Apuntes de Ciberseguridad: Gobierno y gestión de TI: COBIT, Marcos complementarios y Auditoria de seguridad

Ruben Apablaza Muñoz
-OZonE-

COBIT

- Control OBjectives for Information and related Technology
- OBJETIVOS:
  - Entrega de valor
  - Gestión de riesgos
  - Optimización de recursos
  - Medición del desempeño
- Marco de referencia desarrollado por ISACA para el gobierno y gestión de TI
- La última versión es la 2019

Principios CLAVE de COBIT

- 1. Satisfacer las necesidades de las partes interesadas
  - Reconoce la importancia de identificar y SATISFACER las expectativas de TODAS las partes interesadas de la organización.
- 2. Cubrir la empresa de extremo a extremo
  - El gobierno de TI debe abarcar las áreas relevantes tales como:
    - Infraestructura tecnológica
    - Procesos de negocio
    - Seguridad de la información
- 3. Aplicar un marco único integrado
  - Promueve la coherencia, facilita la comunicación y mejora la eficacia de las practicas de gobernanza de TI.
- 4. Facilitar un enfoque holístico
  - Al adoptar un enfoque holístico, las organizaciones pueden comprender mejor el impacto de las decisiones de TI en toda la empresa y tomar decisiones informadas que beneficien a la organización en su conjunto. Esto ayuda a identificar interdependencias, mitigar riesgos y optimizar la asignación de recursos.
- 5. Separar la gobernanza de la gestión
  - Este principio enfatiza la distinción entre gobernanza (establecer objetivos, supervisar y garantizar el cumplimiento) y gestión (implementar estrategias, ejecutar planes y alcanzar objetivos). Al hacer esto se pueden establecer roles y responsabilidades claros, mejorar la rendición de cuentas y optimizar los procesos de toma de decisiones. Esto es importante porque ayuda

a mantener el equilibrio de poderes, reducir los conflictos de intereses y promover una cultura de transparencia.
    - https://www.itamg.com/cobit/

- La principal característica es su capacidad de alinear las actividades de TI con los objetivos estratégicos de la organización, asegurando que la TI respalde y contribuya al éxito empresarial.
- Se complementa con guías detalladas, modelos de procesos, listas de verificación y casos de estudio.

Estructura de responsabilidades y Roles

- COBIT establece una estructura CLARA de responsabilidades y roles en la gestión de TI.
- Algunas formas como lo hace:
  - Definición de procesos claros.
    - Identifica y describe los procesos de TI necesarios para el gobierno efectivo.
  - Matriz RACI
    - Responsable
    - Aprobador
    - Consultado
    - Informado
  - Asignación de roles clave
    - Define las responsabilidades y AUTORIDADES de los roles importantes, los que toman las decisiones.
  - Mapeo a objetivos estratégicos
    - Enlaza los procesos de TI con los procesos estratégicos de la organización.

Matriz RACI

- Herramienta de gestión de proyectos y procesos que se utiliza para definir y comunicar roles y responsabilidades dentro de una organización o equipo.
- RESPONSABLE
  - Responsables de realizar la tarea.
- APROBADOR
  - Quien toma la última decisión
- CONSULTADO
  - Quien da información o asesoramiento de la tarea
- INFORMADO
  - Reciben actualización o comunicación sobre el progreso, pero no tienen un rol activo en la ejecución.

Ejemplo practico

Implementación de COBIT en una organización y/o empresa

1. EVALUACION INICIAL
   - Se evalúa el actual gobierno de TI y se determinan las áreas de mejora.
2. DEFINICION DE PROCESOS
   - Se identifican los procesos de TI CRITICOS y se definen claramente las actividades, responsabilidades y roles asociados.
3. ASIGNACION DE RESPONSABILIDADES
   - Se establece la matriz RACI
4. FORMACION Y CAPACITACIÓN
   - Se capacita a los empleados para capacitarlos con COBIT y sus responsabilidades en el gobierno de TI.
5. SEGUIMIENTO Y MEJORA CONTINUA
   - Se evalúa continuamente la efectividad del gobierno de TI y se aplican mejoras en caso de ser necesario.

Marcos de referencia *COMPLEMENTARIOS*

- ITIL (Information Technology Infraestructure Library)
  - Se centra en la prestación de servicios de TI de manera eficiente y efectiva.
  - Enfoque en procesos y mejores prácticas.
- ISO 27001
  - Estándar internacional de gestión de seguridad de la información.
  - Mas enfocado en la evaluación de la seguridad de la información.
  - Implementación de controles específicos y evaluación de auditorias internas y externas.

Ambos marcos son *COMPLEMENTARIOS* y pueden ser utilizados en conjunto para mejorar la seguridad de la información, cumplir con los requisitos normativos (ISO 27001) y cumplir los objetivos del negocio (ITIL).

Auditoria de seguridad

Proceso sistemático para evaluar y mejorar la seguridad de la información.

- Objetivos
  - Evaluación de controles
    - Se verifica la *efectividad de los controles de seguridad*.
  - Detección de vulnerabilidades
    - Detectar y *mitigar* vulnerabilidades y riesgos de seguridad.
  - Cumplimiento normativo
    - Verificar el cumplimiento de las políticas, regulaciones y estándares de seguridad *tanto internos como externos*, asegurándose que se cumple con leyes y regulaciones de la industria.
  - Documentación de auditoria
    - Se documentan los *hallazgos y recomendaciones resultantes*, proporcionando una base para la mejora continua.

Tipos de auditoría DE SEGURIDAD

- INTERNA
  - Realizada por personal interno para evaluar políticas y procedimientos internos de seguridad.
- EXTERNA
  - Por auditores externos independientes desde una perspectiva imparcial.
- DE CUMPLIMIENTO
  - Centrada en verificar el cumplimiento de leyes, regulaciones y estándares de seguridad.
- DE PROCESOS
  - Revisa los procesos específicos relacionados con la seguridad de la información.

Además de estas 4 se señalan las siguientes:

- Forense
  - Identificar y recopilar evidencias digitales.
- Web
  - Conocer la seguridad de apps y servicios.
- Código
  - Pruebas de calidad
- Hacking Ético
  - Realizar test de intrusión
- Vulnerabilidades
  - Detectar los posibles agujeros de seguridad
- Redes
  - Mapear la red de dispositivos conectados
- Físicas
  - Proteger externamente la zona perimetral

Roles y responsabilidades de los auditores

- AUDITOR LIDER
  - Planificación y coordinación
  - Asegurar cumplimiento de objetivos
- AUDITORES DE CAMPO
  - Recolección de evidencia
  - Entrevistas y pruebas de seguridad
- AUDITADOS
  - Proporcionar acceso a información
  - Cooperar con el proceso de auditoria


cybersecurity
incubenapablaze
dutsdirbih
Made by OZonE
cybersecurity