

## Resumen Auditoria

### 1. Gestión de la calidad de los recursos informáticos

#### ¿Qué es la calidad?

- Es el conjunto de propiedades y características de un producto o servicio, que confiere su aptitud para satisfacer las necesidades dadas

#### En los proyectos se distinguen 3 procesos de gestión de calidad

1. Planificación de la calidad
2. Aseguramiento de la calidad
3. Control de calidad

#### Auditoria de la calidad

- Revisión estructurada de las otras actividades de la administración de la calidad
- Sirven para reducir inconvenientes, errores, mejorar la eficacia de la empresa y acercarla a los niveles de calidad reconocibles en el mercado y ante la competencia
- Se centra en la observación y análisis del sistema con miras a mejorar la calidad en dichos sistemas, procesos y organización.
- Ayuda a ofrecer a nuestros clientes una imagen de calidad y corporación exitosa.

#### Objetivo de la auditoria

- Se centra en la observación y análisis del sistema con miras a mejorar la calidad.

#### ITIL: Servicios de Información

**CMMI:** es un modelo que contiene las mejores prácticas y que provee a las organizaciones de aquellos elementos que son esenciales para que los procesos de negocios sean efectivos.

- Ayuda a mejorar la satisfacción del cliente
- Proporciona un marco y lenguaje común
- Permite a los usuarios puedan enfocarse
- Aporta años de experiencias
- Permiten producir productos y servicios de alta calidad

#### Quiz 12/8

- Es un conjunto de normas de gestión de calidad → **ISO 9000**
- Es el conjunto de propiedades y características de un producto o servicio, que confiere su aptitud para satisfacer las necesidades dadas → **Calidad**
- Sirven para reducir inconvenientes, errores, mejorar la eficacia de la empresa y acercarla a los niveles de calidad reconocibles en el mercado y ante la competencia.  
→ **Auditoría de la Calidad**
- Son mejores prácticas orientadas a la gestión de los servicios de TI, su calidad y procesos. → **ITIL**
- Se centra en la observación y análisis del sistema con miras a mejorar la calidad en dichos sistemas, procesos y organización. → **Auditoría de la Calidad**
- Planificación de la calidad, aseguramiento de la calidad, control de Calidad → **Gestión de la Calidad**

- Muchos riesgos asociados a la entrega del servicio o producto de TI en la organización. Por lo que va a variar según sea el estilo de empresa y de la importancia de los servicios que se presten en la misma. → **Estándares de Calidad**
- La auditoría de calidad consiste en una revisión estructurada de las otras actividades de la administración de la calidad → **Auditoría de la Calidad**

## 2. Riesgos y Control a nivel de TI

### ¿Qué es un riesgo?

- Una situación no deseada
- Una organización no puede lograr sus objetivos
- No existe una certeza sobre la integridad y confiabilidad de los datos
- Incertidumbre de que ocurra una pérdida

**Consecuencia:** resultados tangibles del riesgo

**Exposición:** susceptibilidad o percepción hacia una pérdida

**Amenaza:** es una combinación del riesgo, la consecuencia y la posibilidad de que el evento negativo se materialice.

**Medición:** métrica para identificar el grado de impacto de un riesgo

### Clasificación de los riesgos

#### **RIESGOS CORPORATIVOS -> RIESGOS DE LOS PROCESOS -> :**

**Tecnológicos:** pérdida de información, acceso no autorizado, pérdida de confidencialidad, fraude o hurto

**Ambientales:**

**De imagen:** producto en mal estado, robos, errores de la información

**Económicos:** crédito, liquidez, tasa de interés, mercado

**De personas:**

**Operacionales:** mal uso de productos, problemas de seguridad, error en la operación de los sistemas de TI

**De direccionalidad:**

**Legal:** atrasos en pago de impuestos, atrasos en pagos

### Administración del Riesgo

- Mejora la toma de decisiones mediante un proceso constante y participativo basado en el conocimiento y guía de riesgos.
- Proceso interactivo e iterativo base en el conocimiento, evaluación y manejo de riesgos y sus impactos.

### Beneficios para la organización

- Facilita el logro de los objetivos de la organización
- Hace a la organización más segura y consciente de sus riesgos
- Mejoramiento continuo del Sistema control Interno
- Optimiza la asignación de recursos

### Beneficios para la Auditoría

- Soporta el logro de los objetivos de la Auditoría

- Estandariza en el método de trabajo
- Evaluaciones enfocadas en riesgos
- Mayor cobertura de la administración de riesgos}

### **Pasos**

1. Establecer marco general
2. Identificar riesgos
3. Análisis de riesgos
4. Evaluar y priorizar riesgos
5. Tratamiento del riesgo
6. Monitoreo y revisión

### **Tópicos para identificar riesgos**

1. Debe impactar los objetivos
2. No deben ser causales o factores
3. Son amenazas
4. Se trata de identificar
5. Deben ser de alto nivel

**Control:** respuesta de la administración entre el riesgo

- Evitar
- Trasladar
- Asumir
- Reducir

### **Objetivos de Control**

Determinar la existencia de controles adecuados para proteger los recursos comprometidos en los sistemas:

1. Protección de los activos de la empresa
2. Obtención de información veraz
3. Promoción de la eficiencia en la operación del negocio

### **Objetivos de Control Definidos**

- Confidencialidad
- Disponibilidad
- Integridad
- Obj de totalidad
- Obj existencia
- Obj exactitud

### **Controles Institucionales y de TI**

- Al nivel de Alta Gerencia: se fijan en los obj institucionales, establecen políticas y toman decisiones
- A nivel de procesos Institucionales: se aplican controles para actividades específicas de la institución
- Controles generales de TI: para soportar los procesos institucionales proporcionan servicio por lo de forma compartida.

### **Controles Generales**

Son aquellos que están incrustados en los procesos y servicios de TI, ejemplo: desarrollo de sistemas, administración de cambios, seguridad.

### **Controles de Aplicación**

Están incluidos en las aplicaciones del proceso operativo, ejemplo: integridad, precisión, validez, autorización.

### **Quiz 19/8**

- Relacionado con los derechos laborales de los empleados, hacienda pública, etc. → **Riesgos legales**
- Mejora la toma de decisiones mediante un proceso constante y participativo basado en el conocimiento y guía de riesgos. → **Administración del riesgo**
- No existe una certeza sobre la integridad y confiabilidad de los datos. → **Riesgos tecnológicos**
- Una organización no puede lograr sus objetivos → **Riesgo**
- Riesgos de uso del artículo/servicio por parte de los clientes. → **Riesgos operacionales**

## **3. Auditoria de los servicios de TIC**

Proceso de comunicación de resultados

- Discusión sobre el curso de la Auditoria con el nivel operativo y gerencial de la entidad
- Preparar un borrador de informe para la entidad
- Discutir el borrador del informe con el nivel gerencial
- Remitir informe a la alta dirección de la entidad
- Trabajo cierra el proceso principal de la auditoría, con independencia de que haya otras actividades importantes como la supervisión o el seguimiento del progreso
- Deben incluir una opinión

### **El informe**

- Es el elemento final y más trascendente del proceso de una auditoria.
- No hay ninguna estructura de informe que sea norma.

### **Requerimientos de un informe**

- La expresión del objetivo
- Alcance
- Los resultados
- Que cumplan con la Norma 2420

### **Estructura del Informe**

I. Información introductoria

I. Antecedentes

II. Objetivos de la Auditoría

III. Alcance de la Auditoría

IV. Base legal, Objetivos y estructura orgánica de la entidad

- V. Principales funcionarios
- II. Control Interno
- III. Observaciones de Auditoría
- IV. Conclusiones
- V. Recomendaciones
- VI. Firmas responsables (únicamente borrador)

#### **Consejos de un informe**

- La conclusión de primero
- No recargar frases
- Resaltar puntos de mejora
- Evitar el lenguaje negativo

## **4. Comunicación de los resultados**

#### **Retos de Gerentes**

- Planeación estratégica de TI
- Integrar y alinear las metas
- Implementar la mejora continua
- Demostrar el valor de negocio de TI

#### **Principios de la estructura**

-> Requerimientos del negocio -> Recursos de TI -> Procesos de TI ->

#### **Recursos de TI**

- Información
- Aplicaciones
- Infraestructura
- Personas

#### **- Recursos**

1. Principios, Políticas y marcos
2. Procesos
3. Estructuras Organizacionales
4. Cultura, Ética y Comportamiento
5. Información
6. Servicios, Infraestructura y Aplicaciones
7. Personas, Habilidades y Competencias

#### **Ciclo de Vida del Servicio**

1. Estrategia
2. Diseño
3. Transición
4. Operación
5. CSI

## **Definiciones**

**Servicio:** un medio para entregar el valor a los clientes, facilitándoles los resultados que quieren obtener.

- Facilita los recursos
- Mejora el desempeño
- Reduce las limitaciones

## **Definiciones**

**Acuerdo:** un documento que describe un pacto formal

**SLA:** un acuerdo entre el proveedor de servicios de TI y un cliente

**OLA:** un acuerdo entre el proveedor de servicios de TI y otra parte de la misma organización

## **ITSM**

- Conjunto de capacidades organizacionales especializadas para proveer valor a los clientes, en forma de servicios.
- Funciones + Procesos = Capacidad
- Obj: asegurar que los servicios de TI están alineados a las necesidades del negocio.

## **4 P del ITSM**

- Proveedores - Socios
- Personas
- Producto - Tecnología
- Procesos

**Cliente:** contrata los servicios de TI

**Usuario:** usuario de servicio de TI en el lado del negocio

## **Niveles de Servicio**

- Negociar
- Cumplir
- Monitorizar
- Expectativa

## **5. Hallazgos**

**Título:** describe el asunto

**Condición:** que sucedió

**Criterio:** que se incumplió

**Causa:** porque se incumplió

**Efecto:** que conlleva

**Conclusión:** no aplica

**Recomendación:** como eliminar la causa

**Reacción de la administración:** no aplica