Diseño de indicadores y métricas para la creación de un cuadro de mando de seguridad

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones - MISTIC

Autor: Carles Olivé Vernet

Índice

1. Contexto y objetivos
2. Estructura del trabajo
3. ISO/IEC27000 como marco normativo
4. Selección y valoración de controles
5. Implementación del Cuadro de Mando
6. Conclusiones y próximos pasos

Contexto y objetivos

Contexto

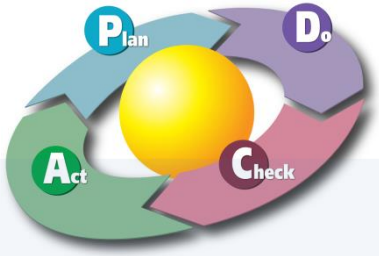
- Proyecto centrado en una compañía en pleno desarrollo de un SGSI
- Disponibilidad / Integridad / Confidencialidad
- Necesidad de medir el grado de madurez del SGSI para su mejora contínua

Objetivos

- Selección de métricas/controles de Seguridad TIC
- Valoración inicial de los controles
- Diseño e implementación de un cuadro de mando para el SGSI corporativo

Estructura del trabajo

ISO 27001



Documentación SGSI → Selección de controles → Análisis madurez controles SGSI → Diseño Cuadro de Mando

ISO/IEC27000 como marco normativo

La serie de normas **ISO/IEC 27000:2013** establece una metodología concreta y pautada para la implementación, mantenimiento y mejora contínua de un SGSI mediante el ciclo de Deming o PDCA (Plan-Do-Check-Act).

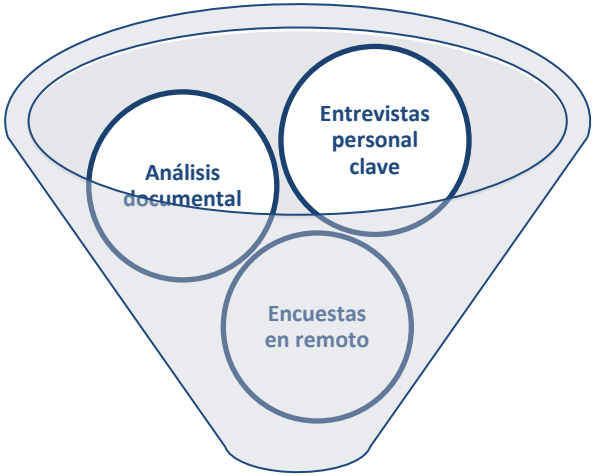
ISO/IEC 27002:2013 enmarca los objetivos de control según **dominios** de la seguridad de la información.

Selección y valoración de controles

ISO/IEC 27001:2013 **114 controles**

Dominio	ID del Control	Descripción del Control	Objetivo del Control	Aspecto a valorar
5. Políticas de seguridad de la información	5.1.1	Documento de Política de Seguridad de la Información	Comprobar que se definen, aprueban y comunican las políticas de seguridad de la información.	¿Se ha definido un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes?
7. Seguridad relativa a los recursos humanos	7.2.2	Capacitación, educación y concientización en seguridad información	Formaciones en temas de seguridad de la información	¿Todos los empleados y los usuarios de terceros (si son relevantes) reciben la formación adecuada y actualizaciones regulares en las políticas y procedimientos de seguridad?
8. Gestión de activos	8.1.1	Inventario de activos	Existencia de un inventario de activos	¿Existe un inventario de activos de información, software, hardware, servicios, personal, etc.?
9. Control de acceso	9.2.4	Gestión de información secreta de autenticación de usuarios	Existencia de un procedimiento para contraseñas de primer uso	¿Existe un procedimiento formalizado para la gestión de contraseñas?
11. Seguridad física y del entorno	11.2.2	Instalaciones de suministro	Prevención contra fallos de alimentación en equipos	¿Los equipos están protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro?
12. Seguridad de las operaciones	12.3.1	Copias de seguridad de la información	Realización y verificación de copias de seguridad	¿Se realizan copias de backup regulares y verificación de las mismas?
13. Seguridad de las comunicaciones	13.1.3	Segregación en redes	División en dominios lógicos por perímetros de seguridad	Para las grandes redes, ¿se dividen en dominios lógicos separados protegidos por un perímetro definido de seguridad, que restringe las capacidades de conexión de los usuarios?
14. Adquisición , desarrollo y mantenimiento de los sistemas de la información	14.2.6	Entorno de desarrollo seguro	Entorno de desarrollo seguro	¿Se dispone de entornos de desarrollo seguros?
15. Relación con proveedores	15.1.2	Requisitos de seguridad en contratos con terceros	Requisitos de seguridad en contratos con terceros	¿El acceso de terceras partes se formaliza a través de contratos? ¿Los contratos recogen las condiciones de seguridad?
16. Gestión de incidentes de seguridad de la información	16.1.5	Respuesta ante incidentes de seguridad de la información	Respuesta ante incidentes de seguridad de la información	¿Los incidentes de seguridad de la información son respondidos de acuerdo con los procedimientos documentados?

Selección y valoración de controles

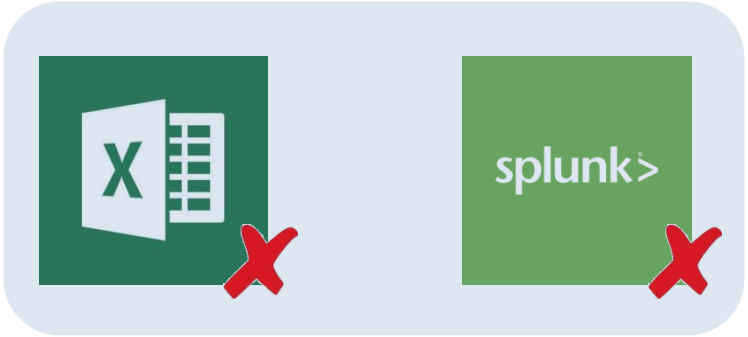


Valor control (0-5)

VALOR	GRADO MADUREZ	DESCRIPCIÓN
0	Inexistente	El proceso no se encuentra implementado ni existen evidencias de que sea mínimamente ejecutado
1	Inicial	El proceso se ejecuta de forma puntual, no organizada ni documentada
2	Repetible	El proceso se encuentra implementado de facto pero no existe un procedimiento formal
3	Definido	El proceso se encuentra implementado y documentado formalmente (**valor objetivo)**
4	Gestionado	El proceso se encuentra implementado, documentado formalmente y es monitorizado y/o gestionado
5	Optimizado	El proceso está totalmente implementado, gestionado y se han establecido mejoras en su ciclo de mejora continua

Selección de la herramienta para el Cuadro de Mando

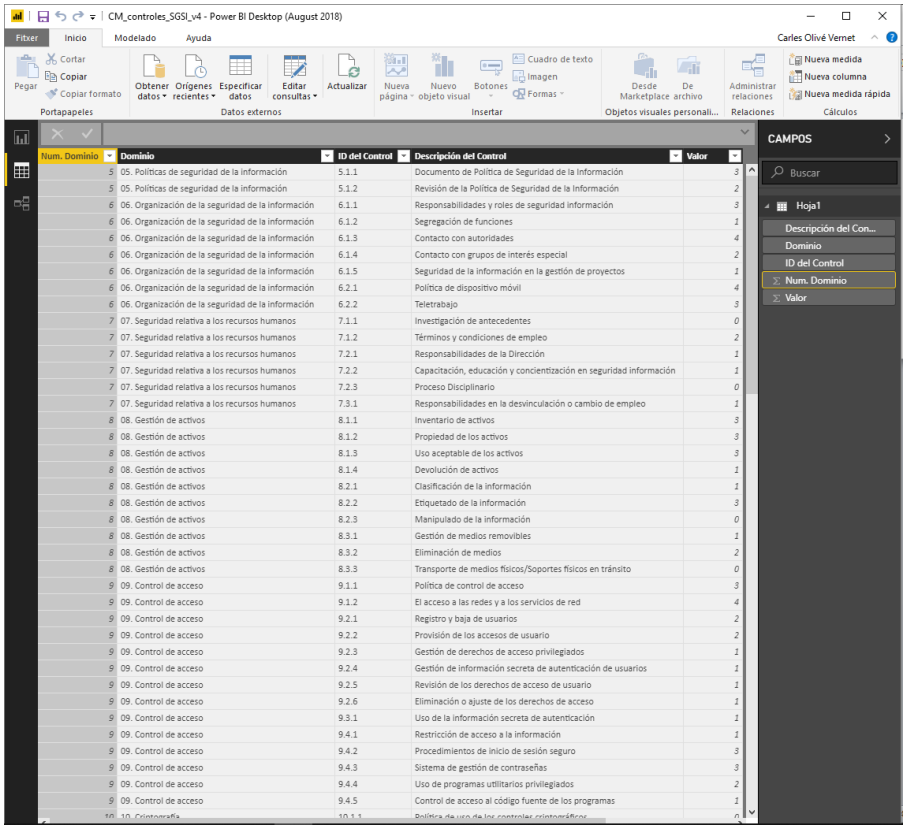
- Gratuita en versión Desktop
- Gestión de datos sencilla a partir de hoja MS Excel
- Diseño de consultas y dashboards sencillo y con resultado visual potente
- Posibilidad de publicar el cuadro de mando *online*



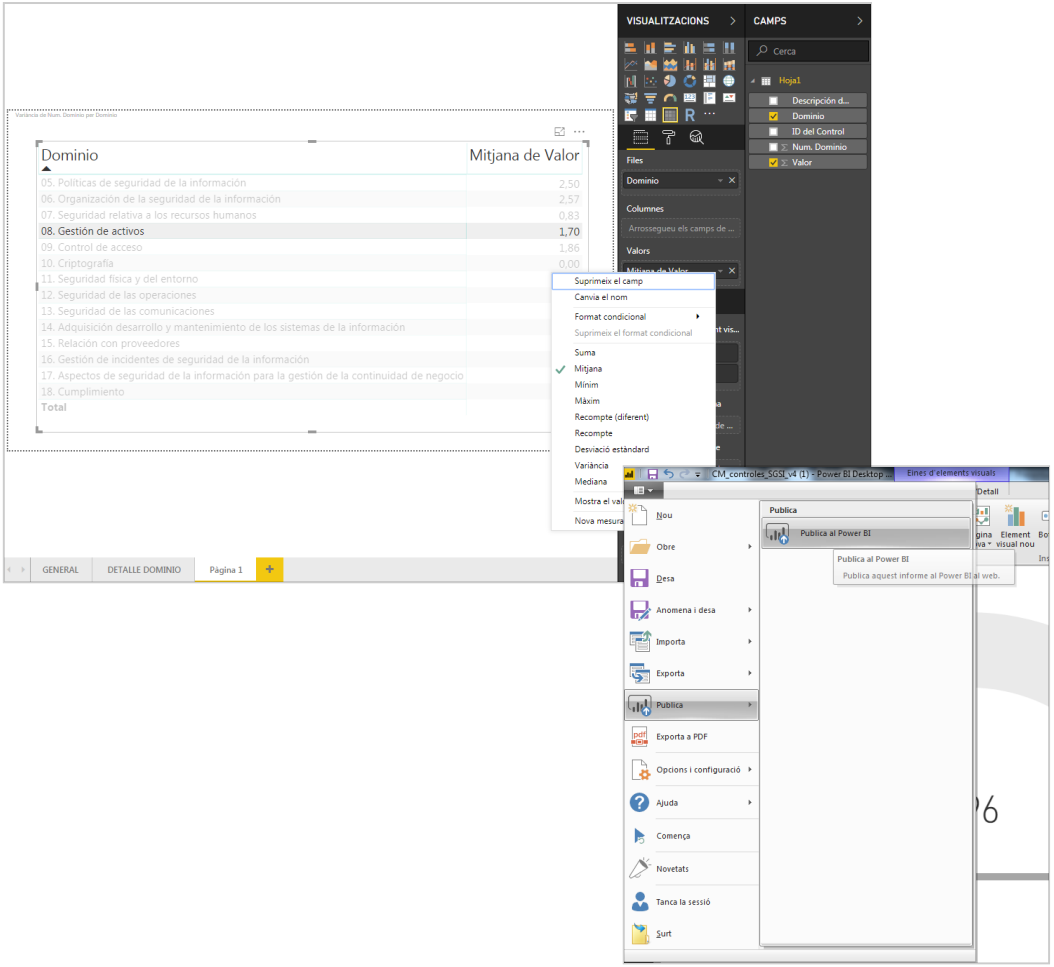
Preparación y carga de datos

1. Optimización de las celdas (celdas combinadas, ordenación en origen, etc.)
2. Normalización de los tipos de datos (campos numéricos, de texto, etc.)
3. Carga de datos a MS Power BI

Num. Dominio	Dominio	ID del Control	Descripción del Control	Valor
5	05. Políticas de seguridad de la información	5.1.1	Documento de Política de Seguridad de la Información	3
5	05. Políticas de seguridad de la información	5.1.2	Revisión de la Política de Seguridad de la Información	2
6	06. Organización de la seguridad de la información	6.1.1	Responsabilidades y roles de seguridad información	3
6	06. Organización de la seguridad de la información	6.1.2	Segregación de funciones	1
6	06. Organización de la seguridad de la información	6.1.3	Contacto con autoridades	4
6	06. Organización de la seguridad de la información	6.1.4	Contacto con grupos de interés especial	2
6	06. Organización de la seguridad de la información	6.1.5	Seguridad de la información en la gestión de proyectos	1
6	06. Organización de la seguridad de la información	6.2.1	Política de dispositivo móvil	4
6	06. Organización de la seguridad de la	6.2.2	Teletrabajo	3

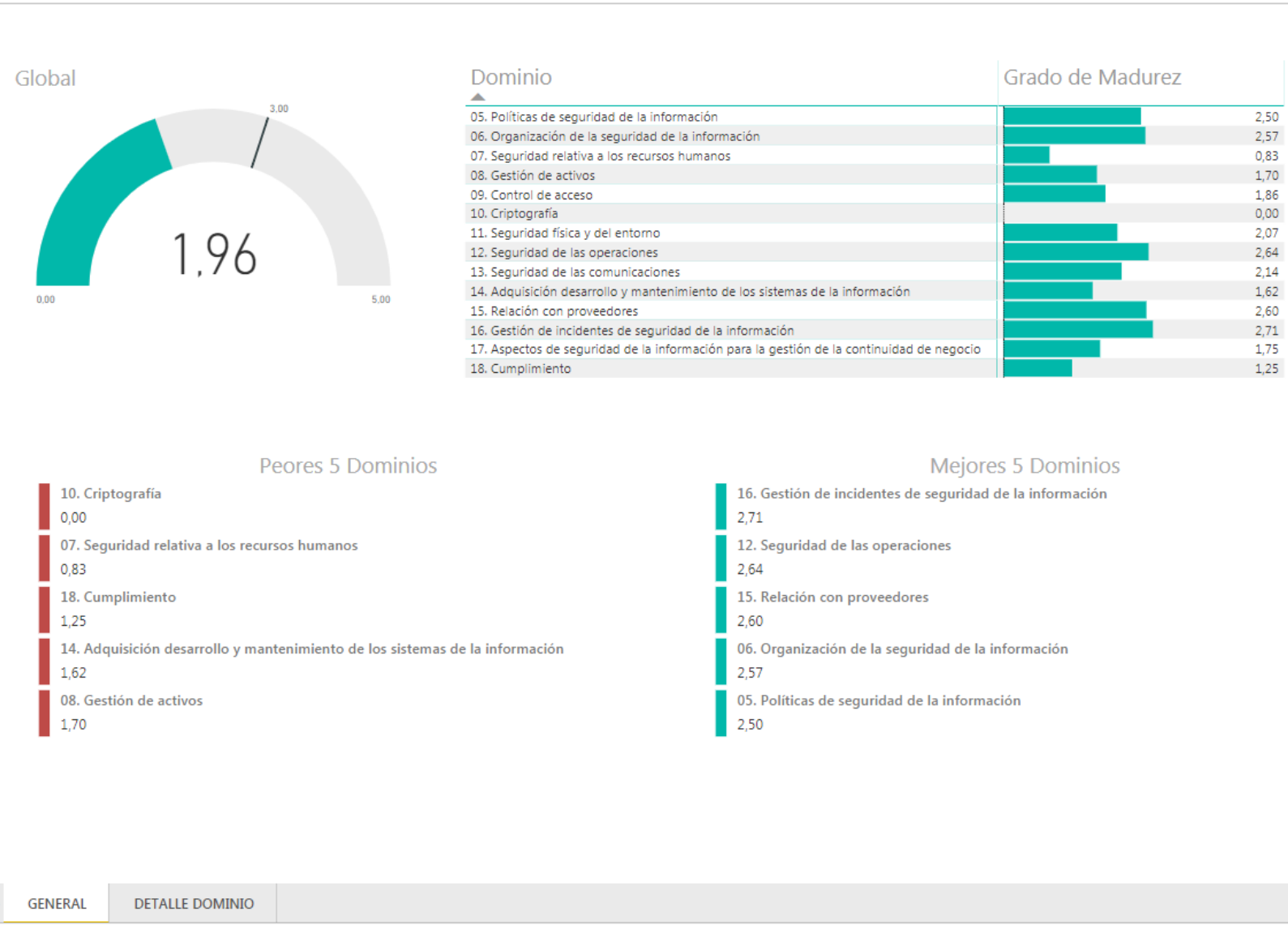


Diseño de paneles – Creación de gráficos e informes/vistas

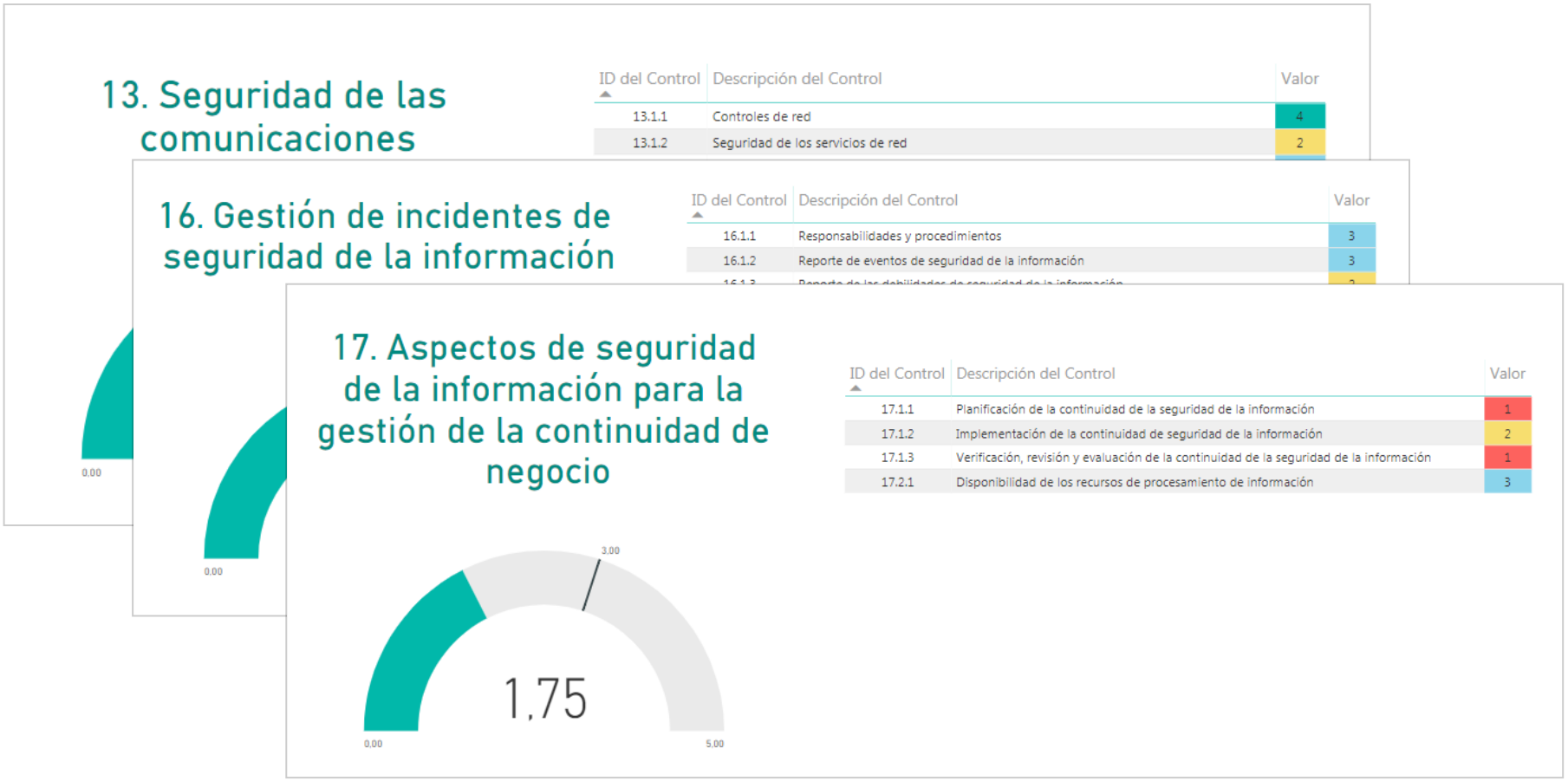


1. Elección de la visualización (tabla, diagrama indicador, gráfico de barras…)
2. Campos a mostrar en la visualización
3. Valores asociados a los campos (mediana, recuento, etc.)
4. Parámetros visuales (tamaño y posición del gráfico, tipo de fuente, etc.)
5. Configuración de vista detalle o *drilldown*
6. Publicación del cuadro de mando para su visualización *online*

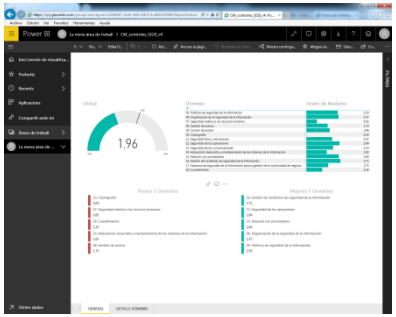
Diseño de paneles – Vista GENERAL



Diseño de paneles – Vista DETALLE DOMINIO (*drilldown* desde Vista GENERAL)



Cuadro de Mando – Resultado y *demo*



Conclusiones y próximos pasos

Conclusiones

- Cuadro de mando disponible para la compañía
- Primera propuesta de plan de acción 2019 sobre el SGSI
  - *Foco: desarrollo teórico de controles y dominios*

Próximos pasos

- Análisis periódico e iterativo (PDCA)
- Modificaciones de la información presentada en el CM
- Difusión y concienciación sobre Seguridad TIC en la compañía


рахмат
danke
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
спасибо
faafetai lava
mersi
barka
welalin
tack
dank je
misaotra
matondo
paldies
grazzi
vinaka
blagodaram
kiitos
dankie
dhanyavad
thank you
gracias
tapadh leat
хвала
asante
manana
obrigada
bedankt
hvala
mauruuru
enkosi
dziękuję
mochchakkeram
djiere dieuf
go raibh maith agat
chnorakaloutioun
gratias ago
gracies
sulpáy
taiku
chokrane
obrigado
sobodi
dėkuji
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
mèsi
najis tuke
ありがとう
tanemirt
grazie
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
мерси
kam sah hamnida
감사합니다
xièxie
ευχαριστώ
merci