Medidas de seguridad en el tratamiento de datos personales

Víctor Chapela

victor@sm4rt.com

Problemática

- Hoy se gestionan **vulnerabilidades**, se deberían gestionar **riesgos**
- La **gestión por vulnerabilidades** genera distorsiones grandes
  - Controles **excesivos** o
  - Controles **deficientes**
- A las empresas **NO** se les debe dar la libertad de gestionar los riesgos de otros
- **Seguridad** es el principal costo de cumplimiento para las empresas

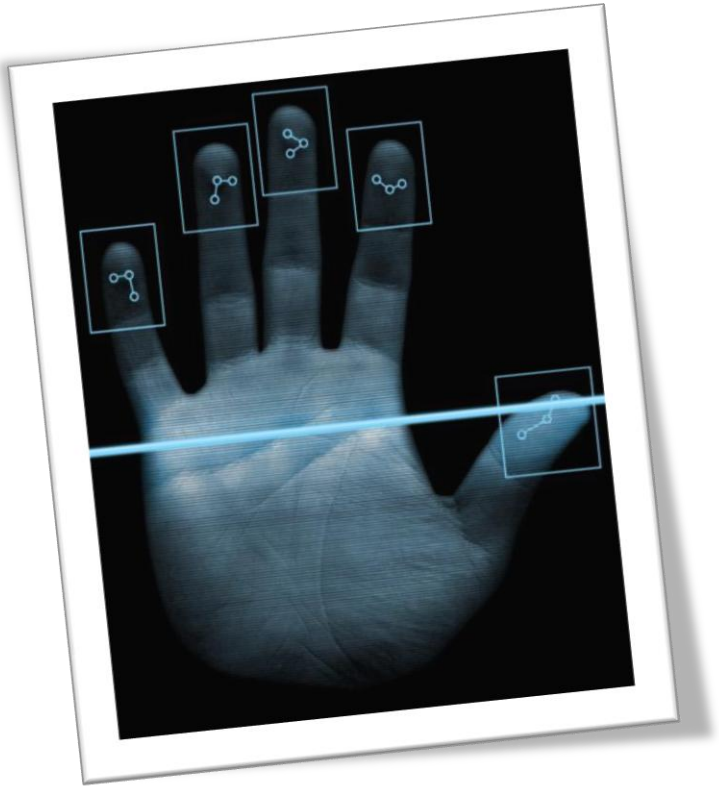
Eficiente y Eficaz

¿ISO 27000?

1. La ley **NO** busca aumentar la **seguridad de las empresas**
2. Busca sólo **aumentar la seguridad de los datos personales** en resguardo de las empresas
3. ISO 27000 – Propone controles de alto nivel para mitigar los **riesgos que la empresa considere relevantes**
4. Implantar controles **<>** reducir riesgo
5. + Controles → + Costo
6. Riesgos materializados → cuestan dinero
7. + Controles **<>** – Riesgos
8. Equilibrio entre controles y riesgo

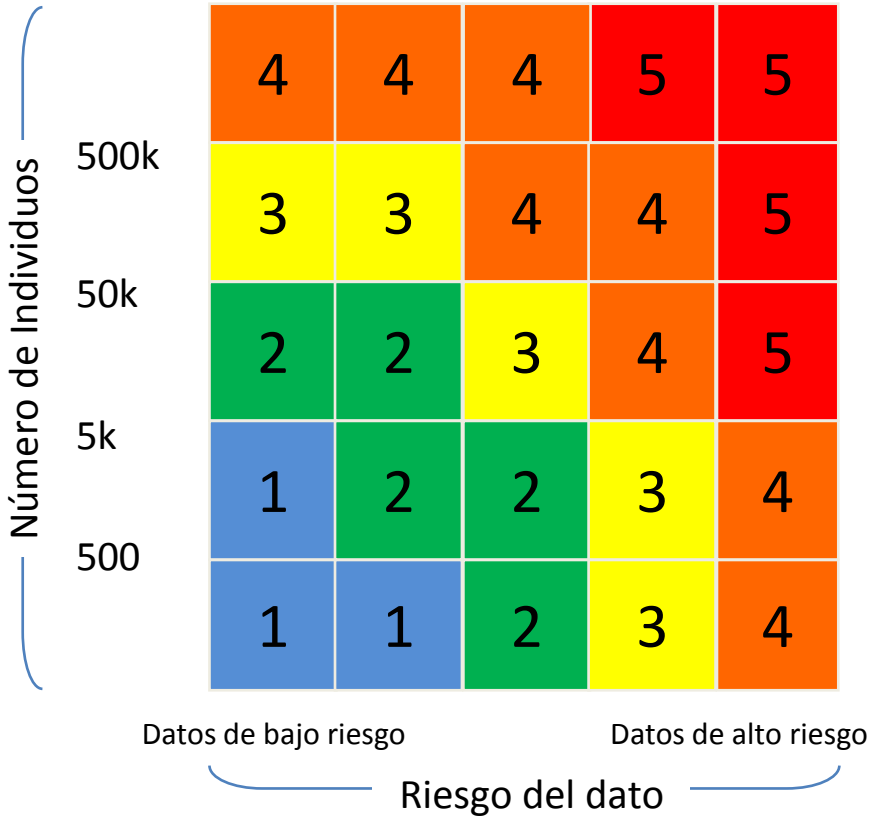
Objetivo Principal

- **Prevenir el acceso no autorizado a Datos Personales**



1ª Estrategia

- **Mitigar con base en el riesgo:**
  - **Por tipos de datos**
  - **Por número de individuos**



2ª Estrategia

- **Alinear incentivos**
  - Compensar la diferencia entre **impacto interno** para la empresa y la **amenaza externa**
  - Reducir el **riesgo para el individuo** cuando no hay incentivos para que el responsable lo haga
    - Riesgo reputacional
    - Riesgo económico
    - Riesgo de integridad personal

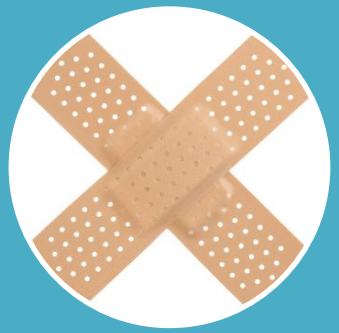
3 tipos de riesgos

Intencional

Anonimicidad

Oportunista

Complejidad



Accidental

Probabilidad

RIESGO

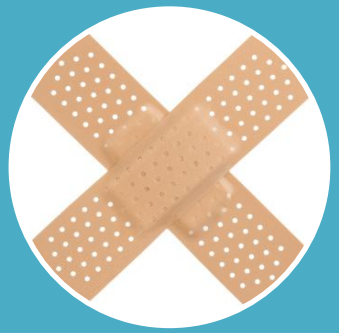
Incentivos Distintos

Intencional

Mínimo Esfuerzo

Oportunista

Suma de Esfuerzos



Accidental

Mejor Esfuerzo

El mitigación del riesgo en relación al esfuerzo

Disponibilidad siempre ha sido la meta principal


Facilitar
Acceso e Interacción


Riesgo Accidental es mitigado
por medio de Redundancia

¿Cómo mitigamos nuestro riesgo oportunista?

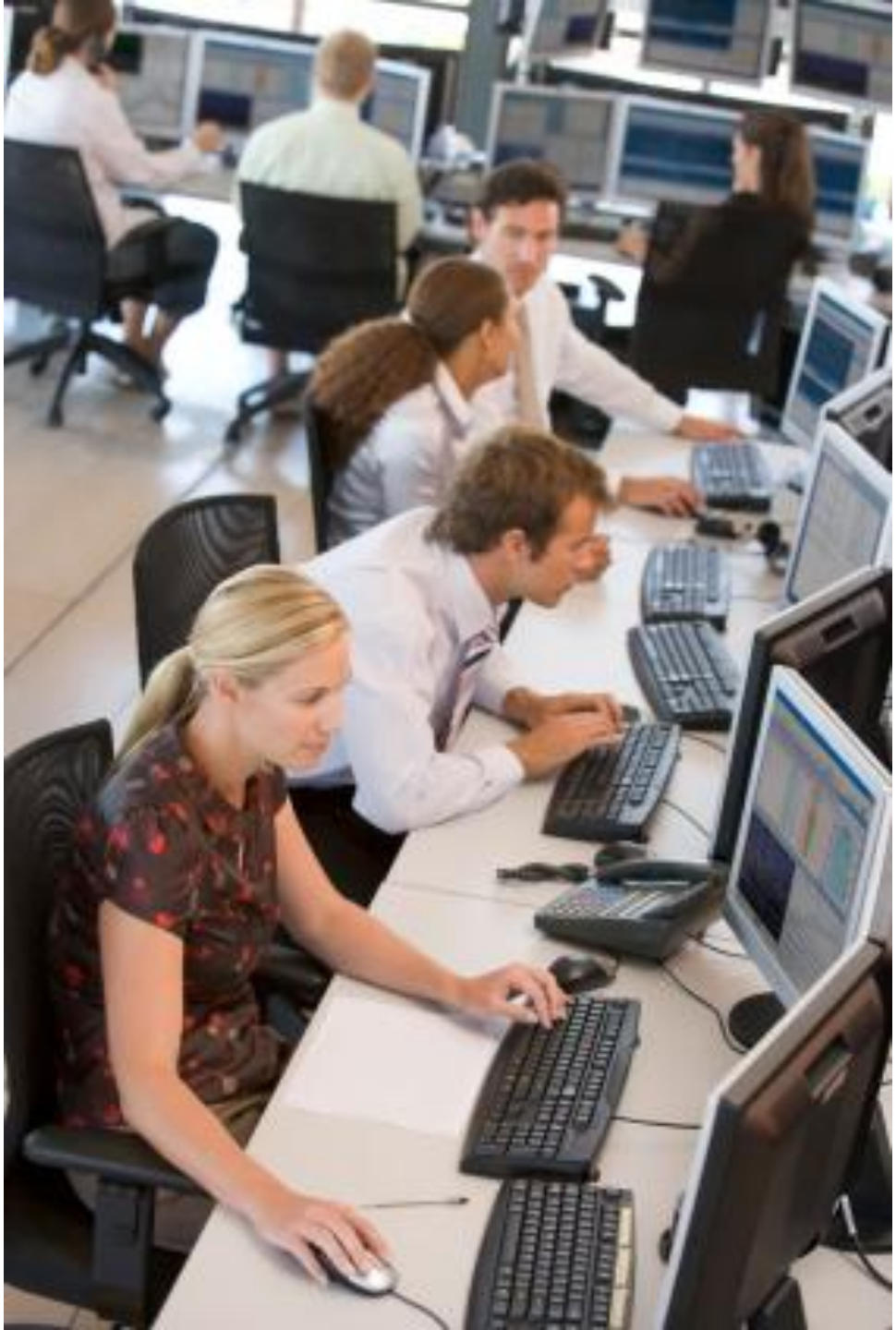

Para reducir Riesgos Oportunistas
necesitamos construir bardas


Entre más grandes…

…y
mejores controles
incluyas…


... más resistente va a ser.

Pero seguimos necesitando dar acceso…



La **analogía militar** **no aplica**

Necesitamos usar la analogía médica


Necesitamos mantener nuestros
sistemas y redes
sanos

Entender sus signos vitales

Usar mejores prácticas

Introducir sólo componentes sanos

Complementar con parches & actualizaciones

Aislarlos de amenazas externas

Generar alertas

Guardar logs

Riesgo Oportunista Digital es como la Salud

La Suma de los esfuerzos me mantiene Sano

...y define el tamaño de nuestra **barda**

¿Cómo mitigamos nuestro riesgo intencional?

El **riesgo intencional** es gestionado **aislando y filtrando** nuestra información crítica

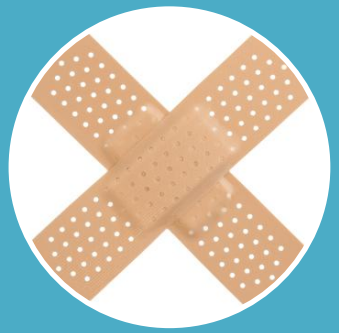
Valor

Intencional

Valor para terceros

Oportunista

Valor por interrelación



Accidental

Valor para la organización

Riesgo

Controles divididos en dos grupos:

¿Disponibilidad?
Impacto al Negocio

BIA

¿Confidencialidad e Integridad?
Valor de Mercado y Conectividad

IVA

Riesgo Intencional

- **Riesgo Intencional** =

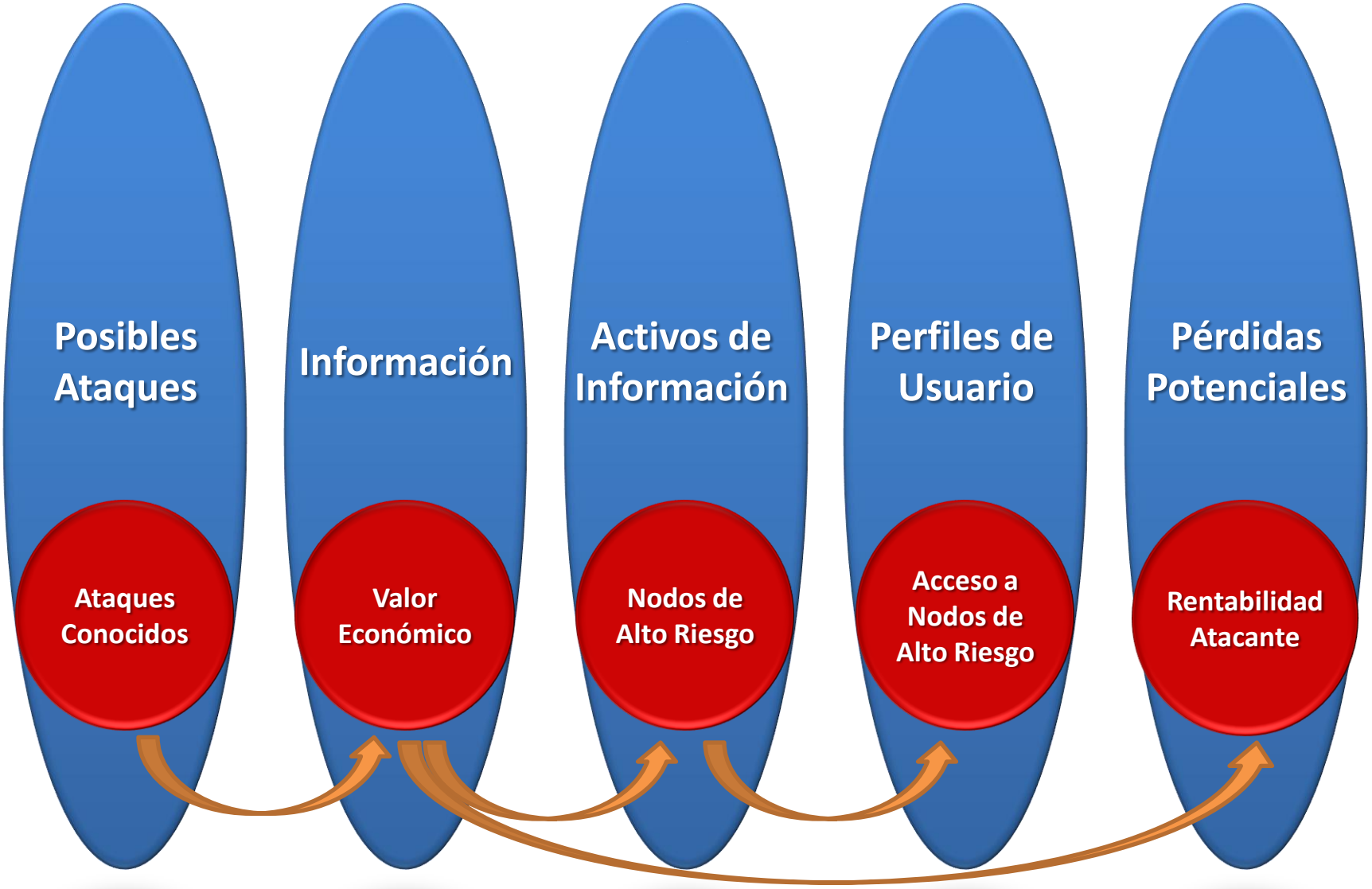
  Impacto x ***Probabilidad***

  Amenaza x ***Accesibilidad***

- ***Impacto*** es **determinado al estimar** el **valor económico**
- ***Probabilidad*** es **medida al calcular** **conexiones potenciales**

¿Cómo se calcula el valor de la información? (la amenaza)

Intencionalidad

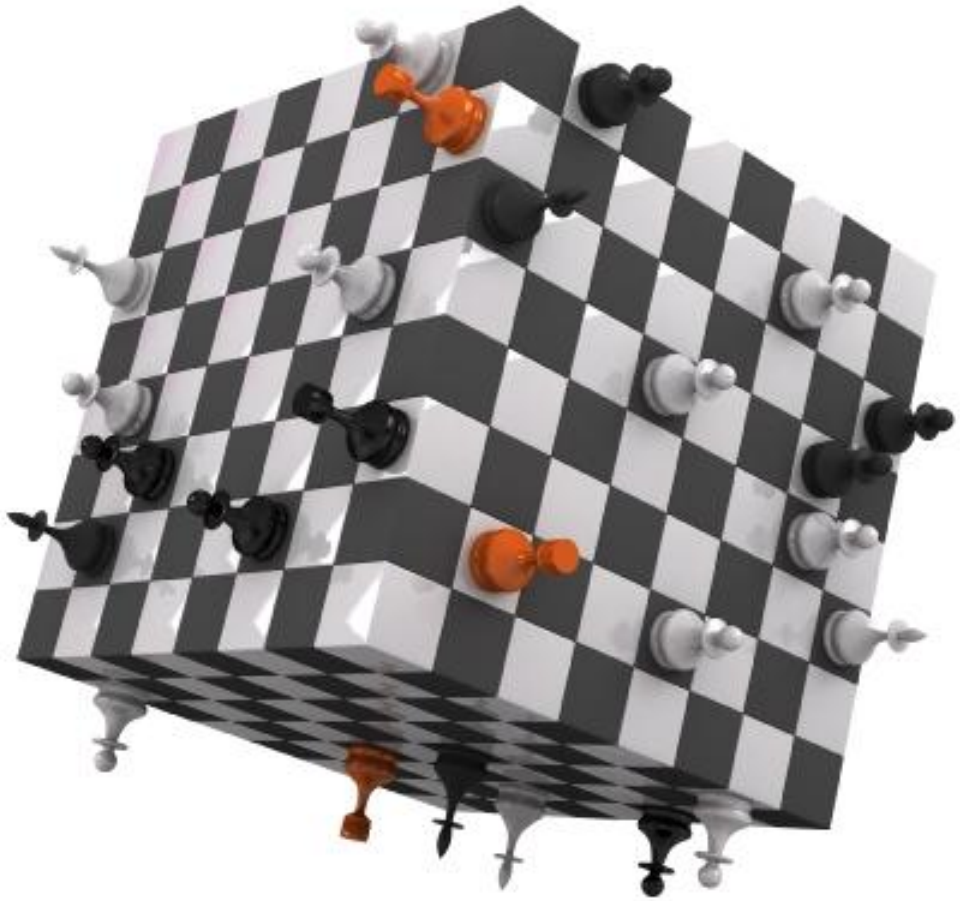


Necesitamos aceptar riesgo

El número de jugadas potenciales es infinta

Con miles de partidas simultáneas

En un ambiente altamente dinámico

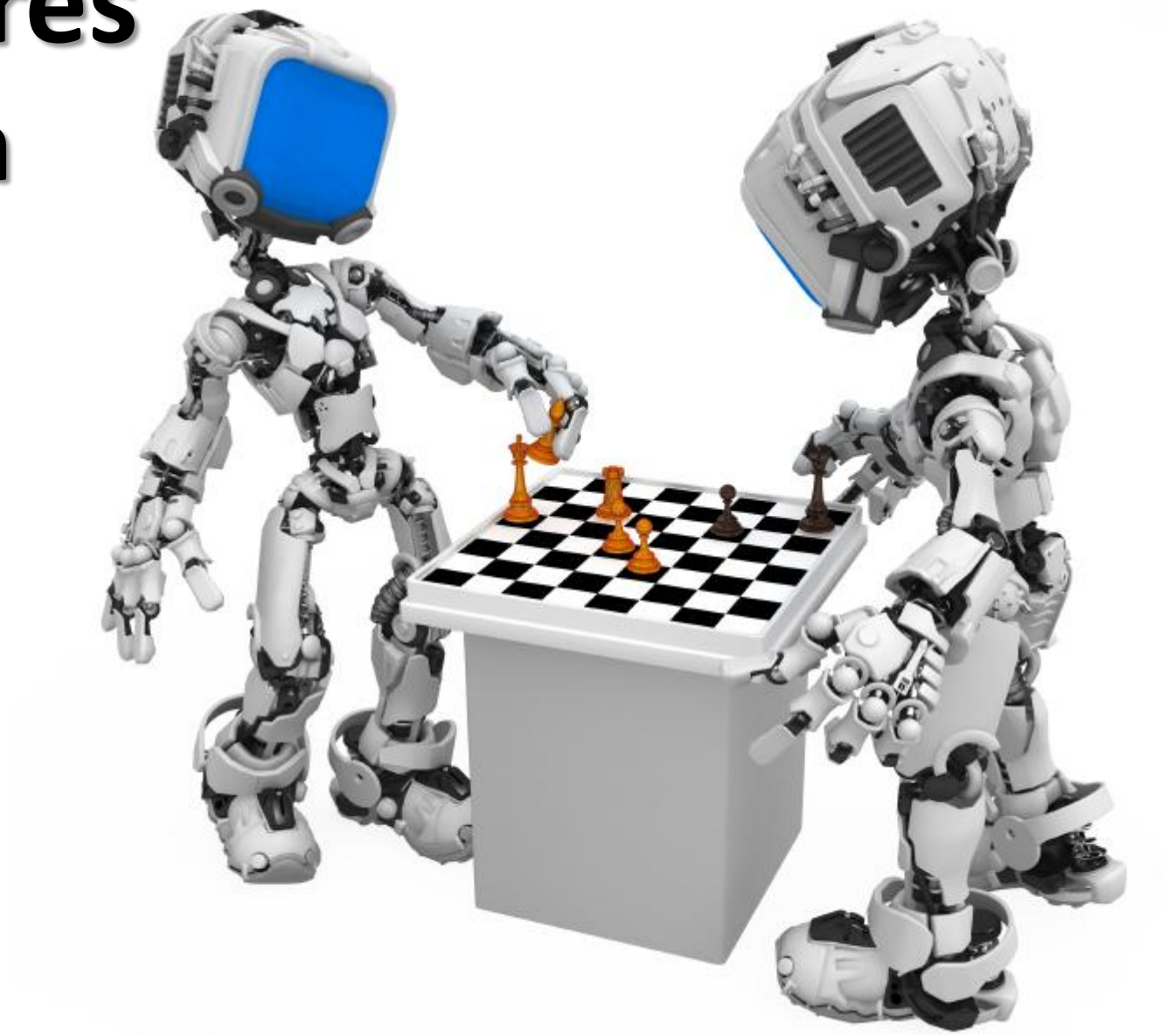


El tablero cambia diario


Las piezas
cambian
diario

Las reglas cambian diario

Jugadores cambian diario



El **fin** justifica los **medios**

Al prevenir **riesgo intencional**

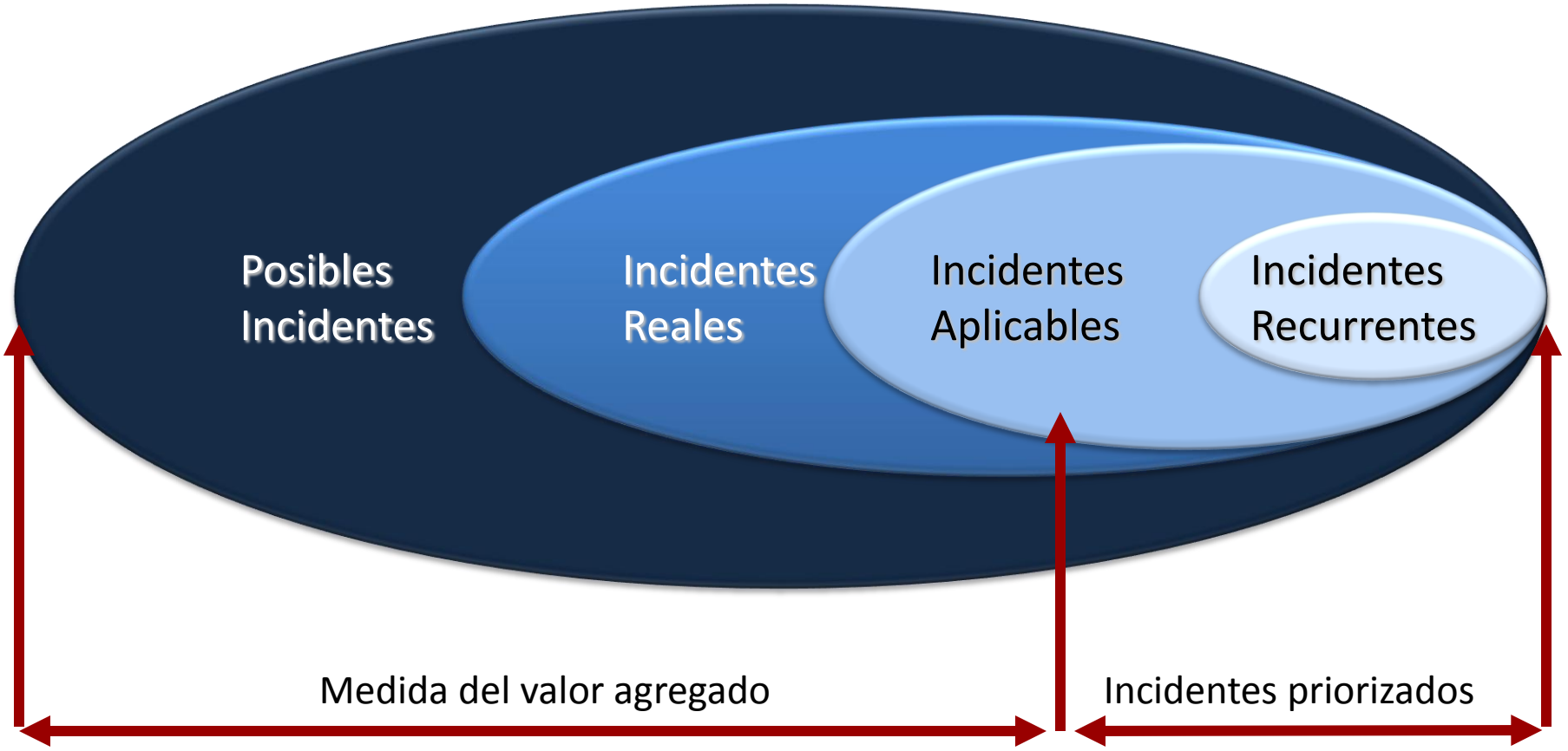
Nada menor
que asegurar
todos
los **vectores**
es suficiente

La defensa debe ser optimizada

Optimizar la velocidad


Optimizar recursos

Método de gestión por valor



Definición del valor de la información por tipo de dato

Así es como estimamos

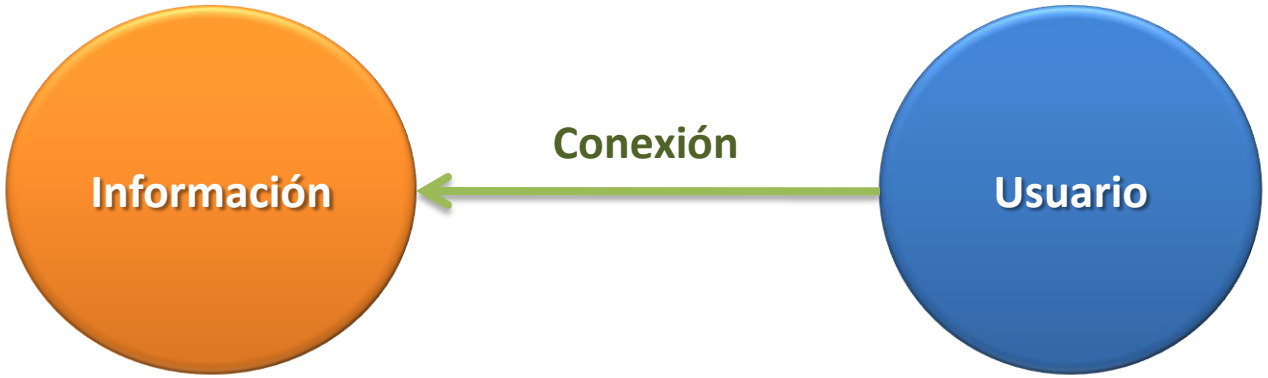
amenaza

¿Cómo se calcula la vulnerabilidad?


Activos y
Perfil de Usuarios


Activos y
Perfil de Usuarios

Accesos



Nodos de Información

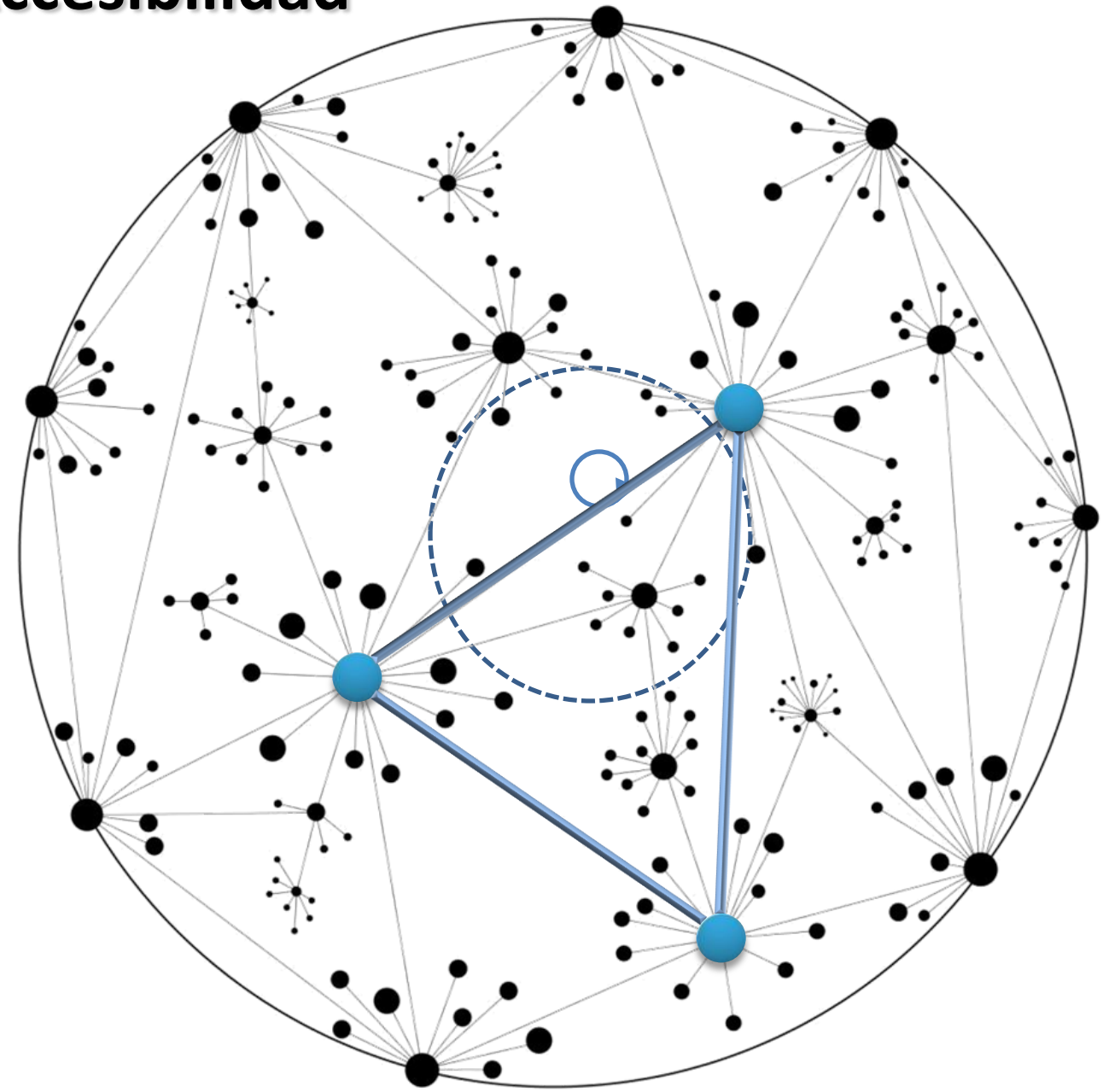
- Transfer
- Process
- Store

Nodos de Usuario

- Consulta

Segmentar por Accesos

Medir Accesibilidad



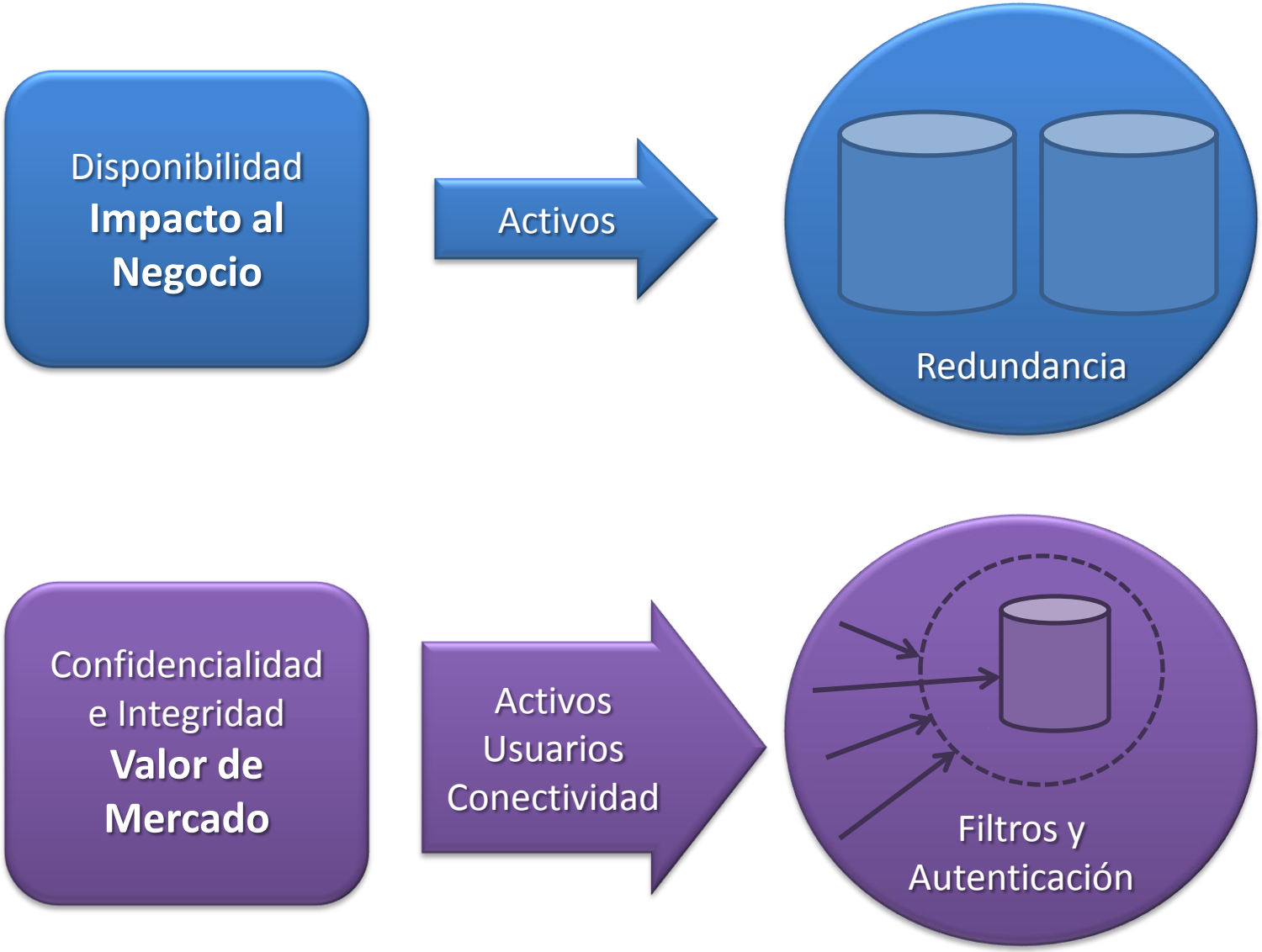
Agrupando Riesgo Intencional

Grupo de Usuarios

Sistema

Segmento de Red

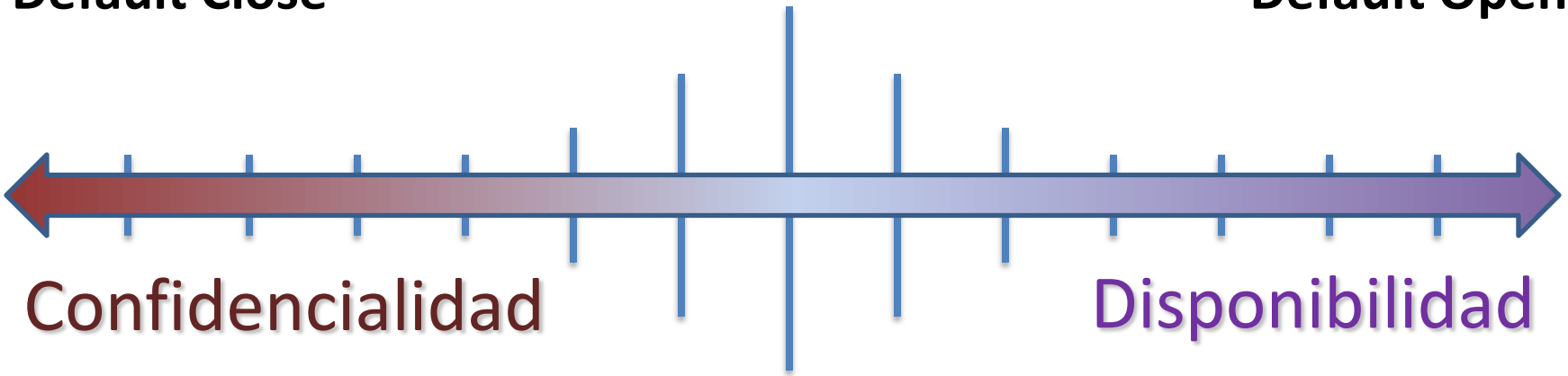
Tipo de Dato


Disponibilidad
Impacto al Negocio
Activos
Redundancia
Confidencialidad e Integridad
Valor de Mercado
Activos
Usuarios
Conectividad
Filtros y Autenticación

Accesibilidad

Default Close

Default Open



Enfocar controles en los riesgos principales

Determinar las

fronteras

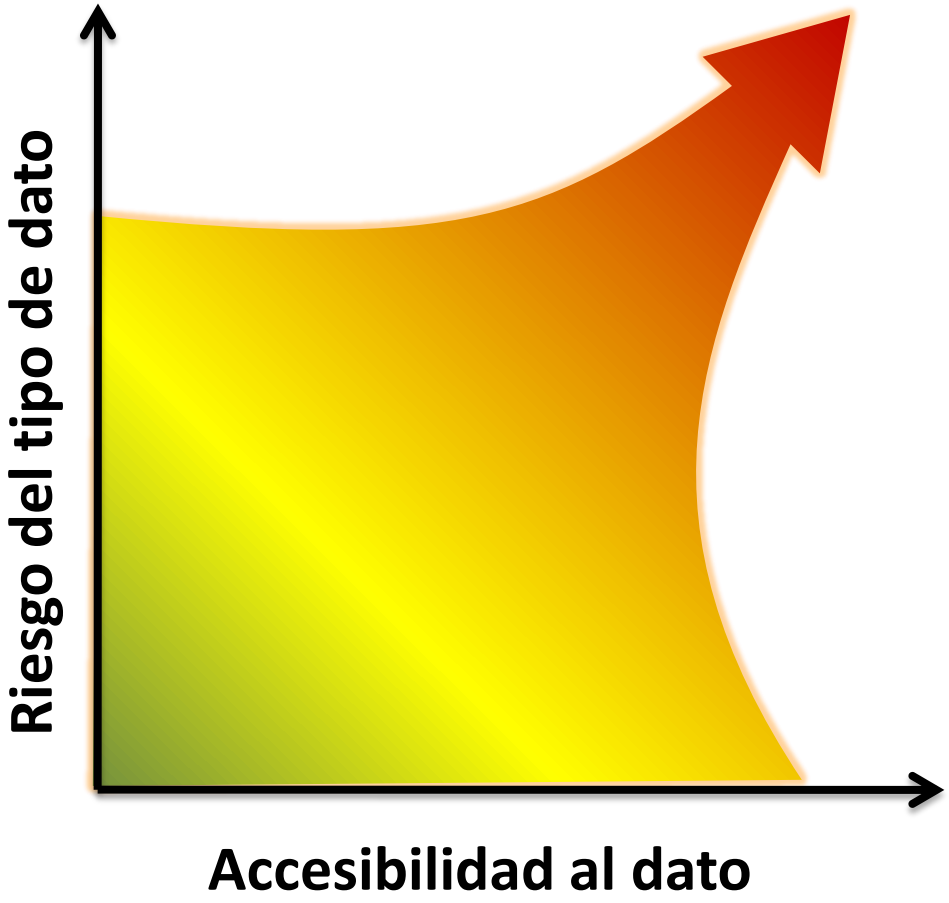
de **confianza**

¿Cómo aplica todo esto en una ley de privacidad?

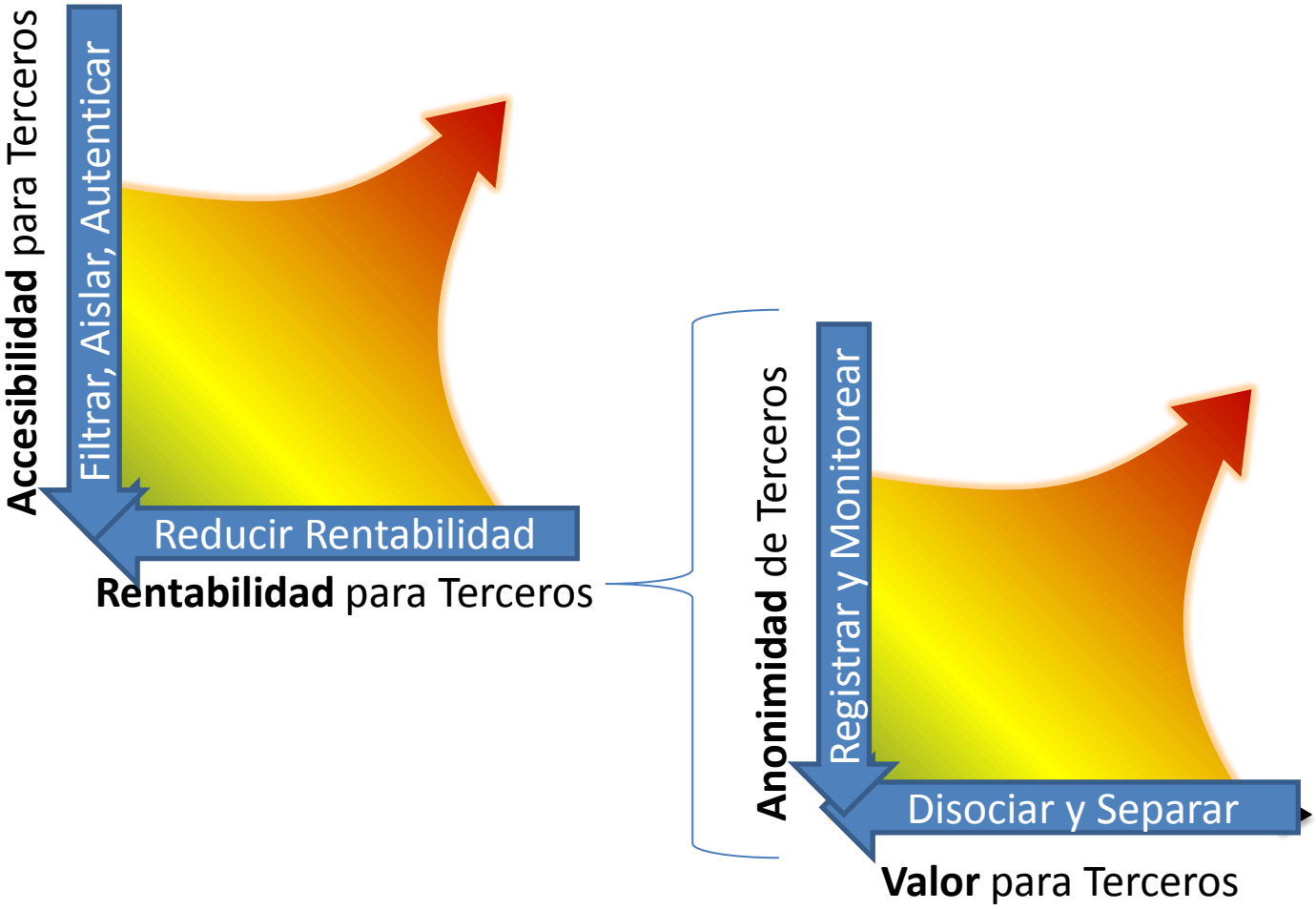
Riesgo por tipo de dato

	Personal	Sensible
Bajo Valor	Bajo	Medio
Alto Valor	Medio	Alto

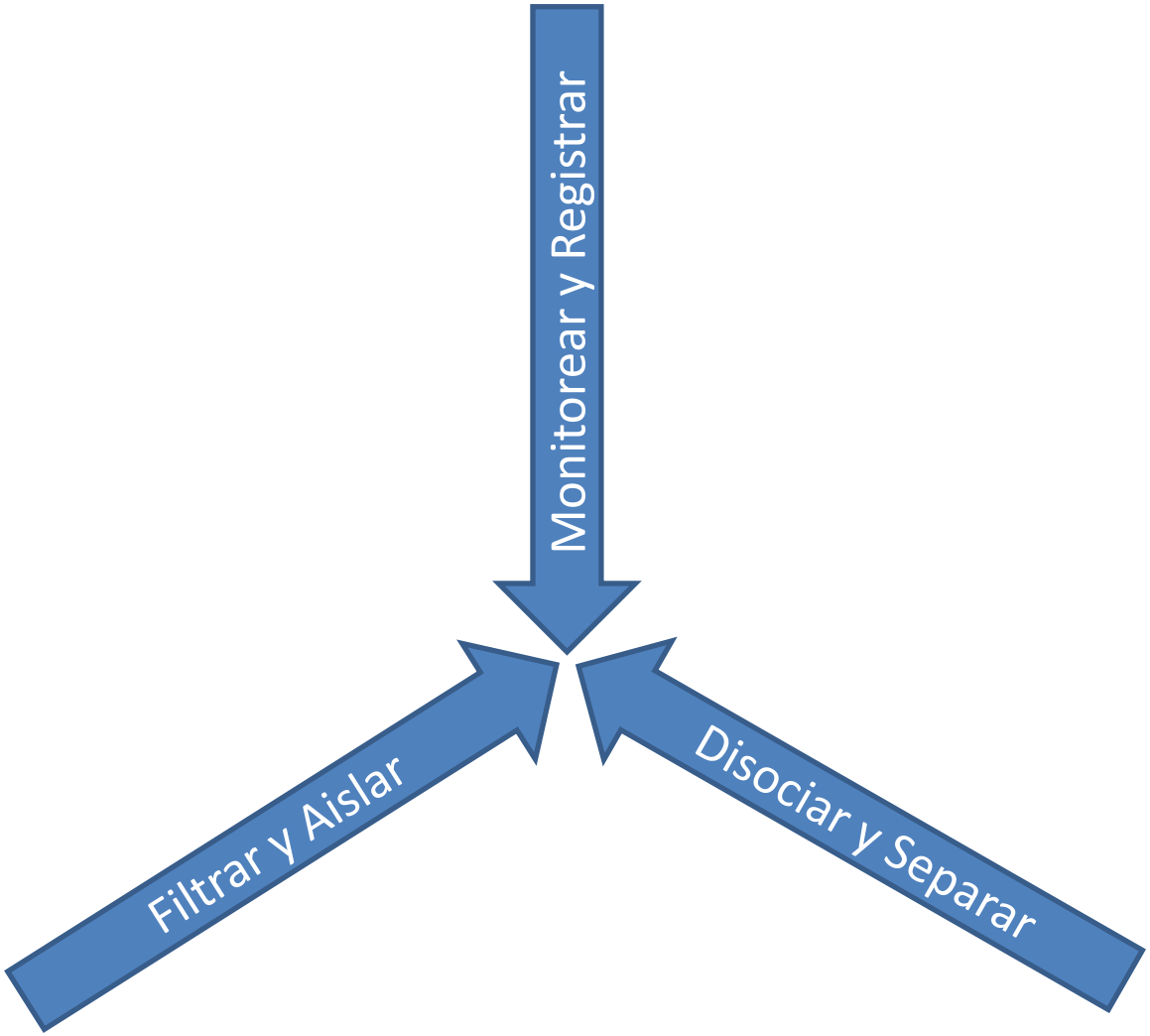
Riesgo para el individuo por tipo de dato



Riesgo Intencional



Reducir el riesgo para el individuo por medio de tres estrategias



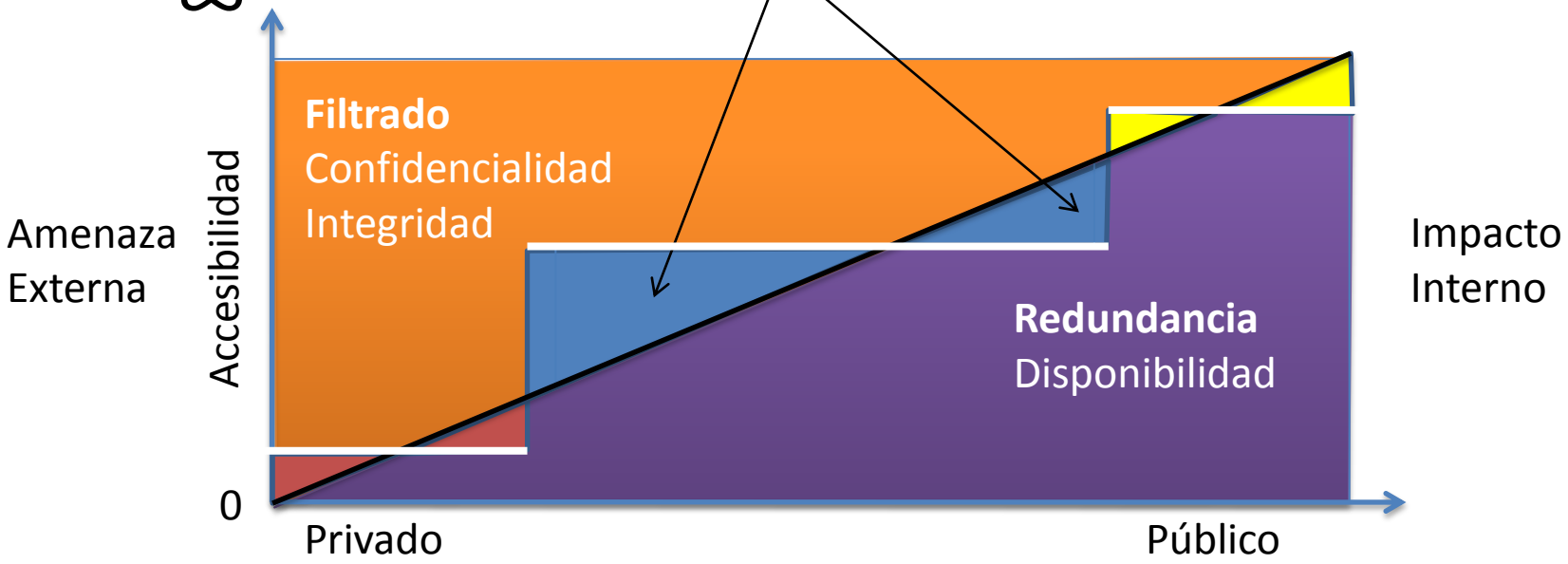
Filtrar y Aislar

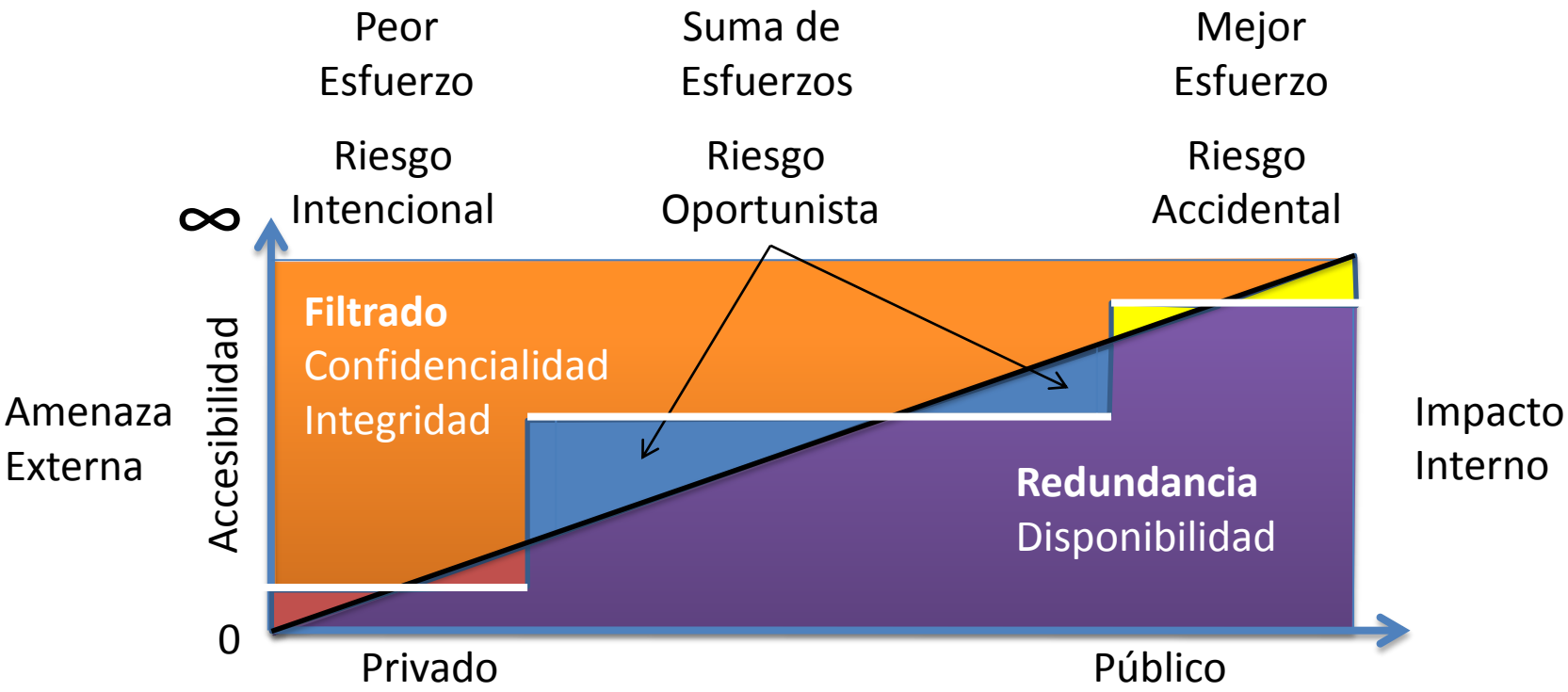
- Controles mínimos de **Accesibilidad**

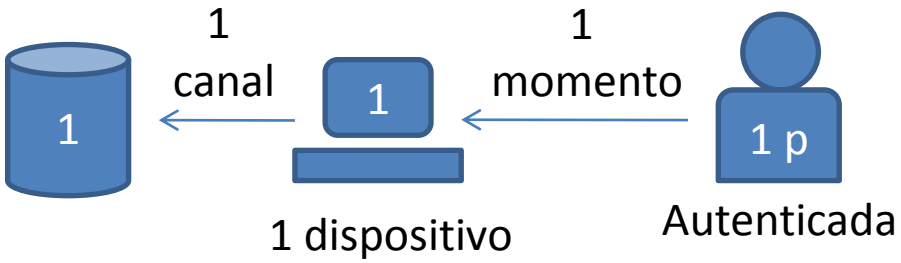
Riesgo Intencional

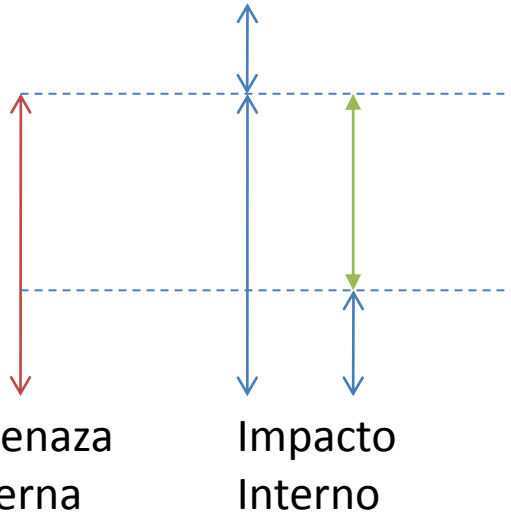
Riesgo Oportunista

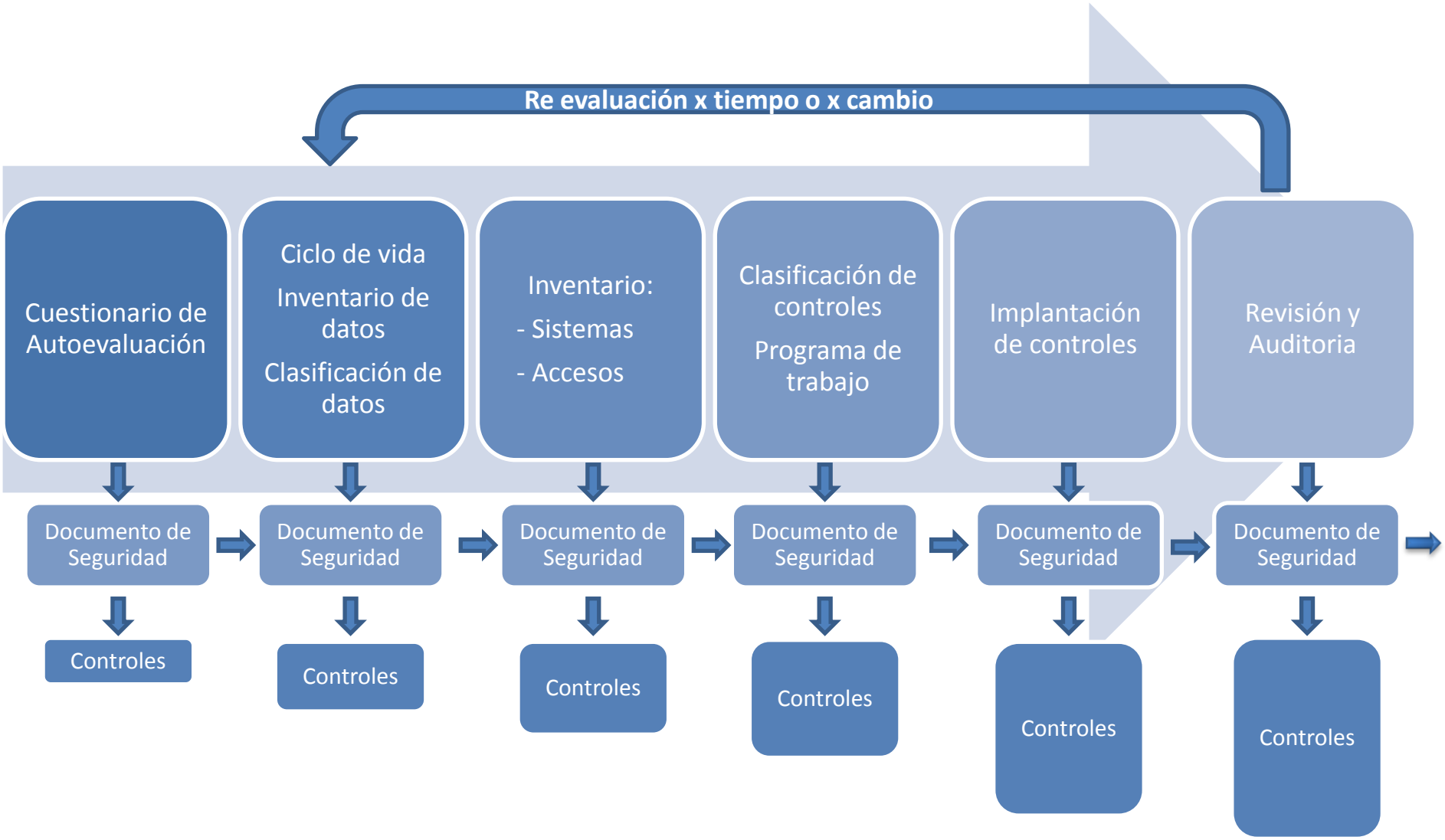
Riesgo Accidental




Peor
Esfuerzo
Suma de
Esfuerzos
Mejor
Esfuerzo
Riesgo
Intencional
Riesgo
Oportunista
Riesgo
Accidental
∞
Accesibilidad
0
Filtrado
Confidencialidad
Integridad
Redundancia
Disponibilidad
Amenaza
Externa
Impacto
Interno
Privado
Público


1
1
canal
1
momento
1 p
1 dispositivo
Autenticada


Amenaza
Externa
Impacto
Interno


Re evaluación x tiempo o x cambio
Cuestionario de Autoevaluación
Ciclo de vida
Inventario de datos
Clasificación de datos
Inventario:
- Sistemas
- Accesos
Clasificación de controles
Programa de trabajo
Implantación de controles
Revisión y Auditoria
Documento de Seguridad
Documento de Seguridad
Documento de Seguridad
Documento de Seguridad
Documento de Seguridad
Documento de Seguridad
Controles
Controles
Controles
Controles
Controles
Controles

Proporcional

- 80% de los negocios sólo tengan que llenar el cuestionario de autoevaluación
- 80% de los controles mínimos deberían estar ya implantados en la mayoría de las industrias
  - Reutilización de controles
- A menor riesgo se reduce el alcance, el proceso y la profundidad

Consideraciones en los criterios

- **Autoregulación de Seguridad**
  - Ejemplo: PCI-DSS o CNBV
- **Por tipo de dato**
  - Secuestros y extorsión
  - Anti-spam
    - Correo electrónico
    - Teléfonos
    - Dirección
  - VIP no se puede proteger
- **Cloud computing**
  - Adaptar los controles para que se cumplan los objetivos en este entorno
- **Transitorios**
  - 18 meses para la implementación de controles

Eficiente

Eficaz

Medidas de seguridad en el tratamiento de datos personales

Víctor Chapela

victor@sm4rt.com