Universitat Oberta de Catalunya

uoc.edu

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

Alumno: Carles Olivé Vernet

Trabajo Final de Máster: Máster Interuniversitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Directora: Ángela María García Valdés

Empresa: Instituto Nacional de Ciberseguridad (INCIBE)

Fecha: Diciembre de 2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño de indicadores y métricas para la creación de un cuadro de mando de seguridad*
Nombre del autor:	*Carles Olivé Vernet*
Nombre del consultor/a:	*Ángela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	12/2018
Titulación:	Máster Interuniversitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Cuadro de mando, SGSI, Indicadores*

Resumen del Trabajo

La mayoría de compañías están desarrollando una dependencia creciente respecto a la tecnología. Ante esta perspectiva, resulta cada vez más esencial mantener la integridad, confidencialidad y disponibilidad de los sistemas y de la información que éstos manejan y almacenan para alcanzar sus objetivos estratégicos. Esta necesidad se hace aún más patente a raíz del incremento de ciberataques en el entorno tecnológico actual. Además, ciertas compañías proveen servicios catalogados como esenciales por los estamentos gubernamentales y que, por lo tanto, deben ser sujetos a controles de seguridad exhaustivos. Finalmente, normas legales como el reciente RGPD obligan a las empresas a realizar una reflexión exhaustiva sobre la seguridad en sus servicios TIC.

La serie de normas ISO/IEC 27000 establece una metodología sencilla y pautada para el desarrollo, implementación y mantenimiento de Sistemas de Gestión de la Seguridad de la Información (SGSI) a partir de 14 dominios.

En este trabajo se desarrollarán los controles de seguridad asociados a estos 14 dominios que debe valorar y medir una compañía en fase de implantación de ese SGSI. Posteriormente, en base a la valoración de dichos controles, se diseñará e implantará un cuadro de mando a alto nivel que permita a la compañía conocer el grado de madurez en materia de Seguridad de la Información y ayude a la toma de decisiones estratégicas para la mejora continua del SGSI.

Abstract

Most companies are developing an increasing dependence on technology. Given this perspective, it is more and more essential to maintain the integrity, confidentiality and availability of the systems and the information they manage and store to achieve their strategic objectives. This need is even more evident as a result of the increase in cyber-attacks in the global technological environment. In addition, certain companies provide services categorized as essential by governmental bodies and, therefore, must be subject to exhaustive security controls. Finally, legal regulations such as the recent GDPR require companies to carry out an exhaustive reflection on the security of their ICT services.

The ISO / IEC 27000 series establishes a simple and step-by-step methodology for the development, implementation and maintenance of Information Security Management Systems (ISMS) following its 14 domains.

In this work, the security controls that a company have to assess and measure along these 14 domains will be developed. Subsequently, based on the assessment of these controls, a high-level scorecard will be designed and implemented with the aim of letting the company know the maturity level in Information Security and help strategic decision making for improvement cycle of the ISMS.

Tabla de contenido

1. Introducción

1.1. Contexto y justificación

La compañía sujeto de análisis de este Trabajo de Final de Máster (TFM) está desarrollando un Sistema Gestor de la Seguridad de la Información (SGSI) siguiendo los estándares de la normativa ISO/IEC 27000.

Dentro del desarrollo del SGSI se prevé la selección, tratamiento e implementación de controles de seguridad. Estos controles serán seleccionados y priorizados en función del análisis de riesgos realizado en la compañía.

En este contexto, uno de los puntos clave será la medición de los controles establecidos para que realmente aporten valor en el desarrollo del SGSI puesto que, como reza la clásica máxima de gestión empresarial, “no se puede controlar lo que no se puede medir”.

1.2. Objetivos

Este proyecto tendrá por objetivo la identificación y documentación de los controles de seguridad seleccionados en el desarrollo e implantación del SGSI de la compañía y el establecimiento de métricas e indicadores para su seguimiento.

Cabe destacar que la medición de los controles de un SGSI es un proceso continuo e iterativo y por lo tanto, debe desarrollarse, ampliarse con nuevos controles y/o modificarse en función del propio desarrollo del SGSI y de la evaluación continua de riesgos que se efectúe en la compañía. La realización de este TFM debe desembocar en una primera versión del cuadro de mando de seguridad de la compañía que permita realizar un análisis inicial del grado de madurez de su SGSI y la identificación del plan de trabajo posterior relacionado con su desarrollo.

2. Plan de trabajo

2.1. Metodología

Por un lado, a nivel específico del proyecto de selección e implantación de los controles, la compañía analizada utiliza como referencia la norma general ISO/IEC27000, centrándose especialmente en las normas ISO/IEC 27001 como marco de gestión del SGSI, ISO/IEC27002 como referencia de los dominios y controles del SGSI y la ISO/IEC 27004 en cuanto a mejores prácticas en la medición de los controles del SGSI.

Asimismo tendremos en cuenta el ciclo de Deming PDCA (Plan-Do-Check-Act), intentando que coincida la implementación del proyecto con las fases seguidas en el mismo SGSI a analizar. Como se ha comentado anteriormente, se prevé que este trabajo desemboque en una primera versión del cuadro de mando que puede ser analizada y mejorada iterativamente a posteriori.

Finalmente, se realizará un análisis *gap* o análisis de brecha para identificar el desempeño en materia de seguridad de la información y las diferencias entre el estado actual y el deseado para cada uno de los dominios que establece el estándar. Este tipo de análisis puede favorecer que a posteriori la compañía pueda optar a la certificación de la ISO/IEC 27001:2013.

Por otro lado, a nivel de gestión del proyecto, se trabajará teniendo en cuenta como guía metodológica las buenas prácticas recomendadas por el Project Management Book of Knowledge (PMBOK).

2.2. Listado de tareas (EDT)

A continuación se relaciona la lista de tareas a llevar a cabo durante el transcurso de este proyecto.

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Diseño de indicadores y métricas para la creación de un cuadro de mando de seguridad	**48 días**	**lun 08/10/18**	**mié 12/12/18**	
Recopilación de documentación del SGSI	10 días	lun 08/10/18	vie 19/10/18	
Selección de controles a medir	10 días	lun 22/10/18	vie 02/11/18	2
Alcance del proyecto técnico definido	0 días	vie 02/11/18	vie 02/11/18	3
Entrevistas con actores implicados en el desarrollo del SGSI en la compañía	10 días	lun 05/11/18	vie 16/11/18	3
Análisis del grado de madurez de los controles del SGSI	5 días	lun 19/11/18	vie 23/11/18	5
Estudio de herramientas para la creación de un cuadro de mando de seguridad	15 días	lun 05/11/18	vie 23/11/18	3
Diseño del cuadro de mando del SGSI	5 días	lun 26/11/18	vie 30/11/18	6;7
Primera versión del cuadro de mando del SGSI implementada	0 días	vie 30/11/18	vie 30/11/18	8
Análisis del estado del SGSI (a partir del cuadro de mando)	5 días	lun 03/12/18	vie 07/12/18	9
Puntos de mejora y próximos pasos	3 días	lun 10/12/18	mié 12/12/18	10
Redacción de la memoria	60 días	lun 08/10/18	vie 28/12/18	
Confección del vídeo de presentación	5 días	mar 01/01/19	lun 07/01/19	
Defensa del TFM	5 días	lun 14/01/19	vie 18/01/19	

fig. 1. Estructura de descomposición del trabajo (EDT) del proyecto

2.3. Planificación

Se establece la siguiente planificación temporal para el desarrollo del proyecto, teniendo en cuenta las fechas establecidas para la entrega de la memoria y para la defensa del propio TFM.

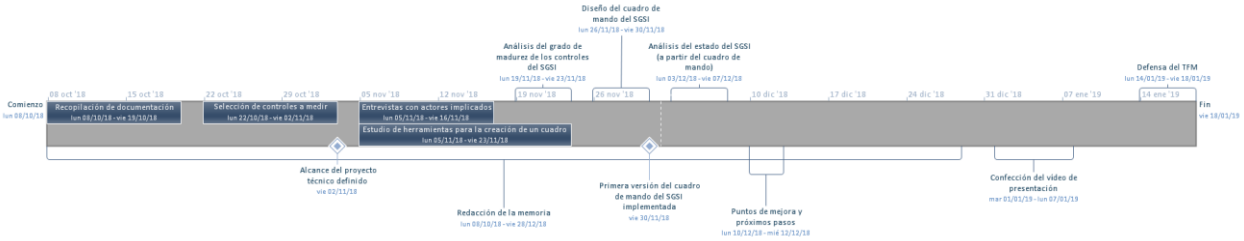


fig. 2. Cronograma del proyecto

2.4. Entregables

Se prevé, como resultado y entregable de este proyecto, además de esta memoria del TFM, una primera versión del cuadro de mando para el SGSI de la compañía implementada en la herramienta seleccionada a partir de la tarea "*Estudio de herramientas para la creación de un cuadro de mando de seguridad*".

3. Recopilación de documentación del SGSI

La compañía analizada se encuentra en pleno desarrollo de su Cuerpo Normativo de Seguridad. Este desarrollo está basado en ISO/IEC 27002:2013. El objetivo de la implantación del SGSI es establecer las directrices necesarias para evitar la alteración, pérdida, indisponibilidad y tratamiento o acceso no autorizado a la información de la compañía. Además también se tendrá en cuenta el control de acceso físico a las ubicaciones donde se encuentran equipos sensibles para la organización, como el CPD, salas de comunicaciones, etc. Finalmente se pretende abordar la vertiente humana en cuanto al compromiso de toda persona o entidad relacionada con la compañía en referencia al tratamiento de la información durante todo su ciclo de vida.

Al término del desarrollo del SGSI se dispondrá de los documentos de Política de Seguridad de la compañía y de 13 normativas basadas en los dominios de la ISO/IEC 27002:2013:

- Aspectos organizativos para la seguridad
- Seguridad ligada a los recursos humanos
- Clasificación y control de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad ligada a las operaciones
- Seguridad ligada a las comunicaciones
- Desarrollo y mantenimiento de sistemas
- Seguridad ligada a los proveedores
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad del negocio
- Cumplimiento

El cuadro de mando desarrollado en este proyecto deberá medir la madurez de la organización en cada uno de los controles establecidos sobre los dominios anteriores, ayudando a identificar puntos de mejora y a priorizar las líneas de trabajo que se deberán abordar a posteriori en cuanto a la seguridad de la información de la compañía.

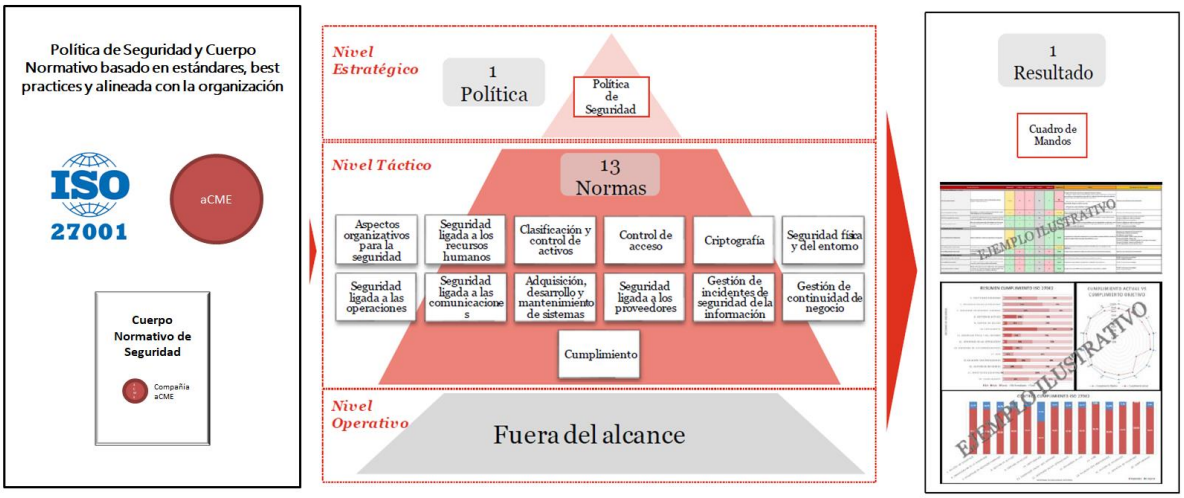


fig. 3. ISO27001 como marco del proyecto

Hasta el momento de presentar este proyecto se cuenta con los siguientes documentos desarrollados y recopilados para este TFM:

- Política de Seguridad TIC
- Normativa de Gestión de Activos
- Normativa de Control de Acceso a los Sistemas de Información
- Normativa de Seguridad en las Operaciones
- Normativa de Respuesta a Incidentes Ciber
- Procedimiento de control de acceso CPD
- Procedimiento Operativo – DDoS
- Procedimiento Operativo – Fuga de Información
- Procedimiento Operativo – Intrusión
- Procedimiento Operativo – Phishing
- Procedimiento Operativo – Ransomware

La revisión de estos documentos es la base inicial para establecer un primer contacto con el grado de madurez del SGSI de la compañía. En el proceso de análisis se correlará la información recogida en base a entrevistas y a la documentación de detalle de cada ámbito con las pautas que estas normativas establecen para valorar el estado del arte actual en cuanto a seguridad de la información.

4. Selección de controles

Siguiendo las recomendaciones de ISO/IEC 27002:2013 en cuanto a dominios, hemos establecido inicialmente los controles detallados en el ***Anexo A: Tabla de selección de controles*** como alcance a evaluar en este proyecto. Además de la descripción y el objetivo del control, se adjuntan cuestiones específicas que se deberán responder a partir del análisis documental y de las entrevistas con personas clave y que permitirán obtener el estado del arte actual en cada ámbito. En total se abordan los **114 controles** especificados por la norma ISO/IEC 27001:2013.

5. Entrevistas con los actores implicados en el desarrollo del SGSI en la compañía

5.1. Organización de la seguridad

La compañía analizada para este TFM cuenta con un Área de Tecnología interna, encargada del desarrollo de proyectos y de la prestación de los servicios TIC. Dicha Área de Tecnología cuenta con varios departamentos y especialistas dedicados a los distintos campos TIC: comunicaciones, sistemas de información y desarrollo, arquitectura de servidores y sistemas, tecnologías específicas de Negocio, etc. Además cuenta con dos centros de control y supervisión de los sistemas de información y de las telecomunicaciones.

Además, determinadas personas clave de esta Área de Tecnología conforman y participan en los organismos y roles específicos en el ámbito de la seguridad TIC establecidos hasta la fecha. En este sentido, la compañía tiene establecidos los siguientes roles y comités:

- Director Global de Seguridad
    - Rol ocupado por el Director Ejecutivo de la compañía y validador del SGSI.

- Comité Global de Seguridad
    - Formado por los responsables de seguridad de los distintos ámbitos (seguridad física, seguridad de las tecnologías de la información, seguridad de la tecnologías de la operación), además de los que se considera necesario en cada momento.

- Comité de Ciberseguridad
    - Formado por los siguientes roles:
        - Director Ejecutivo del Área de Tecnología
        - Director de Infraestructuras Tecnológicas y Operación de Tecnologías y Sistemas
        - Director de Sistemas de Información
        - Director de Tecnologías de Negocio
        - Director de Tecnologías Digitales y de Cliente
        - Responsable de Operación de Sistemas de Información
        - Responsable de Operación de Telecomunicaciones
        - Responsable de Arquitectura de Sistemas
        - Responsable de Seguridad TIC

- CISO (Chief Information Security Officer)
    - Rol ocupado por el Director de Infraestructuras Tecnológicas y Operación de Tecnologías y Sistemas

- Responsable de Seguridad TIC

- Director del proyecto de desarrollo e implantación del SGSI en la compañía y orquestador de las actividades referentes a la seguridad TIC en los distintos ámbitos del Área de Tecnología.

5.2. Entrevistas con personal clave

En este punto del proyecto, se han realizado entrevistas con algunos de los actores anteriormente descritos, que han sido identificados como clave en la gestión de la seguridad TIC con el fin de obtener conocimiento sobre las distintas tareas y controles que se llevan a cabo.

A tal efecto, para agilizar el traspaso y recogida de información minimizando la necesidad de mantener reuniones presenciales, se han enviado las preguntas específicas mostradas en el apartado anterior a modo de guion y acta para cada uno de los 14 dominios de la ISO/IEC 27000:2013 y sus controles a analizar.

6. Análisis del grado de madurez de los controles del SGSI

6.1. Grados de madurez

En base a la información recogida de las entrevistas con el personal clave y del análisis de la documentación existente, se realizará una primera valoración del grado de madurez en la implantación de los distintos controles. Para ello, se plantea un análisis *gap* donde se identifican los siguientes posibles niveles siguiendo el modelo CMMI (Capability Maturity Model Integration):

Valor	Grado de 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

tabla 1. Valores posibles del grado de madurez de los controles del SGSI

Dado que nos encontramos en las primeras fases del desarrollo del SGSI en la compañía, consideraremos el nivel ***3 – Definido*** como **valor objetivo** del grado de madurez, tanto para los controles como para cada uno de los dominios. Las iniciativas de mejora que se establezcan deberán aproximar a la compañía a este objetivo.

6.2. Asignación de valores a los controles

En el ***ANEXO B: Tabla asignación de valores a los controles*** se presentan los valores asignados a cada uno de los controles predefinidos y una breve justificación de esta asignación.

7. Estudio de herramientas para la creación de un cuadro de mando de seguridad

7.1. Herramientas analizadas

Durante el transcurso del proyecto, se han analizado 3 posibles herramientas para presentar el resultado del análisis GAP visto anteriormente en forma de cuadro de mando. Estas herramientas son Splunk, Microsoft Excel y Microsoft Power BI. A continuación mostramos las principales características en forma de puntos fuertes y puntos débiles de cada una de ellas.

SPLUNK:

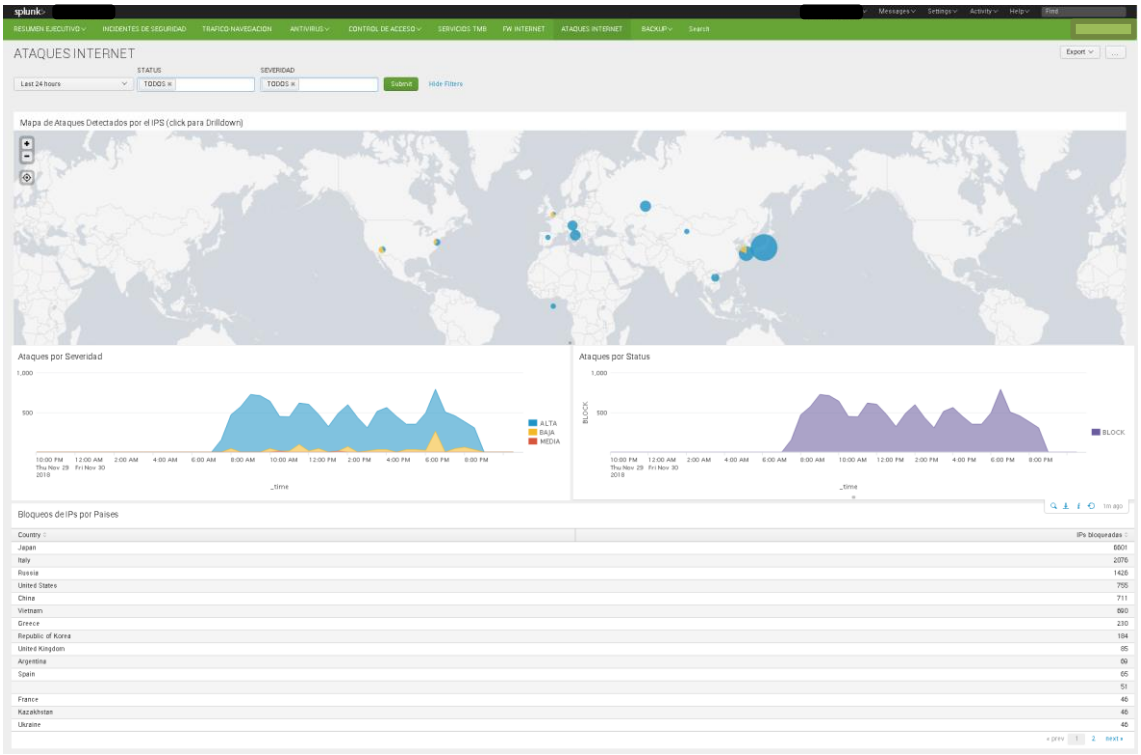


fig. 4. Ejemplo de cuadro de mando con Splunk

PROS	CONTRAS
Es una herramienta muy potente de análisis y gestión de múltiples fuentes de datos estructurados y no estructurados orientada a Big Data	Dificultad en la programación de consultas y dashboards
Gran potencialidad gráfica	Coste de licencias en base a cantidad de datos procesados
Capacidad de crear alertas en función de los eventos recogidos	Puede resultar un producto demasiado complejo para la elaboración un cuadro de mando basado en datos que caben en un Excel

tabla 2. Análisis de la herramienta Splunk

MS EXCEL:

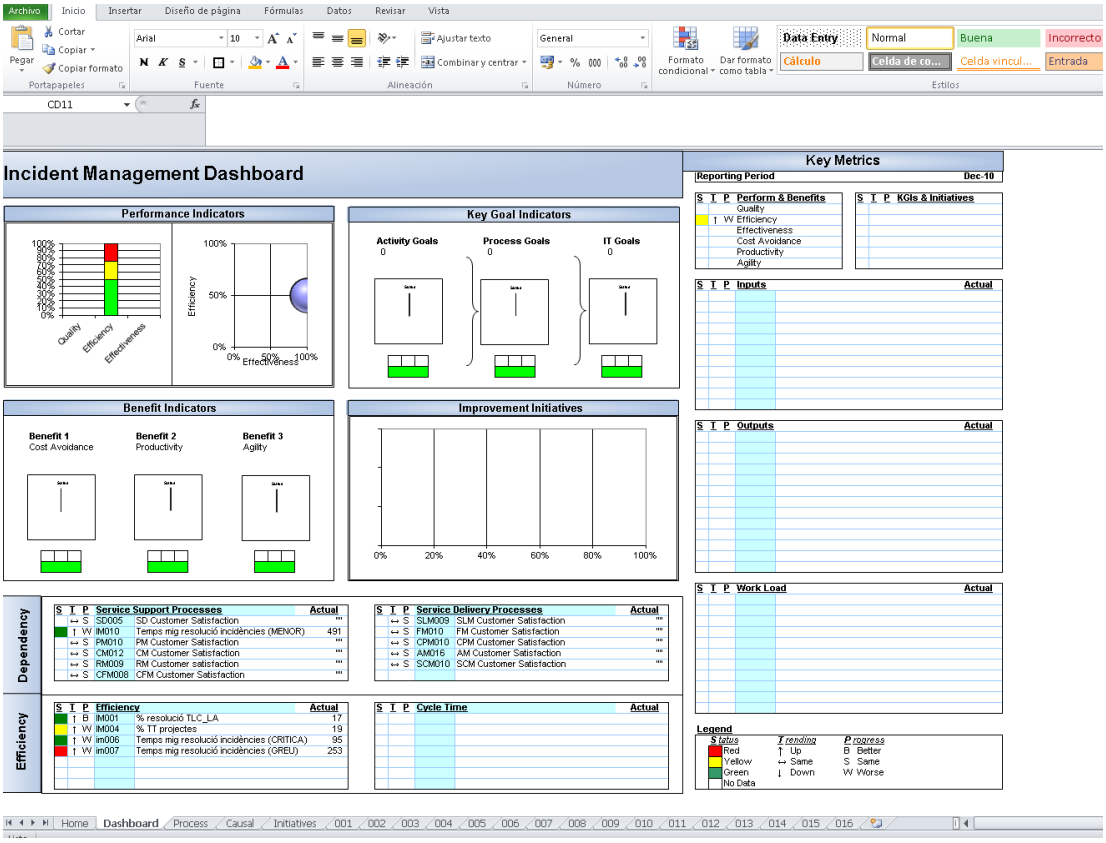


fig. 5. Ejemplo de cuadro de mando con MS Excel

PROS	CONTRAS
Es una herramienta bien conocida y sencilla de manejar los datos (si están bien estructurados)	Los gráficos habituales pueden resultar poco atractivos para la consulta de un cuadro de mando
Tiene capacidades gráficas sencillas de implementar	La creación de gráficos poco habituales puede resultar tediosa
Se pueden crear informes estáticos (pdf) a partir de él	No es posible compartir un informe dinámico sin compartir todos los datos “en crudo”

tabla 3. Análisis de la herramienta MS Excel

MS POWER BI

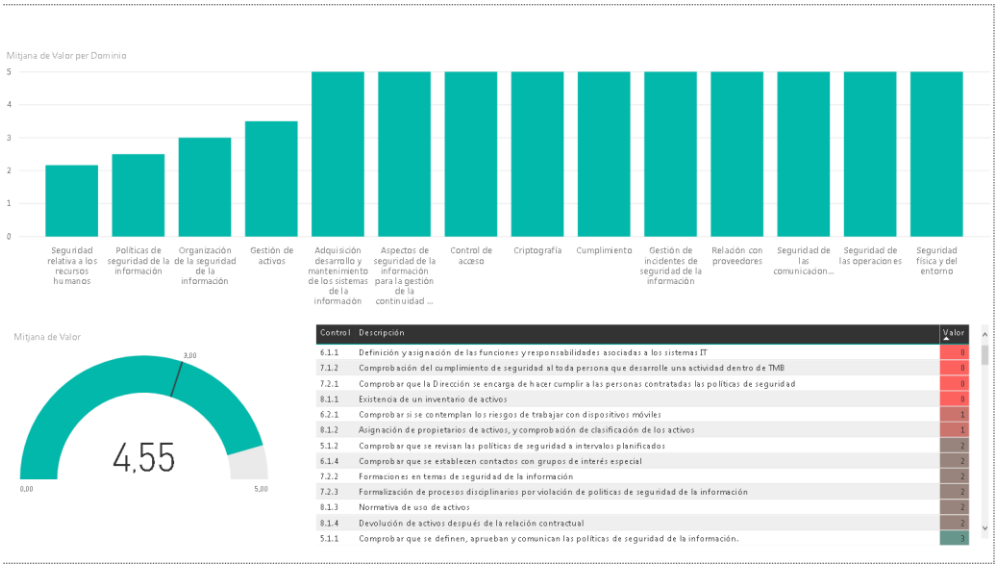


fig. 6. Ejemplo de cuadro de mando con MS Power BI

PROS	CONTRAS
La gestión de los datos es sencilla puesto que para nuestro caso se basaría en una hoja Excel	El tipo de gráficos puede resultar limitado en función de la información a mostrar, aunque existen bibliotecas adicionales de tipos de gráfico
La compañía cuenta con licencia para publicación de informes y cuadros de mando online	Es necesaria una cuenta corporativa de Microsoft para acceder a ciertas funcionalidades de la herramienta
Facilita el diseño e implementación de cuadros de mando de forma sencilla y, a la vez, con un resultado visual potente	En el caso de datos basados en Excel, puede ser necesario un tratamiento previo de los datos para normalizar todos los campos (celdas combinadas, tipos de dato numéricos o de texto, etc.)

tabla 4. Análisis de la herramienta Splunk

Finalmente se ha decidido utilizar la herramienta MS Power BI. En esta decisión han pesado especialmente los siguientes factores:

- Es una herramienta gratuita en su versión Desktop, con la cual se pueden crear y compartir cuadros de mando.
- El diseño e implementación del cuadro de mando resulta muy sencilla utilizando como fuente de datos una o varias hojas Excel y a su vez se obtiene una mayor capacidad gráfica y de interacción que una tabla o gráfico dinámicos en el propio MS Excel. No es necesario conocer ningún lenguaje de base de datos como puede requerir Splunk ya que se basa en concepto WYSIWYG (What You See Is What You Get).
- La compañía cuenta adicionalmente con licencia para publicar internamente los cuadros de mando, de forma que cualquier usuario autorizado podrá tener a su alcance un cuadro de mando dinámico referente a la seguridad de la información.

8. Diseño del cuadro de mando del SGSI

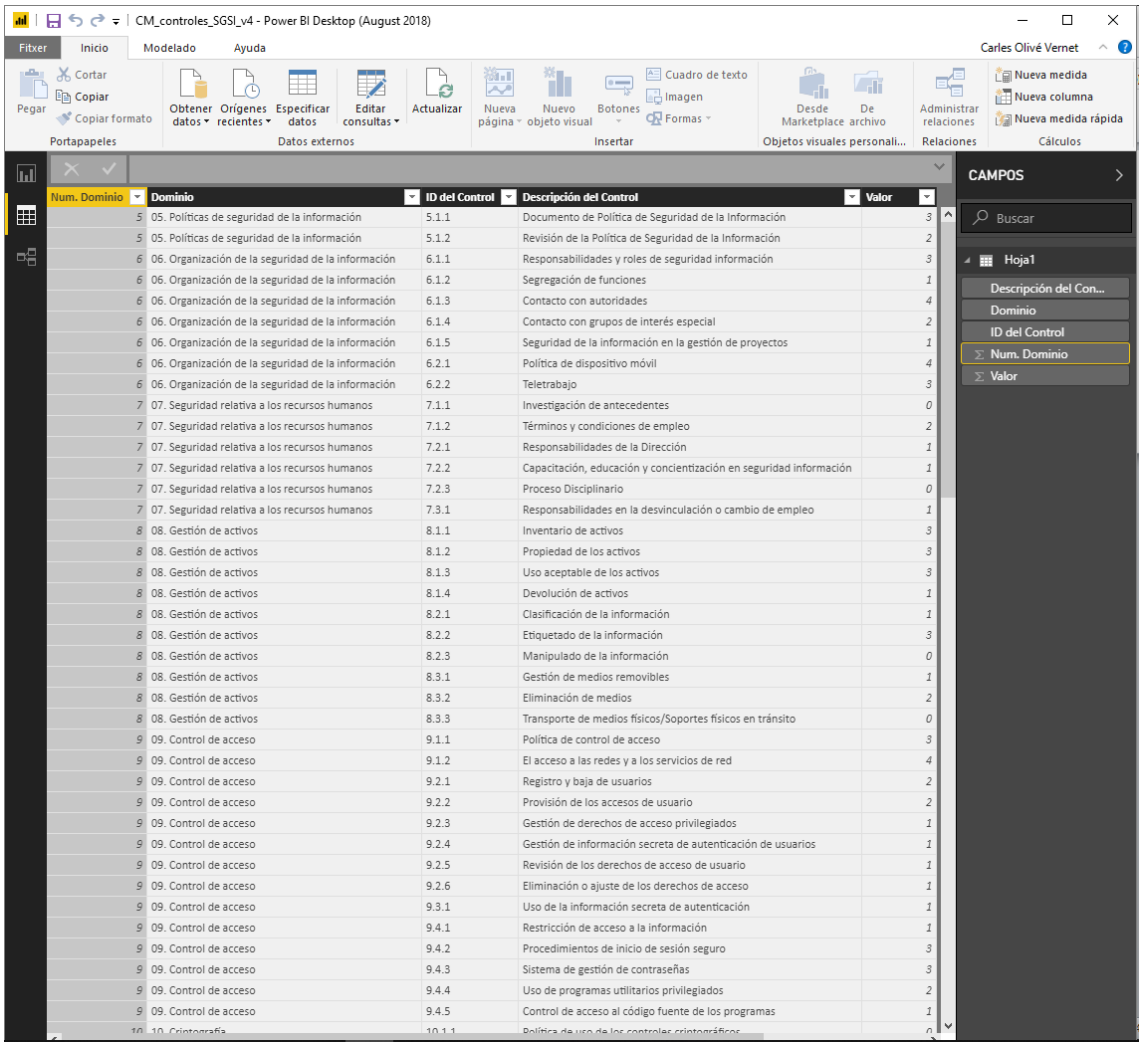
8.1. Carga de datos

Como hemos visto en el capítulo anterior, hemos elegido la herramienta Microsoft Power BI para construir el cuadro de mando del SGSI de la compañía. Antes de empezar a generar los informes y consultas, hemos generado una tabla optimizada para la carga de datos a Power BI a partir de la tabla ***ANEXO B: Tabla asignación de valores a los controles***. De esta forma corregimos posibles errores a causa de celdas combinadas, valores numéricos como texto, etc. Esta tabla de carga se adjunta en el ***ANEXO C: Tabla valoración controles SGSI (carga MS Power BI)*** y tiene el siguiente aspecto:

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 información	6.2.2	Teletrabajo	*3*
7	07. Seguridad relativa a los recursos humanos	7.1.1	Investigación de antecedentes	*0*
7	07. Seguridad relativa a los recursos humanos	7.1.2	Términos y condiciones de empleo	*2*
7	07. Seguridad relativa a los recursos humanos	7.2.1	Responsabilidades de la Dirección	*1*
7	07. Seguridad relativa a los recursos humanos	7.2.2	Capacitación, educación y concientización en seguridad información	*1*
7	07. Seguridad relativa a los recursos humanos	7.2.3	Proceso Disciplinario	*0*
7	07. Seguridad relativa a los recursos humanos	7.3.1	Responsabilidades en la desvinculación o cambio de empleo	*1*

fig. 7. Muestra de la "Tabla valoración controles SGSI.xlsx"

Una vez construida la tabla anterior, cargamos los 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 información	6.2.2	Teletrabajo	3
7	07. Seguridad relativa a los recursos humanos	7.1.1	Investigación de antecedentes	0
7	07. Seguridad relativa a los recursos humanos	7.1.2	Términos y condiciones de empleo	2
7	07. Seguridad relativa a los recursos humanos	7.2.1	Responsabilidades de la Dirección	1
7	07. Seguridad relativa a los recursos humanos	7.2.2	Capacitación, educación y concientización en seguridad información	1
7	07. Seguridad relativa a los recursos humanos	7.2.3	Proceso Disciplinario	0
7	07. Seguridad relativa a los recursos humanos	7.3.1	Responsabilidades en la desvinculación o cambio de empleo	1
8	08. Gestión de activos	8.1.1	Inventario de activos	3
8	08. Gestión de activos	8.1.2	Propiedad de los activos	3
8	08. Gestión de activos	8.1.3	Uso aceptable de los activos	3
8	08. Gestión de activos	8.1.4	Devolución de activos	1
8	08. Gestión de activos	8.2.1	Clasificación de la información	1
8	08. Gestión de activos	8.2.2	Etiquetado de la información	3
8	08. Gestión de activos	8.2.3	Manipulado de la información	0
8	08. Gestión de activos	8.3.1	Gestión de medios removibles	1
8	08. Gestión de activos	8.3.2	Eliminación de medios	2
8	08. Gestión de activos	8.3.3	Transporte de medios físicos/Soportes físicos en tránsito	0
9	09. Control de acceso	9.1.1	Política de control de acceso	3
9	09. Control de acceso	9.1.2	El acceso a las redes y a los servicios de red	4
9	09. Control de acceso	9.2.1	Registro y baja de usuarios	2
9	09. Control de acceso	9.2.2	Provisión de los accesos de usuario	2
9	09. Control de acceso	9.2.3	Gestión de derechos de acceso privilegiados	1
9	09. Control de acceso	9.2.4	Gestión de información secreta de autenticación de usuarios	1
9	09. Control de acceso	9.2.5	Revisión de los derechos de acceso de usuario	1
9	09. Control de acceso	9.2.6	Eliminación o ajuste de los derechos de acceso	1
9	09. Control de acceso	9.3.1	Uso de la información secreta de autenticación	1
9	09. Control de acceso	9.4.1	Restricción de acceso a la información	1
9	09. Control de acceso	9.4.2	Procedimientos de inicio de sesión seguro	3
9	09. Control de acceso	9.4.3	Sistema de gestión de contraseñas	3
9	09. Control de acceso	9.4.4	Uso de programas utilitarios privilegiados	2
9	09. Control de acceso	9.4.5	Control de acceso al código fuente de los programas	1
10	10. Criptografía	10.1.1	Política de uso de los controles criptográficos	0

fig. 8. Vista de la carga de datos a MS Power BI

Para nuestro cuadro de mando, utilizaremos simplemente una tabla. Si fuese necesario utilizar varias tablas relacionadas, se podría modelar con la propia herramienta:

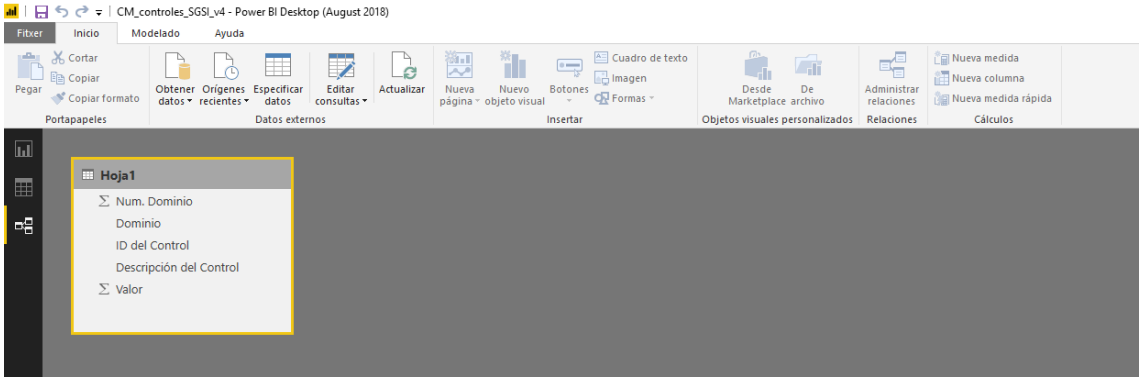


fig.9. Esquema de datos utilizados

8.1. Diseño de paneles e informes

Para la presentación de la información referente al grado de madurez de los distintos controles y dominios del SGSI utilizaremos dos vistas: GENERAL y DETALLE DOMINIO.

La primera de ellas, GENERAL, mostrará el estado general de implantación del SGSI. En concreto, en este apartado del informe presentaremos lo siguiente:

- Valor global del grado de madurez del SGSI
- Valor del grado de madurez de cada uno de los dominios
- Top5 de Mejores Dominios
- Top5 de Peores Dominios

Una vez elegidos los objetos visuales de MS Power BI que consideramos óptimos para presentar esta información, el resultado obtenido para la vista GENERAL es el siguiente:

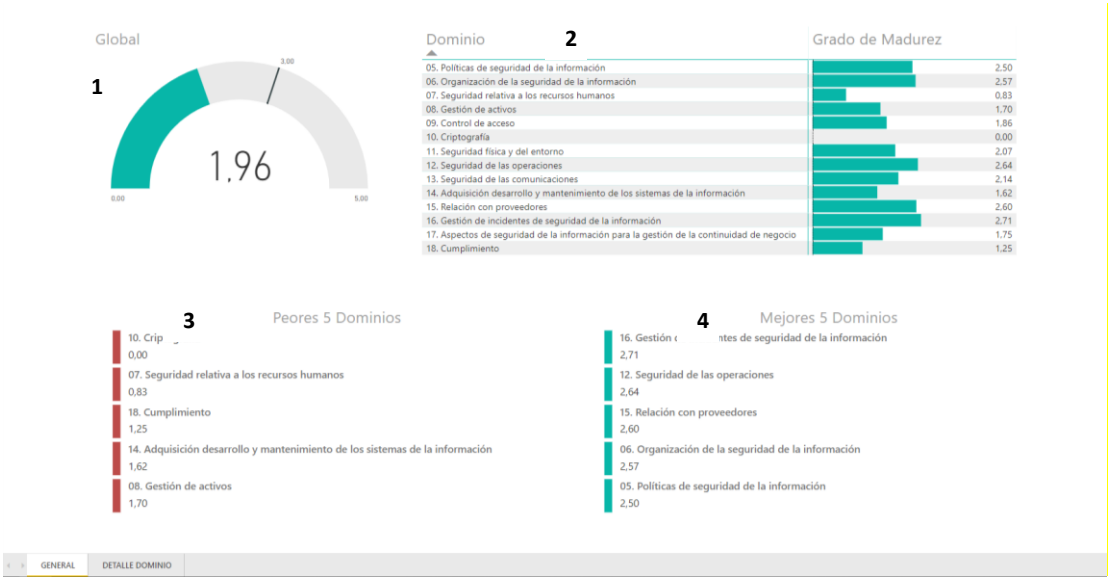


fig.10. Vista GENERAL del cuadro de mando

El elemento **1** es un diagrama medidor del grado madurez global del SGSI. Hemos representado el valor objetivo que, recordemos, habíamos fijado en *3 – Definido*.

El elemento **2** representa el listado de dominios de referencia junto con el valor promedio del grado de madurez de sus propios controles. Lo mostramos tanto en valor como en un diagrama de barras incrustado en la tabla para una mejor interpretación.

El elemento **3** es un listado de los 5 peores dominios en cuanto a desarrollo. De esta forma resaltamos los principales aspectos a mejorar en cuanto a implantación del SGSI de la compañía.

Finalmente el elemento **4** es un listado de los 5 mejores dominios en cuanto a madurez. Los valores mostrados no necesariamente tienen que ser considerados como "suficientes" (de

hecho en esta primera iteración ninguno de ellos consigue el valor objetivo prefijado) pero sí obtenemos una idea sobre los puntos en los que se ha avanzado más hasta la fecha.

Para el informe DETALLE DOMINIO, presentaremos la siguiente información:

- Descripción del dominio consultado
- Indicador general para el dominio consultado
- Lista de controles del dominio consultado y grado de madurez de cada uno de ellos

Utilizaremos la funcionalidad de MS Power BI "*Obtención de detalles*" (*Drill down* en inglés) para poder acceder a esta vista DETALLE DOMINIO desde la anterior vista GENERAL. De esta forma, los usuarios podrán navegar desde el informe principal al de detalle y viceversa, filtrando la información deseada en cada momento de forma dinámica.

Una vez elegidos los objetos visuales que consideramos más adecuados para la información que queremos mostrar, el resultado obtenido para la vista DETALLE DOMINIO es el siguiente:

fig.11. Vista DETALLE DOMINIO del cuadro de mando

El elemento **1** es un botón que permite regresar a la vista GENERAL, desde donde hemos accedido a esta vista DETALLE DOMINIO.

El elemento **2** muestra la descripción del dominio sobre el que estamos focalizando el análisis.

El elemento **3** muestra el listado exhaustivo de controles referentes al dominio seleccionado, junto con la valoración de cada uno de ellos. Se ha añadido un código de colores para resaltar el estado de los controles (0/1 rojo, 2 amarillo, 3 azul, 4/5 verde).

El elemento **4** muestra la valoración global del dominio seleccionado.

El detalle de la presentación de todos los dominios puede consultarse en el ***ANEXO D: Capturas de pantalla del CM con MS Power BI***.

9. Análisis del estado del SGSI

Aunque el objetivo de este TFM es el propio diseño del cuadro de mando visto en los apartados anteriores, utilizaremos la información que ahora este cuadro de mando proporciona de forma visual y ordenada para obtener un primer análisis del estado de implantación del SGSI en la compañía analizada. En concreto, identificaremos los controles y dominios menos desarrollados para plasmar un plan de trabajo y/o de proyectos sobre ellos.

MEJORES 5 DOMINIOS:

Los dominios más desarrollados en cuanto a despliegue de los controles de seguridad asociados son los siguientes:

- 16. Gestión de incidentes de seguridad de la información
- 12. Seguridad de las operaciones
- 15. Relación con proveedores
- 06. Organización de la seguridad de la información
- 05. Políticas de seguridad de la información

Los dominios 12 y 16, relacionados con las operaciones de seguridad y la gestión de incidentes han sido desarrollados de facto a lo largo de los últimos años aunque sin seguir una metodología específica. Los departamentos de operaciones tienen como función la respuesta a incidentes en los sistemas (también en aspectos de seguridad) y la realización de tareas específicas sobre seguridad de las TIC como operaciones sobre firewalls, administración de parches, gestión de antivirus… Por ese motivo, puestas esas funciones en perspectiva SGSI, los dominios donde podemos englobar esas tareas obtienen una mejor valoración.

En cuanto a los dominios 05 y 12, son los primeros que se han abordado en la implantación del SGSI en la compañía ya que a partir de estos, deben desarrollarse el resto de normativas y controles.

PEORES 5 DOMINIOS:

Los dominios menos desarrollados en esta primera valoración del grado de madurez del SGSI son:

- 10. Criptografía
- 07. Seguridad relativa a los recursos humanos
- 18. Cumplimiento
- 14. Adquisición, desarrollo y mantenimiento de los sistemas de información
- 08. Gestión de activos

Los controles de estos dominios no han sido abordados anteriormente en la compañía. En todo caso existen algunas iniciativas que pueden englobarse en ellos como por ejemplo, la

existencia de una CMDB incipiente que está todavía en fase de desarrollo e información interna. Por lo tanto, esos dominios deberán ser motivo de una revisión inicial con la perspectiva y ordenamiento que sugiere la metodología ISO/IEC 27000.

En base a este análisis *at-a-glance* y a la información específica por cada dominio, podemos proponer un plan de acción más detallado para tener en cuenta en la planificación del siguiente plan de proyectos anual de la compañía. Nuestra propuesta es la siguiente:

- Validación final por parte de la Alta Dirección y publicación de la Política General (DOM. 05)
- Primera reflexión entre ámbitos TIC y de Personal sobre la Seguridad relativa a RRHH y normativas relacionadas (DOM. 07 y DOM. 18)
- Evolución de CMDB y establecimiento como única base de datos corporativa (DOM. 08)
- Desarrollo del resto de cuerpo normativo (DOM. 05 y dominios específicos que se aborden)
- Revisión de los permisos de administración/acceso privilegiado a los distintos sistemas y redes (DOM. 09)
- Primera reflexión sobre el estado y necesidades de los sistemas TIC en cuanto a Criptografía (DOM. 10)
- Revisar las copias de respaldo de los sistemas y establecer procedimientos de comprobación y restauración de los mismos (DOM. 12 y DOM. 17)
- Establecer las figuras de Operación de Seguridad específicas (Security Operations Center) para la monitorización contínua de la Seguridad TIC y atención ante incidentes de Seguridad (DOM. 12 y DOM. 16)
- Primera reflexión conjunta de los departamentos TIC y jurídicos de la compañía sobre las normativas y conceptos legales de aplicación sobre los sistemas y entornos de Seguridad TIC, como el RGPD u otros conceptos de cumplimiento legal (DOM. 18)

En general, este primer plan de acción se focaliza en el desarrollo teórico de controles y dominios. Una vez se hayan desarrollado estos marcos teóricos, se podrán abordar controles más técnicos y específicos para cada uno de los dominios.

10. Puntos de mejora y próximos pasos

Este trabajo ha sido desarrollado teniendo en cuenta el estado actual de la implantación del SGSI en la compañía y siendo interrogadas las personas que se han considerado clave para cada uno de los dominios. Es posible que la información que puedan aportar otros departamentos o personas clave puede modificar el grado de madurez existente hasta la fecha. Como hemos expuesto repetidamente, el gobierno de la Seguridad TIC, así como su desarrollo, debe realizarse de forma iterativa en un ciclo de mejora contínua. Por lo tanto, un primer punto que deberá cerrarse a partir de este trabajo es la **ejecución de ese análisis periódico**.

Por otro lado, hemos desarrollado un cuadro de mando bajo una perspectiva teórica sobre la información de la que querríamos disponer. En fases posteriores **pueden aparecer nuevas necesidades de disponibilidad de información en el cuadro de mando**. La elección de MS Power BI como herramienta para el CM facilita esa evolución, ya sea añadiendo nuevos datos o mostrando los existentes de otras formas.

Finalmente, es necesario seguir haciendo hincapié en todos los estamentos, desde la alta dirección hasta los usuarios finales, de la existencia de este marco de Seguridad en las TIC, publicando el compendio de buenas prácticas, los avisos de vulnerabilidades y alertas tempranas, etc. En general, **debe difundirse para toda la compañía que la Seguridad es un elemento clave** del cual todos deben ser conocedores y partícipes como empleados y como usuarios.

11. ANEXOS

11.1. ANEXO A: Tabla de selección de controles

Dominio	ID del Control	Descripción del Control	Objetivo del Control	Descripción (a modo de pregunta)
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?
	5.1.2	Revisión de la Política de Seguridad de la Información	Comprobar que se revisan las políticas de seguridad a intervalos planificados	¿Las políticas de seguridad de la información se revisan a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia?
Organización de la seguridad de la información	6.1.1	Responsabilidades y roles de seguridad información	Definición y asignación de las funciones y responsabilidades asociadas a los sistemas IT	¿Están definidas y asignadas las principales funciones y responsabilidades asociadas a la seguridad de los sistemas de información?
	6.1.2	Segregación de funciones	Segregación de tareas dentro de la compañía	¿Se ha considerado la segregación de ciertas tareas con el objeto de reducir las posibilidades de modificaciones no autorizadas o un mal uso de los datos o servicios?
	6.1.3	Contacto con autoridades	Comprobar que se establecen contactos con autoridades	¿La compañía establece contactos con autoridades para la gestión de incidencias, gestión de continuidad y anticipación a cambios legislativos?
	6.1.4	Contacto con grupos de interés especial	Comprobar que se establecen contactos con grupos de interés especial	¿La compañía mantiene contactos con grupos de especial interés o fórums de especialistas en seguridad y asociaciones profesionales?
	6.1.5	Seguridad de la información en la gestión de proyectos	Metodología de desarrollo seguro del ciclo de vida de los proyectos	¿La compañía ha definido una metodología de desarrollo seguro en el ciclo de vida de sus proyectos?
	6.2.1	Política de dispositivo móvil	Comprobar si se contemplan los riesgos de trabajar con dispositivos móviles	¿Existe una política formal que contemple los riesgos de trabajar con dispositivos de Informática móvil?
	6.2.2	Teletrabajo	Comprobar si se autorizan y controlan las actividades de Teletrabajo	¿Todas las actividades de teletrabajo se encuentran autorizadas y controladas por la Dirección?
Seguridad relativa a los recursos humanos	7.1.1	Investigación de antecedentes	Comprobación de antecedentes no penales ni laborales por parte de la compañía antes de la contratación	¿Se realizan comprobaciones de los empleados si el puesto de trabajo implica el acceso a recursos de tratamiento de la información?
	7.1.2	Términos y condiciones de empleo	Comprobación del cumplimiento de seguridad al toda persona que desarrolle una actividad dentro de la compañía	¿Se les exige al personal, contratistas y terceros cumplimiento de RGPD confidencialidad, etc. y responsabilidades concretas de seguridad?
	7.2.1	Responsabilidades de la Dirección	Comprobar que la Dirección se encarga de hacer cumplir a las personas contratadas las políticas de seguridad	¿La Dirección es la responsable de contratar a personal, contratistas y terceras partes conocedores de las funciones y responsabilidades en materia de seguridad y motivados / concienciados para cumplir con las políticas de seguridad de la organización?
	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?

	7.2.3	Proceso Disciplinario	Formalización de procesos disciplinarios por violación de políticas de seguridad de la información	¿Se ha formalizado un procedimiento disciplinario para empleados que violen las políticas y procedimientos de seguridad de la Entidad?
	7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Comunicación por parte de la compañía durante un cambio laboral de las responsabilidades del trabajador	¿Se comunica por escrito el cese de las responsabilidades, indicando las responsabilidades legales y requerimientos de seguridad, y si aplica, responsabilidades sobre confidencialidad?
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.?
	8.1.2	Propiedad de los activos	Asignación de propietarios de activos, y comprobación de clasificación de los activos	¿El propietario se encarga de asegurar que la información y activos están clasificados y lo revisa periódicamente?
	8.1.3	Uso aceptable de los activos	Normativa de uso de activos	¿La compañía ha definido normas de uso aceptable de información y activos asociados (p. ej. Correo electrónico, Internet, móviles, etc.)?
	8.1.4	Devolución de activos	Devolución de activos después de la relación contractual	¿El fin de la relación contractual está formalizado en referente a la devolución del software, documentos y equipos que hayan sido necesarios?
	8.2.1	Clasificación de la información	Existencia de guías de clasificación	¿Existen guías de clasificación, incluyendo requerimientos de seguridad?
	8.2.2	Etiquetado de la información	Existencia de un etiquetado de información	¿Existen procedimientos para el marcado y tratamiento de la información?
	8.2.3	Manipulado de la información	Existencia de procedimientos de manipulado de información	¿Se han establecido procedimientos de utilización y almacenamiento de la información para protegerla de malos usos y revelaciones no autorizadas?
	8.3.1	Gestión de medios removibles	Existencia de procedimientos para la gestión de soportes removibles	¿Existen procedimientos para la gestión de los soportes removibles?
	8.3.2	Eliminación de medios	Protocolo de eliminación de soportes	Los soportes son eliminados de manera segura cuando no son ya necesarios y a través de procedimientos formalizados?
	8.3.3	Transporte de medios físicos/Soportes físicos en tránsito	Protocolos de transporte de soportes fuera de la compañía	¿Durante el transporte, fuera de los límites físicos de la organización, los soportes que contengan información están protegidos contra accesos no autorizados, usos indebidos o deterioro?
Control de acceso	9.1.1	Política de control de acceso	Existencia de una política de control de acceso	¿La política de control de accesos está establecida, documentada y revisada en base a los requerimientos del negocio?
	9.1.2	El acceso a las redes y a los servicios de red	Acceso a redes por partes de usuarios autorizados	¿Los usuarios sólo tienen acceso directo a los servicios para los que estén autorizados de forma específica?
	9.2.1	Registro y baja de usuarios	Existencia de procedimientos de registro de usuarios	¿Existe un procedimiento de registro de usuarios?
	9.2.2	Provisión de los accesos de usuario	Asignación de identificadores únicos a usuarios	¿Todos los usuarios disponen de un identificador único para su uso personal y exclusivo?
	9.2.3	Gestión de derechos de acceso privilegiados	Existencia de workflow de aprobación para la asignación y uso de privilegios	¿La asignación y uso de los privilegios está restringida y controlada?
	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?
	9.2.5	Revisión de los derechos de acceso de usuario	Revisión de derechos de acceso de usuarios	¿Se revisan los derechos de acceso de los usuarios en intervalos regulares?
	9.2.6	Eliminación o ajuste de los derechos de acceso	Eliminación de derechos de acceso a usuarios dados de baja	Tras la finalización de contrato, ¿los derechos de acceso son revisados y eliminados en caso de ser necesario?

	9.3.1	Uso de la información secreta de autenticación	Existencia de una guía de buenas prácticas de contraseñas	¿Existen buenas prácticas para la definición y uso de las contraseñas?
	9.4.1	Restricción de acceso a la información	Existencia de controles para restringir el acceso a la información	¿Se siguen controles aplicados para restringir el acceso a la información?
	9.4.2	Procedimientos de inicio de sesión seguro	Procedimiento seguro de inicio de sesión, desactivación tras periodo de inactividad en terminales	¿Se sigue un procedimiento seguro de inicio de sesión? ¿Se desactivan tras un periodo definido de inactividad los terminales situados en lugares de alto riesgo o que sirvan sistemas de alto riesgo?
	9.4.3	Sistema de gestión de contraseñas	Centralización de contraseñas	¿Se tienen en consideración los sistemas de gestión de contraseñas?
	9.4.4	Uso de programas utilitarios privilegiados	Control y restricción de sistemas capaces de eludir medidas de control del sistema	¿El uso de aquellas utilidades del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones se encuentra controlado y restringido?
	9.4.5	Control de acceso al código fuente de los programas	Restricción del acceso a la librería de programas fuente	¿Cuáles de las siguientes medidas se utilizan para restringir el acceso a la librería de programas fuente?
Criptografía	10.1.1	Política de uso de los controles criptográficos	Uso de controles criptográficos en el trato de información	¿Se dispone de una política que cubra el uso de controles criptográficos para la protección de la información?
	10.1.2	Gestión de claves	Protección de claves de cifrado	¿Se protegen todas las claves de cifrado contra su modificación y destrucción, y en el caso de las claves privadas, su divulgación?
Seguridad física y del entorno	11.1.1	Perímetro de seguridad física	Seguridad física en áreas con información sensible	¿Se han definido perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información?
	11.1.2	Controles físicos de entrada	Controles físicos de entrada	¿Las áreas seguras deberían están protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado?
	11.1.3	Seguridad de oficinas, despachos y recursos	Seguridad física en oficinas	¿Se han definido procedimientos de seguridad física para las oficinas, despachos y recursos? ¿Se han aplicado?
	11.1.4	Protección contra las amenazas externas y ambientales	Protección contra las amenazas externas y ambientales	¿Se han diseñado procedimientos de seguridad física contra desastres naturales, ataques provocados por el hombre o accidentes? ¿Se han implantado?
	11.1.5	Trabajo en áreas seguras	Diseño de procedimientos para el trabajo en áreas seguras	¿Se han diseñado procedimientos para trabajar en las áreas seguras? ¿Se han implantado?
	11.1.6	Áreas de carga y descarga	Control de las áreas de carga y descarga	¿Se controlan los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados?
	11.2.1	Emplazamiento y protección de equipos	Comprobación de la situación física de los equipos para evitar amenazas	¿Los equipos se han situado de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados?
	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?

	11.2.3	Seguridad del cableado	Protección del cableado contra intercepciones, interferencias o daños	¿El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información está protegido frente a interceptaciones, interferencias o daños?
	11.2.4	Mantenimiento de los equipos	Mantenimiento de los equipos	¿Los equipos reciben un mantenimiento correcto que asegure su disponibilidad y su integridad continuas?
	11.2.5	Retirada de materiales propiedad de la empresa	Retirada de materiales propiedad de la empresa	¿Es posible extraer equipos, información o software de las instalaciones sin autorización previa?
	11.2.6	Seguridad de los equipos fuera de las instalaciones	Aplicación de medidas de seguridad a equipos fuera de las instalaciones de la compañía	¿Se están aplicando medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones?
	11.2.7	Reutilización o eliminación segura de equipos	Eliminación segura de todo equipo que se desee eliminar	¿Los soportes de almacenamiento se comprueban para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos?
	11.2.8	Equipo de usuario desatendido	Existencia de guía de buenas prácticas para equipos desatendido	¿Se disponen de guías de buenas prácticas acerca de los requerimientos de seguridad y procedimientos para proteger los equipos desatendidos?
	11.2.9	Política de puesto de trabajo despejado	Política de puesto de trabajo despejado	¿Existe una política de escritorio limpio y despejado?
Seguridad de las operaciones	12.1.1	Documentación de procedimientos de las operaciones	Existencia de documentación de procedimientos de las operaciones	¿Existe documentación y mantenimiento de los procedimientos de operación identificados por la Política de Seguridad?
	12.1.2	Gestión de cambios	Existencia de procedimientos para la gestión de cambios de equipo, SW y procedimientos	Responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio en todos los cambios de equipo, SW y procedimientos
	12.1.3	Gestión de capacidades	Prevención de requisitos de capacidad, incluyendo demanda actual y proyecciones	¿Se prevén los requisitos de capacidad? Para ello hay que comprobar las demandas actuales y las proyecciones de los requerimientos futuros de capacidad.
	12.1.4	Separación de los recursos de desarrollo, prueba y operación	Separación de los distintos entornos	¿Existe una separación de los recursos para desarrollo, prueba y producción?
	12.2.1	Controles contra el código malicioso	Existencia de controles para detectar y prevenir código malicioso, así como concienciación a usuarios	¿Existen controles para detectar el software dañino y prevenirse contra él, junto a adecuados procedimientos para concienciar a los usuarios?
	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?
	12.4.1	Registro de eventos	Registro de eventos	¿Se auditan los registros obtenidos de las actividades de los usuarios, excepciones y eventos de seguridad informática para detectar eventos, ser almacenados y consultados en investigaciones?
	12.4.2	Protección de la información de registro	Protección de la información de registro	¿La información publicada está protegida para evitar modificaciones no autorizadas?
	12.4.3	Registros de administración y operación	Registros de actividad de administradores y operadores	¿Las actividades del administrador y operadores quedan registradas?
	12.4.4	Sincronización del reloj	Sincronización de reloj para todos los equipos	¿Se sincronizan los relojes de los sistemas para garantizar la exactitud de los registros de auditoría?
	12.5.1	Instalación del software en explotación	Control de instalaciones de SW en equipos corporativos	¿Se controla la instalación de SW en los Sistemas Operativos?
	12.6.1	Gestión de las vulnerabilidades técnicas	Gestión de las vulnerabilidades técnicas, modelado de amenazas	¿La compañía dispone de información sobre las vulnerabilidades que afectan a sus sistemas periódicamente para así poder evaluar las vulnerabilidades y

				tomar las medidas necesarias?
	12.6.2	Restricción en la instalación de software	Restricción en la instalación de software	¿Se han implantado mecanismos que limiten lo instalación de software no autorizado al personal de la compañía?
	12.7.1	Consideraciones sobre la auditoria de sistemas de información	Planificación sobre requisitos y actividades de auditoria que comprueban los SO para minimizar interrupciones	¿Se han considerado medidas para controlar la planificación de las tareas de verificación de los sistemas de producción con objetivo de minimizar el riesgo de interrupción de los procesos de negocio?
Seguridad de las comunicaciones	13.1.1	Controles de red	Implementación de controles para asegurar datos en las redes de equipos corporativos, protección de servicios conectados contra acceso no autorizados	¿Los gestores de redes han implantado los controles y medidas para conseguir y conservar la seguridad de los datos en las redes de ordenadores, así como la protección de los servicios conectados contra accesos no autorizados?
	13.1.2	Seguridad de los servicios de red	Identificación de todos los controles para las redes de la compañía	¿Están identificados todos los controles y niveles de seguridad para las distintas redes existentes en la organización, incluidos cualquier acuerdo de servicio de un proveedor externo?
	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?
	13.2.1	Políticas y procedimientos para la transferencia de información.	Revisión de procedimientos de transferencia de información	¿Los procedimientos están diseñados para proteger la información guardando los principios de disponibilidad, integridad y confidencialidad?
	13.2.2	Acuerdos sobre transferencia de información	Identificación y gestión de responsabilidades en procesamiento, transmisión y almacenado de la información	¿Se gestionan las responsabilidades en el procesamiento, transmisión y almacenado de la información?
	13.2.3	Mensajería electrónica	Protección de la información en los correos electrónicos	¿La información contenida en el correo electrónico está protegida adecuadamente?
	13.2.4	Acuerdos de confidencialidad o no divulgación	Utilización de acuerdos de confidencialidad	¿Se usan acuerdos de confidencialidad o no divulgación para notificar qué información es secreta o confidencial?
Adquisición desarrollo y mantenimiento de los sistemas de la información	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Comprobación de que los requerimientos de negocio para sistemas especifican requerimientos de control	¿Los requerimientos de negocio para sistemas nuevos o mejoras a sistemas existentes, ¿especifican los requerimientos de control?
	14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Comprobación de la protección de información en el comercio electrónico	¿La información contenida en el comercio electrónico está protegida?
	14.1.3	Protección de las transacciones de servicios de aplicaciones	Protección de transferencias on-line	¿La información empleada en las transacciones online está protegida para evitar transacciones incompletas, alteradas, no autorizadas o duplicadas?
	14.2.1	Política de desarrollo seguro	Existencia de procedimientos para el desarrollo seguro de aplicaciones	¿Existen procedimientos formalizados para el desarrollo seguro de aplicaciones, teniendo en cuenta controles de seguridad en cada una de las fases del desarrollo?
	14.2.2	Procedimiento de control de cambios en sistemas	Existencia de procedimientos de control de cambios	¿Existen procedimientos formalizados de control de cambios que aseguren que la seguridad y los procedimientos de control no están debilitados?
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Revisión de sistemas de aplicaciones después de cambios	¿Se revisan y prueban los sistemas de aplicaciones cuando se efectúan cambios, con el objeto de garantizar que no impactan adversamente en las operaciones o a la seguridad?

	14.2.4	Restricciones a los cambios en los paquetes de software	Revisión o modificación de paquetes SW proporcionados por proveedores	¿Se usan los paquetes de SW proporcionados por los proveedores sin modificación?
	14.2.5	Principios de ingeniería de sistemas seguros	Metodología de ingeniería de seguridad en procesos de la organización	¿Se dispone de una metodología de ingeniería de seguridad en todos los procesos de la organización (negocio, datos, aplicaciones, tecnología)?
	14.2.6	Entorno de desarrollo seguro	Entorno de desarrollo seguro	¿Se dispone de entornos de desarrollo seguros?
	14.2.7	Externalización del desarrollo de software	Externalización del desarrollo de software	¿Qué aspectos se contemplan a la hora de externalizar el desarrollo?
	14.2.8	Pruebas funcionales de seguridad de sistemas	Realización de pruebas de seguridad en sistemas durante el desarrollo	¿Se realizan pruebas de seguridad en los sistemas durante cada fase de su desarrollo y antes de su puesta en producción?
	14.2.9	Pruebas de aceptación de sistemas	Pruebas de aceptación de sistemas	¿Se han establecido criterios de aceptación para sistemas (y versiones) nuevos o mejorados, desarrollando con ellos las pruebas adecuadas antes de su aceptación?
	14.3.1	Protección de los datos de prueba	Protección de los datos de prueba	¿Se controlan y protegen los datos de prueba?
Relación con proveedores	15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Existencia de política de seguridad de la información con los proveedores	¿Se acuerdan y documentan los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización?
	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?
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Seguimiento de políticas de seguridad durante toda la cadena de suministro de tecnología	¿Se incluyen requisitos en los acuerdos con proveedores para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos?
	15.2.1	Control y revisión de la provisión de servicios del proveedor	Control y revisión de la provisión de servicios del proveedor	¿Se realizan validaciones de datos a lo largo del ciclo del proceso?
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Gestión de cambios en la provisión del servicio del proveedor	¿Se controlan los cambios hechos por la organización para implementar mejora en los servicios presentes, desarrollo de nuevas aplicaciones, modificación y actualización de políticas y procedimientos y creación de nuevos controles?
Gestión de incidentes de seguridad de la información	16.1.1	Responsabilidades y procedimientos	Establecimiento de responsabilidades y procedimientos ante incidentes de seguridad	¿Se han establecido las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información?
	16.1.2	Reporte de eventos de seguridad de la información	Existencia de procedimiento de comunicación de eventos de seguridad	¿Existe un procedimiento formal de comunicación de los eventos de seguridad de la información, respuesta ante incidentes y escalada?
	16.1.3	Reporte de las debilidades de seguridad de la información	Existencia de procedimiento formal de comunicación de debilidades de información	¿Se ha definido un procedimientos para que los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información puedan notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios?
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Evaluación y decisión sobre los eventos de seguridad de la información	¿Los eventos de seguridad de la información están siendo evaluados y se clasifican como 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?
	16.1.6	Aprendiendo de los incidentes de seguridad de la información	Instalación de mecanismos para monitorizar y cuantificar los tipos, volúmenes y costes de los incidentes de seguridad y fallos de funcionamiento	Instalación de mecanismos para monitorizar y cuantificar los tipos, volúmenes y costes de los incidentes de seguridad y fallos de funcionamiento
	16.1.7	Recolección de evidencia	Recolección de evidencia	¿Se han definido procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia? ¿Se están aplicando dichos procedimientos?
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.1.1	Planificación de la continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información	¿Se tienen en cuenta medidas de seguridad de la información y de continuidad en los procesos de negocio frente a situaciones adversas, por ejemplo, durante una crisis o desastre?
	17.1.2	Implementación de la continuidad de seguridad de la información	Implementación de la continuidad de seguridad de la información	¿La organización ha establecido, documentado, implantado y mantiene procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa?
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿La organización comprueba los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas?
	17.2.1	Disponibilidad de los recursos de procesamiento de información	Implementación de recursos de tratamiento de la información	¿Los recursos de tratamiento de la información son implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad?
Cumplimiento	18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Identificación de la legislación aplicable y los requisitos contractuales	¿Se tienen en cuenta requisitos legales en las medidas de seguridad aplicadas a los sistemas de información de la organización?
	18.1.2	Derechos de propiedad intelectual	Implementación de procedimientos para garantizar el cumplimiento de derechos de propiedad intelectual	¿Se han implantado procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados?
	18.1.3	Protección de registros	Protección de registros	¿Los registros están protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio?
	18.1.4	Privacidad y protección de los datos personales	Garantía de la protección y privacidad de datos	¿Se garantiza la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicable?
	18.1.5	Regulación de controles criptográficos	Regulación de controles criptográficos	¿Los controles criptográficos se utilizan de acuerdo con todos los contratos, leyes y regulaciones pertinentes?
	18.2.1	Revisión independiente a la seguridad de la información	Revisión independiente a la seguridad de la información	¿Se revisa de manera independiente la efectividad de la Política de Seguridad?
	18.2.2	Cumplimiento de las políticas y normas de seguridad	Cumplimiento de las políticas y normas de seguridad	¿Se realizan auditorías independientes a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad?
	18.2.3	Revisión del cumplimiento técnico	Revisión del cumplimiento técnico	¿La Dirección se asegura de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y

				cualquier otro requisito de seguridad aplicable?

11.2. ANEXO B: Tabla asignación de valores a los controles

Dominio	ID del Control	Descripción del Control	Valor	Justificación
Políticas de seguridad de la información	5.1.1	Documento de Política de Seguridad de la Información	*3*	Existe un documento de Política de Seguridad de la Información publicado y se están desarrollando las normativas y procedimientos en base a éste
	5.1.2	Revisión de la Política de Seguridad de la Información	*2*	Se efectúan alguna revisiones de la Política de Seguridad pero aún sin una periodicidad ni mecanismos oficializados
Organización de la seguridad de la información	6.1.1	Responsabilidades y roles de seguridad información	*3*	Existe una organización definida y recogida en una normativa específica, aunque todavía faltan ciertas figuras
	6.1.2	Segregación de funciones	*1*	En varios ámbitos de servicio tecnológico la autorización y ejecución de los procesos no están segregadas
	6.1.3	Contacto con autoridades	*4*	Existe un protocolo definido e implantado de contacto e intercambio de información con organismos estatales
	6.1.4	Contacto con grupos de interés especial	*2*	Ciertas personas tienen contacto con foros técnicos y de interés pero no están formalizados ni extendidos
	6.1.5	Seguridad de la información en la gestión de proyectos	*1*	En el desarrollo de algunos proyectos se añade la perspectiva de Seguridad pero de forma no generalizada ni estándar
	6.2.1	Política de dispositivo móvil	*4*	Existe una normativa de gestión del parque de dispositivos móviles y se ejecuta el control de forma centralizada
	6.2.2	Teletrabajo	*3*	Existe un procedimiento específico para el control de accesos por VPN desde casa para los empleados, aunque hay otras perspectivas que no se tienen en cuenta
Seguridad relativa a los recursos humanos	7.1.1	Investigación de antecedentes	*0*	No se efectúa la investigación de antecedentes en las incorporaciones a la plantilla
	7.1.2	Términos y condiciones de empleo	*2*	En general, los contratos de empleados y proveedores incluyen cláusulas específicas de seguridad pero no reflejan la política de seguridad
	7.2.1	Responsabilidades de la Dirección	*1*	La Dirección no exige ni realiza un seguimiento exhaustivo de la aplicación de la política de seguridad, excepto en algún caso puntual
	7.2.2	Capacitación, educación y concientización en seguridad información	*1*	Se han efectuado algunas publicaciones y notificaciones a usuarios pero no existe ni se ejecuta un plan de capacitación o información específico
	7.2.3	Proceso Disciplinario	*0*	No existe un proceso disciplinario establecido
	7.3.1	Responsabilidades en la desvinculación o cambio de empleo	*1*	Se realizan algunas acciones técnicas ante la baja o cambio de un empleado pero no siempre ni de forma procedimentada
Gestión de activos	8.1.1	Inventario de activos	*3*	Existe una CMDB definida e implantada, aunque aún se está desarrollando
	8.1.2	Propiedad de los activos	*3*	Los activos están relacionados con el propietario (responsable) del servicio en la CMDB

	8.1.3	Uso aceptable de los activos	*3*	Existe una normativa de uso aceptable aunque no se revisa su cumplimiento de forma exhaustiva
	8.1.4	Devolución de activos	*1*	No existe un procedimiento de devolución de activos aunque se realiza a nivel personal en determinados casos
	8.2.1	Clasificación de la información	*1*	Existe un esquema de clasificación de la información incipiente
	8.2.2	Etiquetado de la información	*3*	Existe un procedimiento de etiquetado de la información publicado, aunque todavía en una fase temprana de ejecución
	8.2.3	Manipulado de la información	*0*	No existe un procedimiento de manipulación de la información
	8.3.1	Gestión de medios removibles	*1*	Existen algunos mecanismos de desecho de medios pero no está alineado con el esquema de clasificación de la información
	8.3.2	Eliminación de medios	*2*	Existe un mecanismo de eliminación de equipos (servidores) no formalizado
	8.3.3	Transporte de medios físicos/Soportes físicos en tránsito	*0*	No existe un mecanismo referente a este punto
Control de acceso	9.1.1	Política de control de acceso	*3*	Existen políticas de control de acceso y están alineadas con el nivel de riesgo asociado a la información accedida pero no se registran los accesos ni se revisan periódicamente
	9.1.2	El acceso a las redes y a los servicios de red	*4*	Existe una política de control de acceso a la red y a los servicios en red que incluye un procedimiento de autorización y se monitoriza el uso de los servicios de red
	9.2.1	Registro y baja de usuarios	*2*	Existe un mecanismo de registro y baja pero no está documentado
	9.2.2	Provisión de los accesos de usuario	*2*	Se gestiona la provisión de accesos pero la normativa está todavía en desarrollo
	9.2.3	Gestión de derechos de acceso privilegiados	*1*	Existen ciertos mecanismos técnicos no documentados de acceso privilegiado pero no se monitoriza el uso de estos usuarios
	9.2.4	Gestión de información secreta de autenticación de usuarios	*1*	No hay una gestión de la información secreta, aunque existen plataformas que lo ejecutan *per se*
	9.2.5	Revisión de los derechos de acceso de usuario	*1*	No se revisan de forma habitual los derechos de acceso de los usuarios
	9.2.6	Eliminación o ajuste de los derechos de acceso	*1*	No se revisan de forma habitual los derechos de acceso de los usuarios
	9.3.1	Uso de la información secreta de autenticación	*1*	No hay una gestión de la información secreta, aunque existen plataformas que lo ejecutan *per se*
	9.4.1	Restricción de acceso a la información	*1*	Alguna plataforma controla el acceso a la información pero no se realiza de forma homogénea y controlada
	9.4.2	Procedimientos de inicio de sesión seguro	*3*	Existen protocolos definidos e implantados de inicio de sesión en los equipos corporativos
	9.4.3	Sistema de gestión de contraseñas	*3*	Existe un sistema de gestión y recuperación de contraseñas definido y compartido con los usuarios finales

	9.4.4	Uso de programas utilitarios privilegiados	*2*	El uso de las herramientas de administración está restringido pero no existe un procedimiento de autorización de administradores
	9.4.5	Control de acceso al código fuente de los programas	*1*	No existe una política de control de acceso al código fuente pero los desarrolladores ejecutan ciertos mecanismos
Criptografía	10.1.1	Política de uso de los controles criptográficos	*0*	No existe una política sobre el uso de controles criptográficos
	10.1.2	Gestión de claves	*0*	No existe una política de gestión de claves criptográficas
Seguridad física y del entorno	11.1.1	Perímetro de seguridad física	*2*	Los sistemas de información se encuentran en el CPD corporativo, pero no existe una normativa específica
	11.1.2	Controles físicos de entrada	*2*	Las salas técnicas cuentan con sistemas de control de acceso aunque no existe una normativa específica
	11.1.3	Seguridad de oficinas, despachos y recursos	*1*	Aunque hay algunas salas de operación con restricciones de acceso, muchas ubicaciones no cuentan con ningún mecanismo
	11.1.4	Protección contra las amenazas externas y ambientales	*2*	La ubicación de CPD tiene en cuenta ciertos criterios ambientales, aunque no hay una documentación específica
	11.1.5	Trabajo en áreas seguras	*1*	No existe un control establecido de trabajo en áreas seguras, aunque se suele informar a los gestores de las áreas
	11.1.6	Áreas de carga y descarga	*0*	No existe ninguna iniciativa referente a este campo
	11.2.1	Emplazamiento y protección de equipos	*4*	Existe una política de emplazamiento y protección de equipos y existen controles que impiden los accesos no autorizados a las zonas de trabajo pero no se consideran los riesgos físicos y medio ambientales de las ubicaciones
	11.2.2	Instalaciones de suministro	*4*	Se protegen los equipos de posibles fallos de suministros de consumo, existen controles que detectan funcionamientos incorrectos y existen diversas fuentes alternativas de suministro que se prueban periódicamente
	11.2.3	Seguridad del cableado	*4*	Se protegen los sistemas de cableado de electricidad/telecomunicaciones, se controla el acceso a las salas de cables y existen blindajes electromagnéticos para proteger los cables
	11.2.4	Mantenimiento de los equipos	*4*	Se realiza un mantenimiento de los equipos que está alineado con las indicaciones y especificaciones del proveedor y existe un listado del personal autorizado para realizar el mantenimiento de los equipos
	11.2.5	Retirada de materiales propiedad de la empresa	*1*	No existe un procedimiento de control de salida de activos fuera de las dependencias de la organización aunque se tiene en cuenta en algunos casos
	11.2.6	Seguridad de los equipos fuera de las instalaciones	*1*	No existe un procedimiento de control de salida de activos fuera de las dependencias de la organización
	11.2.7	Reutilización o eliminación segura de equipos	*1*	No existe un procedimiento de reutilización/retirada de dispositivos de almacenamiento y se deja a cada usuario

	11.2.8	Equipo de usuario desatendido	*2*	Existen medidas de regulación de los equipos desatendidos pero no se realiza una concienciación periódica al respecto
	11.2.9	Política de puesto de trabajo despejado	*2*	Existen medidas de seguridad que regulan el puesto de trabajo despejado y el bloqueo de pantalla pero no se realiza una concienciación periódica al respecto
Seguridad de las operaciones	12.1.1	Documentación de procedimientos de las operaciones	*3*	Existen procedimientos de operación documentados y están disponibles para los usuarios que los necesitan pero no cubren todos los sistemas
	12.1.2	Gestión de cambios	*4*	Existe una política de gestión de cambios, está implantada y gestionada por un Gestor de Cambios y el CAB
	12.1.3	Gestión de capacidades	*4*	Se identifican requisitos de capacidad de los sistemas y se realiza una monitorización de la situación
	12.1.4	Separación de los recursos de desarrollo, prueba y operación	*2*	Sólo en algunos entornos se cuenta con infraestructura y recursos de desarrollo y/o prueba
	12.2.1	Controles contra el código malicioso	*4*	Existen controles contra código malicioso, existe una política que prohíbe el uso no autorizado de software, existen controles de prevención/detección de uso de código no autorizado
	12.3.1	Copias de seguridad de la información	*3*	Existe una política de backup de los sistemas pero no se realizan pruebas de recuperación periódicamente
	12.4.1	Registro de eventos	*3*	Existe un registro de eventos de seguridad en distintas herramientas pero sólo se revisan puntualmente
	12.4.2	Protección de la información de registro	*1*	Existen controles de protección sobre los registros de información pero no se registran los accesos a los registros creados
	12.4.3	Registros de administración y operación	*1*	Existen ciertos registros de actividad de administradores/operadores del sistema pero no existe un procedimiento de autorización para activar/desactivar los registros
	12.4.4	Sincronización del reloj	*3*	Existe un sistema de cronometría que sincroniza la mayoría de los sistemas (aunque no todos)
	12.5.1	Instalación del software en explotación	*4*	Los desarrolladores tienen control de versiones y capacidad de roll-back, aunque no está alineado con el resto de los procesos de gestión tecnológica
	12.6.1	Gestión de las vulnerabilidades técnicas	*2*	Se ejecutan análisis de distintos entornos en busca de vulnerabilidades técnicas (algunos de forma continua) pero sin un protocolo de actuación establecido
	12.6.2	Restricción en la instalación de software	*2*	Existen mecanismos de restricción de instalación de software pero no se controla su aplicación
	12.7.1	Consideraciones sobre la auditoria de sistemas de información	*1*	Se están implantando los primeros controles de auditoría de seguridad TIC
Seguridad de las comunicaciones	13.1.1	Controles de red	*4*	Existe un procedimiento de gestión de redes, están implantados controles especiales para controlar los datos que son transmitidos por las redes y se monitoriza la red
	13.1.2	Seguridad de los servicios de red	*2*	Existen mecanismos de seguridad implantados para los servicios en red pero no se han definido los niveles de servicio necesarios para ellos

	13.1.3	Segregación en redes	*3*	Existe segregación de redes y está documentado el criterio de segregación pero no existe un tratamiento especial para las redes inalámbricas ni se controlan los usuarios conectados a ellas
	13.2.1	Políticas y procedimientos para la transferencia de información.	*2*	No existe una política de intercambio de información aunque existen algunos mecanismos establecidos (FTP, entornos colaborativos…)
	13.2.2	Acuerdos sobre transferencia de información	*1*	Existen algunos mecanismos incipientes de control de la información enviada a terceros
	13.2.3	Mensajería electrónica	*2*	Existen mecanismos de protección de comunicaciones electrónicas (antispam, control de enlaces, etc.) sin una política establecida
	13.2.4	Acuerdos de confidencialidad o no divulgación	*1*	En algunos contratos con terceros se incluyen acuerdos de confidencialidad pero no se identifica la información sensible ni está procedimentado
Adquisición desarrollo y mantenimiento de los sistemas de la información	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	*1*	Sólo en algunos proyectos se consideran los requisitos de seguridad para nuevos/actualizados sistemas de información
	14.1.2	Asegurar los servicios de aplicaciones en redes públicas	*4*	Se consideran los requisitos de seguridad en servicios de aplicaciones que pasan por redes públicas, los requisitos para proteger información confidencial y se registra la actividad
	14.1.3	Protección de las transacciones de servicios de aplicaciones	*2*	Existen controles de protección de las transacciones en red pero no se utilizan firmas electrónicas en el proceso
	14.2.1	Política de desarrollo seguro	*1*	No existen mecanismos homogéneos de desarrollo seguro aunque los desarrolladores lo tienen en cuenta de forma individual
	14.2.2	Procedimiento de control de cambios en sistemas	*2*	Existe un control de cambios en desarrollos software pero alejado del resto de la Gestión de Cambios
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	*1*	Las pruebas posteriores a los cambios se ejecutan según el propio criterio del técnico implantador del cambio
	14.2.4	Restricciones a los cambios en los paquetes de software	*1*	En función del sistema se utiliza un criterio más o menos restrictivo en cuanto a cambios en los paquetes de software
	14.2.5	Principios de ingeniería de sistemas seguros	*1*	No existen principios comunes de ingeniería de sistemas seguros, sino que cada desarrollador utiliza su criterio
	14.2.6	Entorno de desarrollo seguro	*2*	Existe un entorno de desarrollo seguro pero no está documentado
	14.2.7	Externalización del desarrollo de software	*3*	Se controla la externalización de desarrollo software y se crean contratos de licencia, propiedad del código y derechos de la propiedad intelectual
	14.2.8	Pruebas funcionales de seguridad de sistemas	*1*	Sólo en algunos casos se efectúan pruebas de los controles de seguridad aplicados
	14.2.9	Pruebas de aceptación de sistemas	*2*	En general, existe un plan de aceptación específico para cada entorno, pero sin una política común y homogénea
	14.3.1	Protección de los datos de prueba	*0*	No existe un procedimiento de selección de datos de prueba
Relación con proveedores	15.1.1	Política de seguridad de la información en las relaciones con los proveedores	*2*	Se documentan los requisitos de seguridad para proveedores pero no existe un procedimiento de gestión de

				relaciones con proveedores
	15.1.2	Requisitos de seguridad en contratos con terceros	*2*	Se consideran los requisitos de seguridad en los contratos con proveedores pero no se especifican las obligaciones respecto a controles de seguridad
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	*2*	Se consideran los requisitos de seguridad para las cadenas de suministro en los contratos con proveedores pero no se especifican respecto a controles de seguridad
	15.2.1	Control y revisión de la provisión de servicios del proveedor	*4*	Se monitorizan los servicios prestados por proveedores, se define a un responsable para cada uno de los servicios prestados y se revisa el servicio prestado periódicamente
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	*3*	Se consideran los cambios en los contratos con proveedores pero no se consideran los cambios de controles para mejorar la seguridad
Gestión de incidentes de seguridad de la información	16.1.1	Responsabilidades y procedimientos	*3*	Existe un procedimiento de gestión de incidentes y se identifica a los responsables
	16.1.2	Reporte de eventos de seguridad de la información	*3*	Existe un procedimiento de gestión de eventos de seguridad y se ha implantado inicialmente
	16.1.3	Reporte de las debilidades de seguridad de la información	*2*	Se analizan y reportan puntualmente debilidades en distintos sistemas y redes pero no existe un procedimiento establecido
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	*3*	Se analizan los eventos de seguridad detectados y existen algunos procedimientos de tratamiento de ciertos eventos
	16.1.5	Respuesta ante incidentes de seguridad de la información	*4*	Existe una normativa de respuesta ante incidentes y éstos son clasificados y analizados de forma específica en base a procedimientos
	16.1.6	Aprendiendo de los incidentes de seguridad de la información	*3*	Se documentan los incidentes en una base de datos de conocimiento para su posterior consulta
	16.1.7	Recolección de evidencia	*1*	Sólo en casos muy específicos se recogen y custodian las evidencias de los incidentes
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.1.1	Planificación de la continuidad de la seguridad de la información	*1*	Los planes de continuidad de negocio se circunscriben al ámbito tecnológico pero no existe una reflexión a alto nivel
	17.1.2	Implementación de la continuidad de seguridad de la información	*2*	Para algunos servicios tecnológicos se cuenta con un plan de continuidad (centro de gestión alternativo)
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*1*	No se comprueba el estado de los planes de continuidad de forma generalizada, más allá de iniciativas puntuales
	17.2.1	Disponibilidad de los recursos de procesamiento de información	*3*	Los sistemas se diseñan e implementan siempre con criterios de redundancia mínima para maximizar su disponibilidad
Cumplimiento	18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	*1*	La información referente a legislación aplicable no es conocida más allá de los departamentos jurídicos

	18.1.2	Derechos de propiedad intelectual	*0*	No se aplican criterios de propiedad intelectual
	18.1.3	Protección de registros	*2*	Existen diferentes mecanismos de protección de registros (bases de datos securizadas, mecanismos de backup, etc.) pero no existe una normativa específica
	18.1.4	Privacidad y protección de los datos personales	*3*	Existen mecanismos para garantizar la privacidad y protección de datos personales y se cuenta con una política específica a tal efecto
	18.1.5	Regulación de controles criptográficos	*0*	No existe una política de regulación de controles criptográficos
	18.2.1	Revisión independiente a la seguridad de la información	*1*	Se realizan revisiones internas referentes a la seguridad de la información
	18.2.2	Cumplimiento de las políticas y normas de seguridad	*1*	Sólo puntualmente se revisa el cumplimiento de las políticas y normas de seguridad
	18.2.3	Revisión del cumplimiento técnico	*2*	Los sistemas y servicios TIC son controlados bajo perspectivas de disponibilidad y gestión pero habitualmente sin tener en cuenta la dimensión de la seguridad de la información

11.3. ANEXO C: Tabla valoración controles SGSI (carga 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 información	6.2.2	Teletrabajo	3
7	07. Seguridad relativa a los recursos humanos	7.1.1	Investigación de antecedentes	0
7	07. Seguridad relativa a los recursos humanos	7.1.2	Términos y condiciones de empleo	2
7	07. Seguridad relativa a los recursos humanos	7.2.1	Responsabilidades de la Dirección	1
7	07. Seguridad relativa a los recursos humanos	7.2.2	Capacitación, educación y concientización en seguridad información	1
7	07. Seguridad relativa a los recursos humanos	7.2.3	Proceso Disciplinario	0
7	07. Seguridad relativa a los recursos humanos	7.3.1	Responsabilidades en la desvinculación o cambio de empleo	1
8	08. Gestión de activos	8.1.1	Inventario de activos	3
8	08. Gestión de activos	8.1.2	Propiedad de los activos	3
8	08. Gestión de activos	8.1.3	Uso aceptable de los activos	3
8	08. Gestión de activos	8.1.4	Devolución de activos	1
8	08. Gestión de activos	8.2.1	Clasificación de la información	1
8	08. Gestión de activos	8.2.2	Etiquetado de la información	3
8	08. Gestión de activos	8.2.3	Manipulado de la información	0
8	08. Gestión de activos	8.3.1	Gestión de medios removibles	1
8	08. Gestión de activos	8.3.2	Eliminación de medios	2
8	08. Gestión de activos	8.3.3	Transporte de medios físicos/Soportes físicos en tránsito	0
9	09. Control de acceso	9.1.1	Política de control de acceso	3
9	09. Control de acceso	9.1.2	El acceso a las redes y a los servicios de red	4
9	09. Control de acceso	9.2.1	Registro y baja de usuarios	2
9	09. Control de acceso	9.2.2	Provisión de los accesos de usuario	2
9	09. Control de acceso	9.2.3	Gestión de derechos de acceso privilegiados	1
9	09. Control de acceso	9.2.4	Gestión de información secreta de autenticación de usuarios	1

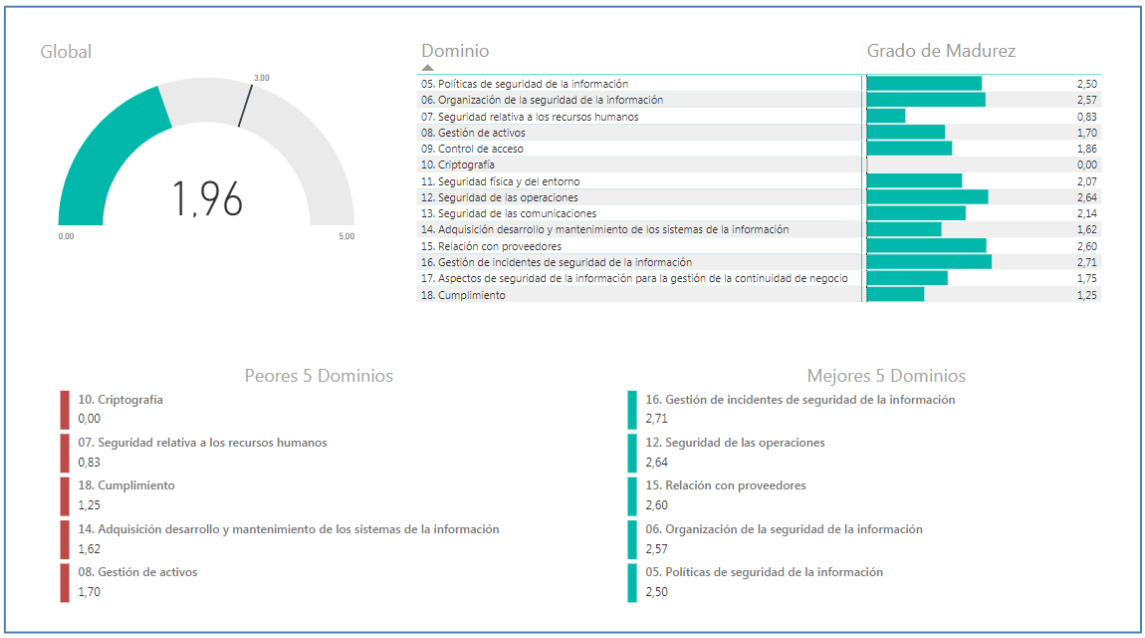
9	09. Control de acceso	9.2.5	Revisión de los derechos de acceso de usuario	1
9	09. Control de acceso	9.2.6	Eliminación o ajuste de los derechos de acceso	1
9	09. Control de acceso	9.3.1	Uso de la información secreta de autenticación	1
9	09. Control de acceso	9.4.1	Restricción de acceso a la información	1
9	09. Control de acceso	9.4.2	Procedimientos de inicio de sesión seguro	3
9	09. Control de acceso	9.4.3	Sistema de gestión de contraseñas	3
9	09. Control de acceso	9.4.4	Uso de programas utilitarios privilegiados	2
9	09. Control de acceso	9.4.5	Control de acceso al código fuente de los programas	1
10	10. Criptografía	10.1.1	Política de uso de los controles criptográficos	0
10	10. Criptografía	10.1.2	Gestión de claves	0
11	11. Seguridad física y del entorno	11.1.1	Perímetro de seguridad física	2
11	11. Seguridad física y del entorno	11.1.2	Controles físicos de entrada	2
11	11. Seguridad física y del entorno	11.1.3	Seguridad de oficinas, despachos y recursos	1
11	11. Seguridad física y del entorno	11.1.4	Protección contra las amenazas externas y ambientales	2
11	11. Seguridad física y del entorno	11.1.5	Trabajo en áreas seguras	1
11	11. Seguridad física y del entorno	11.1.6	Áreas de carga y descarga	0
11	11. Seguridad física y del entorno	11.2.1	Emplazamiento y protección de equipos	4
11	11. Seguridad física y del entorno	11.2.2	Instalaciones de suministro	4
11	11. Seguridad física y del entorno	11.2.3	Seguridad del cableado	4
11	11. Seguridad física y del entorno	11.2.4	Mantenimiento de los equipos	4
11	11. Seguridad física y del entorno	11.2.5	Retirada de materiales propiedad de la empresa	1
11	11. Seguridad física y del entorno	11.2.6	Seguridad de los equipos fuera de las instalaciones	1
11	11. Seguridad física y del entorno	11.2.7	Reutilización o eliminación segura de equipos	1
11	11. Seguridad física y del entorno	11.2.8	Equipo de usuario desatendido	2
11	11. Seguridad física y del entorno	11.2.9	Política de puesto de trabajo despejado	2
12	12. Seguridad de las operaciones	12.1.1	Documentación de procedimientos de las operaciones	3
12	12. Seguridad de las operaciones	12.1.2	Gestión de cambios	4
12	12. Seguridad de las operaciones	12.1.3	Gestión de capacidades	4
12	12. Seguridad de las operaciones	12.1.4	Separación de los recursos de desarrollo, prueba y operación	2
12	12. Seguridad de las operaciones	12.2.1	Controles contra el código malicioso	4
12	12. Seguridad de las operaciones	12.3.1	Copias de seguridad de la información	3
12	12. Seguridad de las operaciones	12.4.1	Registro de eventos	3
12	12. Seguridad de las operaciones	12.4.2	Protección de la información de registro	1
12	12. Seguridad de las operaciones	12.4.3	Registros de administración y operación	1

12	12. Seguridad de las operaciones	12.4.4	Sincronización del reloj	3
12	12. Seguridad de las operaciones	12.5.1	Instalación del software en explotación	4
12	12. Seguridad de las operaciones	12.6.1	Gestión de las vulnerabilidades técnicas	2
12	12. Seguridad de las operaciones	12.6.2	Restricción en la instalación de software	2
12	12. Seguridad de las operaciones	12.7.1	Consideraciones sobre la auditoria de sistemas de información	1
13	13. Seguridad de las comunicaciones	13.1.1	Controles de red	4
13	13. Seguridad de las comunicaciones	13.1.2	Seguridad de los servicios de red	2
13	13. Seguridad de las comunicaciones	13.1.3	Segregación en redes	3
13	13. Seguridad de las comunicaciones	13.2.1	Políticas y procedimientos para la transferencia de información.	2
13	13. Seguridad de las comunicaciones	13.2.2	Acuerdos sobre transferencia de información	1
13	13. Seguridad de las comunicaciones	13.2.3	Mensajería electrónica	2
13	13. Seguridad de las comunicaciones	13.2.4	Acuerdos de confidencialidad o no divulgación	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.1.2	Asegurar los servicios de aplicaciones en redes públicas	4
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.1.3	Protección de las transacciones de servicios de aplicaciones	2
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.1	Política de desarrollo seguro	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.2	Procedimiento de control de cambios en sistemas	2
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.4	Restricciones a los cambios en los paquetes de software	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.5	Principios de ingeniería de sistemas seguros	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.6	Entorno de desarrollo seguro	2
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.7	Externalización del desarrollo de software	3
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.8	Pruebas funcionales de seguridad de sistemas	1
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.2.9	Pruebas de aceptación de sistemas	2
14	14. Adquisición desarrollo y mantenimiento de los sistemas de la información	14.3.1	Protección de los datos de prueba	0
15	15. Relación con proveedores	15.1.1	Política de seguridad de la información en las relaciones con los proveedores	2
15	15. Relación con proveedores	15.1.2	Requisitos de seguridad en contratos con terceros	2
15	15. Relación con proveedores	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	2
15	15. Relación con proveedores	15.2.1	Control y revisión de la provisión de servicios del proveedor	4

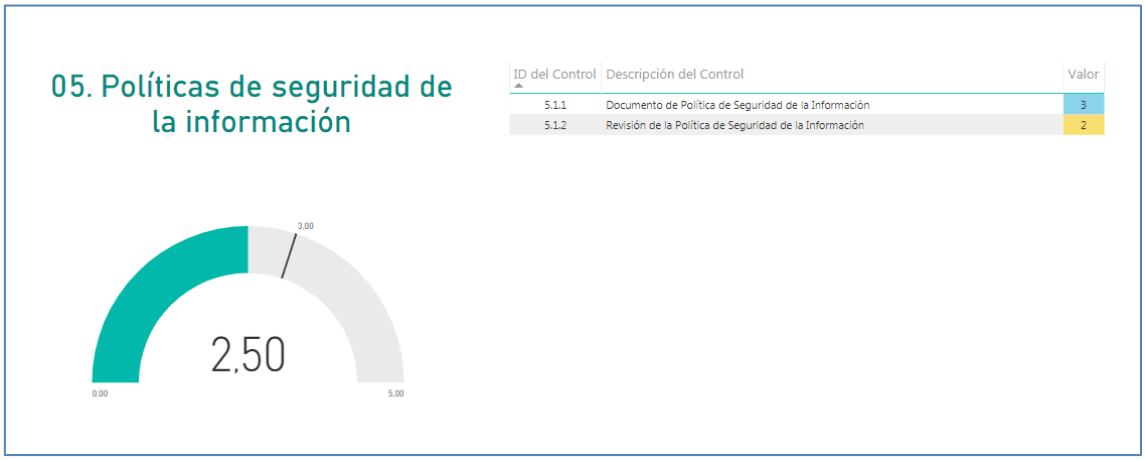
15	15. Relación con proveedores	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	3
16	16. Gestión de incidentes de seguridad de la información	16.1.1	Responsabilidades y procedimientos	3
16	16. Gestión de incidentes de seguridad de la información	16.1.2	Reporte de eventos de seguridad de la información	3
16	16. Gestión de incidentes de seguridad de la información	16.1.3	Reporte de las debilidades de seguridad de la información	2
16	16. Gestión de incidentes de seguridad de la información	16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	3
16	16. Gestión de incidentes de seguridad de la información	16.1.5	Respuesta ante incidentes de seguridad de la información	4
16	16. Gestión de incidentes de seguridad de la información	16.1.6	Aprendiendo de los incidentes de seguridad de la información	3
16	16. Gestión de incidentes de seguridad de la información	16.1.7	Recolección de evidencia	1
17	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.1.1	Planificación de la continuidad de la seguridad de la información	1
17	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.1.2	Implementación de la continuidad de seguridad de la información	2
17	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1
17	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	17.2.1	Disponibilidad de los recursos de procesamiento de información	3
18	18. Cumplimiento	18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	1
18	18. Cumplimiento	18.1.2	Derechos de propiedad intelectual	0
18	18. Cumplimiento	18.1.3	Protección de registros	2
18	18. Cumplimiento	18.1.4	Privacidad y protección de los datos personales	3
18	18. Cumplimiento	18.1.5	Regulación de controles criptográficos	0
18	18. Cumplimiento	18.2.1	Revisión independiente a la seguridad de la información	1
18	18. Cumplimiento	18.2.2	Cumplimiento de las políticas y normas de seguridad	1
18	18. Cumplimiento	18.2.3	Revisión del cumplimiento técnico	2

11.4. ANEXO D: Capturas de pantalla del CM con MS Power BI

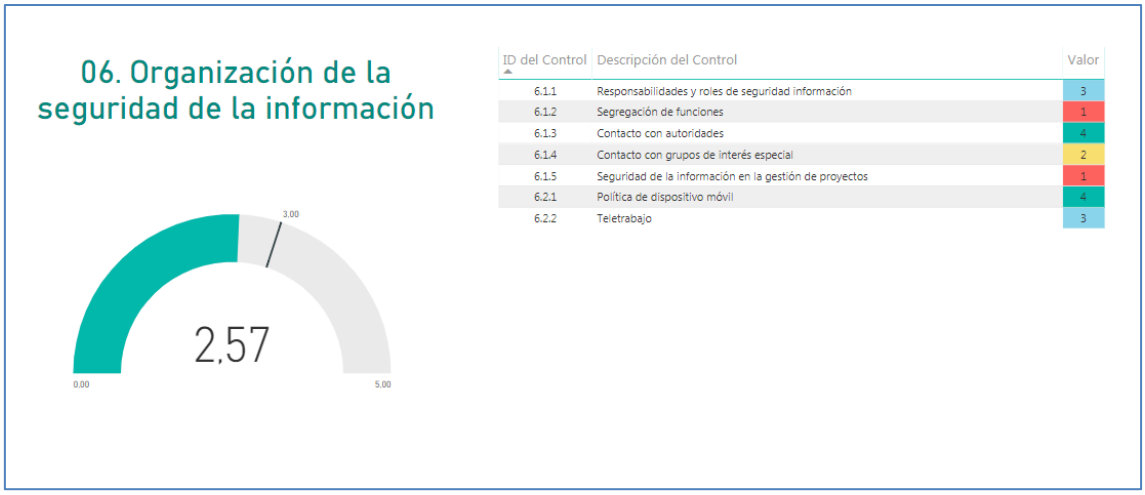
Captura 1: Estado Global del SGSI



Captura 2: Detalle Dominio 05. Políticas de seguridad de la información

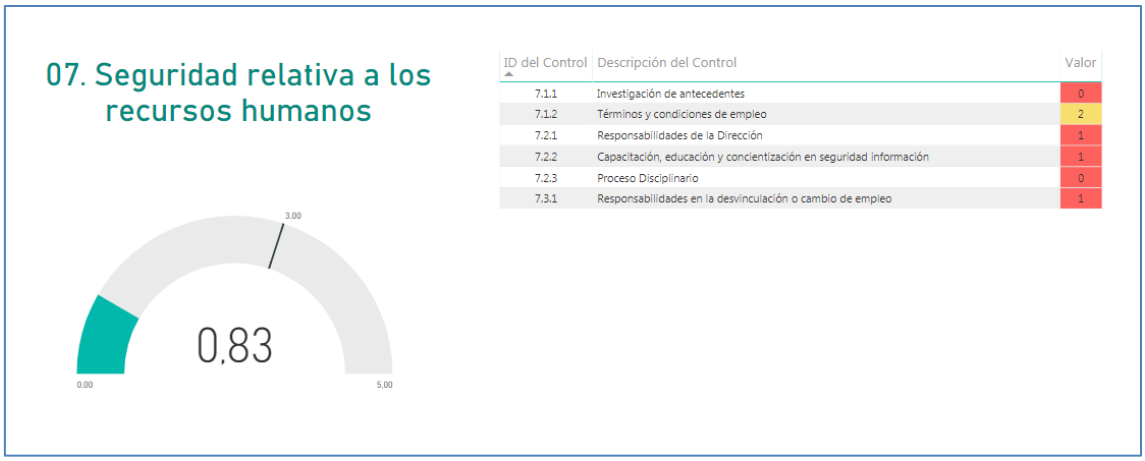


Captura 3: Detalle Dominio 06. Organización de la seguridad de la información



ID del Control	Descripción del Control	Valor
6.1.1	Responsabilidades y roles de seguridad información	3
6.1.2	Segregación de funciones	1
6.1.3	Contacto con autoridades	4
6.1.4	Contacto con grupos de interés especial	2
6.1.5	Seguridad de la información en la gestión de proyectos	1
6.2.1	Política de dispositivo móvil	4
6.2.2	Teletrabajo	3

Captura 4: Detalle Dominio 07. Seguridad relativa a los recursos humanos

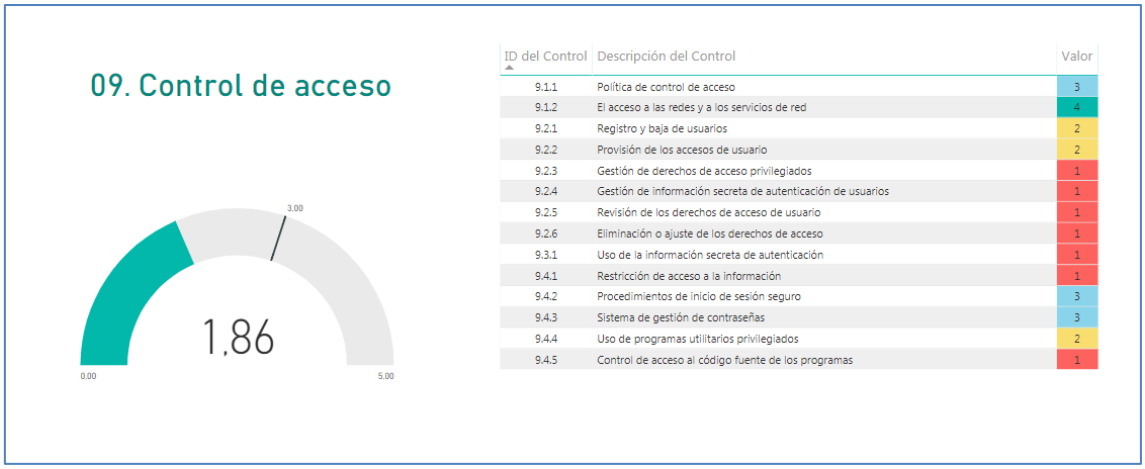


ID del Control	Descripción del Control	Valor
7.1.1	Investigación de antecedentes	0
7.1.2	Términos y condiciones de empleo	2
7.2.1	Responsabilidades de la Dirección	1
7.2.2	Capacitación, educación y concientización en seguridad información	1
7.2.3	Proceso Disciplinario	0
7.3.1	Responsabilidades en la desvinculación o cambio de empleo	1

Captura 5: Detalle Dominio 08. Gestión de activos

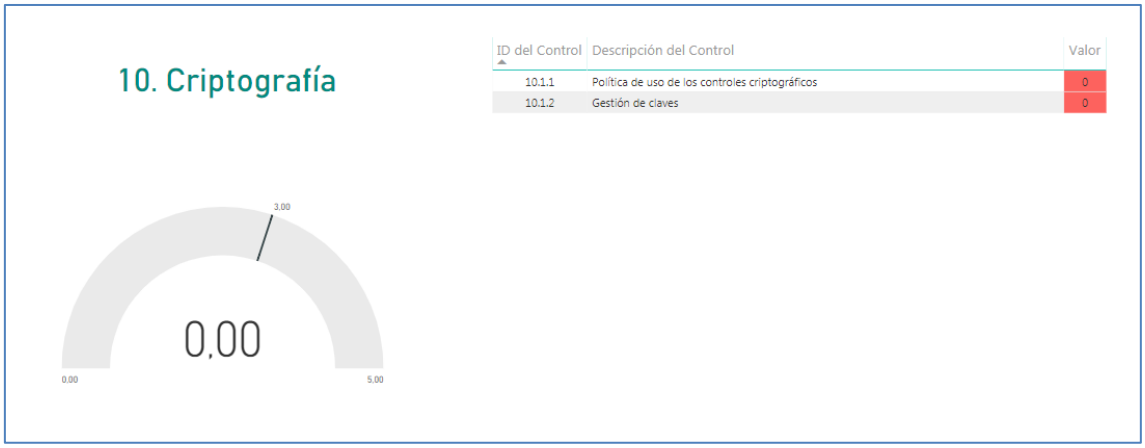
ID del Control	Descripción del Control	Valor
8.1.1	Inventario de activos	3
8.1.2	Propiedad de los activos	3
8.1.3	Uso aceptable de los activos	3
8.1.4	Devolución de activos	1
8.2.1	Clasificación de la información	1
8.2.2	Etiquetado de la información	3
8.2.3	Manipulado de la información	0
8.3.1	Gestión de medios removibles	1
8.3.2	Eliminación de medios	2
8.3.3	Transporte de medios físicos/Soportes físicos en tránsito	0

Captura 6: Detalle Dominio 09. Control de acceso



ID del Control	Descripción del Control	Valor
9.1.1	Política de control de acceso	3
9.1.2	El acceso a las redes y a los servicios de red	4
9.2.1	Registro y baja de usuarios	2
9.2.2	Provisión de los accesos de usuario	2
9.2.3	Gestión de derechos de acceso privilegiados	1
9.2.4	Gestión de información secreta de autenticación de usuarios	1
9.2.5	Revisión de los derechos de acceso de usuario	1
9.2.6	Eliminación o ajuste de los derechos de acceso	1
9.3.1	Uso de la información secreta de autenticación	1
9.4.1	Restricción de acceso a la información	1
9.4.2	Procedimientos de inicio de sesión seguro	3
9.4.3	Sistema de gestión de contraseñas	3
9.4.4	Uso de programas utilitarios privilegiados	2
9.4.5	Control de acceso al código fuente de los programas	1

Captura 7: Detalle Dominio 10. Criptografía



ID del Control	Descripción del Control	Valor
10.1.1	Política de uso de los controles criptográficos	0
10.1.2	Gestión de claves	0

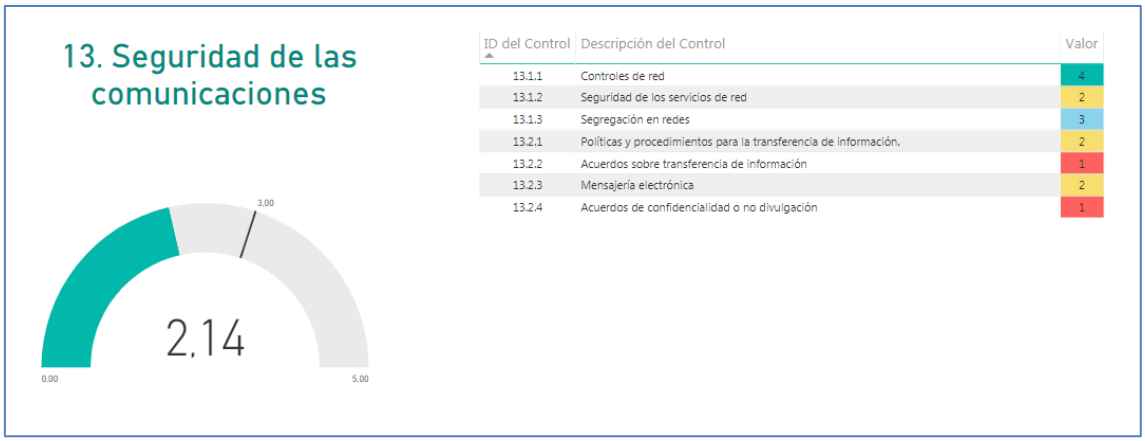
Captura 8: Detalle Dominio 11. Seguridad física y del entorno

ID del Control	Descripción del Control	Valor
11.1.1	Perímetro de seguridad física	2
11.1.2	Controles físicos de entrada	2
11.1.3	Seguridad de oficinas, despachos y recursos	1
11.1.4	Protección contra las amenazas externas y ambientales	2
11.1.5	Trabajo en áreas seguras	1
11.1.6	Áreas de carga y descarga	0
11.2.1	Emplazamiento y protección de equipos	4
11.2.2	Instalaciones de suministro	4
11.2.3	Seguridad del cableado	4
11.2.4	Mantenimiento de los equipos	4
11.2.5	Retirada de materiales propiedad de la empresa	1
11.2.6	Seguridad de los equipos fuera de las instalaciones	1
11.2.7	Reutilización o eliminación segura de equipos	1
11.2.8	Equipo de usuario desatendido	2
11.2.9	Política de puesto de trabajo despejado	2

Captura 9: Detalle Dominio 12. Seguridad de las operaciones

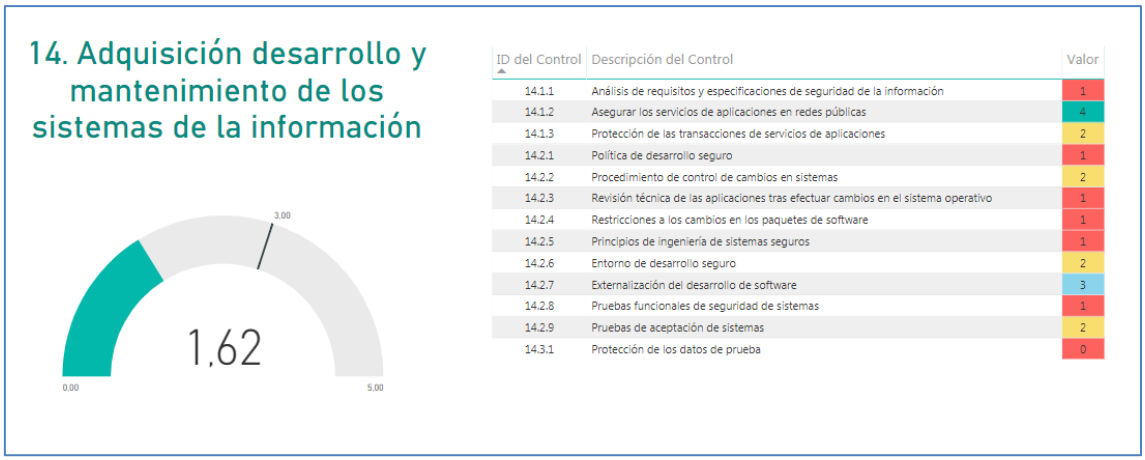
ID del Control	Descripción del Control	Valor
12.1.1	Documentación de procedimientos de las operaciones	3
12.1.2	Gestión de cambios	4
12.1.3	Gestión de capacidades	4
12.1.4	Separación de los recursos de desarrollo, prueba y operación	2
12.2.1	Controles contra el código malicioso	4
12.3.1	Copias de seguridad de la información	3
12.4.1	Registro de eventos	3
12.4.2	Protección de la información de registro	1
12.4.3	Registros de administración y operación	1
12.4.4	Sincronización del reloj	3
12.5.1	Instalación del software en explotación	4
12.6.1	Gestión de las vulnerabilidades técnicas	2
12.6.2	Restricción en la instalación de software	2
12.7.1	Consideraciones sobre la auditoria de sistemas de información	1

Captura 10: Detalle Dominio 13. Seguridad de las comunicaciones



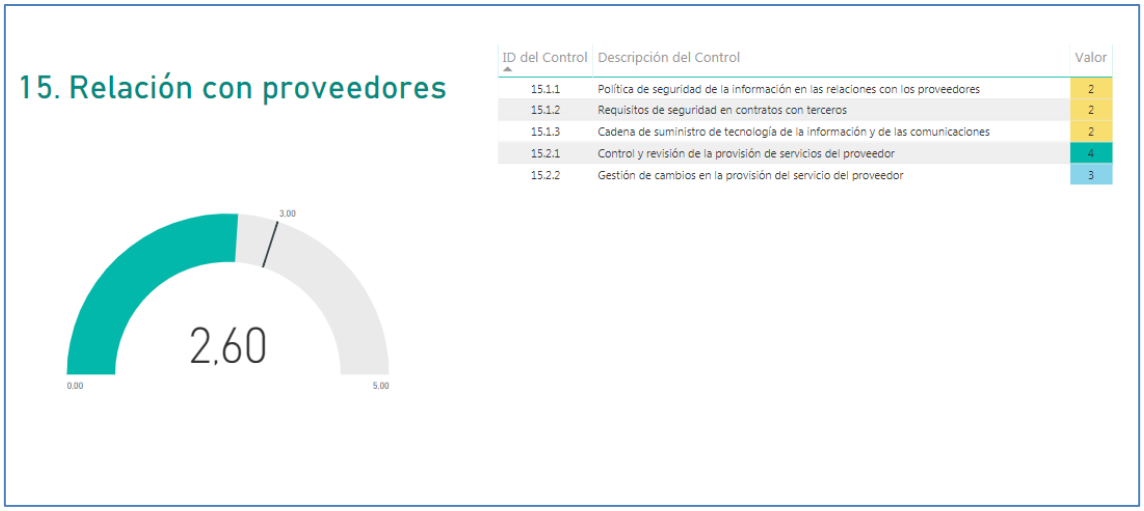
ID del Control	Descripción del Control	Valor
13.1.1	Controles de red	4
13.1.2	Seguridad de los servicios de red	2
13.1.3	Segregación en redes	3
13.2.1	Políticas y procedimientos para la transferencia de información.	2
13.2.2	Acuerdos sobre transferencia de información	1
13.2.3	Mensajería electrónica	2
13.2.4	Acuerdos de confidencialidad o no divulgación	1

Captura 11: Detalle Dominio 14. Adquisición, desarrollo y mantenimiento de los sistemas de la información



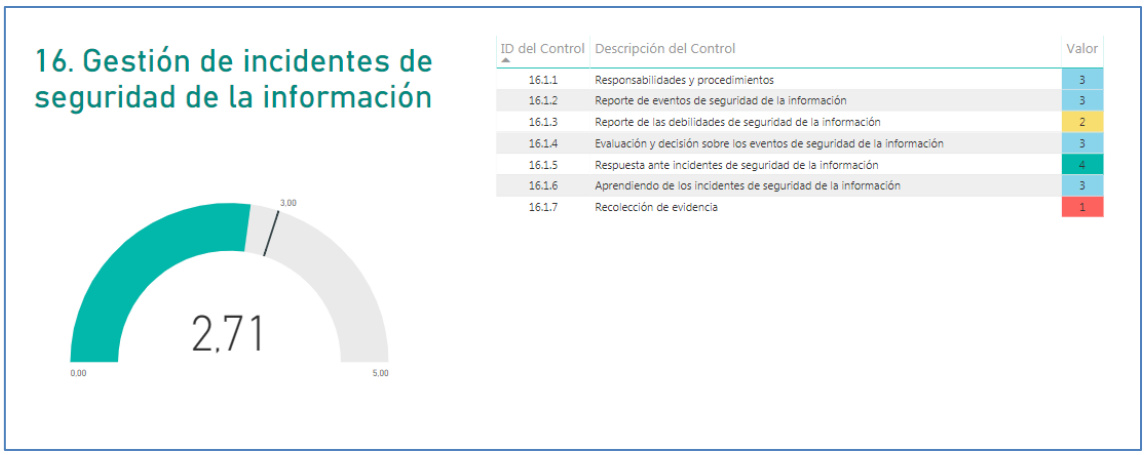
ID del Control	Descripción del Control	Valor
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	1
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	4
14.1.3	Protección de las transacciones de servicios de aplicaciones	2
14.2.1	Política de desarrollo seguro	1
14.2.2	Procedimiento de control de cambios en sistemas	2
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	1
14.2.4	Restricciones a los cambios en los paquetes de software	1
14.2.5	Principios de ingeniería de sistemas seguros	1
14.2.6	Entorno de desarrollo seguro	2
14.2.7	Externalización del desarrollo de software	3
14.2.8	Pruebas funcionales de seguridad de sistemas	1
14.2.9	Pruebas de aceptación de sistemas	2
14.3.1	Protección de los datos de prueba	0

Captura 12: Detalle Dominio 15. Relación con proveedores



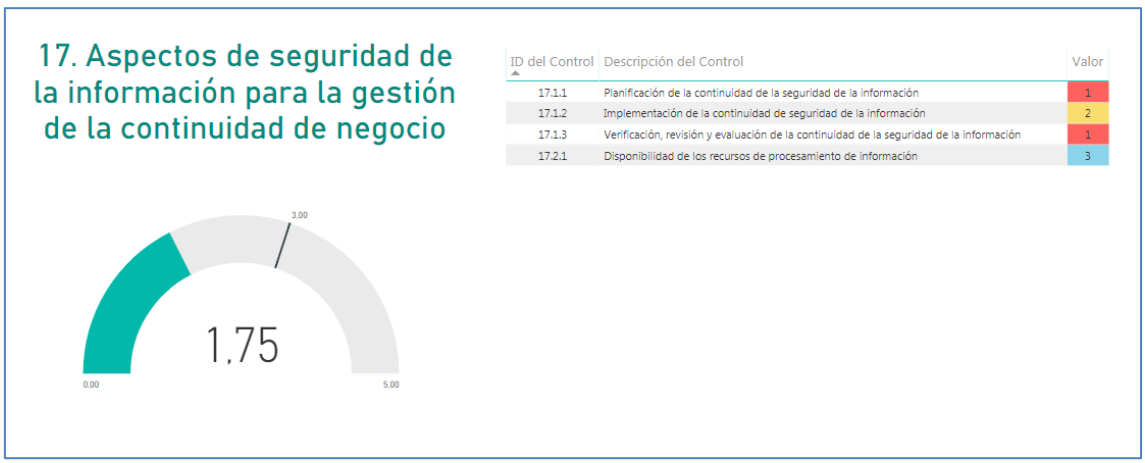
ID del Control	Descripción del Control	Valor
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	2
15.1.2	Requisitos de seguridad en contratos con terceros	2
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	2
15.2.1	Control y revisión de la provisión de servicios del proveedor	4
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	3

Captura 13: Detalle Dominio 16. Gestión de incidentes de seguridad de la información



ID del Control	Descripción del Control	Valor
16.1.1	Responsabilidades y procedimientos	3
16.1.2	Reporte de eventos de seguridad de la información	3
16.1.3	Reporte de las debilidades de seguridad de la información	2
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	3
16.1.5	Respuesta ante incidentes de seguridad de la información	4
16.1.6	Aprendiendo de los incidentes de seguridad de la información	3
16.1.7	Recolección de evidencia	1

Captura 14: Detalle Dominio 17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio



ID del Control	Descripción del Control	Valor
17.1.1	Planificación de la continuidad de la seguridad de la información	1
17.1.2	Implementación de la continuidad de seguridad de la información	2
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1
17.2.1	Disponibilidad de los recursos de procesamiento de información	3

Captura 15: Detalle Dominio 18. Cumplimiento

ID del Control	Descripción del Control	Valor
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	1
18.1.2	Derechos de propiedad intelectual	0
18.1.3	Protección de registros	2
18.1.4	Privacidad y protección de los datos personales	3
18.1.5	Regulación de controles criptográficos	0
18.2.1	Revisión independiente a la seguridad de la información	1
18.2.2	Cumplimiento de las políticas y normas de seguridad	1
18.2.3	Revisión del cumplimiento técnico	2