COBIT Security Baseline

- **Adquisición e Implementación**

Identificar soluciones automatizadas

10. Considerar la seguridad cuando se identifican soluciones automatizadas

Adquirir y mantener la infraestructura tecnológica

11. Garantizar que la infraestructura tecnológica soporte apropiadamente las prácticas de seguridad automatizadas
12. Considerar que requerimientos de seguridad adicionales son necesarios para proteger la infraestructura
13. Identificar y monitorear los fuentes para mantenerlos actualizados con los parches de seguridad

Desarrollar y mantener procedimientos

14. Asegurar que el personal conoce cómo integrar la seguridad en los procedimientos del día a día

Instalar y acreditar sistemas

15. Probar el sistema verificando los requisitos funcionales y operacionales de seguridad
16. Realizar la aceptación final de seguridad, evaluando todos los resultados contra las metas de negocio y los requisitos de seguridad

Administrar cambios

17. Evaluar todos los cambios, incluidos los parches, para establecer el impacto sobre la seguridad; basado en el impacto, realizar una adecuada comprobación antes de a hacer el cambio
18. Registrar y autorizar todos los cambios, incluidos los parches

COBIT Security Baseline

- **Entrega y Soporte**

Definir y administrar niveles de servicio

19. Asegurar que la gerencia establezca los requisitos de seguridad y regularmente efectúe revisiones del cumplimiento de los acuerdos de nivel de servicio

Administrar servicios prestados por terceros

20. Evaluar la capacidad profesional de terceros y asegurar que ellos proporcionan la seguridad adecuada
21. Considerar la dependencia de terceros proveedores de servicios por los requisitos de seguridad

Garantizar un servicio continuo

22. Identificar las funciones de negocio e información críticas y aquellos recursos que son críticos para dar soporte
23. Establecer los principios básicos para salvaguardar y reconstruir los servicios de TI
24. Definir qué necesita ser resguardado y almacenado externamente para apoyar la recuperación del negocio

Garantizar la seguridad de los sistemas

25. Implementar las reglas para controlar el acceso a los servicios en base a las necesidades individuales
26. Asegurar que se asigna la responsabilidad para administrar todas las cuentas de usuario y 'tokens' de seguridad para controlar dispositivos, etc..
27. Detectar, registrar e informar violaciones de seguridad importantes
28. Asegurar que las instrucciones de seguridad son adecuadas y cumplen con las obligaciones contractuales
29. Forzar el uso de software antivirus y mantener actualizadas las definiciones
30. Definir la política sobre qué información puede entrar y salir de la organización y configurar la red en concordancia

COBIT Security Baseline

- **Entrega y Soporte (continuación)**

Administrar la configuración

31. Asegurar que el inventario de la configuración de TI es regularmente completado y actualizado
32. Revisar regularmente si todo el software instalado está autorizado y licenciado apropiadamente

Administrar datos

33. Someter los datos a una variedad de controles para verificar la integridad durante la entrada, el procesamiento, el almacenamiento y la distribución
34. Distribuir salidas sensibles solamente al personal autorizado
35. Definir los períodos de retención, requerimientos de archivo y condiciones de almacenamiento para documentos de entrada y salida, datos y programas

Administrar Instalaciones

36. Seguridad física de las instalaciones y activos de TI
37. Proteger el equipamiento de almacenamiento y redes informáticas del daño, robo, pérdida accidental e intercepción

COBIT Security Baseline

- **Monitoreo y Evaluación**

Monitorear los procesos — Adecuados controles internos de acceso

38. Disponer de personal clave que periódicamente monitoree que :
    - los controles de seguridad de acceso son adecuados en comparación a los requerimientos definidos y a las vulnerabilidades actuales
    - las expectativas de seguridad que son necesarias monitorear en forma permanente
    - evalúe cuán bien están funcionando los mecanismos de seguridad y cuán bien se están verificando las debilidades
    - las excepciones se tratan oportunamente
    - el cumplimiento de controles clave

Obtener aseguramiento independiente

39. Obtener, dónde sea necesario, recursos externos competentes para revisar los mecanismos de control de seguridad de información; los accesos otorgados de relativos a la seguridad de información en el cumplimiento de leyes, regulaciones y obligaciones contractuales

COBIT & ISO 17799

Adquisición e Implementación			
Objetivo de Control		ISO 17799	COBIT
Administración de Cambios			
Asegurar que todos los cambios, incluyendo parches, que soportan los objetivos empresariales son realizados de manera segura.	Evaluar todos los cambios, incluso los parches, para establecer el impacto en la integridad, exposición o pérdida de datos sensibles, la disponibilidad de servicios críticos, y validez de transacciones importantes. Basado en este impacto, realice una comprobación adecuada antes de hacer el cambio.	8.1, 10.5	**AI5**: 5.7 **AI6**: 6.4
Asegurar que los procesos de negocio no son impactados en el día a día	Registrar y autorizar todos los cambios, incluso los parches (los cambios de emergencia posiblemente después de hechos)		

COBIT Security Baseline

'Kits' de supervivencia

- Usuarios domésticos
- Usuarios Profesionales
- Gerentes
- Ejecutivos
- Alta Gerencia
- Junta Directiva/Síndicos

COBIT Security Baseline

- **'Kit' de supervivencia N° 1–Usuarios Domésticos**
  - Riesgos de información específicos para Usuarios Domésticos
    - Falta de conocimiento de los peligros del uso de Internet
    - Uso de sistemas operativos viejos y desactualizados
    - Exposición a pornografía u otros medios de comunicación indeseables
    - Uso descontrolado por niños, amigos, etc.,
    - Trabajar desde casa, exponiendo a la información corporativa a nuevas amenazas

COBIT Security Baseline

- **Usuarios Domésticos:** *Precauciones de seguridad para no técnicos*
  - Elegir la actualizaciones automáticas del software de seguridad
  - Instalar y mantener actualizadas las aplicaciones
  - Desconectar la computadora de la red, cuando no está en uso
  - Usar software, proveedores y ‘websites’ reconocidos
  - Hablar con los niños sobre amenazas y riesgos

COBIT Security Baseline

- **Usuarios Domésticos:** *Precauciones de seguridad para técnicos*
  - Asegurar que la protección del software antivirus está configurada correctamente (analizar adjuntos)
  - Use un ‘firewall’
  - No ejecute programas de origen desconocido
  - Usar herramientas de software para generar resguardos (back-up)
  - Contactar a los proveedores de servicio con respecto a brechas de seguridad
  - Hacer un disco de 'buteo' para recuperar en el caso que el equipo sea dañado o comprometido

COBIT Security Baseline

- **'Kit' de supervivencia Nº 2–Usuarios Profesionales**
  - Riesgos de información específicos para Usuarios Profesionales
    - Falta de conocimiento de políticas corporativas de seguridad y procedimientos y de las responsabilidades personales,
    - Pobre apreciación del valor de la información de la organización
    - Acceso compartido con colegas o amigos
    - Mezcla entre la computación laboral y personal
    - Uso de dispositivos de computación cuando está fuera de la oficina

COBIT Security Baseline

- **Usuarios Profesionales:** Lo '*que hay que hacer'...*
  - Proceda a:
    - comprender su responsabilidad personal e informarse
    - informar incidentes de seguridad y asuntos concernientes
    - hacer resguardos regularmente; cambiar las contraseñas; cerrar con llave su oficina
    - Utilizar eficazmente la información sensible

COBIT Security Baseline

- **Usuarios Profesionales:** Lo que '*no hay que hacer'...*
  - No:
    - desatienda el sistema por períodos prolongados
    - divulgue los datos sensibles a grupos no autorizados
    - saltee las reglas de conexión a red; no desactive la verificación de virus o de recuperación de software
    - ignore los incidentes de seguridad
    - introduzca/cambie dispositivos del equipo sin autorización

COBIT Security Baseline

- **`Kit' de supervivencia Nº 3 – Gerentes**
  - Riesgos de información específicos para Gerentes
    - Dificultades para reconocer el impacto de la brecha de seguridad
    - Falta de conciencia de los riesgos de seguridad
    - Dificultades para brindar directrices
    - Dificultades para monitorear las actividades del personal
    - Dificultades para identificar incidentes o debilidades de seguridad
    - Dificultades para tomar seriamente la seguridad e implementar medidas

COBIT Security Baseline

- **Gerentes:** *Condiciones para verificar*
  - El personal es informado con respecto los papeles y responsabilidades; entrenamiento; recursos de la seguridad
  - Se protege la privacidad y los derechos de propiedad intelectual
  - Usuarios clave prueban la medidas de seguridad
  - Establecer reglas para autorización de cambio y evaluación de impacto
  - Establecer procedimientos de continuidad de operaciones
  - Garantizar que se han establecido protecciones físicas
  - La organización es informada de nuevas amenazas vía evaluaciones de riego

COBIT Security Baseline

'Kit' de supervivencia Nº 4 – Ejecutivos

- Riesgos de información específicos para Ejecutivos
  - Falta de apreciación de la mayoría de los riesgos significativos
  - Dificultades para comunicar la culture/marco de seguridad apropiado
  - Dificultades para delegar las responsabilidades de administración de riesgo
  - Dificultades para identificar donde existen debilidades de seguridad
  - Dificultades para supervisar las actividades de administración de riesgo

COBIT Security Baseline

- **Ejecutivos:** *Preguntas para responder*
  - ¿Cuándo fue completada la última evaluación de riesgo? ¿Esto dio como resultado procedimientos adecuados que aseguran el cumplimiento con las leyes y regulaciones?
  - ¿Qué están haciendo otros? ¿Cómo se compara la organización?
  - ¿Qué entrenamiento existe en seguridad de información? ¿Es adecuado?
  - ¿Qué medidas de protección se establecieron sobre seguridad física de los activos? ¿Son adecuadas?
  - ¿Se estableció un programa de seguridad? ¿Se asignó la responsabilidad de rendir cuentas?

COBIT Security Baseline

- **Ejecutivos:** *Lista de Acciones*
  - Establecer y ejecutar un programa de administración de riesgo
  - Definir/Implementar un estándar de seguridad con normas, métricas, prácticas y procedimientos
  - Asegurar que la estrategia de seguridad de información mitiga y mide los riesgos de manera costo-efectiva, con mínimas interrupciones del negocio
  - Asegurar que los procesos de negocio críticos y la infraestructura de soporte son resistentes a las fallas
  - Garantizar que la seguridad de información encaja dentro del estándar de gobierno de seguridad de información
  - Confeccionar un registro de información, servicios y transacciones disponibles
  - Asegurar que la seguridad de la información es parte integral del ciclo de vida de TI

COBIT Security Baseline

- **'Kit' de Supervivencia Nº 5 – Alta Gerencia**
  - Riesgos de Información específicos para la Alta Gerencia
    - Falta de apreciación de los riesgos significativos
    - Dificultades para asignar una cultura/marco de seguridad apropiada
    - Dificultades para incluir la responsabilidad de la seguridad en el equipo de gerencial
    - Dificultades para identificar las debilidades críticas de la seguridad
    - Dificultades para supervisar las inversiones de administración de riesgo y medir los beneficios obtenidos
    - Dificultades para dirigir la administración de riesgo y conocer cuál es el riesgo residual remanente

COBIT Security Baseline

- **Alta Gerencia:** *Preguntas para responder*
  - ¿Cómo se mantiene informada la Junta de los problemas de seguridad de información?
  - ¿Cuánto se está gastando en seguridad de información?
  - ¿La alta gerencia es consciente de los últimos problemas de seguridad?
  - ¿Cuál es la mejor práctica de la industria? ¿Cómo se compara la empresa?
  - ¿Cuáles son los activos de información alcanzados por las leyes y regulaciones? ¿Qué ha hecho la alta gerencia para asegurar el cumplimiento?

COBIT Security Baseline

- **Alta gerencia:** *Lista de Acciones*
  - Establecer:
    - la organización de seguridad y su función para el desarrollo y entrada en vigencia de las políticas
    - la responsabilidad, rendición de cuenta, y autoridad para las funciones de seguridad
    - programas de continuidad de negocio y de tecnología - claros y pragmáticos- que se prueban y se mantienen

COBIT Security Baseline

- **Alta Gerencia:** *Lista de Acciones (cont.)*
  - Dirigir las auditorías de seguridad de información
  - Incluir la seguridad en las descripciones de puesto de trabajo y aplicar premios y medidas disciplinarias
  - Desarrollar una información clara y regular del estado de la seguridad de información de la organización a la junta directiva; informe sobre el cumplimiento de las políticas, acciones de remediación y proyectos de seguridad

COBIT Security Baseline

‘Kit’ de Supervivencia Nº 6 – Junta Directiva/Síndicos

- Riesgos de Información específicos para los miembros de la Junta Directiva
  - Falta de conocimiento de las exposiciones de riesgo
  - Falta de conocimiento de requisitos legales y de regulaciones
  - Dificultades para entender impacto de las fallas de la seguridad en el negocio, y efecto potencial en los ‘stakeholders’, los segmentos de mercado, la competitividad,
  - Incapacidad para administrar el monitoreo de la capacidad de manejo de riesgos
  - Dificultades para poner el “tone at the top ” con respecto a la seguridad
  - Dificultades para juzgar el valor de propuestas de inversión de seguridad

COBIT Security Baseline

Junta Directiva/Síndicos: *Preguntas para responder*

- ¿Cuándo fue la última vez que la alta gerencia se involucró en las decisiones relacionadas con seguridad?
- ¿La alta gerencia sabe quién es responsable por la seguridad? ¿Todos están al tanto?
- ¿La empresa padeció ataque de virus últimamente?
- ¿La seguridad es considerada un pensamiento posterior o un requisito previo?
- ¿Cuáles serían las consecuencias de un incidente serio de seguridad?
- ¿La Junta Directiva ha solicitado una auditoría independiente de la seguridad de información?

COBIT Security Baseline

- **Junta Directiva/Síndicos:** *Lista de Acciones*
  - Establecer directrices: valores culturales, política/estrategia, perfil de riesgo global, prioridades
  - Asignar responsabilidades a la gerencia – inversiones, monitoreo e informes de seguridad
  - Asegurar que el Comité de Auditoría comprende su papel
  - Informes requeridos de progresos en seguridad y los problemas para auditores
  - Desarrollar prácticas de administración de crisis

Preguntas y respuestas

Rusenas
AUDITORES Y CONSULTORES

Juan de Dios Bel
SOCIO

jbel@rusenas.com.ar
Cel. 54.9.11.4449.6898
www.rusenas.com.ar

Tel/Fax 54.11.4815.9779
Cerrito 836, 3º piso of. 5/6
C1010AAR-Buenos Aires
Argentina

¡Gracias!

Juan de Dios Bel, CISA, CISM
jbel@rusenas.com.ar