

Gobierno TI, Seguridad, Riesgo y Cumplimiento



1

**Times are changin'
Gestión 100% integrada de
Las Contingencias T.I.
Y la Continuidad del Negocio**

PLATAFORMA G.R.C. OPERACIONAL 100% PRÁCTICA, 100% TELEFÓNICA

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

Cumplimiento Normativo

- Datos Personales
- Requisitos Legales
- PCI-DSS
- Regulaciones
- Auditoría Interna
- Infraestructuras Críticas

Mejores Prácticas

- ISO 27001
- ISO 22301 (Continuidad de Negocio y DRP)
- ITIL / ISO 20000
- ISO 9001 / 14001

Procesos Gestionados

- Servicios a Clientes 100% gestionados
- Procesos Internos 100% gestionados
- Cumplimiento Legal
- Cuadros de Mando

Gobierno T.I. Monitorización Continua

- Orientada a Negocio
- En Tiempo Real
- SLAs (Servicio)
- KPIs (Rendimiento)
- KRIs (Riesgo)

Arquitectura Empresarial

Modelado Visual de Activos y Dependencias conforme a TOGAF Capa de Negocio (Servicios, Procesos, Recursos), Sistemas y Tecnología

Telefonica GRC Powered by GESCONSULTOR

Organización - SGSI Consultora Demos GesConsultor ES ES Consultor Genérico

Inicio

Arquitectura Empresarial

Arquitectura Empresarial (CMDB)

Representación Gráfica

Monitorización Continua

Gobierno

Riesgo

Privacidad

ISO 27001

ISO 9001

P.N.I.C.

PCI-DSS

E.N.I.

Compliance

Cohit

Negocio

Negocio

Sistemas Aplicaciones

Tecnología

GRC Intelligence: Cuadros de Mando

Indicadores Altamente Visuales. 1ª Implementación Internacional de ISO 27004

Nr. SIEM Alerts [Editar Indicador]

[Analizar]

Mostrar periodos Hasta Fecha 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 %			Atención: Número de alertas peligro.
04/11/2013	05/11/2013		26	10		260.00 %			Peligro: Se están produciendo un número excesivo de alertas.
03/11/2013	04/11/2013		37	10		370.00 %			Peligro: Se están produciendo un número excesivo de alertas.
02/11/2013	03/11/2013		42	10		420.00 %			Peligro: Se están produciendo un número excesivo de alertas.
01/11/2013	02/11/2013		36	10		360.00 %			Peligro: Se están produciendo un número excesivo de alertas.
31/10/2013	01/11/2013		29	10		290.00 %			Peligro: Se están produciendo un número excesivo de alertas.
30/10/2013	31/10/2013		21	10		210.00 %			Peligro: Se están produciendo un número excesivo de alertas.



Centro de Trabajo ISO 27001

Operaciones Cumplimiento

Fuente de Requisitos: Esquema Nacional de Seguridad

Escala: Escala

Propietario:

Tipo de Tarea:

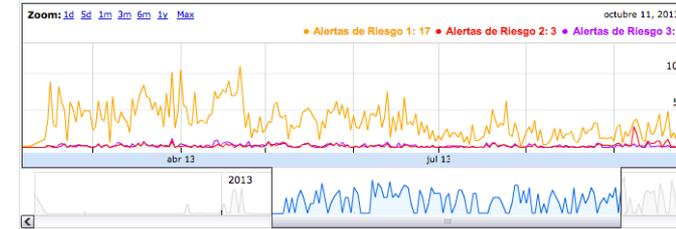
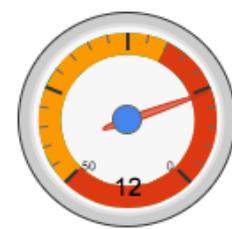
Tipo de Proyecto:

Gráfica de Radar

Gráfica Extendida

Color: Leyenda: Estado, Hasta, Descripción

- L1 - Inicial / AG - 21
- L2 - Planificación, anal. inicial - 40
- L3 - Proceso definido - 61
- L4 - Documentación y revisión - 81
- L5 - Operado - 101



1

Cumplimiento Normativo

Responsabilidad Social Corporativa



Legislación y Estándares más habituales

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

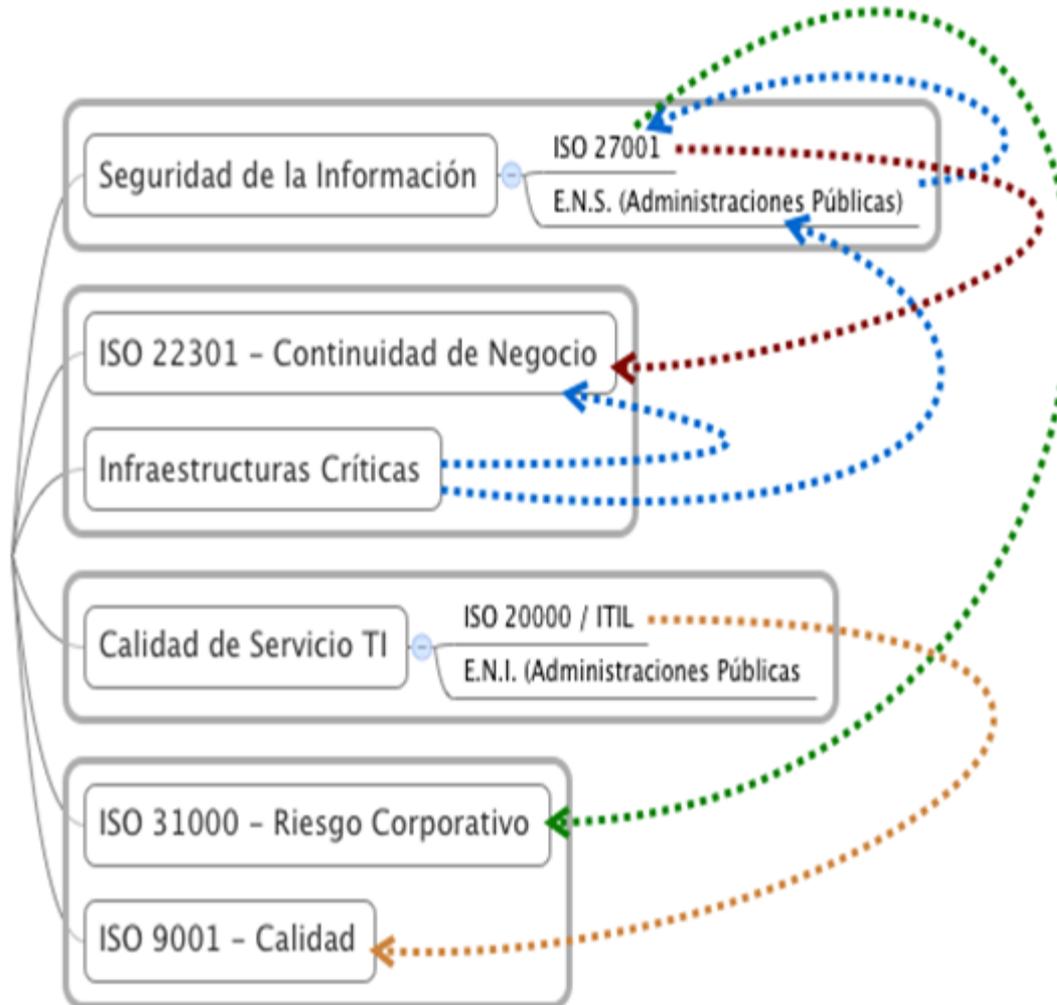
Cargue desde Microsoft Excel sus propios requisitos:

- Legales
- Regulatorios
- Contractuales



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



3

Resiliencia

Seguridad TI, Riesgo
y Continuidad de Negocio

Valoración / Criticidad del Activo conforme a ISO 27005 / ISO 31.000

Dimensiones Clásicas (Confidencialidad, Integridad, Disponibilidad) y/o Personalizadas y Criterios de Impacto Personalizados

Telefonica GRC Powered by GESCONSULTOR Organismo Público Consultora Demos GesConsultor ES Consultor Genérico

Volver a la CMDB Arquitectura Empresarial - Configuración

Lista Business Service Fecha de Creación: 02/06/2014 Usuario: consultor
 (Business Service) Consulta de Estado Financiero Fecha Actualización: Usuario: consultor

Entidad **Valoración** Dependencias Activos Impactados Monitorización Riesgos Continuidad de Negocio

Valoración por Dimensión y Criterio de Impacto

Nivel a Asignar Mostrar Leyenda

ISO/IEC 27001:2013

	Confidencialidad	Integridad	Disponibilidad
S			
O Negocio	Muy Bajo	Muy Bajo	Bajo
/ Legal	Bajo	Bajo	Medio
E Estatutario	Medio	Medio	Alto
C Regulatorio	Alto	Alto	Muy Alto
2 Contractual	Alto	Muy Alto	Muy Alto
7			
0			
0			
4			

B.I.A. (Análisis de Impacto en el Negocio)

Nivel a Asignar Mostrar Leyenda

MAGERIT

B.I.A. (Análisis de Impacto en el Negocio) Escalas de Tiempo Personalizadas y Escalas y Criterios de Impacto Personalizados

- Representación Gráfica
- Monitorización Continua
- Gobierno
- Riesgo
- Privacidad
- ISO 27001
- P.N.I.C.
- PCI-DSS
- E.N.I.
- E.N.S.
- Compliance
- Cobit
- Gestor Documental
- Operaciones
- Herramientas

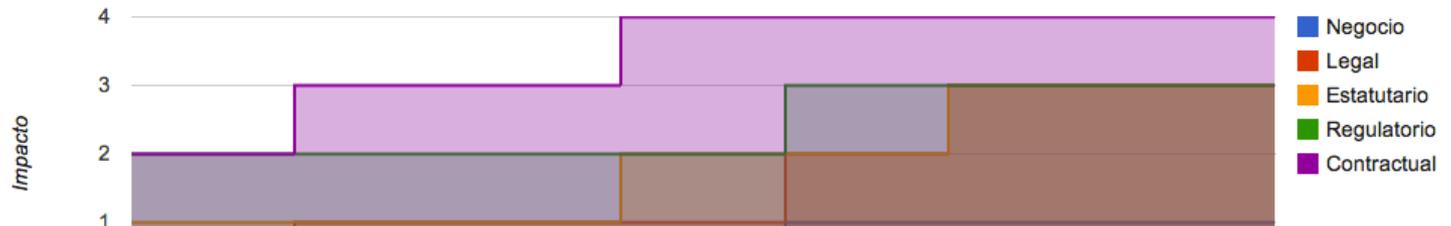
B.I.A. (Análisis de Impacto en el Negocio)

Nivel a Asignar

Mostrar Leyenda

MAGERIT							
	< 1 hora	< 4 horas	< 8 horas	< 1 día	< 3 días	< 1 semana	>= 1 semana
Negocio	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Bajo	Bajo
Legal	Muy Bajo	Bajo	Bajo	Bajo	Medio	Alto	Alto
Estatutario	Bajo	Bajo	Bajo	Medio	Medio	Alto	Alto
Regulatorio	Medio	Medio	Medio	Medio	Alto	Alto	Alto
Contractual	Medio	Alto	Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto

B.I.A. (Análisis de Impacto en el Negocio)



B.I.A. - Dependencias

Dependencias necesarias para restaurarse un Activo

100% gestionadas (incluyendo RTO, RPO y Tiempos de Buffer/Supervivencia)

Telefonica GRC Powered by GESCONSULTOR Organismo Público Consultora Demos GesConsultor ES Consultor Genérico

Volver a la CMDB Arquitectura Empresarial - Configuración

Lista Business Service Fecha de Creación: 02/06/2014 Usuario: consultor
(Business Service) Consulta de Estado Financiero Fecha Actualización: Usuario: consultor

Entidad Valoración Dependencias Activos Impactados Monitorización Riesgos Continuidad de Negocio

Buscar:

Alinear

- Grupo
- Junction
- Sistema de Información
- Servicio de Sistema de Información
- Base de Datos
- Objeto de Base de Datos
- Esquema de Base de Datos
- Tabla de Base de Datos
- Evento de Negocio
- Función de Negocio
- Proceso de Negocio
- Rol
- Business Service
- Ubicación
- Producto
- Organización
- Persona

```

graph TD
    A[Asesor Online  
MaxRTD: 72 h] -- 0 h --> B[Consulta de Estado Financier  
MTPD: 72 h  
RTO: 24 h  
MaxRTD: 72 h]
    B -- 0 h --> C[Gestión Financiera de Usuario  
MTPD: 72 h  
RTO: 16 h  
MaxRTD: 72 h]
    C -- 0 h --> D[Departamento Contable  
MaxRTD: 72 h]
    C -- 0 h --> E[Rob Stark  
MaxRTD: 72 h]
    
```

B.I.A. - Activos Impactados

Activos Impactados cuando hay un Impacto sobre la Disponibilidad
100% gestionadas (incluyendo RTO, RPO y Tiempos de Buffer/Supervivencia)

Telefonica GRC Powered by GESCONSULTOR Organismo Público Consultora Demos GesConsultor ES ES Usuario: consultor

Inicio Arquitectura Empresarial Arquitectura Empresarial (CMDB) Representación Gráfica Monitorización Continua Gobierno Riesgo Privacidad ISO 27001 P.N.I.C. PCI-DSS E.N.I. E.N.S. Compliance

Lista Servidor (Server) Dell Server Fecha de Creación: 13/06/2014 Usuario: consultor Fecha Actualización: Usuario: consultor

Entidad Valoración Dependencias **Activos Impactados** Monitorización Riesgos Continuidad de Negocio

Buscar:

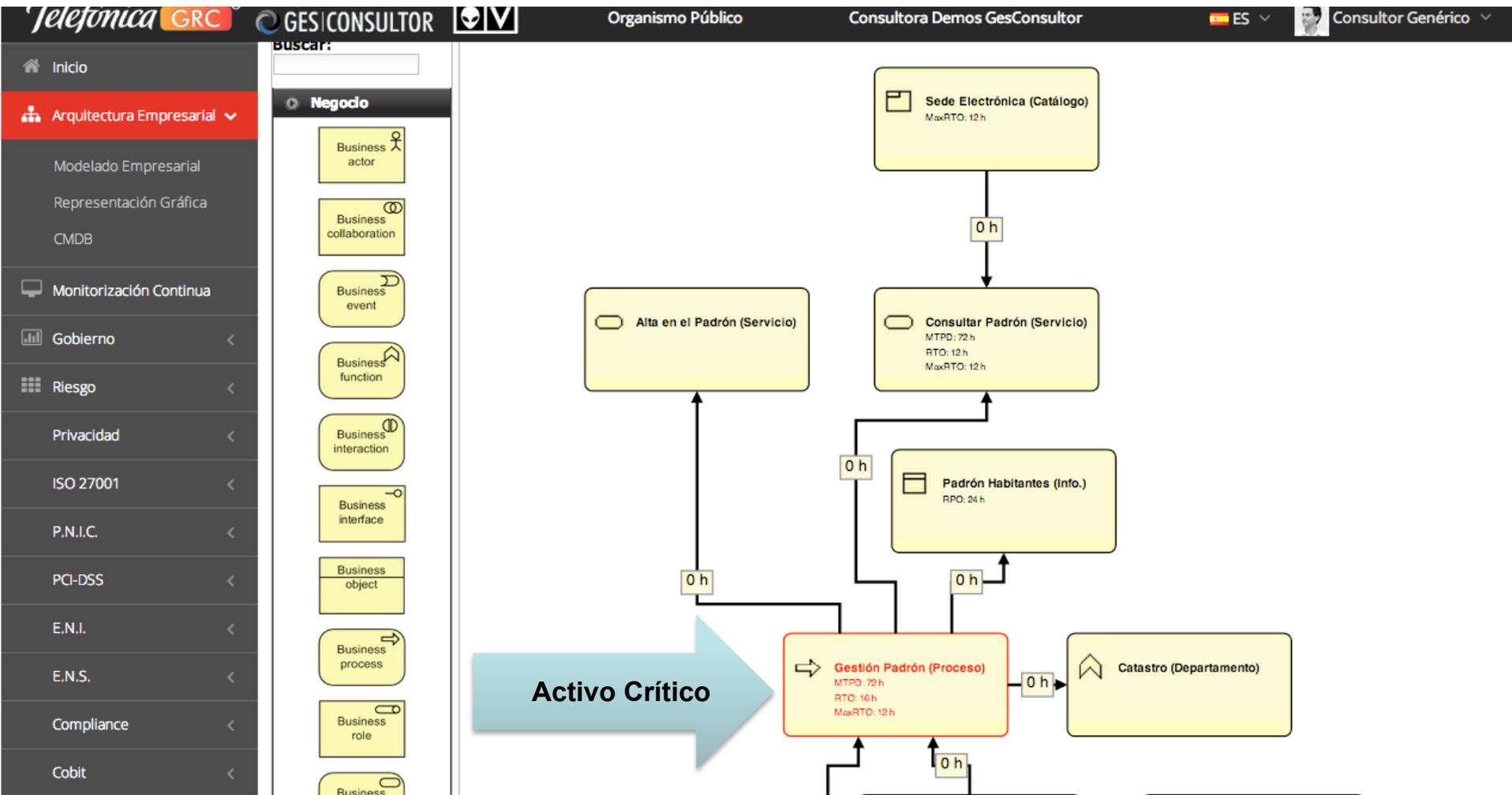
Allnear

- Grupo
- Junction
- Sistema de Información
- Servicio de Sistema de Información
- Base de Datos
- Objeto de Base de Datos
- Esquema de Base de Datos
- Tabla de Base de Datos
- Evento de Negocio
- Función de Negocio
- Proceso de Negocio
- Rol
- Business Service
- Ubicación
- Producto
- Organización
- Persona
- Posición/Cargo
- Información de

B.I.A. –Nodos Críticos que no cumplen los objetivos comprometidos

Identificación de los Recursos cuyos RTO

no permite cumplir los MTPD de Procesos o Servicios o RTO de otros Recursos Impactados



2

Dando vida al Modelo

Gobierno T.I. de la Seguridad y
los Servicios en Tiempo Real

Materialización de Incidentes de Continuidad y otros Riesgos

Integración con los Sistemas de Monitorización

Activación y Notificación Automática de Eventos de Continuidad sobre Activos de Negocio

Telefonica GRC Powered by GESCONSULTOR Organización - SGSI Consultora Demos GesConsultor ES ES Consultor Genérico

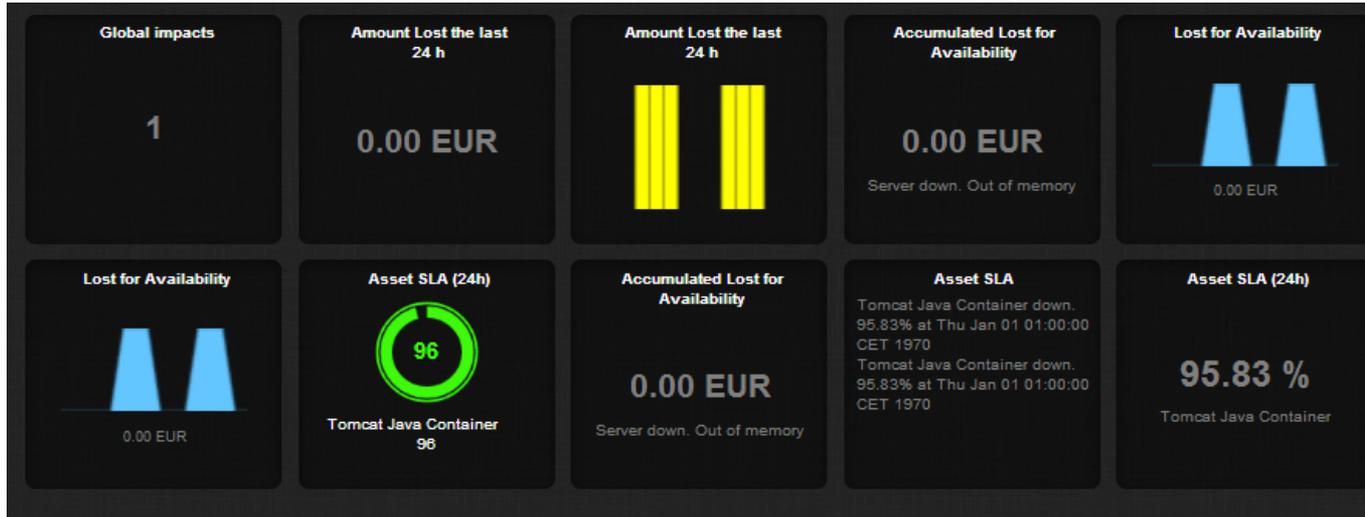
Dominios de Monitorización Continua (NIST SP 800-137)

Inicio	Activos Gestión de ARQUITECTURA EMPRESARIAL	Configuración Gestión de la CMDB	Redes Gestión de MONITORIZACIÓN	Malware Gestión de ANTI-VIRUS
Arquitectura Empresarial	Vulnerabilidades Gestión de SIEM - ESCÁNER	Parches Gestión de PARCHES DE SISTEMAS	Eventos Gestión de SIEM	Incidentes Gestión de SERVICE DESK
Monitorización Continua	Licencias Gestión de CMDB	Información Gestión de la PLATAFORMA D.L.P.	Software Aseguramiento del CALIDAD DEL SOFTWARE	
Gobierno	Políticas Digitales Gestión de SIEM - POLÍTICAS	A.P.T.s Gestión de SIEM - COMPORTAMIENTO		
Riesgo				
Privacidad				
ISO 27001				
ISO 9001				
P.N.I.C.				
PCI-DSS				
E.N.I.				
Compliance				
Cobit				
Gestor Documental				

Materialización de Incidentes de Continuidad y otros Riesgos

Dashboard en Tiempo Real (tipo Wall-Mount)

Cada Dashlet se actualiza sin refrescos de página (tecnología WebSockets)



Indicador	Tipos de Visualización		Indicador	Tipos de Visualización	
Importe Perdido las últimas 24 h	PeityBar		Pérdidas Acumuladas por impacto en Integridad (últimos 365 días)	PeityBar	
	BigNumber			BigNumber	
Porcentaje de Disponibilidad de un Activo (SLA de disponibilidad)	Terminal Log		Pérdidas Acumuladas por impacto en Confidencialidad (últimos 365 días)	PeityBar	
	Percentage			BigNumber	
	CircleStatus		Número de Impactos en Confidencialidad	BigNumber	
Contador de Servicios actualmente Caídos	BigNumber		Número de Impactos en Integridad	BigNumber	
Pérdidas Acumuladas por impacto en Disponibilidad (últimos 365 días)	PeityBar		Número de Impactos en Disponibilidad	BigNumber	
	BigNumber		Número de Impactos (Global)	BigNumber	
				Raindrops	

Telefonica
