ENS
indicadores
824 + ITS + inés

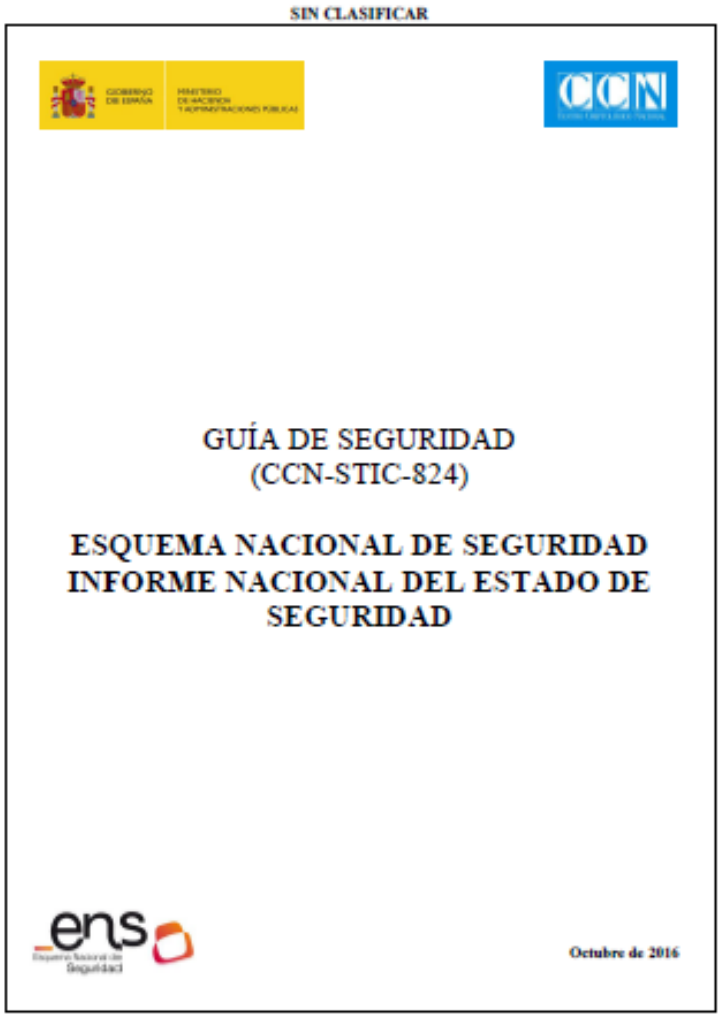
José A. Mañas

enero de 2017

índice

824 - ENS

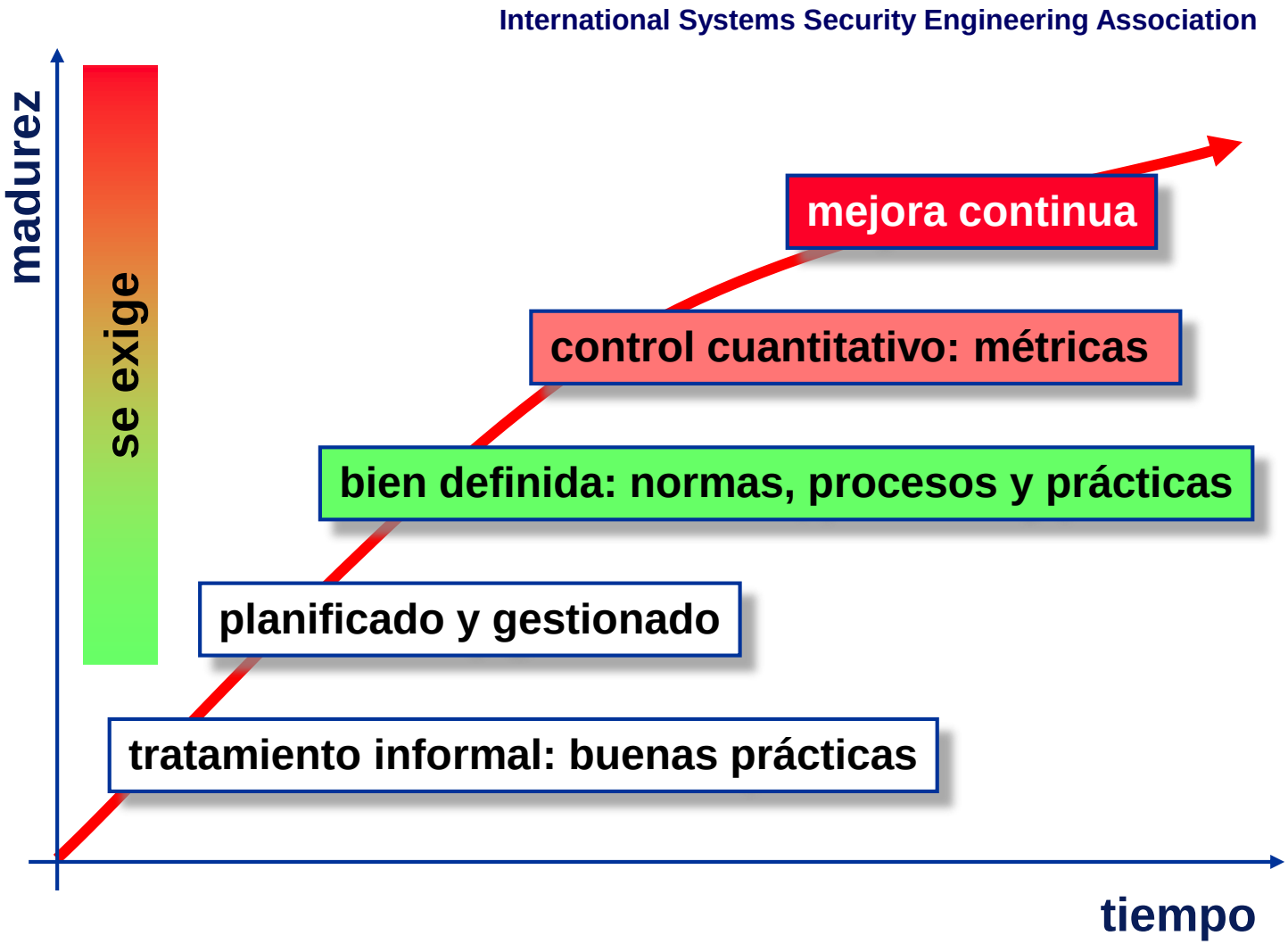
1. **métricas e indicadores**
2. KRI – indicadores críticos



métricas

- regla #1
  - todo se puede medir
    la cuestión es saber
    - ¿qué nos interesa?
    - ¿que vamos a decidir en base a la medida?
- tipos de medidas
  - clases sin orden
  - clases ordenadas
  - valores numéricos

ejemplo: madurez



objetivos

- Saber dónde estamos
  - indicadores de cumplimiento
- Saber si lo estamos haciendo bien
  - indicadores de eficacia – si estamos seguros
    - indicadores de impacto en el negocio
  - indicadores de eficiencia – si el coste es proporcionado
- Para poder tomar decisiones = gestionar la seguridad
  - medias preventivas
  - reacción
  - recuperación
  - previsión de contingencias

¿qué?

- Se pueden recopilar y medir infinitas cosas
  - ¡será por datos?
- Sólo nos debe preocupar lo que nos da una respuesta (positiva negativa)
  a nuestras preocupaciones

"No hay viento favorable
para el barco que no sabe adónde va."
L. A. Seneca

tipos

- datos: inventario

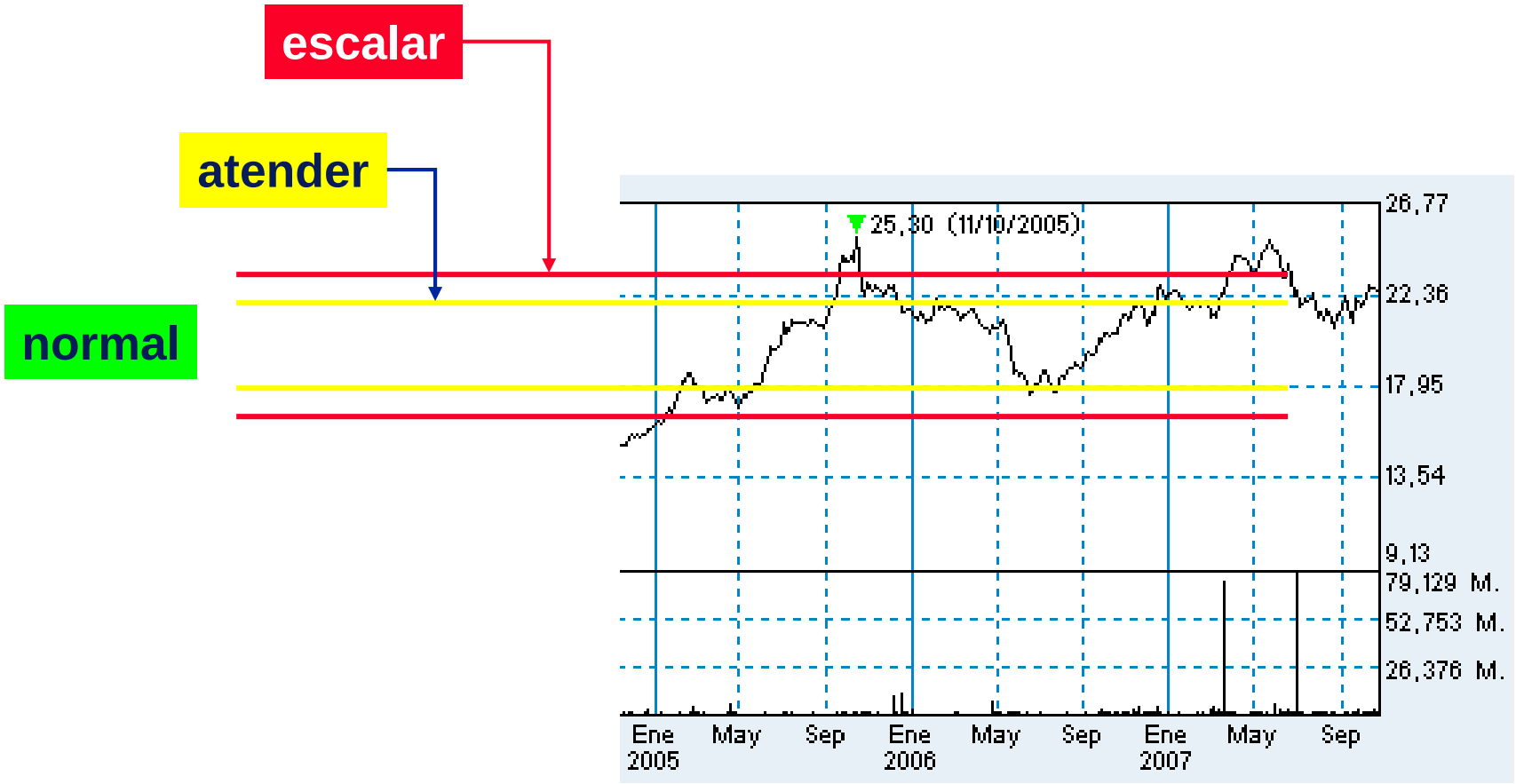
- implantación: el objetivo es el 100%
- de eficacia: conseguir los objetivos
- de eficiencia: con un consumo proporcionado
- de misión: objetivo de negocio

- predictivos: anticipan problemas
- detección de problemas
- forenses: análisis

fuentes de información

- Inventario
  - para relativizar: principio de proporcionalidad
- Cumplimiento
  - útil para anticipar problemas
- Auditorías técnicas y de negocio
  - útiles para anticipar problemas
- Medidas de procesos
  - eficiencia y anticipación
- Sistema de gestión de incidencias
  - eficacia del sistema de seguridad
- Registros de actividad (logs)
  - síntomas de compromiso / evaluación de impacto

umbrales


escalar
atender
normal
25,30 (11/10/2005)
26,77
22,36
17,95
13,54
9,13
79,129 M.
52,753 M.
26,376 M.
Ene 2005
May
Sep
Ene 2006
May
Sep
Ene 2007
May
Sep

cumplimiento: anexo ii

- Objetivo de madurez

	madurez					
	L0	L1	L2	L3	L4	L5
ALTA	L0	L1	L2	L3	L4	L5
MEDIA	L0	L1	L2	L3	L4	L5
BAJA	L0	L1	L2	L3	L4	L5
categoría						

30. Umbrales de madurez; véase sección 2.1.

categoría	rojo inferior	amarillo inferior	nivel adecuado
ALTA	≤L2	≤L3	L4 o superior
MEDIA	≤L1	≤L2	L3 o superior
BAJA	≤L0	≤L1	L2 o superior

- Índices
  - de madurez: valor medio de las medidas aplicables
  - de cumplimiento: ídem acotado por el objetivo

procesos críticos

el orden importa y mucho

Proceso	madurez
Proceso de autorización [org.4]	
Análisis de riesgos [op.pl.1]	
Gestión de derechos de acceso [op.acc.4]	
Gestión de incidentes [op.exp.7]	
Concienciación y formación [mp.per.3 + mp.per.4]	
Configuración de seguridad [op.exp.2] + Gestión de la configuración [op.exp.3]	
Mantenimiento [op.exp.4] + Gestión de cambios [op.exp.5]	
Continuidad de operaciones [op.cont.1 op.cont.2 op.cont.3 mp.if.9 mp.per.9 mp.eq.9 mp.com.9 mp.info.9 mp.s.9 op.ext.9]	

indicadores

valoración

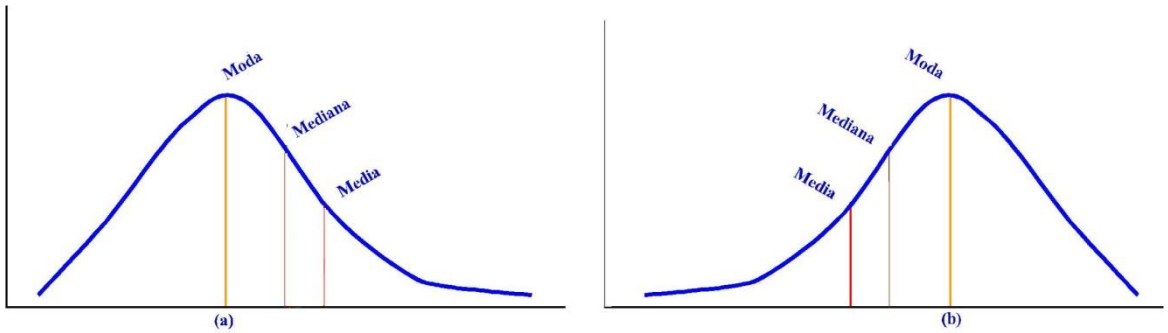
- Estimación de la eficacia de las medidas del ENS

-	NA	no aplica
0%	L0	inexistente
10%	L1	inicial / ad hoc
50%	L2	reproducible, pero intuitivo
80%	L3	proceso definido
90%	L4	gestionado y medible
100%	L5	optimizado

madurez

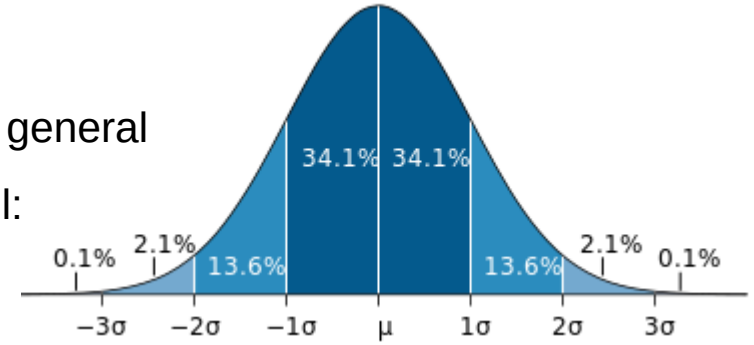
valores numéricos

- estadísticos
  - nos interesa el valor “medio”
  - nos interesa la dispersión de valores
- “valor medio”
  - media – media aritmética
  - Q(50) – mediana
    - el 50% está por debajo
    - el 50% está por arriba
    - es menos sensible a los valores extremos

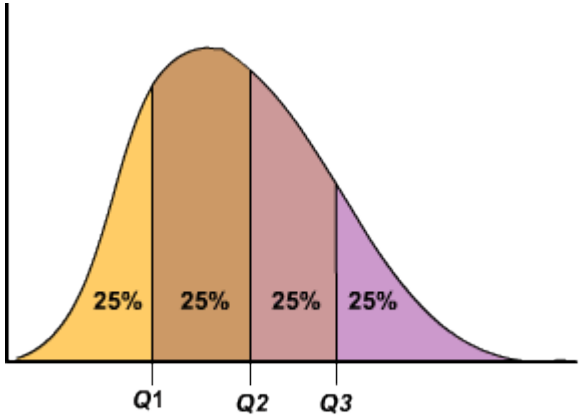


valores numéricos

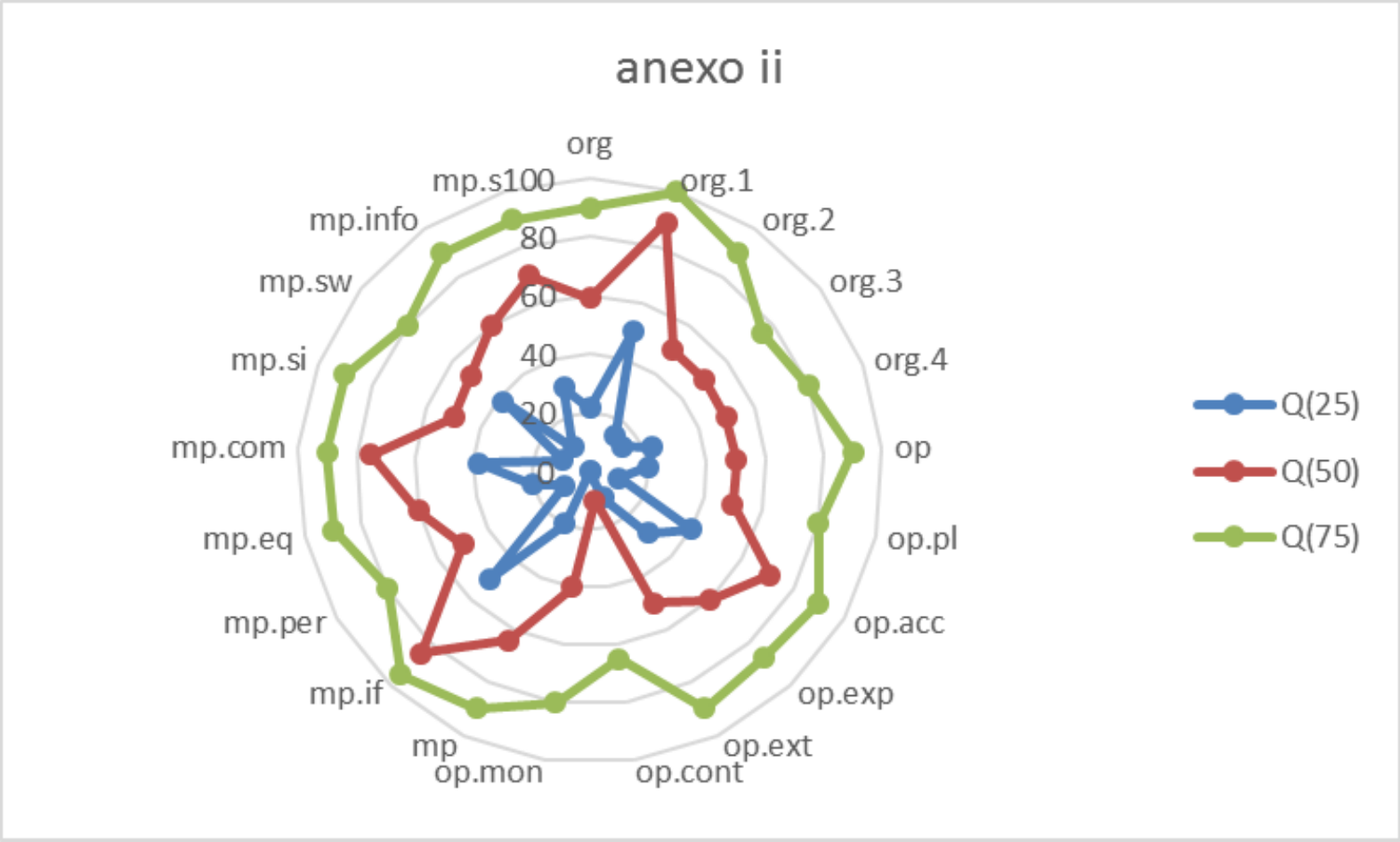
- medida de la dispersión
  - std – desviación estándar muestral
    - es difícil darle una interpretación en general
    - si la distribución es gausiana es fácil:



- cuartiles
  - **el 50% está por debajo de Q(50)**
    el 50% está por encima
  - **el 50% está entre Q(25) y Q(75)**
  - el 25% está por debajo de Q(25)
    el 75% está por encima
  - el 75% está por debajo de Q(75)
    el 25% está por encima



madurez anexo ii



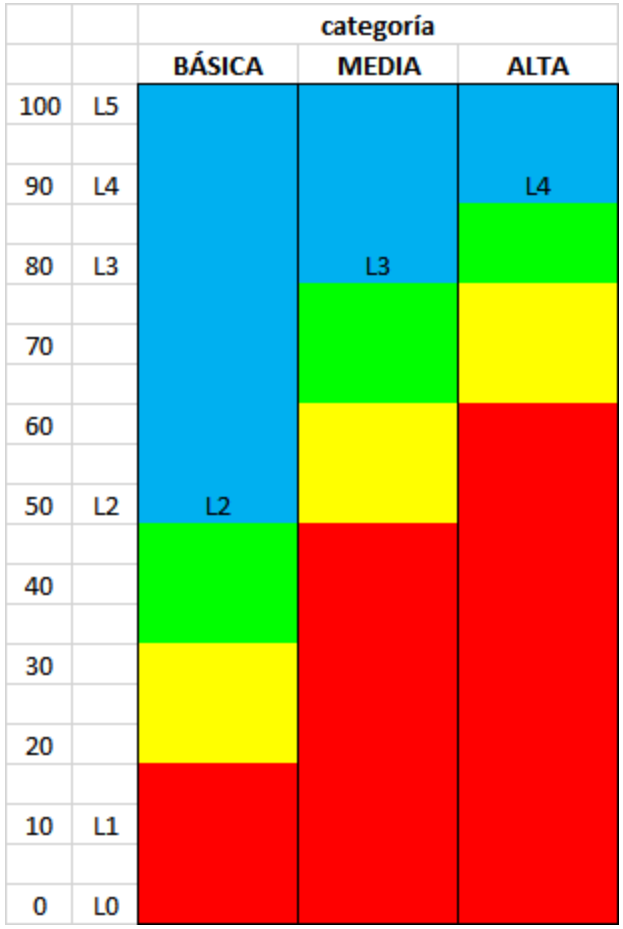
nota

- IM – indicador de madurez
  - 0 .. 100
  - mide la madurez de todas las medidas del anexo ii que sean útiles (aplicables) para la seguridad del sistema
  - la interpretación depende de la categoría
- IC – indicador de cumplimiento
  - 0 .. 100
  - mide la cercanía al nivel de madurez adecuado en función de la categoría del sistema
    - sólo las medidas que son obligatorias por anexo ii
    - sólo las medidas que son útiles (aplicables)
  - valor absoluto

nota: otras interpretaciones

- IM – índice de madurez
  - mide la seguridad real
  - a más alto, más seguro es el sistema
- IC – índice de cumplimiento
  - mide la seguridad formal
  - a más alto, más cumplidor es el organismo

IM - índice de madurez



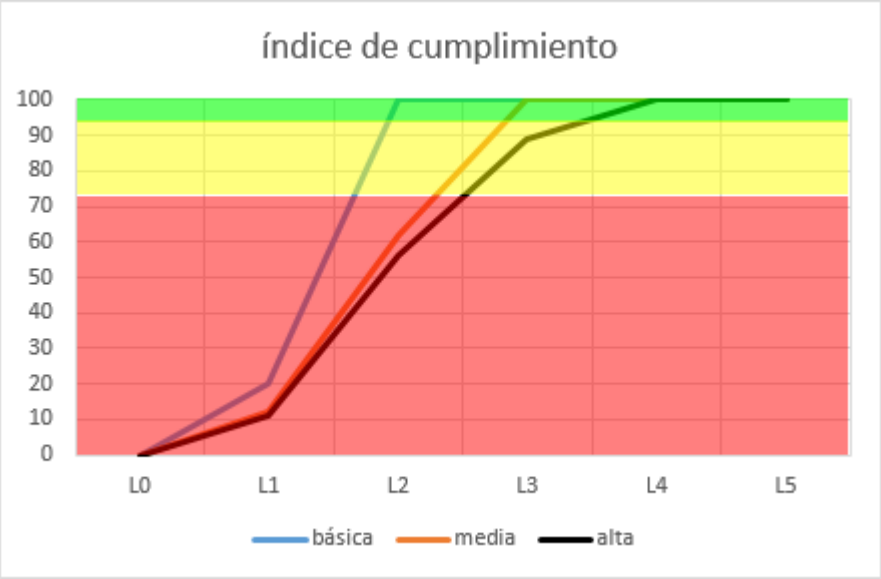
de más
correcto
insuficiente
peligroso

Umbrales: Índices de madurez

categoría	rojo inferior	amarillo inferior	nivel adecuado
ALTA	< 66%	< 80%	> 80%
MEDIA	< 50%	< 66%	> 66%
BAJA	< 20%	< 33%	> 33%

indicadores

IC - índice de cumplimiento



Umbrales: Índice de cumplimiento (IC)

categoría	rojo	amarillo	adecuado
ALTA	< 75	< 95	> 95
MEDIA	< 75	< 95	> 95
BÁSICA	< 75	< 95	> 95

```python
def cumplimiento(cat, puntos):
    if cat == "ALTA":
        return min(100, puntos * 100.0 / 90)

    if cat == "MEDIA":
        return min(100, puntos * 100.0 / 80)

    if cat == "BASICA":
        return min(100, puntos * 100.0 / 50)
```

métricas de tiempos

- Conjuntos de medidas temporales
  - tiempo de respuesta a un usuario
  - tiempo de cierre de un incidente
- No nos preocupan los extremos sino la tendencia
  - Tmin – buena suerte
  - Tmax – mala suerte
  - T(50) mediana
    - cubre el 50% de los casos
    - objetivo de mejora a medio largo plazo
  - T(90) percentil 90
    - cubre el 90% de los casos
    - objetivo de mejora a corto plazo

índice

824 - ENS

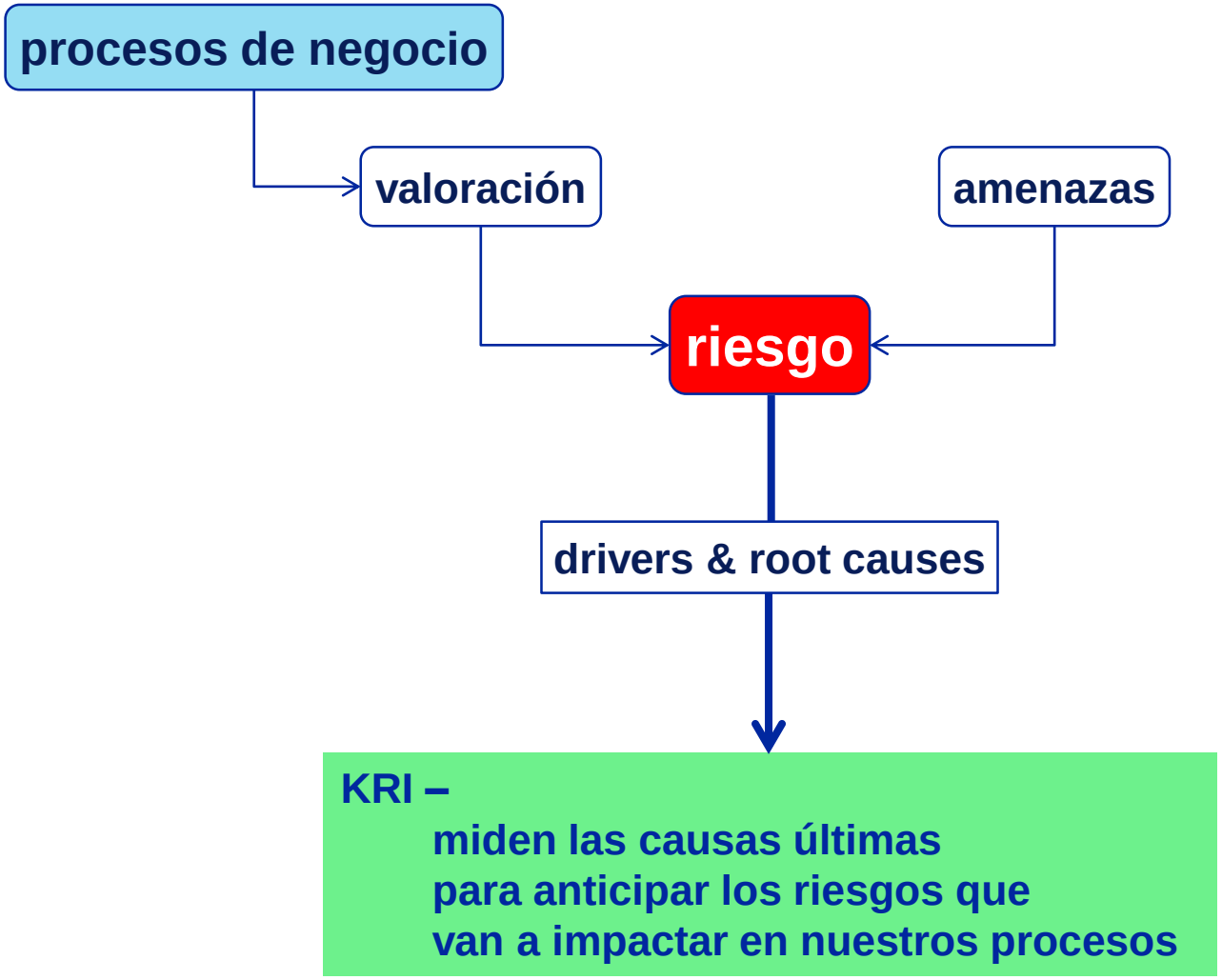
1. métricas e indicadores
2. **KRI – indicadores críticos**

KRI

KRI son métricas que destacan que la organización está sometida o posiblemente se sea sometida a escenarios de riesgo por encima de sus posibilidades
RiskIT, ISACA

- Características
  - Un KRI es una métrica de gestión
    que indica cómo de arriesgada es una actividad
  - Un KPI mide cómo de bien lo hacemos
  - Un KRI avisa de un posible impacto negativo
  - Un KRI es preaviso de posibles sucesos que pueden afectar a la continuidad de las operaciones

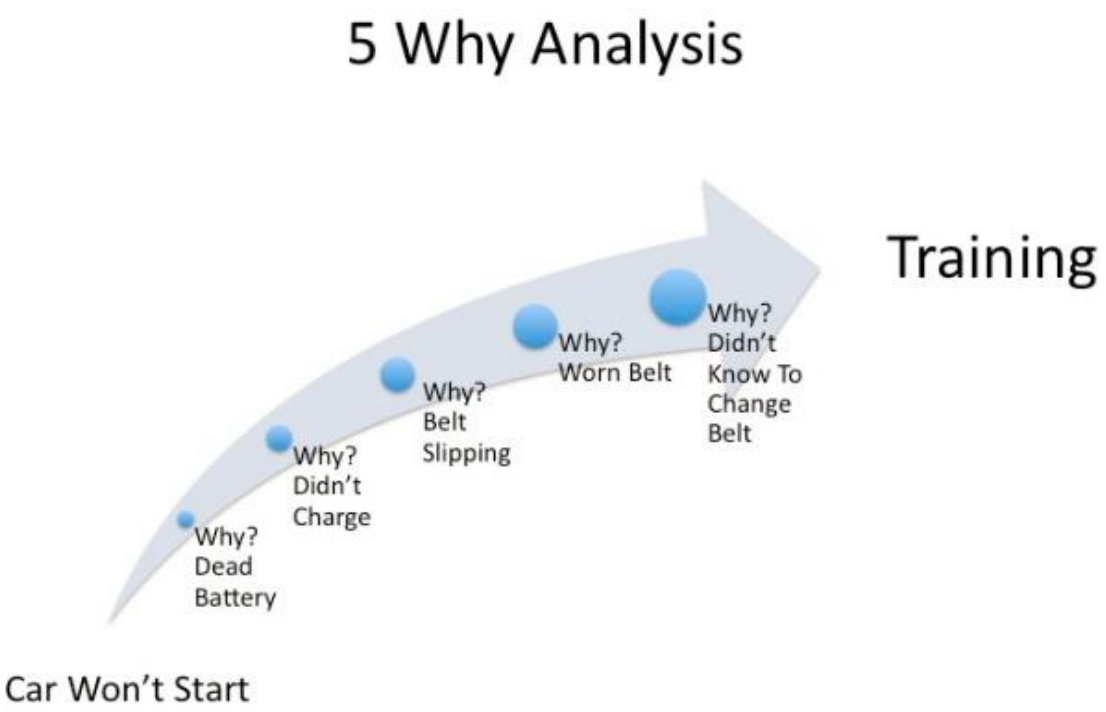
Descubrimiento de KRIs



Leading indicator of event

COSO, 2010

root cause (causa última)



2 preguntas

- ¿qué proceso falló?
- ¿por qué no se detectó a tiempo?

Interés de los KRIs

- Y esto ¿para qué sirve?
  - para tomar decisiones preventivas
    - anticiparse al riesgo
    - deben indicar que se acerca un aumento significativo de la probabilidad de una amenaza que tendría un grave impacto
  - cubrirse las espaldas
    - seguros
  - para profundizar en el análisis y tratamiento con prioridades
    - auto-evaluaciones
    - auditorías internas
  - priorizar recursos / inversiones
    - potenciar el control de ciertas áreas
    - modular el portfolio de productos | servicios

recursos

Recursos dedicados a seguridad TIC sobre el total de recursos dedicados a TIC	
	fracción de horas (en el último periodo anual)

categoría	< 1%	1% - 2%	2% - 4%	4% - 8%	8% - 16%	> 16%
BAJA						
MEDIA						
ALTA						

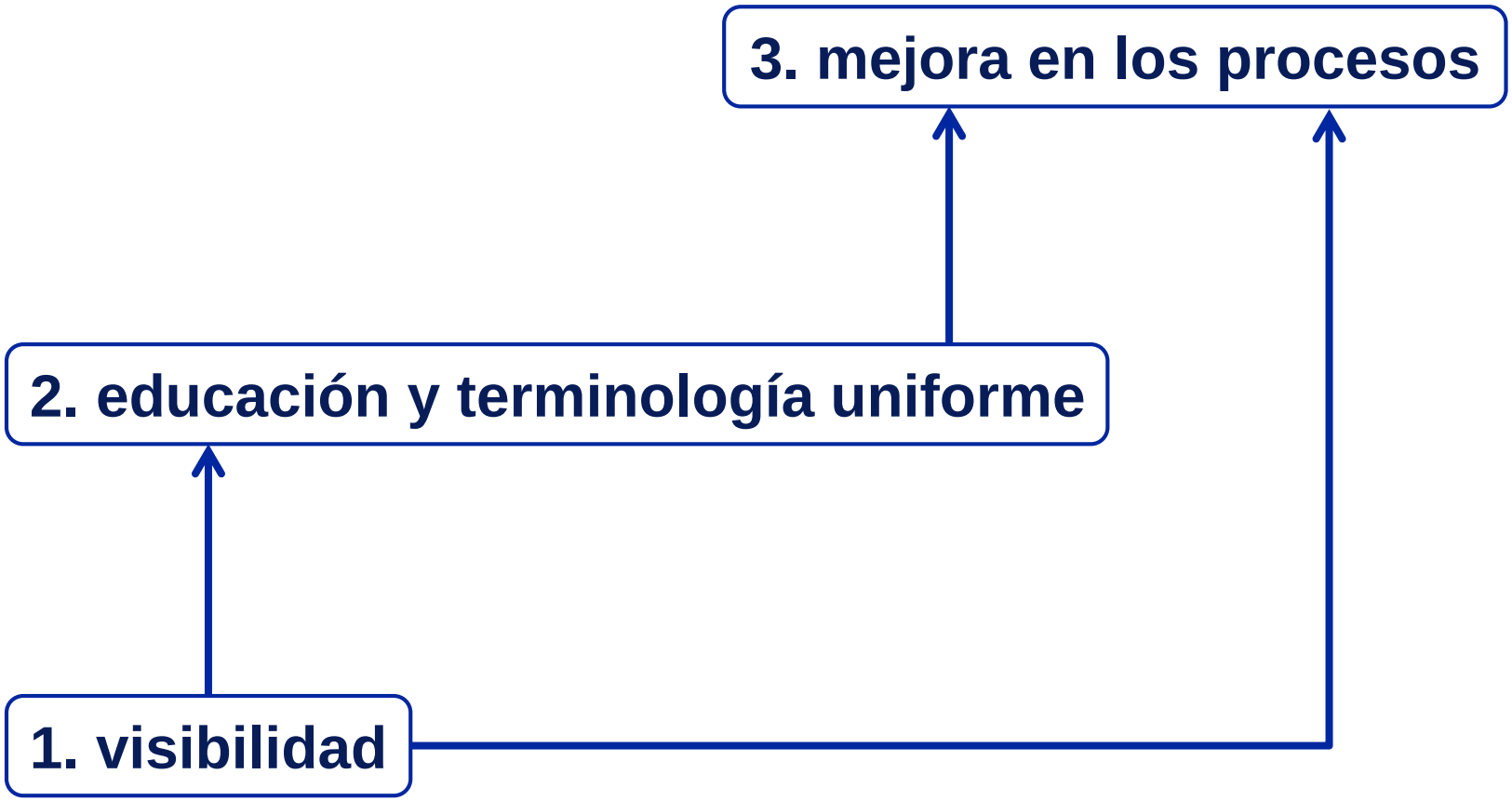
4.7 DESGLOSE DEL PRESUPUESTO

Presupuesto TIC	
☐	fracción del presupuesto TIC dedicado a seguridad TIC
☐	fracción del presupuesto STIC dedicado a concienciación y formación
☐	fracción del presupuesto STIC dedicado a personal externo
☐	fracción del presupuesto STIC dedicado a servicios externos
☐	fracción del presupuesto STIC dedicado a adquisición y mantenimiento de productos

KRI

- Porcentaje de equipos cliente de los usuarios internos sobre el total de equipos del sistema en los que la configuración y su gestión están bajo control exclusivo de los técnicos del organismo
- Porcentaje de equipos de los usuarios internos (BYOD) sobre el total de equipos del sistema
- Porcentaje de equipos de los usuarios internos (BYOD) sobre el total de equipos del sistema en los que la configuración y su gestión están bajo control exclusivo de los técnicos del organismo.
  Es decir, que el usuario NO tiene privilegios de administrador
- Tasa de rotación de personal dedicado a seguridad TIC en el último año

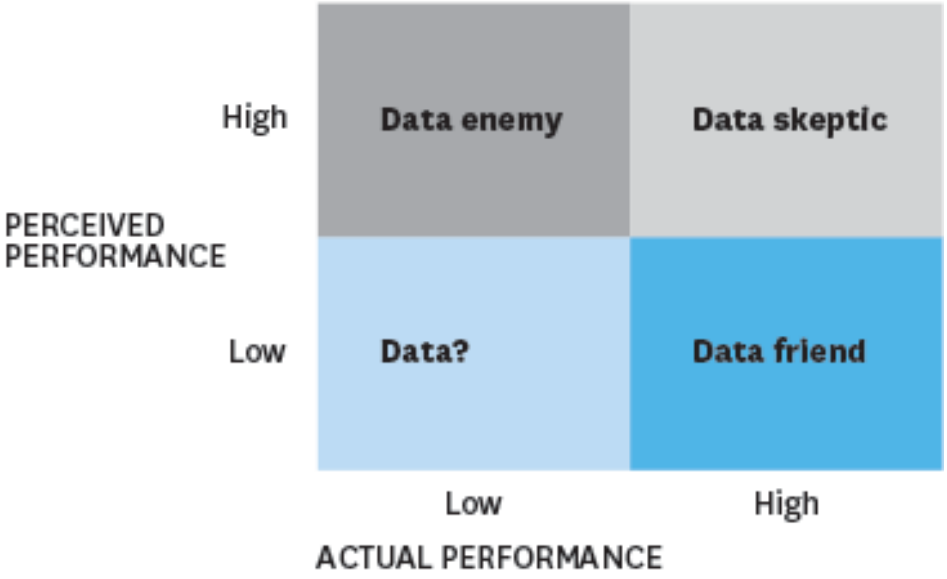
utilidad de las métricas



aliados

FOUR TYPES OF EMPLOYEES AND THEIR WILLINGNESS TO EMBRACE DATA

Star performers are most resistant to data, while unsung workhorses are most likely to embrace it.



SOURCE DOSOMETHING.ORG

HBR.ORG

conclusiones

- a ciegas no vamos a ninguna parte
- saber cómo estamos respecto de los demás nos pone en contexto
- tener medias del colectivo permite orientar los recursos
- hay 2 fases
  - llegar a …
  - mantenerse en …