GE Capital International
Comité de Riesgos de Tecnología

Incrementando la capacidad de supervisión sobre los riesgos tecnológicos con una gobernanza proactiva.

Imagination at work.

GE Capital de un vistazo

2014 NET INCOME
$7.0 Billion

OPERATIONS IN
40+ Countries

2014 ASSETS
$499 Billion

COMMERCIAL CUSTOMERS
500,000+

EMPLOYEES
35,000+

Financiación Comercial.
Financiación al consumo.
Banca tradicional.

imagination at work

Agenda

- Introducción
- Proceso de Mejora Continua
- Métricas
- Cultura del Riesgo

imagination at work

Introducción

Regulación, supervisión, mejora continua

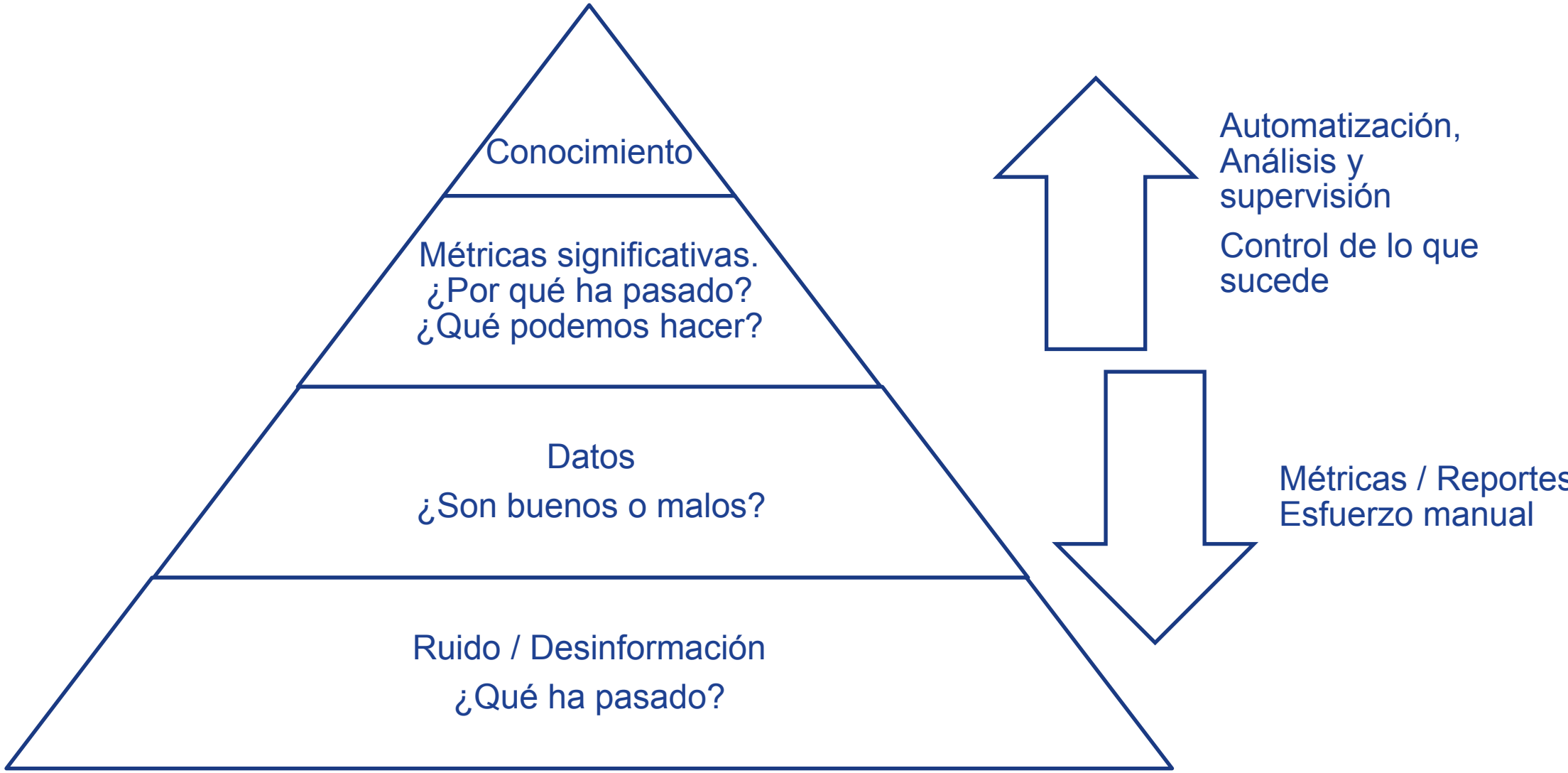
El comité de riesgos de tecnología es un programa iniciado en 2012 para demostrar control y supervisión de las tecnologías de la Información con respecto a las políticas de TI y otros indicadores de salud de las TI.

El programa se inicia a petición de Auditoría Interna, para alinearnos con los requerimientos de, entre otros, el regulador (Reserva Federal EEUU).

Governanza de la diversidad

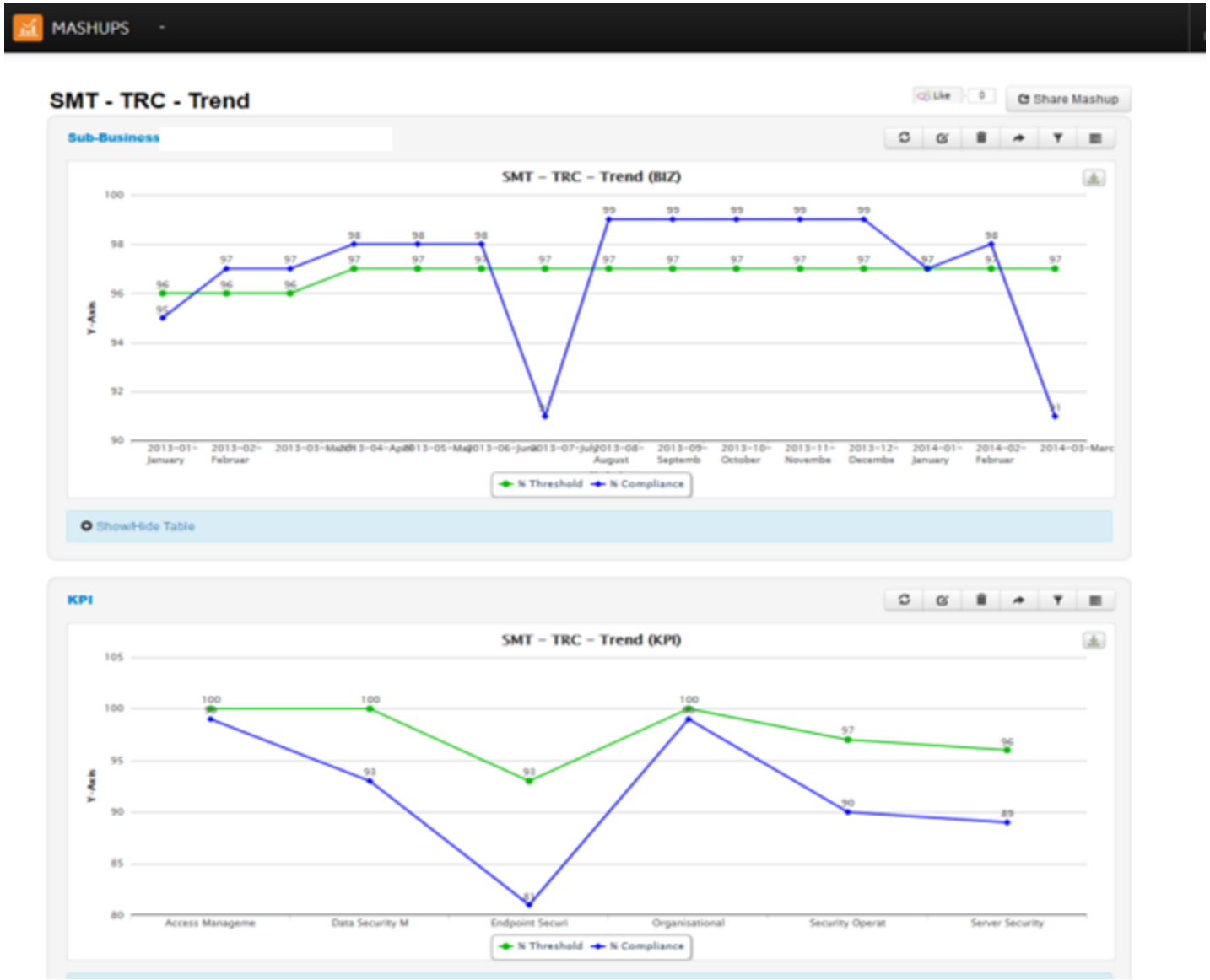
Adicionalmente, el programa está diseñado incluyendo diversas funciones de unificación y normalización de datos para proveer al equipo ejecutivo una visión común de los riesgos en todas las unidades de negocio.

De la Información al conocimiento y control



La visibilidad de los riesgos de las tecnologías es bastante limitada…

Visibilidad de los riesgos de las TI.

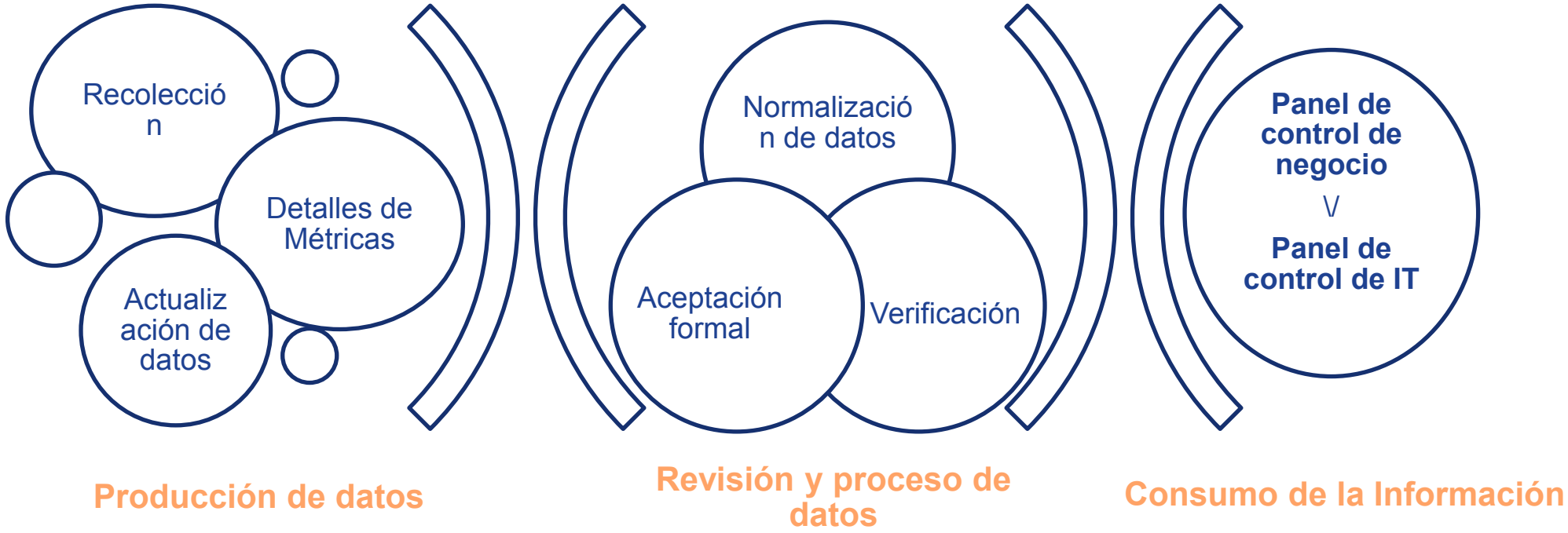


Proceso: Mejora Contínua

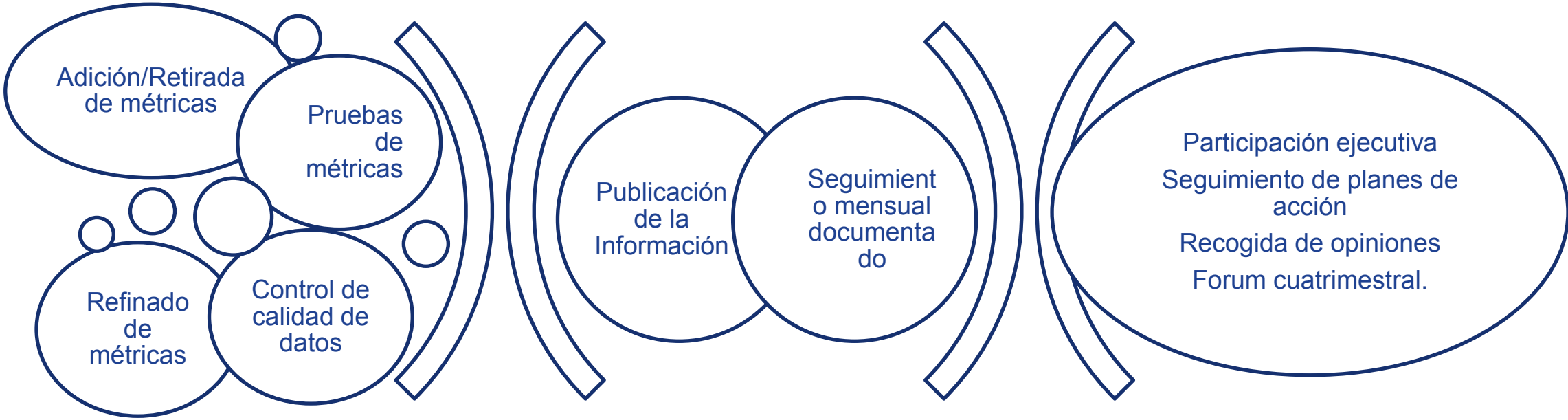
1. Obtener datos.
2. Convertir datos en conocimiento.
3. Mejorar con decisiones basadas en el conocimiento.
4. Vuelta a empezar.

imagination at work

Datos, métricas, reportes e información.



Automatización, Conocimiento, Supervisión y Control



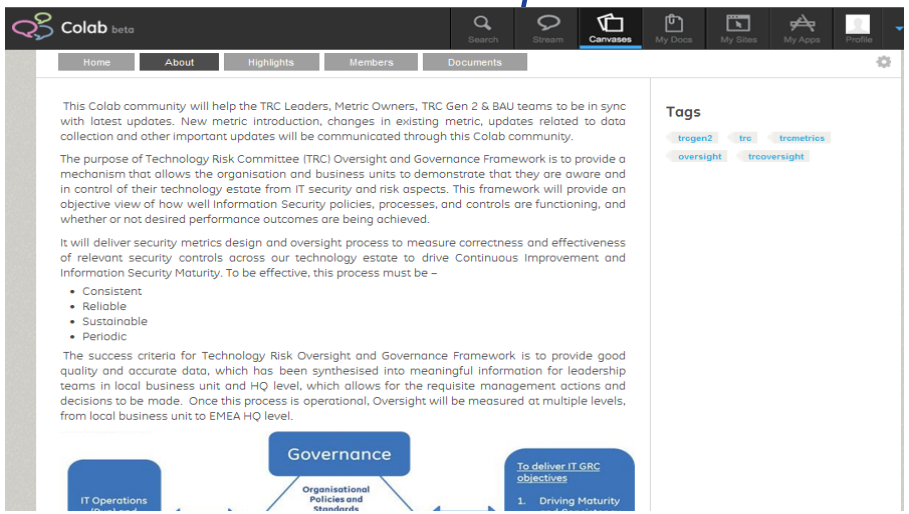
Gestión de Métricas **Ritmo Operacional** **Supervisión y Control**

imagination at work

Amazon Automated Warehouse, automated Governance!

Automatizado, socializado y documentado

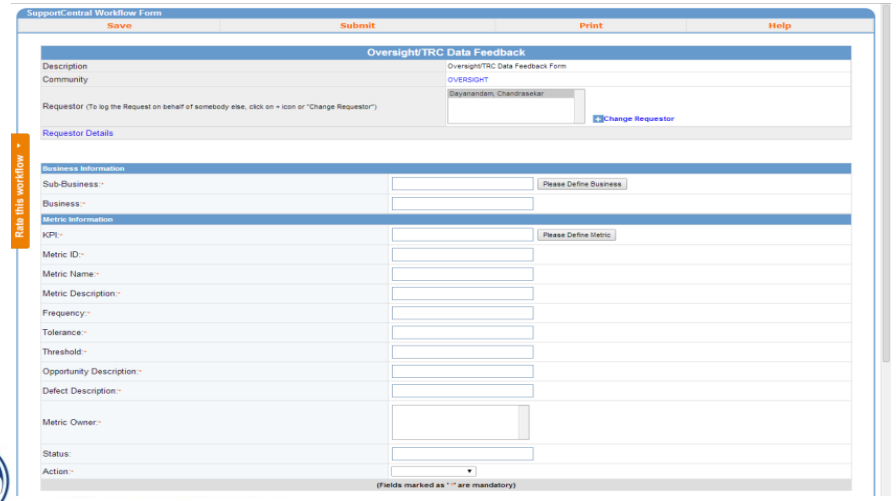
Información pública



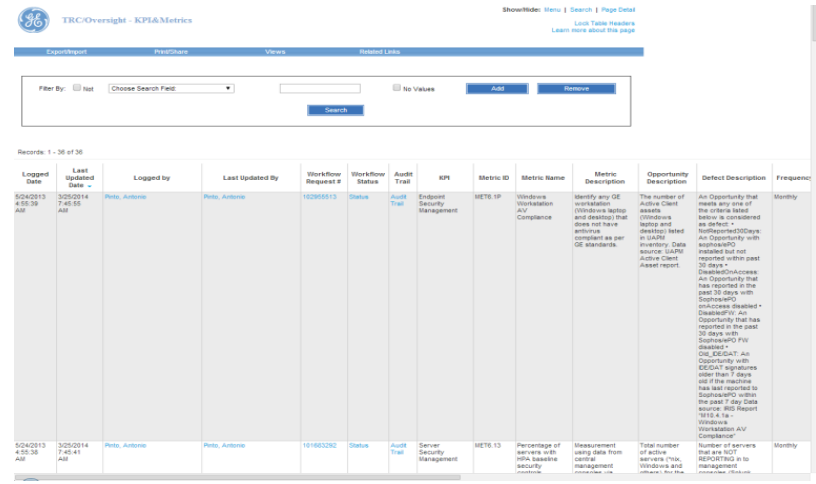
Documentación accesible

Name	Type
Capital EMEA - IT Oversight and Governance Framework v1.2	Word Document
Capital EMEA EMRG - Business TRC SOP v1.1	Word Document
Capital EMEA EMRG - Quarterly TRC SOP v1.1	Word Document
SOP - TRC MET11.1P	Word Document
SOP - TRC MET3.5	Word Document
SOP - TRC MET3.6	Word Document
SOP - TRC MET6.13	Word Document
SOP - TRC MET6.16a	Word Document
SOP - TRC MET6.16P	Word Document
SOP - TRC MET6.17P	Word Document
SOP - TRC MET6.1P	Word Document
SOP - TRC MET6.4P	Word Document
SOP - TRC MET7.6P	Word Document
SOP - TRC MET7.8	Word Document
TRC Oversight Dashboards v1.pdf	PDF File

Procesos automatizados



Información estructurada



Gestión de las Métricas

Hay una tendencia a crear muchas métricas, difíciles de entender por la audiencia.
Es responsabilidad de los equipos de TI el crear métricas comprensibles.

imagination at work

Airbus A380, ¿ De verdad necesito esas 750 métricas ?

Ciclo de vida de las métricas

Diseño y pruebas

Identificar Métricas

Diseño e inventario

Pruebas

Socialización con la audiencia y aceptación

Producción

Aprobación formal.

Documentación.

Puesta en producción

Revisión mensual.

Mejora Contínua

Identificar mejoras, problemas (p.ej. Falsos positivos, etc.).

Publicar los problemas y buscar soluciones.

Aprobar los cambios y mejorar.

Retirada

Revisar si las métricas siguen siendo necesarias.

Documentar razones para retirarlas.

Socializar el cambio.

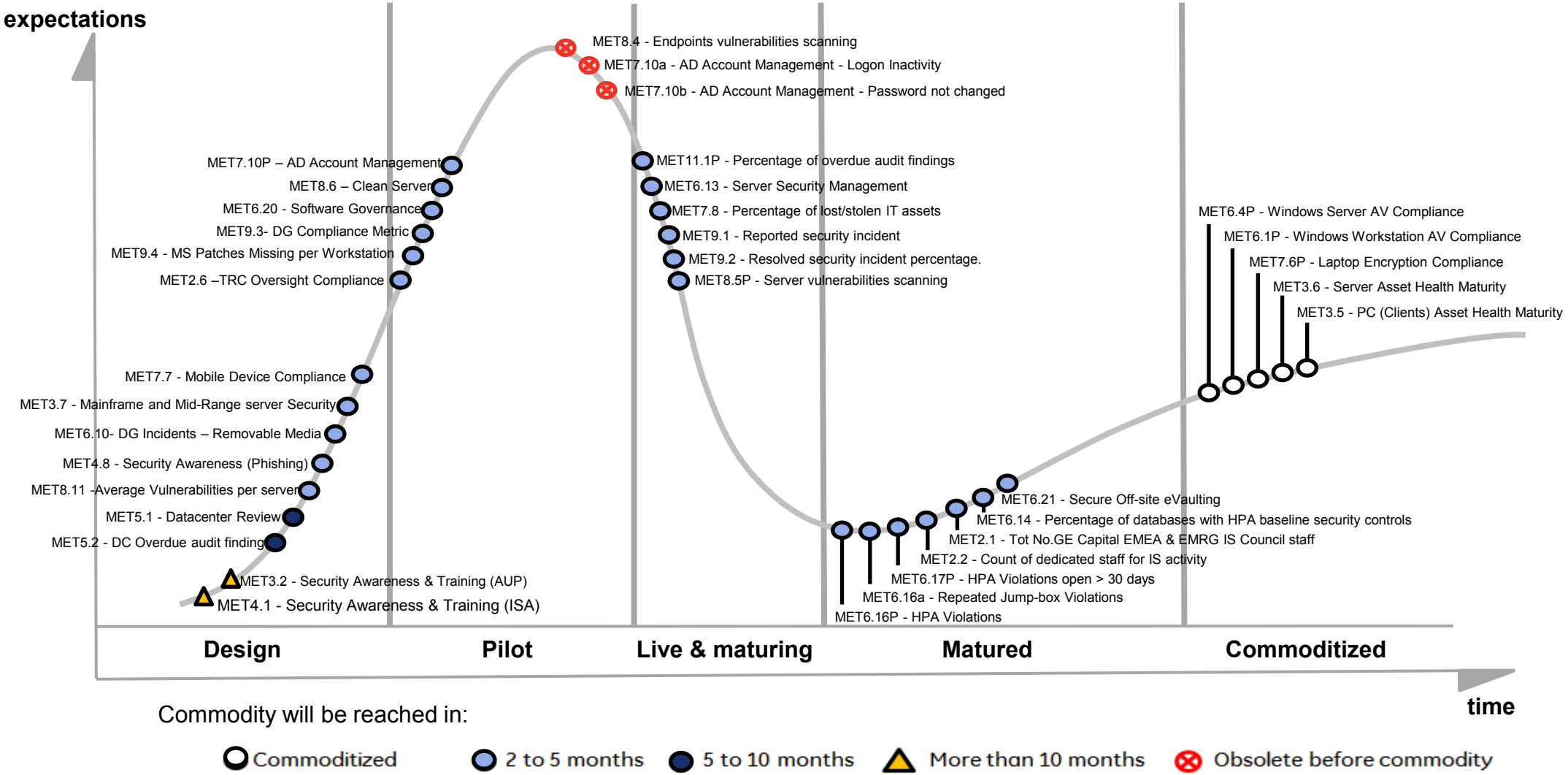
Retirada de las métricas.

Propiedades de las métricas

- **Documentada.** La documentación es pública y accesible
- **Granular.** Porporciona los datos adecuados al nivel organizativo adecuado.
- **Completa.** Cubre todos los activos necesarios.
- **Reproducible.** Con resultados consistentes en el tiempo.
- **Fiable.** Con datos de calidad y correctos.
- **Accionable.** Permite a los actores tomar decisiones y remediar el problema.
- **Inteligible.** Con un propósito y un caso de negocio entendidos.
- **Adecuada.** De acuerdo con las políticas, el apetito de riesgo y tolerancias establecidas.
- **Creíble.** Aceptada por los diferentes actores.
- **Transparente.** Visible de principio a fin para todos los actores.
- **Socializada.** Permitiendo a los actores participar en la implementación de la métrica.

TRC Metrics Hype Cycle

As of Nov 2014. 18 Live Metrics & 6 Pilot Metrics



Commodity will be reached in:

Commoditized | 2 to 5 months | 5 to 10 months | More than 10 months | Obsolete before commodity

imagination at work

Created using as reference the Gartner Hype Cycle model

Cultura corporativa del riesgo

No existe el riesgo cero en las TI, sin riesgo no hay negocio.

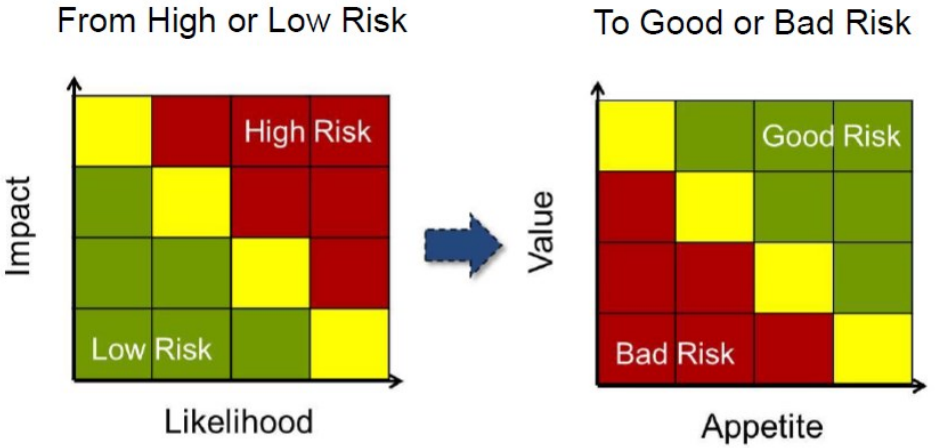
imagination at work

La cultura del riesgo es Imprescindible

- No se trata de imponer miedos, incertezas o dudas al equipo, pero debemos ser sinceros, es IMPOSIBLE garantizar el riesgo cero en las TIC, debemos clarificar que es importante conocer los riesgos y estar preparados para actuar.
- El proceso de supervisión de riesgos de las TIC funciona bien si el equipo directivo está dispuesto a hablar de riesgos y a invertir de manera adecuada para mitigarlos.

El equipo debe estar preparado para responder…

- ¿Cuánto riesgo es aceptable?
- ¿Qué controles son necesarios, cuales no?
- Etc..



imagination at work

Gráficos de Gartner, Paul Proctor, @peproctor

El comité, fuente de supervisión de riesgos

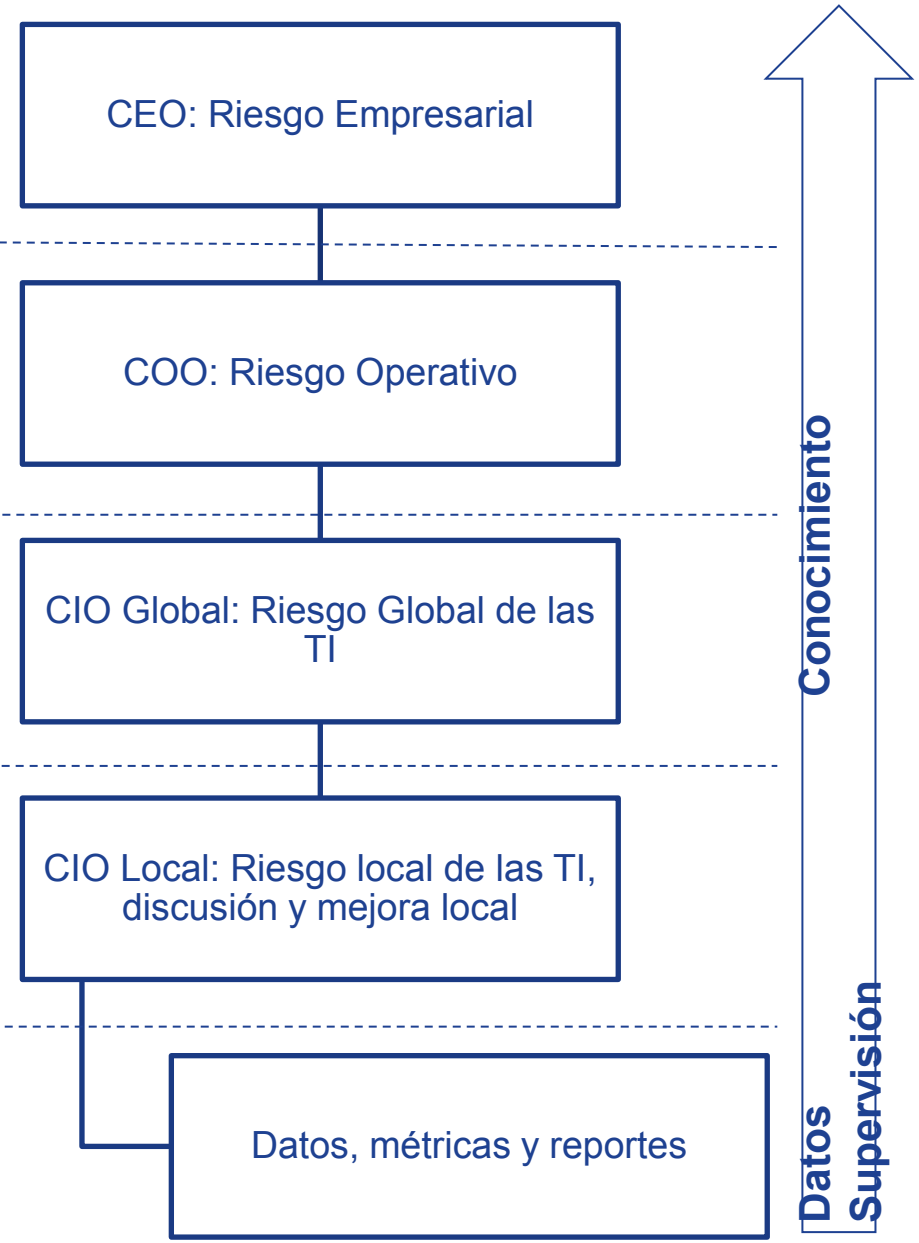
Supervisión de Riesgo Empresarial: El comité de riesgos Operacional informa al de riesgo empresarial de aquellos eventos destacables que pueden impactar a la empresa de forma significativa, aquellos con un impacto material que excede lo acordado previamente.

Supervisión de riesgo Operacional: El comité de riesgos Operativos (Formado por no sólo el dpto de TI) es informado de los principales riesgos y tendencias de las TI , cómo pueden impactar la operativa de negocio y los planes de acción diseñados, pérdidas potenciales, etc…

Supervisión Global: El comité global se reune y es informado de las tendencias y riesgos emergentes. Adicionalmente se discuten planes de acción global.

Conocimiento, Análisis y Acción: Las unidades de negocio, individualmente, analizan los riesgos, discuten y ejecutan planes de acción de forma documentada.

Datos: El proceso recoge y distribuye las métricas acerca de los riesgos de las TI a las unidades de negocio.



?

martin.piqueras@ge.com
martin.piqueras@gmail.com

imagination at work