

# Guía de Tontos

## TP 5.1 - Seguimiento RRHH

### a) Estandares de desempeño

tenemos estandares de:

- Tiempo: "La cantidad de horas trabajadas será de 8hs. diarias, de 9 a 17"
- Cantidad: "La asistencia mensual debe ser igual o superior al 90% de las jornadas totales" "85% de los equipos reparados según plan de mant."
- Calidad: "Informes presentados según formato establecido"  
"Cableado según normativa de CISCO"
- Costo: "Los costos de capacitación no deben exceder el 80% del salario mensual del empleado"  
"El costo de reparación no debe exceder \$10000 mensuales"

### b) Método de Evaluación de desempeño

Puede ser: jerarquía

Reglas y Procedimientos

APO (Admin por objetivos)

SI verticales

Relaciones laterales

Org. Matricial

#### Herramientas

Observaciones

Escala gráfica

Reporte Estadístico

Reporte Oral

Reporte escrito

#### Evaluación

	Aspectos	Optimo	Bueno	Regular	Deficiente	Malo
Jornada	Asistencia	> 95%	93 - 95	88 - 92	85 - 87	< 85
Productividad	Reparaciones realizadas	:	:	:	:	:
Calidad	Formato informes cumplidos					
Responsabilidad	Tiempo promedio de atención					

→ Porcentaje  
→ \$  
→ minutos  
→ cantidad

### c) Programa de seguimiento

Detallar: a) Carga a evaluar

b) Responsable

c) Momento de evaluación

d) Frecuencia

e) Información a obtener (queremos completar el cuadro de arriba)

f) Herramienta de evaluación

g) Devolución de resultados: (cuando, como)

### d) Ciclo Control RRHH

Describir como aplicaste las etapas



### e) Cuando usar estandares y políticas?

- \* estandares → Para llevar a cabo evaluación de desempeño, comparar con teoría.
- \* Políticas → Para definir estandares que se ajusten a los objetivos organizacionales. También para la auditoría.

## TP 5.2 - Seguimiento SI / TI

### 1) Introducción análisis Operacional

$$a) \text{Calcular: Tasa de llegada } (\lambda) = A/T$$

$$\text{Productividad } (x) = C/T$$

$$\text{Utilización } (U) = B/T$$

$$\text{Tiempo medio servicio } (S) = B/C$$

### b) Determinar tiempo medio de respuesta

$$\text{Tiempo Respuesta } (R)$$

$$\text{Número de Trabajos } (N)$$

$$\text{Tiempo de Reflexión } (z)$$

$$R = \frac{N}{x} - z$$

$$c) \text{Ley del Flujo Forzado} \rightarrow X = \frac{XD}{VD} \rightarrow \text{Productividad de } D \\ \text{Obtener } R$$

$$XD = U/S \rightarrow X = \frac{XD}{VD} \rightarrow R = \frac{N}{x} - z$$

$$d) \text{Determinar Utilización} \rightarrow U = X \cdot S$$

$$e) \text{Calcular Demanda de servicio}$$

$$\text{Tiempo total de transmisión} = T_{petición} + T_{servicio}$$

$$D = \left( \text{bits} \times \text{Paquetes enviados} \right) / \text{Ancho de Banda}$$

### 2) Sintonización

$$a) \text{Para qué sirve} \rightarrow \text{Teoría}$$

$$b) \text{Relacionar con Aplicación SI/TI} \rightarrow \text{Determino la capacidad y agusto más equipos para lograrlo}$$

- b) Identificar problemas en un ejemplo  
 c) Solucionarlos

### 3) Upgrading de sistemas

a) Mejorar un procesador bla bla bla

Aplicar ter de Andhal

## TP 5.3 - Laboratorio

### TP 6.1 - Seguridad SI / TI

#### 1) Escenario

a) Vulnerabilidades, amenazas y riesgos

\* Activos amenazados los 6 de teoría

\* Amenaza: "Acceso a los routers"

"Acceso no autorizado al tráfico de red"

+ Vulnerabilidades: "Falla en el sistema de seguridad WPA2"

"Routers que no pueden actualizar firmware"

\* Riesgos: "Probabilidad de Acceso a los router debido a mala definición en el estandar WPA respecto a utilización de claves y afecte la info personal"

Probabilidad de Amenaza debido Vulnerabilidad y afede activo

Clasificación { Logico - fisico      0      Pasivo - Activo  
 Accidental - Deliberado }

#### c) Redactar Políticas

Prohibitiva: "Se puede navegar SOLO en webs con cifrado https"

Medidas: "Navegar con VPN"

(Prevención, Detección, correctivo)  
 "Definir Patrones de contraseñas seguras"

→ TOTAL

#### 2) b) Análisis de Riesgos

Perdida esperada = Perdida potencial (\$) \* Frecuencia

Frecuencia de perdida = Prob. de agresión \* Prob. de éxito

Activo	Descripción	Valor unitario	Cant	Valor Total
Amenaza	Prob. Agresión	Prob. éxito	Frec. Perdida	:

c) Determinar Consecuencias de la amenaza

Primaria: "Perdida de info"

"Perdida de Operatividad"

Secundaria: "Imagen de la empresa"

"Caida de las acciones"

"Perdida de confianza de los clientes" (2)

d) Riesgo Propuesto por Robson  
Aregar Costos \$ a la definición anterior.

## Manejo del Riesgo

Estrategias → Asumir Riesgo  
Prevenir riesgo  
Transferir riesgo  
Reducir riesgo

- \* Definir Contramedidas para cada Riesgo. (Líneas de defensa)
- \* Definir Políticas

## Recuperación ante Desastres

Detallar Fases:

- 1) Evaluar y Comunicar desastres
- 2) Volver a operar provisoriamente
- 3) Restablecer operación de equipos
- 4) Peritaje informático para descubrir origen del ataque.

## TP 6.2 - Auditoría SI

- a) Elementos de auditoría →
- \* Sujeto de la auditoría "Quién"
  - \* Objetivo de la auditoría "Para qué"
  - \* Alcance "Temas a evaluar"
  - \* Planif audit Preliminar "Fuentes para poder auditar"
  - \* Procedimiento auditoría "Etapas y actividades"
  - \* y Pasos p/ recolección de datos
  - \* Procedimientos evaluar la prueba o revisar resultados
  - \* Proc para comunicar a la gerencia
  - \* Reporte de auditoría.
- "Niveles de aceptación, observaciones y posibles formas de recomendar"  
"Objetivos de control"

## b) Áreas de auditoría

informática y otros elementos.

- 1) Evaluación función informática
- 2) Evaluación de sistemas y procedimientos
  - a) Desarrollo de sistemas
  - b) Sistemas instalados
- 3) Evaluación de procesos de datos, sistemas y equipos
- 4) Evaluación de seguridad
- 5) Evaluación de los aspectos legales de los sistemas y la info.

## c) Utilidad de la auditoría

Chamuyo con funcionamiento y calidad del ambiente informático  
Para cumplir objetivos organizacionales → Debilidades y fortalezas

## Plan de auditoría

### 1) Definir alcance y objetivos

"Objetivos teóricos, aplicarlos al escenario"

Alcance: definir los ítems que entran en la auditoría  
Sujetos → función y los sistemas en SI

limitar en el  
área de  
informática

### 2) Fuentes de evidencia

Entrevistas

Manuales

Documentación

Organigrama

Inspecciones directas

Descripción y análisis del Carga

Plan estratégico !!

### 3) Equipo auditor

Contraloría interna → lleva a cabo la auditoría

Jefe de auditoría

Auditor supervisor

Analista de documentación

Auditor administrativo

Auditor de RRHH

Especialista en Seguridad

Especialista en redes

Experto en BD

Experto en desarrollo de Proyectos

} Exponer Funciones a cumplir

### 4) Programa de trabajo

Objetivo	Responsable	Requerimientos iniciales	Fecha Inicio	Fecha Fin	Total de días
"Verificar control del ambiente informático cubre aspectos centrales de la gestión SI/TI "	"Auditor SI, Especialista en Seguridad, Especialista en redes"	"Políticas de control, Entrevistas personal de informática, inventario HW y SW"	"16/10/19"	"29/10/19"	"10"