

# El Gobierno TI y la nueva ISO 27001:2013 OBJETIVOS CONVERGENTES



# 1

## La nueva edición de ISO 27001:2013

Hacia el alineamiento entre estándares

## !!! TENEMOS NUEVA EDICIÓN !!!

- **Después de 8 años ...**
- De innumerables **comités y documentos de trabajo**
- De un **éxito mayor del esperado** en cuanto a implantaciones
- De convertirse en un **referente incluso para los legisladores** (como en Perú, Bolivia, Colombia, Japón, India, China, ... ¿o la Nueva Directiva Europea de Privacidad?)



## Período de Transición a la nueva edición

- **Nuevas certificaciones - Hasta el 1 de Abril 2014:** Se podía solicitar certificarse con la edición 2005 o la edición 2011.
- **Certificaciones existentes:** Deben ser auditadas con la nueva edición como máximo el 1 de Octubre de 2015.

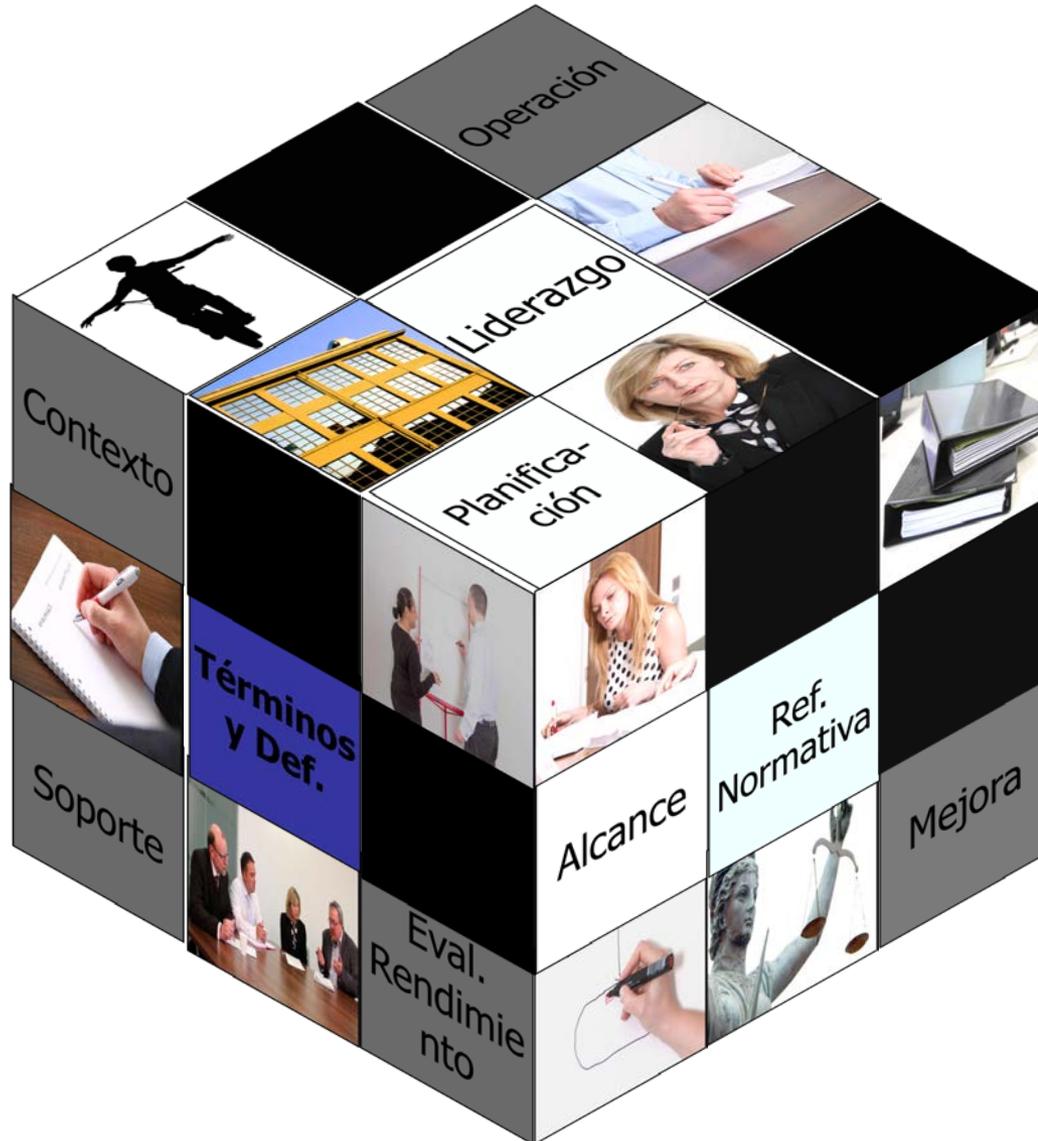


## Principal Cambio: El Anexo SL de la Directiva ISO

¿El suceso más importante desde ISO 9001?



# Principal Cambio: El Anexo SL de la Directiva ISO



# Estructura Común para TODOS los Sistemas de Gestión

## PLAN

### 4 Context of the organization

- Understanding of context
- Expectations of interested parties
- Scope and ISMS

### 5 Leadership

- Management commitment
- IS policy
- Roles, responsibilities and authorities

### 6 Planning

- Actions to address risk and opportunity
- IS objectives

### 7 Support

- Resources
- Competence
- Awareness
- Communication

## DO

### 8 Operation

- Operational planning and control
- Risk assessment
- Risk treatment

## CHECK

### 9 Performance and Evaluation

- Monitoring, measurement, analysis and evaluation
- Internal audit
- Management review

## ACT

### 10 Improvement

- Nonconformity and corrective action
- Continual improvement

# NUEVOS CONTROLES

A.14.2.5

A.16.1.4

A.16.1.4

A.14.2.1

A.6.1.5

A.16.1.5

A.14.2.8

A.14.2.6

A.15.1.3

A.12.6.2

A.15.1.1

## Algunos nuevos Controles

**A.6.1.5. Seguridad de la Información en la Gestión de Proyectos.**

**A.12.6.2. Restricciones en la instalación de software.**

**A.14.2.1. Política de Desarrollo Seguro de Software.**

**A.14.2.5. Principios para la Ingeniería de Sistemas Seguros.**

**A.14.2.6. Seguridad de los Entornos de Desarrollo.**

**A.14.2.8. Testeo de la Seguridad de los Sistemas.**

## Algunos nuevos Controles

**A.15.1.1. Política de Seguridad para las Relaciones con Proveedores.**

**A.15.1.3. Cadena de Suministro de las TIC.**

**A.16.1.4. Auditoría y decisión sobre los Eventos de Seguridad de la Información.**

**A.16.1.5. Respuesta ante Incidentes de Seguridad de la Información.**

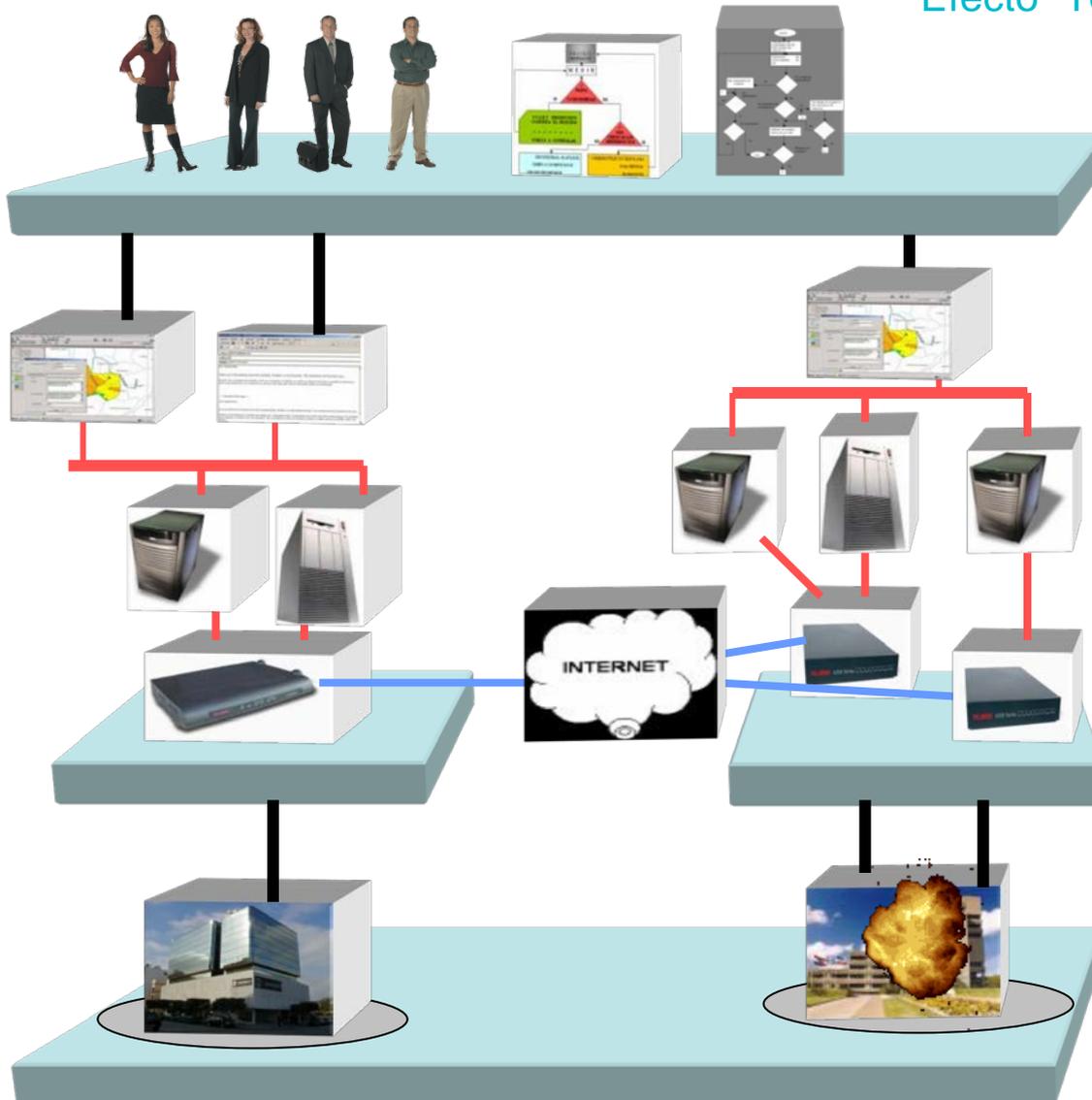
**A.17.2.1. Disponibilidad de las instalaciones de procesamiento de la información.**

# 2

## Nuestra visión del futuro del Gobierno TI

Hacia la convergencia en funciones

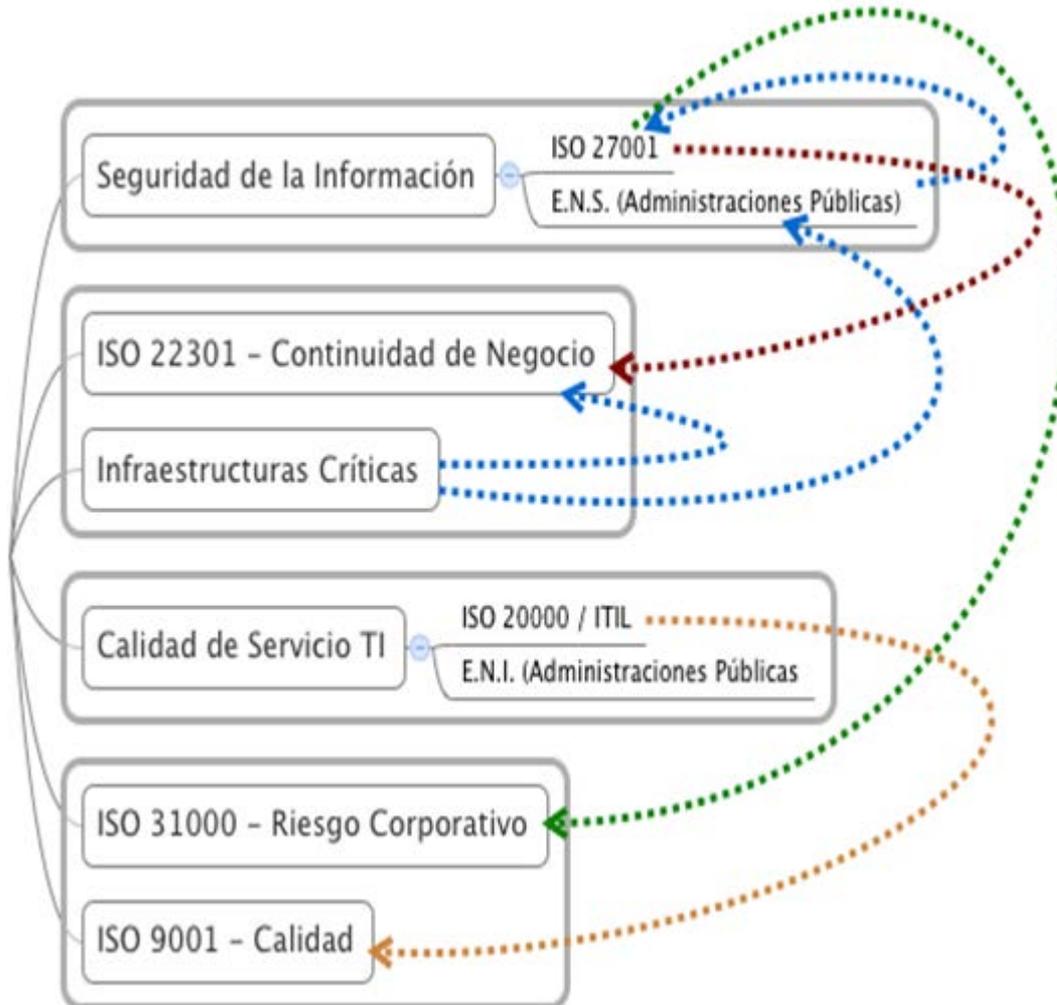
Efecto “Torre de naipes o bola de nieve”



- **Negocio**
  - Procesos de negocio
  - Servicios
- **Sistemas**
  - Aplicaciones Corporativas
- **Tecnología**
  - Software
  - Infraestructura
  - Equipos
  - Telecomunicaciones
- **Infraestructura Física**
  - Dependencias físicas
  - Suministros

# Sistema Integrado de Gestión (S.I.G.)

Un Marco Único de Control que le permite auditar una única vez y determinar el cumplimiento respecto a múltiples estándares que tienen controles equivalentes

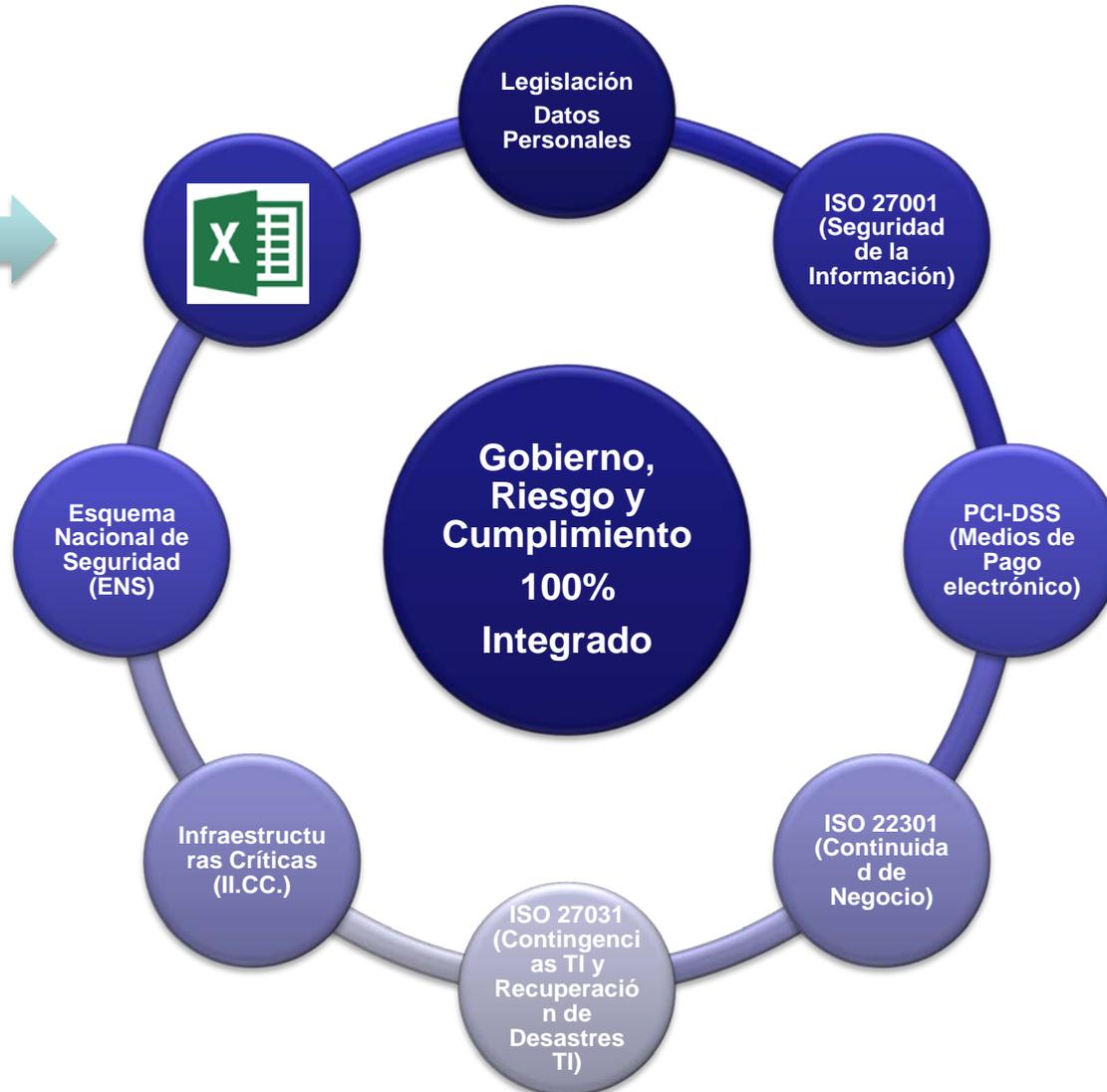


# Legislación y Estándares más habituales

(posibilidad de cargar sus propios Fuentes de Requisitos de Seguridad y Cumplimiento)

**Cargue desde Microsoft Excel sus propios requisitos:**

- **Legales**
- **Regulatorios**
- **Contractuales**



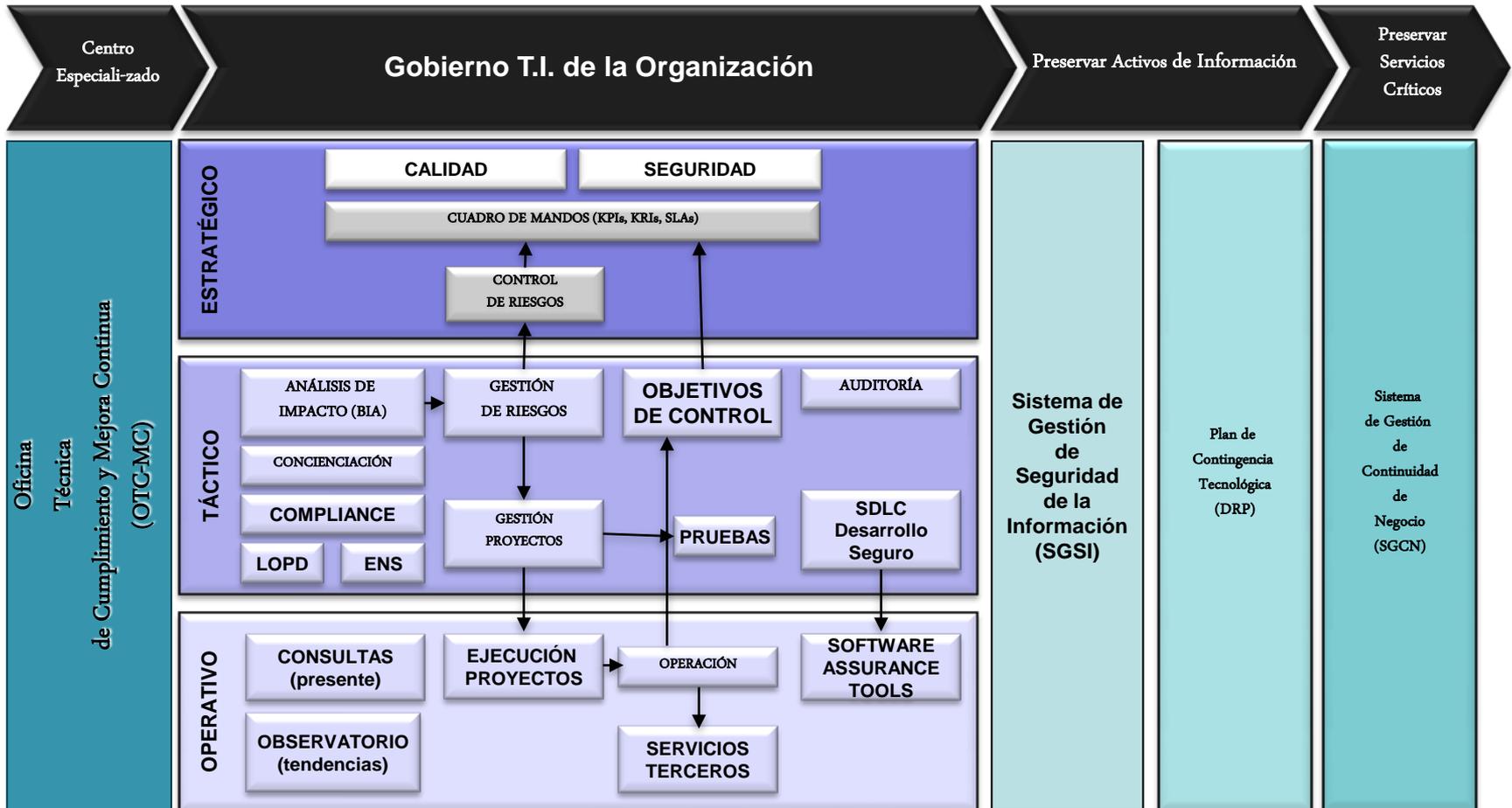
# La Mejora Continua a través de las mejores prácticas

## MARCO PARA LA EVOLUCIÓN DESDE EL MERO CUMPLIMIENTO NORMATIVO AL GOBIERNO T.I. EN TIEMPO REAL



# Oficinas Técnicas de Cumplimiento y Mejora Continua

Enfoque global orientado a la Seguridad, Calidad y Gestión del Riesgo



# Oficinas Técnicas de Cumplimiento

## Ejemplos de Actividades a Desarrollar



# Arquitectura Empresarial – La Clave para unificar la Gestión

## Modelado Visual de la organización conforme al estándar TOGAF y Archimate

### Capa de Negocio (Servicios, Procesos, Recursos), Sistemas y Tecnología

The screenshot displays the GRC server interface. At the top, it shows the GRC server logo, the text "Powered by GESCONSULTOR", and navigation elements including "Organización - SGSI", "Consultora Demos GesConsultor", a language selector for "ES", and a user profile for "Consultor Genérico".

The left sidebar contains a menu with the following items: Inicio, **Arquitectura Empresarial** (highlighted), Arquitectura Empresarial (CMDB), Representación Gráfica, Monitorización Continua, Gobierno, Riesgo, Privacidad, ISO 27001, ISO 9001, P.N.I.C., PCI-DSS, E.N.I., Compliance, and Cobit.

The main area shows a complex Enterprise Architecture diagram. It is organized into three horizontal layers:

- Negocio** (Business): The top layer, containing various business processes and services represented by yellow boxes.
- Sistemas / Aplicaciones** (Systems / Applications): The middle layer, containing application systems represented by light blue boxes.
- Tecnología** (Technology): The bottom layer, containing hardware and infrastructure components represented by light green boxes.

Arrows and lines connect the boxes across the layers, illustrating the relationships and dependencies between business processes, applications, and technology. The text "Negocio", "Sistemas / Aplicaciones", and "Tecnología" is overlaid on the diagram in large, semi-transparent letters.

# HABLEMOS DE NEGOCIO

## No es simplemente tecnología ...

¿Qué criticidad tienen los **Servicios y Procesos de Negocio** sobre los que impactan mis **Sistemas de Información**?

Evaluación de la **Criticidad** de cada Servicio o Proceso de Negocio y determinación de **MTPD, RPO, RTO** y niveles mínimos de Continuidad (**MBCO**)

### BIA

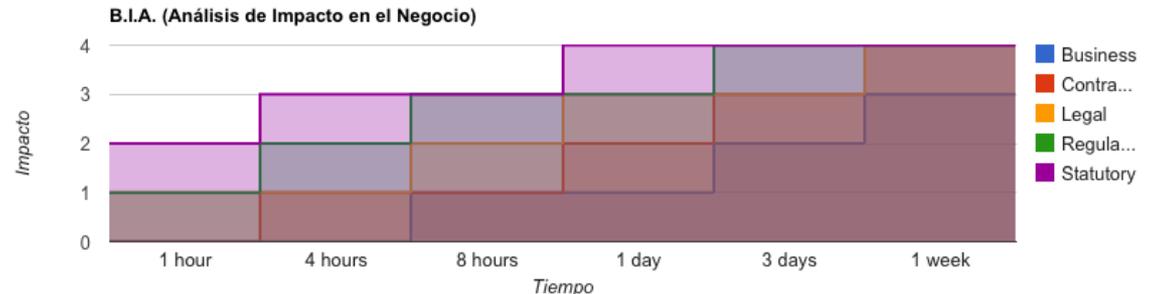
Análisis de Impacto en el Negocio

100% integrado, automatizado y mantenible

NO en ofimática



	1 hour	4 hours	8 hours	1 day	3 days	1 week
Business	Very Low	Very Low	Low	Low	Medium	High
Contractual	Very Low	Low	Low	Medium	High	Very High
Legal	Low	Low	Medium	High	High	Very High
Regulatory	Low	Medium	High	High	Very High	Very High
Statutory	Medium	High	High	Very High	Very High	Very High



# Gestión Unificada del Gobierno TI, Riesgo y Cumplimiento

GRC server

Powered by  
GESCONSULTOR



Organización - SGSI

Consultora Demos GesConsultor

EN



Consultor Genérico

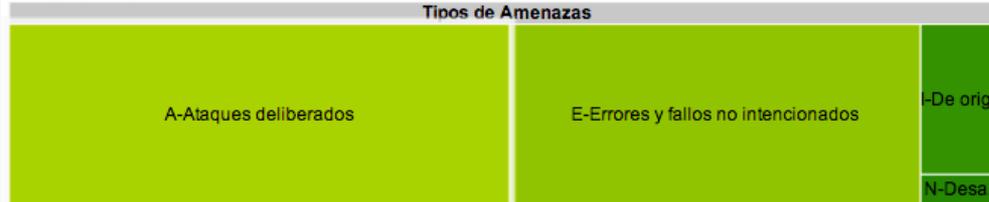
- Home
- Enterprise Architecture
- Continuous Monitoring
- Governance
- Risk
- Privacy
- ISO 27001
- ISO 9001
- P.N.I.C.
- PCI-DSS
- E.N.I.
- Compliance
- Cobit
- Document Management

Hello, Consultor

Risks

Chart 1 Chart 2

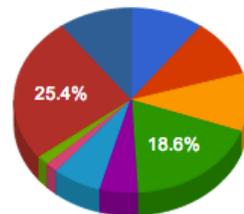
### Riesgos por Tipo de Amenaza



NOTE: To return to the top level to click with the right mouse button.

Assets

### Activos por Tipo



- Aplicaciones (software)
- Datos/Información
- Equipamiento auxiliar
- Equipos informáticos (har...
- Instalaciones
- Personal
- Prestigio de la Empresa/O...

1/2

Gesconsultor.com

@gesconsultor News



- gesconsultor: #iso27001El equipo de @iso27000es nos ofrece todos los controles de ISO27001:2013 en una sola hoja <http://www.iso27000.es/download/ControlesISO27002-2013.pdf...>
- gesconsultor: Acompañamos a IDENTIAN en II Congreso Ib. de Ciberseguridad Industrial @info\_cci <http://goo.gl/Znd1AI pic.twitter.com/Wt30eRi1xP> @GESDATOSC

Vulnerabilities

CCN-CERT NIST (INTECO-CERT) CESICAT



### Últimas Vulnerabilidades

- DSA-2938 - Availability of LTS support for Debian 6.0 / squeeze
- IBM Security Bulletin: ClassLoader manipulation with Apache Struts affecting WebSphere Partner ...
- IBM Security Bulletin: The IBM Smart Analytics System 7600 is affected by a local escalation of ...
- IBM Security Bulletin: Apache Tomcat and FileUpload Vulnerabilities in IBM UrbanCode Release ...

# La Medición es IMPRESCINDIBLE

## ISO 27004, ISO 15939 – Medición de la Seguridad y Procesos TI

**Nr. SIEM Alerts** [ Editar Indicador ]

[ Analizar ]

Mostrar  periodos Hasta  12:00 a.m. Visualización

Fecha Inicial	Fecha Final	Valor Cualitativo	Valor Cuantitativo	Valor Objetivo	Objetivo Alcanzado	Valor Objetivo (%)	Umbral	Tendencia	Decisión
05/11/2013	06/11/2013		12	10		120.00 %			<b>Atención:</b> Número de alertas peligro.
04/11/2013	05/11/2013		26	10		260.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.
03/11/2013	04/11/2013		37	10		370.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.
02/11/2013	03/11/2013		42	10		420.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.
01/11/2013	02/11/2013		36	10		360.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.
31/10/2013	01/11/2013		29	10		290.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.
30/10/2013	31/10/2013		21	10		210.00 %			<b>Peligro:</b> Se están produciendo un número excesivo de alertas.



**Riesgos por Tipo de Amenaza**



## Conclusiones

La nueva edición ISO 27001:2013 está aquí DESDE YA

Hay cambios relevantes tanto en la FORMA como en el FONDO

La convergencia de los Sistemas de Gestión es inevitable

Todo ello ayuda al Gobierno TI

Modelen su Arquitectura Empresarial: es importante y será imprescindible



**GESCONSULTOR**

GOBIERNO T.I. - RIESGO - CUMPLIMIENTO