TÍTULO

ELABORACIÓN DE CUADROS DE MANDO EN LOS PROCESOS DE CIBERSEGURIDAD

AUTOR

Marcelo Daniel González

Esta edición electrónica ha sido realizada en 2023

Tutores	Dr. D. José Luis Martínez Ramos; Dr. D. Ignacio Ortega Mariño
Instituciones	Universidad Internacional de Andalucía; Universidad de Granada; Universidad de Málaga; Universidad de Almería
Curso	*Máster en Transformación digital de empresas (2021-2022)*
©	Marcelo Daniel González
©	De esta edición: Universidad Internacional de Andalucía
Fecha documento	2022

TRABAJO FIN DE MÁSTER

Máster en Transformación digital de empresas

Universidad : Universidad Internacional de Andalucía

Centro: Oficina de Estudios de Posgrado.

"Elaboración de los Cuadros de Mando en los procesos de Ciberseguridad"

Itinerario: Sector Energético

Curso: 2021/2022

Modalidad: Online

Alumno/a: Marcelo Daniel Gonzalez

Director/es:

- Director Académico : José Luis Martínez Ramos
- Director Profesional : Ignacio Ortega Mariño

Resumen

Debido al conflicto actual entre Rusia y Ucrania, los ciberataques, tanto los dirigidos a las infraestructuras de los estados cómo a las empresas, no han dejado de crecer en esta era de Digitalización. Todas las compañías, entre las que se encuentran también las empresas eléctricas están incrementando sus esfuerzos con el objetivo de aumentar las medidas de seguridad para reforzar al máximo las defensas contra estos ataques.
Para vigorizar estos sistemas es muy importante contar con un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la familia de normas ISO 27000 porque aporta una "seguridad basada en datos de comportamiento" que permiten mostrar y demostrar que las cosas se están controlando y que se mantienen dentro de los rangos de valores deseados.
Este trabajo desarrolla cómo fue la reelaboración de los cuadros de mando actualizando y añadiendo nuevos paneles a partir de los controles sugeridos por la Norma ISO27002(Seguridad de la Información) como así también las recomendaciones del framework NIST(National Institute of Standards and Technology) .Esta tarea tuvo lugar en el departamento de Gestión de la Energía Global Iberdrola, teniendo en cuenta que el objetivo central del departamento es abordar el proceso requerido para la certificación de la norma mencionada anteriormente. El tiempo necesario para su realización fue de dos meses y para su desarrollo fueron necesarias capacitaciones con un aprendizaje continuo desde diferentes fuentes de información vinculadas a seguridad de la información y formaciones internas de la compañía en herramientas tales como ARIS(Architecture of Integrated Information Systems), Excel, etc.
Es importante destacar que los resultados fueron favorables en el proceso ya que se logró implementar los cuadros de mando lo que permitirá construir una mejora continua del sistema y una futura certificación.

Palabras Claves: ciberataques, Infraestructuras Críticas, SGSI, ISO27001, controles, Framework NIST, cuadros de mando.

Abstract

Due to the current conflict between Russia and Ukraine, cyberattacks directed at the infrastructure of states and companies have not stopped growing in this era of Digitization. All companies, including energy companies, are increasing their efforts to maximize security to strengthen defences against these attacks as much as possible.

To invigorate these systems, it is extremely important to have an ISMS (Information Security Management System) based on the ISO 27000 family of standards. It provides security based on behavioural data which allows showing and demonstrating that things are being controlled and that they remain within the ranges of the desired values.

This work develops how the dashboards were reworked, updating and adding new panels based on the controls suggested by the ISO27002 Standard (Information Security) as well as the recommendations of the NIST framework (National Institute of Standards and Technology). This task took place in the Iberdrola Global Energy Management department taking into consideration that the main objective of the department is to address the process required for the certification of the aforementioned standard. The time required for its completion was two months. Furthermore, its development demanded training with continuous learning from different sources of information related to information security and internal instruction of the company in tools such as ARIS (Architecture of Integrated Information Systems), Excel, etc.

It is important to highlight that the results were favourable in the process since the dashboards were implemented, which will allow the construction of a continuous improvement of the system and a future certification

Keywords: cyberattacks, Critical Infrastructure, ISMS, ISO27001,controls, Framework NIST,BSC.

ACRONIMOS

Abreviatura	Denominación original	Significado
GEM	Global Energy Management	Gestión de la Energía Global
NIST	National Institute of Standards and Technology	Instituto Nacional de Normas y Tecnología
CM	Cuadro de mando	
SGSI	Sistema de Gestión de Seguridad de la Información	
GDPR	General Data Protección Reglament	Ley de Protección de Datos de carácter personales
LPIC	Ley de Protección de Infraestructuras Criticas	
SoA	Statement of Applicability	Declaración de Aplicabilidad
ISO	International Organization for Standardization	Organización Internacional de Normalización
DPD	Delegado de protección de datos	
IT	Information Technology	Tecnologías de la información
OT	Operational Technology	
CPD	Centro de procesamiento de datos	
ARIS	Architecture of Integrated Information Systems	Arquitectura de Sistemas Integrados de Información
ITEO	Informe Técnico de Evaluación de Oferta	
SIEM	Security Information and Event Management	Seguridad de la Información y Gestión de Eventos
SaaS	Software as a Service	Software como servicio

Índice

Índice de tablas

Índice de ilustraciones

1 INTRODUCCIÓN

1.1 Motivación del trabajo

Debido al avance de las tecnologías disruptivas a pasos agigantados, año tras año las empresas se ven en la obligación de su uso para su crecimiento en todas sus áreas. Cada vez son más las empresas que se ven en la necesidad de apostar a la transformación digital para mantenerse competitivas, lo que las obliga a contemplar la revisión y la inclusión de nuevos escenarios de riesgo y a diseñar o rediseñar estrategias para hacerles frente. Sea de una forma o de otra, esta estrategia no puede dejar de considerar la ciberseguridad como un eje troncal ya que permite acompasar la digitalización del negocio con las medidas que permitirán proteger a la organización. Lo primero será entender que los presupuestos de las mejoras de ciberseguridad se tienen que considerar como una inversión y no como un gasto [1].

"Por lo anteriormente mencionado, es de gran utilidad para las organizaciones la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) el cual está fundamentado sobre la norma ISO27001 y establece un proceso sistemático para la protección ante cualquier amenaza que podría llegar afectar la confidencialidad, integridad o disponibilidad de la información. Este sistema ofrece las mejores prácticas y procedimientos que siendo aplicados correctamente en el ámbito empresarial, proporcionan una mejora continua y apropiada para evaluar los riegos a los que nos enfrentarnos diariamente, establecer controles para una mejor protección y defender así nuestro activo más valioso dentro de la organización, la información"[2].

1.2 Contexto y antecedentes

Gestión de la Energía Global (Global Energy Management) es una Dirección perteneciente al Negocio Liberalizado dentro del Grupo Iberdrola, la cual se encuentra encargada de las operaciones de compra y venta de la electricidad y el gas natural para asegurar el suministro a los clientes al precio y condiciones más competitivas en los distintos países donde Iberdrola está presente (España, Portugal, el Reino Unido, México, Francia, Alemania, Italia, etc.).

Además, es responsable de maximizar el margen de las centrales de generación del grupo operando en los mercados energéticos a corto y largo plazo, como así también controlar en tiempo real la operación global del sistema generador de Iberdrola. Adicionalmente, es responsable del abastecimiento de combustible a las centrales térmicas (gas natural y carbón).

Para poder realizar estas operaciones, GEM cuenta con un equipo de infraestructura y unos equipos de soporte adecuados para respaldar todos los procesos de negocio de la Dirección, así como un equipo de ciberseguridad responsable de velar para que la información se encuentre salvaguardada bajo el punto de vista de la confidencialidad, integridad y disponibilidad; cumplimiento regulatorio y legislativo.

Es por todo ello que el equipo de ciberseguridad ayuda a GEM a prepararse, protegerse, detectar, responder y recuperarse en todos los puntos del ciclo de vida de la seguridad, así como a velar por el cumplimiento de las diferentes normativas corporativas y propias de su ámbito de aplicación en las diferentes etapas: diseño, elaboración y operación de cualquier sistema.

1.2.1 Investigación y Análisis de la Ciberseguridad en la Compañía

La compañía es consciente de la relevancia de liderar la transformación digital en el sector energético, un proceso que constituye una importante palanca para maximizar la creación de valor. En el año 2017, tras sufrir y superar con éxito un incidente de ciberseguridad gracias a la aplicación de las lecciones aprendidas en el departamento, se definió el plan de ciberseguridad 2017-2022 con iniciativas de gran impacto poniendo foco en el refuerzo de las capacidades de: identificar, proteger, detectar, responder y recuperar a partir del marco de trabajo NIST (National Institute of Standards and Technology)[3].

1.2.2 Recopilación de documentación del SGSI (Sistema de Gestión de Seguridad de la Información)

El departamento analizado cuenta con su cuerpo normativo de seguridad con el propósito de definir el objetivo, dirección, principios y reglas básicas para la gestión de la Seguridad de la Información en el departamento. Asimismo, esta Normativa persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, las cuales constituyen los tres componentes fundamentales de la Seguridad de la Información.

También considera el cumplimiento de la legislación española vigente de las normas GDPR (General Data Protection Regalement), LPIC (Ley de Protección de Infraestructuras críticas) y de las normativas que en el ámbito de la Seguridad de la Información que puedan afectar a la compañía.

La importancia de hacer hincapié en la parte humana teniendo en cuenta el compromiso de toda persona o equipo relacionado al tratamiento de información durante su ciclo vital.

A continuación, se hace mención de la documentación que fue necesaria para la elaboración de los cuadros de mando a partir del SGSI en la organización, considerando esto como una primera versión de los mismos y abiertos a una modificación proveniente de las entidades encargadas de la regulación de la norma. Por razones de políticas de la empresa, ante documentación interna es que solamente se hará mención de los documentos:

- Normativa de Ciberseguridad[4].
- Política de Ciberseguridad[5].
- Política de Gestión de Riesgo[5].
- Declaración de Aplicabilidad SOA (statement of applicability)[6].
- Plan de Tratamiento de Riesgos de Seguridad de la Información[7].
- Procedimiento De Coordinación Y Respuesta A Ciber incidentes[8].
- Manual de Gestión de Ciberseguridad de la información[9].

1.2.3 Roles y responsabilidades

La Dirección asegura la asignación y comunicación de responsabilidades y autoridades para las oportunas funciones de la organización a fin de asegurar que el Sistema de Gestión cumple con los requisitos del estándar ISO/IEC 27001:2013, ISO/IEC 27002:2013 e informar sobre el desempeño del SGSI a la Dirección.

En la tabla 1 se identifican los siguientes roles y responsabilidades:

Roles	Responsabilidades
Dirección	• Asegurar que la política sea adecuada a la organización y a su contexto, en caso de ser necesario se aplique la normativa de ciberseguridad. • Establecer los objetivos de seguridad, asegurando que son compatibles con los objetivos de negocio. • Proporcionar los recursos necesarios para implantar, mantener y mejorar de manera continua el SGSI. • Asegurar que se comunica la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información. • Revisar periódicamente el SGSI para asegurar que se consiguen los resultados previstos y su eficacia. • Dirigir y apoyar a los empleados y a otros roles relevantes para lograr una contribución eficiente al SGSI. • Promover la mejora continua del SGSI.
Responsable de Ciberseguridad	• Liderar la implantación, mantenimiento y mejora continua del SGSI. • Liderar el Foro de Ciberseguridad. • Supervisar y reportar el nivel de cumplimiento de la política y objetivos en las áreas y roles pertinentes. • Promover y gestionar la implantación de estándares y buenas prácticas en seguridad de la información. • Promover una cultura de seguridad de la información en GEM • Liderar el proceso de gestión de riesgos de seguridad de la información. • Cooperar con los organismos regulatorios correspondientes, actuar como punto de contacto con dichos organismos y con los interesados. • Evaluar y coordinar la implementación de controles de seguridad de la información en los sistemas y servicios. • Reportar periódicamente el estado de la seguridad de la información a la Dirección. • Dar seguimiento a los incidentes de seguridad de la información.
Foro de Ciberseguridad	• Realizar seguimiento de los proyectos de seguridad de la información en curso. • Realizar seguimiento de los incidentes de seguridad de la información. • Participar y dar apoyo en la implantación, mantenimiento y mejora continua del SGSI. • Otros temas de interés en relación con el estado de la seguridad de la información.
Delegado de	• Proporcionar asesoramiento e información en materia de protección

Protección de Datos (DPD) corporativo	de datos. • Supervisar el cumplimiento de la normativa aplicable en materia de privacidad. • Cooperar con la Autoridad de Control y actuar como punto de contacto con dicha Autoridad y con los interesados. • Promover una cultura de seguridad de los datos personales en la organización. • Respaldar y fomentar la protección de datos por diseño y por defecto. • Liderar el proceso de gestión de riesgos de privacidad.
Infraestructuras	• Responsables de administrar y gestionar la infraestructura tecnológica de GEM, asegurando la disponibilidad de los servicios de hardware, software base y comunicaciones, de acuerdo a las normativas de ciberseguridad y sistemas. • Responsables de implantar medidas de recuperación en GEM .
Soluciones Digitales	• Responsables de la coordinación de proyectos de implantación, desarrollo y actualización de software, de acuerdo a las buenas prácticas de desarrollo IT (Information Technology), de ciberseguridad y de calidad. • También coordinan y gestionan los servicios de soporte y mantenimiento de activos GEM.
Empleados	• Cumplir con los requisitos, buenas prácticas y políticas establecidas en seguridad de la información y privacidad. • Realizar un buen uso de la información y sistemas de información. • Participar de una manera activa en las actividades de formación y concienciación. • Reportar cualquier incidente de seguridad de la información o posible indicio. • No divulgar información sensible para la organización.

Tabla 1. Roles y responsabilidades

1.3 Objetivos

Para dar un contexto detallado sobre los objetivos planteados en este trabajo es importante mencionar parte de la historia de la empresa que llevó a la necesidad de la implementación de un SGSI y a su vez la elaboración de los cuadros de mando de ciberseguridad, que en este último mencionado se basó la realización de este trabajo.

Punto de partida en el año 2017: en mayo de ese año, la compañía sufrió y superó una problemática de ciberseguridad, a partir de ese suceso y habiendo aprendido lecciones se definieron nueve iniciativas de gran impacto para reforzar la seguridad de la misma, focalizándose en la detección de amenazas y recuperación de los sistemas y servicios; a partir de ese momento tuvieron lugar las primeras creaciones de cuadros de mando.

Cierre del plan 2017-2021 y nuevo plan 2021-2023: Tras finalizar el plan anterior, se definió y ejecutó el plan de Ciberseguridad GEM 21-23 incorporando la implementación de un SGSI a partir de la norma ISO 27001 que involucra las actividades de gestión de los Centros de Procesos de Datos (CPD) de GEM y los sistemas de información que dan servicio a los procesos de compraventa de energía en mercados mayoristas, nacionales e internacionales y control en tiempo real del sistema productor; como así también la mejora de los cuadros de mando de ciberseguridad del departamento GEM los cuales analizaremos con más detalles en la sección cuatro.

1.3.1 Objetivo General

El objetivo principal del trabajo es desarrollar la reelaboración de los cuadros de mandos durante el mes de mayo y junio de 2022 que permitan medir el proceso de ciberseguridad del departamento GEM Iberdrola, plazo que fue fijado en base a las fechas de auditorías internas a cargo de la empresa DELLOITTE. Posterior a ello se continuará con auditorías externas con la empresa AENOR para la certificación del SGSI.

1.3.2 Objetivos específicos

Los objetivos específicos fueron seleccionados en base a las herramientas con las que contaba el departamento GEM como una forma de evolucionar en las diferentes etapas que permitan llegar al objetivo general. A partir de todo lo mencionado, el aporte añadido está relacionado con la realización de nuevos paneles que incluirán información sobre la madurez de controles de SGSI y otros donde se desarrolla en base al framework NIST que está dividido en diferentes funciones, tales como: identificar, proteger, detectar, responder y recuperar. Estos paneles aportaron claridad y solidez al departamento GEM y un refuerzo SGSI.

Los objetivos específicos fueron:

- Colaborar en la elaboración de los flujos de los procesos de ciberseguridad, los cuales estaban alineados al framework NIST.
- Definir los indicadores utilizados en los cuadros de mando.
- Elaborar nuevos paneles de control.
- Alimentar indicadores empleados en los cuadros de mando.

1.4 Resumen de resultados

Desde el departamento de ciberseguridad se pudo inferir la necesidad de involucrar a otros departamentos dentro de GEM para la elaboración de SGSI. A partir de su creación se generó una participación activa en lo que respecta a los estándares de la norma ISO27001.

A partir de lo mencionado se puede ver el papel fundamental de los cuadros de mando en su actualización continua ya que la dirección de cada área de GEM tendrá un rol importante en mantener actualizados los ficheros y bases de datos que alimentan los indicadores del cuadro de mando de manera tal de ver su evolución y mejora en el tiempo.

1.5 Competencias utilizadas

Durante el desarrollo de este proyecto ha sido necesario el incremento del aprendizaje en relación a la estructura del departamento GEM, normativas (ISO 27001, normativa interna), políticas de seguridad GEM y los alcances de las mismas para su aplicación y certificación. Vislumbrar el funcionamiento de las áreas y sistemas involucrados para su certificación que fue posible gracias al trabajo continuo y activo del equipo del departamento quiénes llevaron a cabo análisis de bases de datos y ficheros en forma constante, elaborando también los cuadros de mando.

Para esta tarea a lo largo del desarrollo y elaboración de los mismos se comprende las siguientes *competencias básicas*:

- CG4. Saber interpretar el marco normativo básico regulador del ámbito de la Transformación Digital de Empresas.
- CG5. Diferenciar y aplicar de forma eficiente las Tecnologías de la Información y la Comunicación en el ámbito de la Transformación.
- CB7. Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB9. Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10. Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

También fueron necesarias *competencias específicas* para realizar por ejemplo la automatización de los cuadros de mandos (lo cual requirió capacitación constante y profundización de las herramientas); dichas competencias fueron las siguientes:

- CE1. Diferenciar los procesos empresariales y aplicar las tecnologías, plataformas y herramientas adecuadas para la transformación digital.
- CE7. Analizar datos y extraer información relevante de los mismos.
- CE8. Revisar tecnologías para la implementación de sistemas de gestión y explotación de datos.
- CE18. Analizar con espíritu crítico la evolución de la transformación digital dentro de la empresa para apoyar de forma creativa la innovación tecnológica.

1.6 Estructura de la memoria del TFM

Para darle un cuerpo al proyecto presente se lo organizó en diferentes secciones y de la siguiente manera:

Sección 1: Introducción, en la cual se desarrolla la motivación del trabajo, contexto y antecedentes, objetivos, resumen y resultados y competencias utilizadas.

Sección 2: Plan de trabajo, en donde se plantean las metodologías y herramientas utilizadas a lo largo del proyecto incluyendo el listado de tareas.

Sección 3: Elaboración de flujos de los procesos de seguridad de la información, donde se plantea sobre asegurar la privacidad de la empresa.

Sección 4: Desarrollo de los cuadros de mando: en este capítulo se profundiza todo lo relacionado a indicadores, carga de datos, paneles e información.

Sección 5: Resultados, en este apartado se presenta el análisis financiero y resultado final.

Sección 6: Conclusiones finales.

Sección 7: Bibliografía utilizada para el desarrollo del proyecto.

Sección 8: Anexo de material útil para el desarrollo de la memoria.

2 PLAN DE TRABAJO

2.1 Metodología

Para reducir a un mínimo los riesgos de seguridad de la información es fundamental la implementación de un Sistema de Gestión de Seguridad de la Información ya que el mismo nos permite definir una estructura y los procedimientos de trabajo en los sistemas de información, como así también disponer de controles para medir su madurez mediante los cuadros de mando.

Para la elaboración del trabajo se tomó como referencia la norma general ISO27000, centrándose en las normas **ISO/IEC 27001:2013** que establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua como marco de gestión del SGSI. Así también la norma **ISO/IEC27002** como referencia de los dominios y controles del SGSI. Los controles de seguridad de la información brindan orientación para los estándares de seguridad de la información organizacional y ofrecen las mejores prácticas para la gestión de la seguridad de la información. Tiene en cuenta un entorno de seguridad de la información único en la empresa, centrándose en la selección, implementación y gestión de controles de seguridad de las organizaciones.[10]

Así mismo se complementa con el Framework NIST como muestra la ilustración 2.1 que está dividido en diferentes funciones, tales como: identificar, proteger, detectar, responder y recuperar para mejorar la seguridad cibernética de infraestructura crítica [3]

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Ilustración 2.1 NIST Ciber Security Framework

Identificar

Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.[11]

Proteger

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.[11]

Detectar

Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo el descubrimiento oportuno de los mismos.[11]

Responder

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.[11]

Recuperar

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.[11]

2.2 Herramientas

Durante la realización del proyecto se hizo uso de las siguientes herramientas:

- Aris software AG
  En la ilustración 2.2 se presta la herramienta que te permite entender tus procesos de negocios para encontrar cuellos de botella y oportunidades de mejora. Compara el diseño de los procesos con la forma en que se están ejecutando para ver si están en cumplimiento y realiza cambios antes de que el resultado final se vea afectado [12].

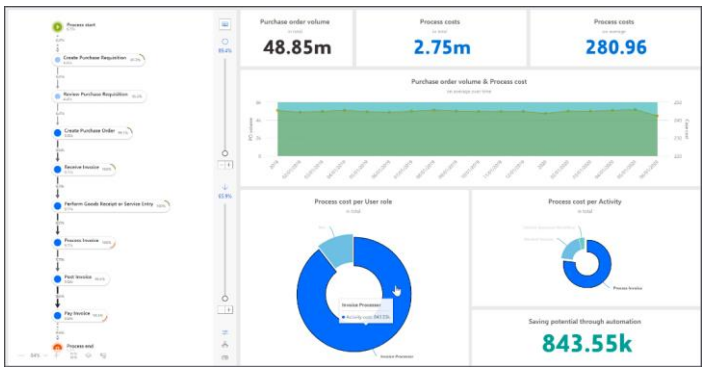


Ilustración 2.2 ARIS Software AG Dashboard Example

- Microsoft Excel.
  Herramienta utilizada para registrar, clasificar una gran cantidad de información de manera eficiente.

- Bases de Datos.
  Herramienta para recopilar y organizar información.

2.2.1 Especificaciones técnicas

Para la elaboración correcta de los cuadros de mando y para que los mismos sean efectivos, son necesarias ciertas especificaciones, se consideran de importancia las siguientes:

Integridad: todo cuadro de mando que pretenda ser efectivo deberá preservar en todo momento la integridad de la estrategia corporativa previamente definida.
Firmeza y solidez: relacionado con lo anterior, un cuadro de mando debe velar por la firmeza y la solidez de la estrategia en la que se enmarca la actividad corporativa.
Flexibilidad: sin perjuicio de lo comentado sobre la firmeza y la solidez, la flexibilidad también debe ser una característica destacada de un cuadro de mando efectivo.
Interactividad: es una propiedad que debe poseer todo cuadro de mando que pretenda ser efectivo, eso es, que los datos y la información que proporcione sean tanto visualizables como modificables y compartibles.

2.3 Listado de tareas

Las distintas actividades en la que se ha dividido el trabajo se han organizado en el tiempo de la siguiente manera. A continuación, la tabla 2 muestra el orden y el tiempo empleado en cada una de las fases:

Periodo de tiempo	Actividad Realizada	Duración
ABRIL	• Elaboración de anteproyecto	1 día
MAYO	• Investigación sobre cuadros de mando.	1 día
	• Estudio de la norma ISO 27001.	2 días
	• Estudio de framework NIST.	1 día
	• Formación en ARIS.	3 días
	• Recopilación de documentación.	5 días
	• Análisis de ficheros para determinación de indicadores.	5 días
	• Creación de cuadros de mando.	10 días
	• Elaboración de la memoria, primera parte.	3 días
JUNIO	• Revisión Final de los cuadros de mando.	5 días
	• Auditorías internas con Deloitte.	5 días
	• Elaboración de la memoria, segunda parte.	12 días
	• Corrección y revisión de la memoria.	5 días
JULIO	• Revisión final de la memoria.	5 días

Tabla 2. Listado de tareas

Por lo tanto, se estima que el tiempo dedicado a la elaboración del trabajo es de 63 días. Es decir 2 meses y 3 días. Aproximadamente en cada día se trabajó 8 h con lo que significan 504 horas.

3 ELABORACIÓN DE FLUJOS DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

Tener plasmado los diversos procesos del departamento como en este caso, el proceso de ciberseguridad es uno de los pilares importantes, ya que es necesario dejar asentado de forma comprensible una determinada secuencia de pasos. se puede realizar un **diagrama de flujo** valiéndose de distintas herramientas informáticas que facilitan la cuestión de forma extrema. Así, este tipo de tareas es mucho más fácil de implementar que lo que era en el pasado. Para confeccionar el diagrama, se suelen utilizar diferentes figuras geométricas como ser rombos, cuadrados o círculos, a partir de ello se pretende dar un determinado proceso o resultado.

La compañía tras el plan de ciberseguridad implementó la herramienta ARIS la cual es un marco de gestión empresarial que ofrece métodos y técnicas para la gestión de procesos de negocio. Mediante esta herramienta implementa todos los procesos del departamento como así también los cuadros de mando organizando la información.

De acuerdo a los flujos de procesos definidos en OTC (Oficina técnica de ciberseguridad) se elaboraron los siguientes procesos:

3.1 Asegurar la ciberseguridad y la privacidad

Como muestra la ilustración 3.1, cuando hablamos de asegurar la ciberseguridad y la privacidad hacemos referencia al proceso mediante el cual se proporciona seguridad a la información tratada por Gestión de la Energía y se garantiza la privacidad de los datos personales de sus empleados. Se presenta la siguiente tabla con el fin de proporcionar una visión organizada del mismo:

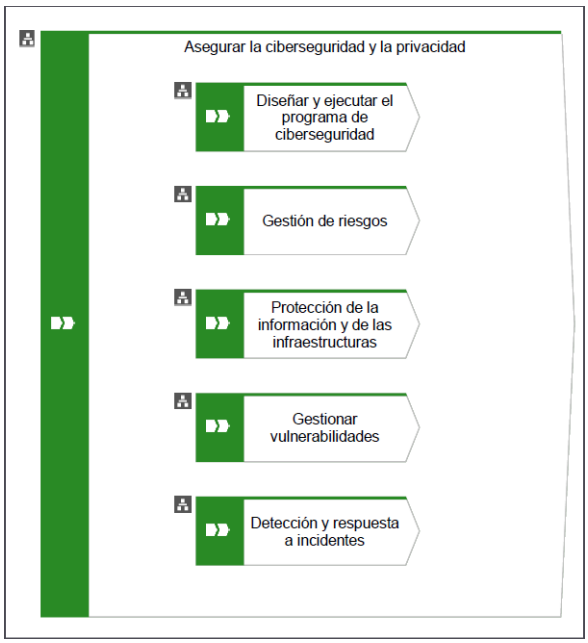


Ilustración 3.1 Cadena de valor de la seguridad de la información

3.1.1 Diseñar y ejecutar el plan de ciberseguridad

En la Ilustración 3.2 se representa el proceso de diseñar y ejecutar el plan de ciberseguridad.

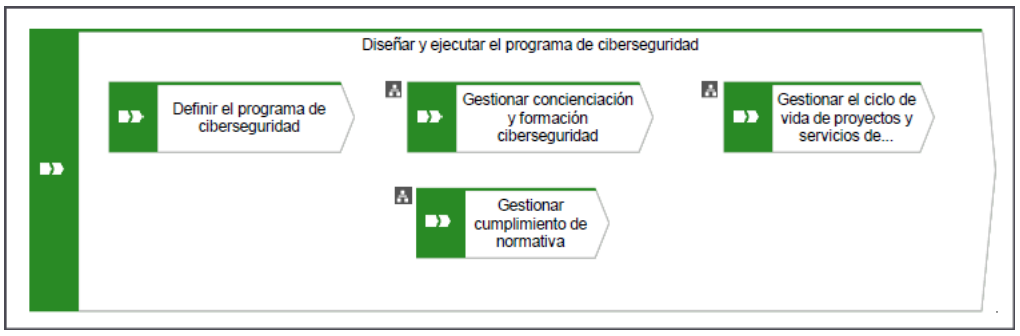


Ilustración 3.2 Proceso de diseño y ejecución del programa ciberseguridad

- **Gestionar concienciación y formación ciberseguridad:** gestionar las distintas actividades de concienciación y formación en ciberseguridad de GEM.
- **Gestionar el ciclo de vida de proyectos y servicios:** gestionar el ciclo de vida de los distintos proyectos y servicios de ciberseguridad de GEM (tanto internos como externos con proveedores) y la implantación de nuevas tecnologías (herramienta, software on-premise, SaaS(Software as a Service).
- **Gestionar cumplimiento de la normativa:** gestionar y asegurar el cumplimiento de la normativa de ciberseguridad, tanto interna como externa, aplicable a GEM

3.1.2 Gestión de riesgos

Procesos relacionados con las capacidades de gestión de riesgos de ciberseguridad del departamento como representa la Ilustración 3.3.

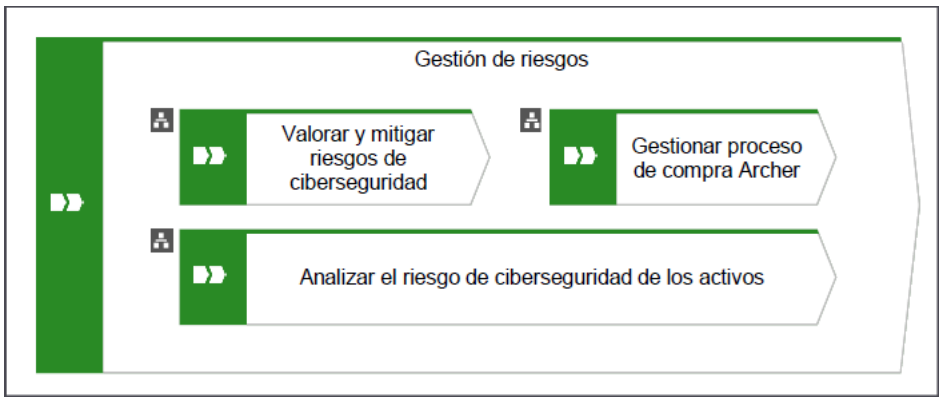


Ilustración 3.3 Proceso de gestión de riesgos

- **Valorar y mitigar riesgos de ciberseguridad.**
- **Gestionar proceso de compra Archer:** el proceso de compras en Archer se divide en tres fases: nueva licitación, gestión de compras y completar el ITEO(Informe Técnico de Evaluación de Oferta).
- **Analizar el riesgo de ciberseguridad de los activos:** análisis de los riesgos de Gestión de la Energía basándose en la evaluación de los activos identificados relacionados con las múltiples amenazas que les aplican.

3.1.3 Protección de la información y de las infraestructuras

La ilustración 3.4 nos muestra los procesos relacionados con las capacidades de protección de la información y de las infraestructuras de GEM.

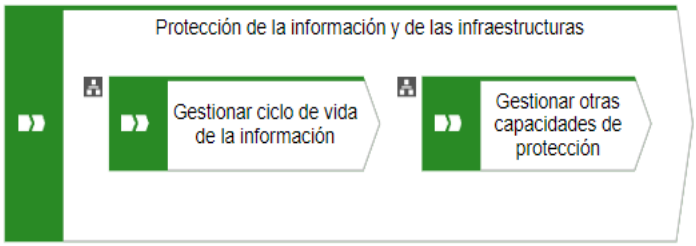


Ilustración 3.4 Protección de Información e infraestructuras

- **Gestionar ciclo de vida de la información:** definición del ciclo de vida de activos de la información para reducir los riesgos, optimizar el coste de su almacenamiento y facilitar la localización de información relevante.
- **Gestionar otras capacidades de protección:** procesos relacionados con las capacidades de protección de las infraestructuras de GEM.

3.1.4 Gestión de las vulnerabilidades

El Proceso está organizado para alinearse con las tres fases principales del ciclo de vida de la gestión de vulnerabilidades. En la Ilustración 3.5 se representa lo mencionado:

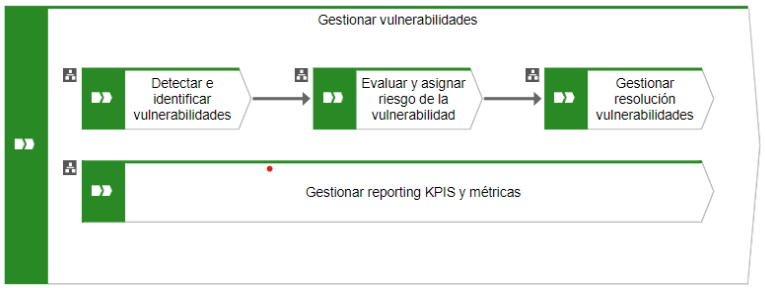


Ilustración 3.5 Proceso de gestionar vulnerabilidades

Detectar e identificar vulnerabilidades: en esta fase se encuentra el proceso de evaluación de la vulnerabilidad, la realización de escaneos y la obtención de resultados. Se proporcionan los requisitos mínimos para que la evaluación garantice un escaneo adecuado y regular.

- **Evaluar y asignar riesgo de la vulnerabilidad.**
- **Gestionar resolución de vulnerabilidades:** los pasos recomendados para garantizar la resolución correcta de las vulnerabilidades. Se alinea con el ciclo de vida de una vulnerabilidad que permanece con el propietario del activo hasta que se resuelve.

3.1.5 Detección y respuesta a incidentes

En la ilustración 3.6, se exponen los procesos relacionados con las capacidades de detección y respuesta a incidentes de ciberseguridad en el departamento.

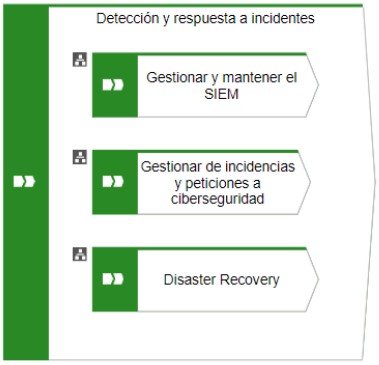


Ilustración 3.6 Procesos de detección y respuesta a incidentes

- **Gestionar y mantener el SIEM:** configurar nuevos sistemas de la red de GEM para que envíen logs de seguridad al Qradar de GEM.
- **Gestionar de incidencias y peticiones a ciberseguridad.**
- **Disaster Recovery**.

4 DESARROLLO DE LOS CUADROS DE MANDO

Esta sección es fundamental en el progreso de este trabajo ya que presenta la reelaboración de los cuadros de mando que es el objetivo principal.

Hablamos de reelaboración debido a que anteriormente se encontraban definidos los siguientes paneles en la compañía que se pueden visualizar en el anexo C: capturas de pantalla CM de Ciberseguridad Antiguo.

- Panel de actividad: dentro de este panel se encontraban las actividades pendientes, en progreso y realizadas por los miembros encargados del área de ciberseguridad.
- Seguimiento de Servicios: este panel representa el gasto en materia de ciberseguridad.
- Ciber incidentes: representa las posibles amenazas o incidentes detectadas a través del equipo SIEM.

Siguiendo con la información expuesta, en primer lugar, se destaca que actualmente todos los procesos de GEM (incluidos los Ciberseguridad) están desplegados y medidos en una plataforma llamada ARIS, herramienta que se utiliza desde el año 2021 en la empresa; entonces fue ésta la que se usó para la elaboración de los cuadros de mando. En segundo lugar, se definieron a los indicadores de relevancia recopilando la fuente de los mismos. En una tercera etapa, se modificaron los cuadros de mando añadiendo los siguientes paneles:

- Objetivo SGSI GEM: objetivos anuales organizados en el framework NIST.
- Madurez de los Controles: paneles que permiten medir la madurez de los controles del SGSI a partir de la Norma ISO 27001.
- Identificar.
- Proteger.
- Detectar.
- Responder.
- Leyenda KPI.

4.1 Definición de indicadores

A partir de la norma ISO/IEC 27002 la cual contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios (guía de apoyo). Los controles que aplican a la organización son recogidos en un documento llamado SOA que una parte se visualiza en la ilustración 4.1 y utilizados como indicadores. El mismo se puede observar en el Anexo A: Declaración de Aplicabilidad (SoA).

Declaración de Aplicabilidad (SoA)					
ID	**Control**	**Descripción del control**	**Nivel de madurez**	**Numérico**	**Documentación de soporte**
5	**A.5 Políticas de seguridad de la información**			**3**	
5.1	**Dirección de gestión de seguridad de la información**				**1.1.Politica_seguridad_corporativa. Consta de:** **politica_proteccion_datos** **Política de riesgos de ciberseguridad** **1.2.politica_general_control_riesgos** **1.3.Requisitos adicionales de Ciberseguridadv.1.ES** **2.Normativa Ciberseguridad GEM** **Framework de Seguridad Cloud (S4)** **Modelo de Gobierno cloud (S4)**
5.1.1	Políticas de seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	L3 - Definido (90%)	3	1.1.Politica_seguridad_corporativa. Consta de: politica_proteccion_datos Política de riesgos de ciberseguridad 1.2.politica_general_control_riesgos 1.3.Requisitos adicionales de Ciberseguridadv.1.ES 2.Normativa Ciberseguridad GEM Framework de Seguridad Cloud (S4) Modelo de Gobierno cloud (S4)
5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	L3 - Definido (90%)	3	1.1.Politica_seguridad_corporativa. Consta de: politica_proteccion_datos Política de riesgos de ciberseguridad 1.2.politica_general_control_riesgos 1.3.Requisitos adicionales de Ciberseguridadv.1.ES 2.Normativa Ciberseguridad GEM Framework de Seguridad Cloud (S4) Modelo de Gobierno cloud (S4)
6	**A.6 Organización de seguridad de la información**			**2,2857143**	

Ilustración 4.1 Figura tabla de valoración de controles

Por otro lado, se añadieron otros indicadores relevantes para el departamento que fueron organizados en base al framework NIST (identificar, detectar, responder, recuperar)[11].

4.2 Carga de datos

La alimentación de los indicadores seleccionados proviene de ficheros alojados en un gestor documental y bases de datos que tiene la compañía alojados en los CPD (Centro de procesamiento de datos).

4.3 Paneles

Para la presentación de la información se tomó como referencia los indicadores mencionados anteriormente organizados de la siguiente manera:

4.3.1 Objetivos SGSI

El panel expuesto en la ilustración 4.2 representa la importancia de la Seguridad de la Información para llevar a cabo con éxito sus objetivos de negocio, se compromete a cumplir los siguientes objetivos en las funciones y niveles pertinentes. La gestión de estos objetivos se realiza a través del documento **"**GEM_Gestión de objetivos_SGSI**"**.

Las acciones para cumplir con los objetivos de seguridad son establecidas y actualizadas con una periodicidad mínima anual, consistentes con la política y aprobadas por parte de la Dirección de GEM [13].

Ilustración 4.2 Panel de Objetivos SGSI GEM

4.3.2 Madurez de los dominios y distintos controles ISO27001

El panel representado en la ilustración 4.3 nos rmuestra la madurez de los dominios y controles recomendados y recogidos en el documento SoA, adicionalmente se visualizan en el Anexo B: Captura de pantalla de CM madurez de los controles que a continuación se describen sus elementos:

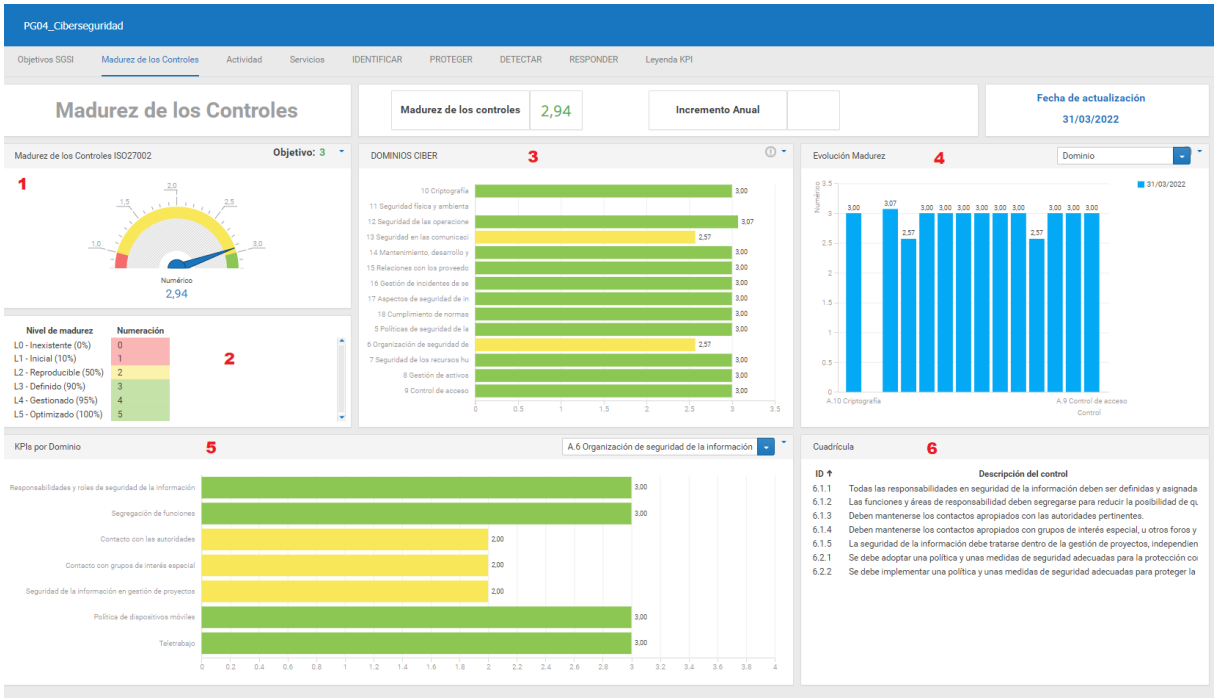


Ilustración 4.3 Panel de Madurez de los Controles

- El **elemento 1** es un diagrama medidor que representa la madurez global del SGSI en el departamento GEM y su objetivo anual.
- El **elemento 2** corresponde a valoraciones que permiten medir la fase en la que se encuentran los indicadores y dominios.
- El **elemento 3** Corresponde al nivel de madurez de cada dominio dentro del departamento GEM.
- El **elemento 4** representa la evolución de los dominios anualmente.
- El **elemento 5** corresponde a una tabla con filtro por dominios en la que se puede visualizar los controles correspondientes.
- El **elemento 6** contiene la descripción de los controles visualizados en el elemento 5.
-

4.3.3 Identificar

El proceso de Identificar, expuesto en la ilustración 4.4 hace hincapié en entender GEM y su contexto para administrar el riesgo de ciberseguridad, de los sistemas, las personas, los activos, los datos y las capacidades y que priorice sus esfuerzos de acuerdo con su estrategia:

El **elemento 1** corresponde a la representación del número de auditorías dentro del departamento GEM, notas de las mismas de acuerdo a su tipo y a su estado, auditorías retrasadas y el listado con fechas con su alcance, estado, incidencias y recomendaciones.

El **elemento 2** se relaciona con el cumplimiento normativo en donde se identifican las aplicaciones que manejan datos personales y las aplicaciones de infraestructuras críticas (número de aplicaciones y auditorías) a su vez, representa las capacitaciones vinculadas a GDPR y LPIC.

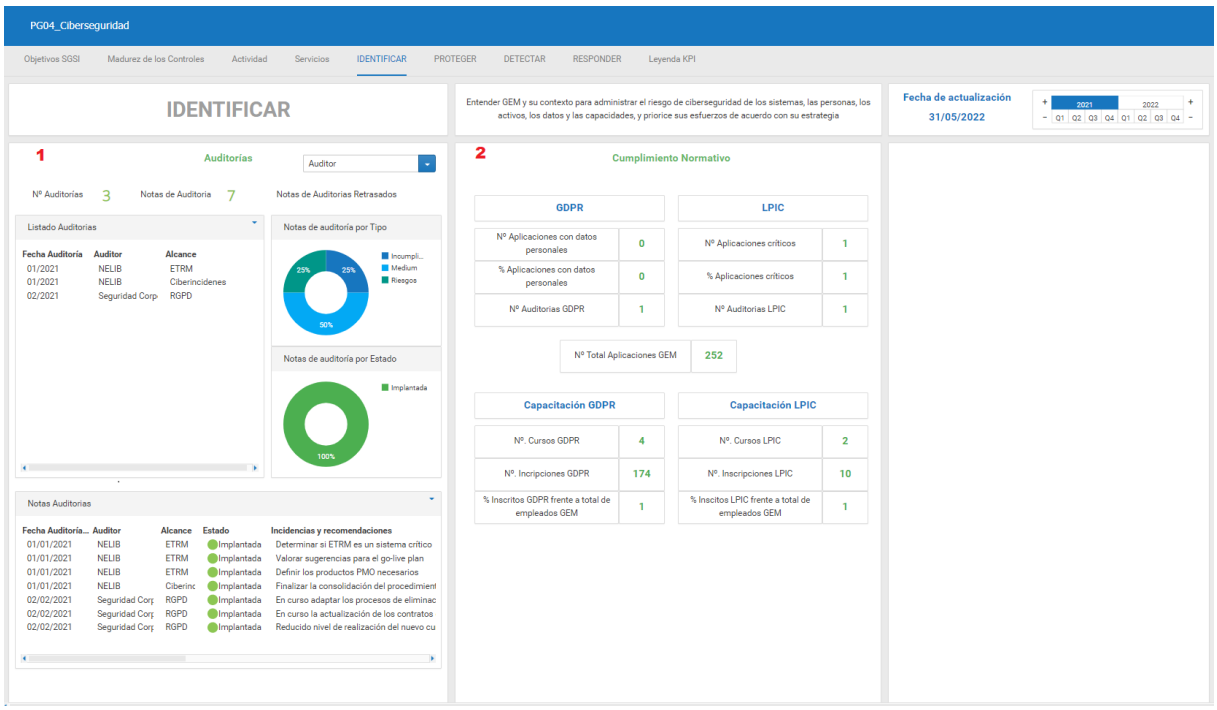


Ilustración 4.4 Panel de Identificación

4.3.4 Proteger

La ilustración 4.5 representa los indicadores vinculados a anticipar, preparar y proteger el negocio ante los riesgos de ciberseguridad.

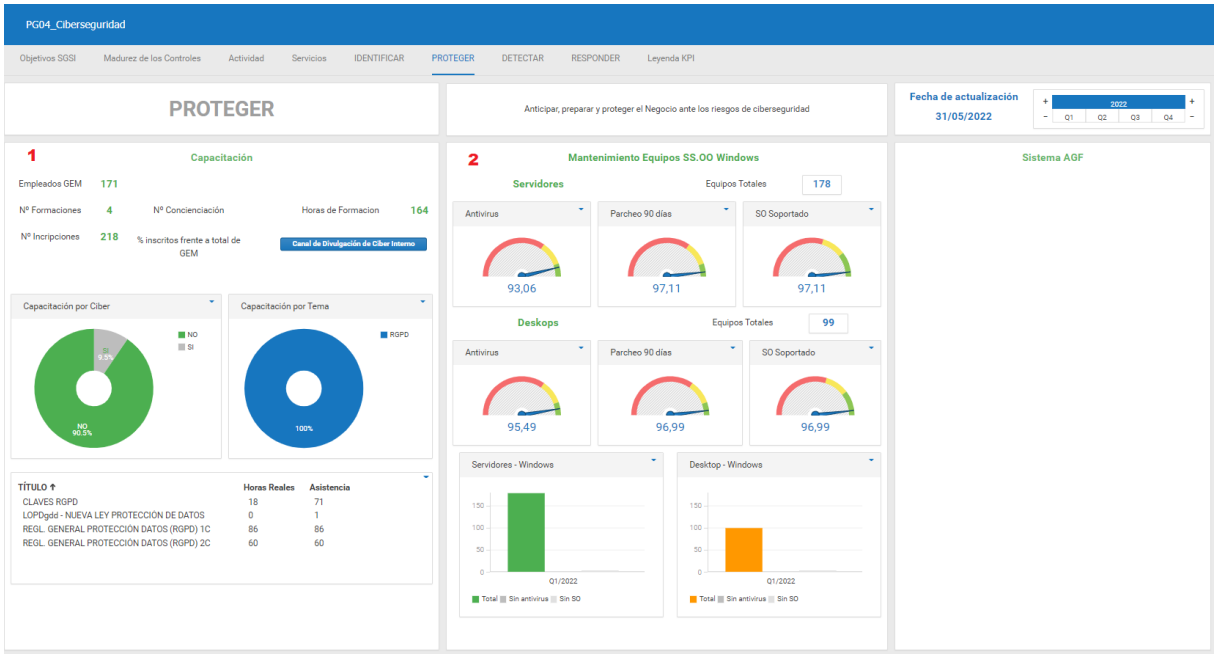


Ilustración 4.5 Panel de Protección

El **elemento 1** representa las formaciones y concienciaciones dentro del departamento GEM en materia de seguridad de información.

El **elemento 2** representa la cantidad de equipos y servidores con antivirus, parches y sistemas operativos.

4.3.5 Detectar

Detectar posibles amenazas o incidentes que puedan impactar en el negocio. Reforzar la detección ante ataques ante el incremento de riesgos. A continuación en la ilustración 4.6 se lo representa.

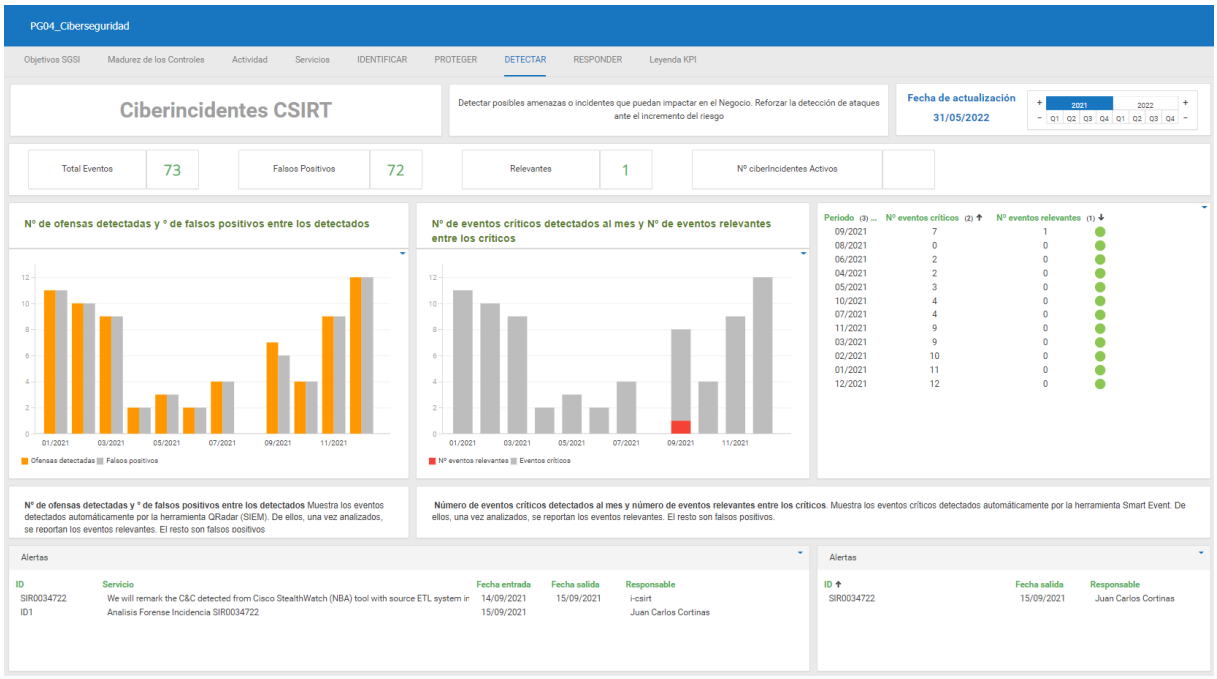


Ilustración 4.6 Panel de Detección

En este panel se visualizan los ciber incidentes detectados por el SIEM (Security Information and Event Management) del departamento en el cual nos proporcionan los eventos divididos en número de ofensas y/o de falsos positivos entre los encontrados, números de eventos críticos detectados al mes y números de eventos relevantes entre críticos.

4.3.6 Responder y recuperar

Responder ante un incidente de ciberseguridad y recuperación en caso de ser necesario. En la ilustración 4.7 se observa lo descripto.

En este panel se puede visualizar el proceso de recuperación, integrado por soluciones automatizadas, ejercicios de Red Team, Backups de equipos y servidores y tiempo medio de detección.

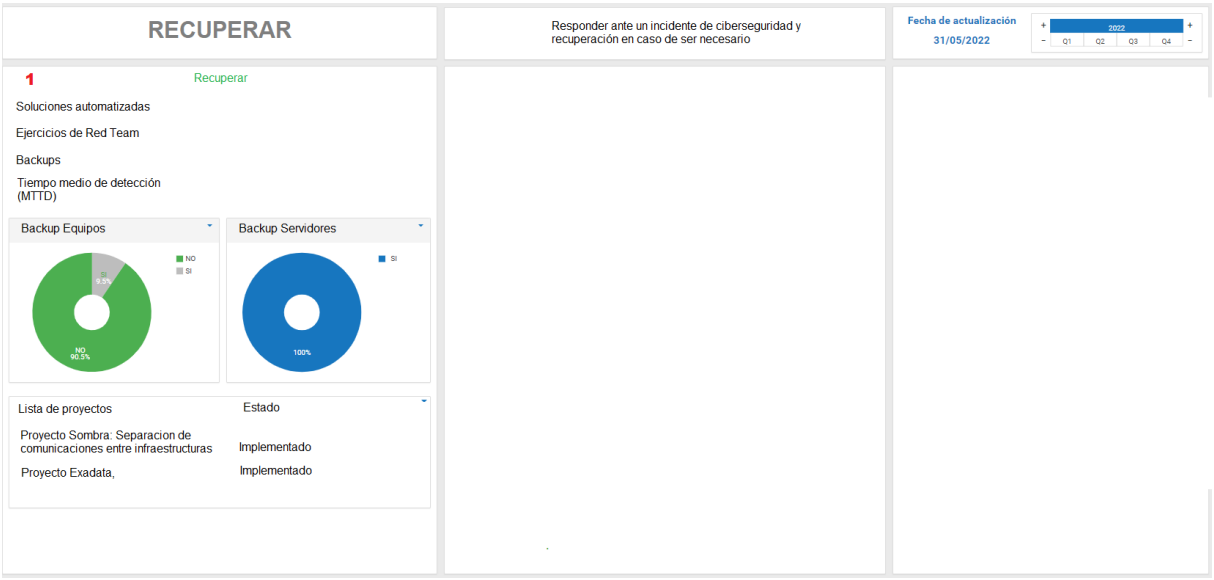
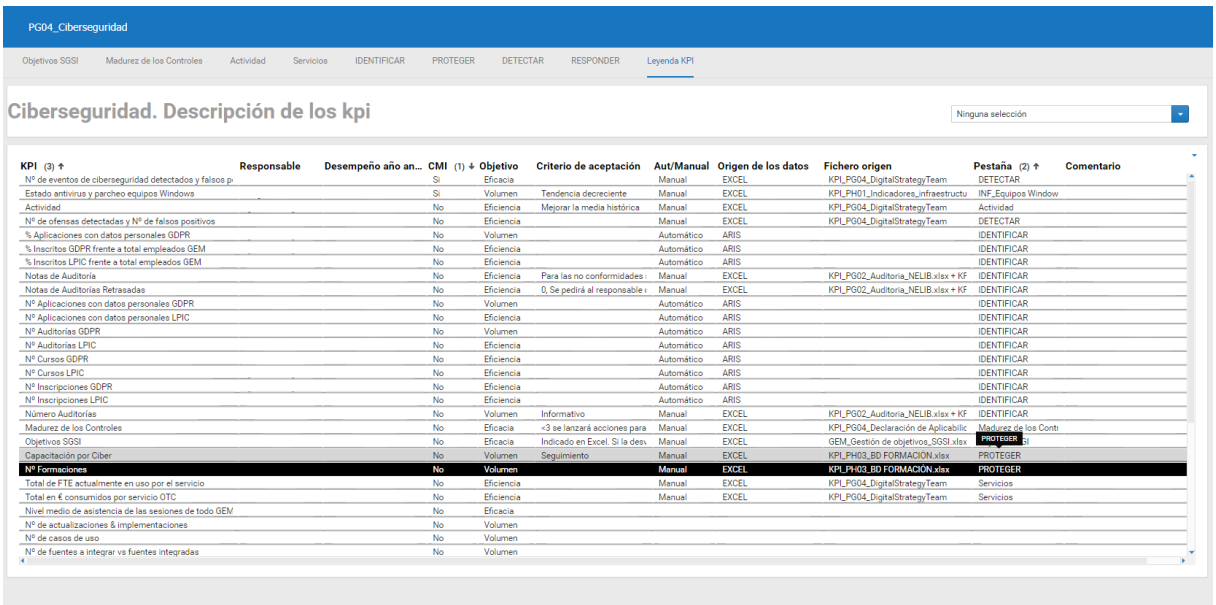


Ilustración 4.7 Panel de Recuperación

4.3.7 Leyenda KPI

En la ilustración 4.8 se visualiza la lista de indicadores con diversas propiedades, entre ellas: responsable de indicadores, ficheros de origen y panel de origen.



KPI (3)	Responsable	Desempeño año an...	CMI (1)	Objetivo	Criterio de aceptación	Aut/Manual	Origen de los datos	Fichero origen	Pestaña (2)	Comentario
Nº de eventos de ciberseguridad detectados y falsos p			Si	Eficacia		Manual	EXCEL	KPI_PG04_DigitalStrategyTeam	DETECTAR	
Estado antivirus y parcheo equipos Windows			Si	Volumen	Tendencia decreciente	Manual	EXCEL	KPI_PH01_Indicadores_Infraestructu	INF_Equipos Window	
Actividad			No	Eficiencia	Mejorar la media histórica	Manual	EXCEL	KPI_PG04_DigitalStrategyTeam	Actividad	
Nº de ofensas detectadas y Nº de falsos positivos			No	Eficiencia		Manual	EXCEL	KPI_PG04_DigitalStrategyTeam	DETECTAR	
% Aplicaciones con datos personales GDPR			No	Volumen		Automático	ARIS		IDENTIFICAR	
% Inscritos GDPR frente a total empleados GEM			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
% Inscritos LPIC frente a total empleados GEM			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Notas de Auditoría			No	Eficiencia	Para las no conformidades	Manual	EXCEL	KPI_PG02_Auditoria_NELIB.xlsx + KF	IDENTIFICAR	
Notas de Auditorías Retrasadas			No	Eficiencia	0, Se pedirá al responsable	Manual	EXCEL	KPI_PG02_Auditoria_NELIB.xlsx + KF	IDENTIFICAR	
Nº Aplicaciones con datos personales GDPR			No	Volumen		Automático	ARIS		IDENTIFICAR	
Nº Aplicaciones con datos personales LPIC			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Nº Auditorías GDPR			No	Volumen		Automático	ARIS		IDENTIFICAR	
Nº Auditorías LPIC			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Nº Cursos GDPR			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Nº Cursos LPIC			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Nº Inscripciones GDPR			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Nº Inscripciones LPIC			No	Eficiencia		Automático	ARIS		IDENTIFICAR	
Número Auditorías			No	Volumen	Informativo	Manual	EXCEL	KPI_PG02_Auditoria_NELIB.xlsx + KF	IDENTIFICAR	
Madurez de los Controles			No	Eficacia	<3 se lanzará acciones para	Manual	EXCEL	KPI_PG04_Declaración de Aplicabilic	Madurez de los Contr	
Objetivos SGSI			No	Eficacia	Indicado en Excel. Si la desv	Manual	EXCEL	GEM_Gestión de objetivos_SGSI.xlsx	PROTEGER	
Capacitación por Ciber			No	Volumen	Seguimiento	Manual	EXCEL	KPI_PH03_BD FORMACION.xlsx	PROTEGER	
Nº Formaciones			No	Volumen		Manual	EXCEL	KPI_PH03_BD FORMACION.xlsx	PROTEGER	
Total de FTE actualmente en uso por el servicio			No	Eficiencia		Manual	EXCEL	KPI_PG04_DigitalStrategyTeam	Servicios	
Total en € consumidos por servicio OTC			No	Eficiencia		Manual	EXCEL	KPI_PG04_DigitalStrategyTeam	Servicios	
Nivel medio de asistencia de las sesiones de todo GEM			No	Eficacia						
Nº de actualizaciones & implementaciones			No	Volumen						
Nº de casos de uso			No	Volumen						
Nº de fuentes a integrar vs fuentes integradas			No	Volumen						

Ilustración 4.8 Leyenda KPI

5 RESULTADOS

Una vez finalizado el proceso de elaboración de los cuadros de mando se pueden ofrecer los siguientes resultados obtenidos del proyecto:

- Los cuadros de mando en su reelaboración tuvieron una marcada importancia como material de aporte para la certificación de la norma ISO 27000.
- Se logró mayor organización en el departamento GEM.
- Los cuadros de mando ayudaron a que los directivos tengan mayor visualización sobre los controles con los que cuenta la norma ISO y su gran importancia.
- Se logró monitorizar todos los parámetros de la empresa y disponer de una imagen real de lo que ocurre dentro de la misma.
- Disponer de esta visión global y real facilitó la toma de decisiones.
- Se añadieron nuevos paneles, los cuales, enriquecieron la organización de diversas áreas de la empresa.

5.1 Análisis financiero

En este apartado se detallará el coste económico desde el punto de vista de ciberseguridad que ha llevado realizar el proyecto teniendo en cuenta las horas dedicadas, las cuales se encuentran mencionadas en la tabla 2. “Listado de tareas”, página….

Han sido necesarias 604 horas y que el coste de cada hora es de 35 euros, sería un total de 17640 euros.

6 CONCLUSIONES

Algunas conclusiones parciales sobre aspectos relevantes durante la ejecución de este trabajo, han sido las siguientes:

Conclusiones respecto a la utilidad e importancia de los cuadros de mando: teniendo en cuenta que este proyecto está basado en la reelaboración y actualización de los cuadros de mando a partir del SGSI, se pudo visualizar que el departamento GEM se organizó mejor, involucrando diferentes áreas de la empresa para mantener actualizados los ficheros y bases de datos que alimentan los indicadores del cuadro de mando.

Otro beneficio que se puede observar es el ahorro de tiempo en las planificaciones futuras, ya que al haber más información organizada y resumida en los cuadros de mando cada equipo tenía mayor claridad sobre los procesos actuales.

El aporte realizado con nuevos paneles hizo posible lo anteriormente mencionado, teniendo como el resultado mas importante, la conformidad de todas las áreas involucradas.

Conclusiones respecto a la utilización de la Norma ISO 27001 en donde fue clave para la empresa su aplicación en la forma en que se ha analizado los dominios y controles, deja abierto un camino de mejoras en base a los objetivos planteados por el departamento GEM.

Conclusiones con respecto al enriquecimiento personal: A partir de la elaboración de este proyecto me permitió (como responsable de poca experiencia en el área de elaboración de cuadros de mandos) conocer con mayor profundidad las virtudes y defectos de los mismos, generándome una visión y facilitándome la detección de oportunidades de mejora.

Como así también fue una gran oportunidad de aprendizaje con el fin de enriquecer mis conocimientos en el área, a la vez de exponer todo lo aprendido en el cursado del master, como una forma de nutrirme de experiencia teórica y práctica dentro de la compañía.

7 Bibliografía

[1] INCIBE, “https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-el-sector-las-asociaciones,” Apr. 01, 2022.

[2] Ing. Felipe Gómez Analista Informático, “https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion#:~:text=Garantiza%20un%20alto%20nivel%20de,parte%20de%20personas%20no%20autorizadas.”

[3] National Institute of Standards and Technology, “https://www.nist.gov/cyberframework/online-learning/components-framework,” Feb. 06, 2018.

[4] Iberdrola GEM, “Normativa Ciberseguridad GEM_v7”.

[5] Iberdrola SA, “11. Política de riesgos de ciberseguridad 2022_Def 003 (002).”

[6] Iberdrola GEM, “Declaración de Aplicabilidad (SoA)”.

[7] Iberdrola GEM, “Asegurar la ciberseguridad y la privacidad.”

[8] Iberdrola GEM, “DIRECCION DE SEGURIDAD CORPORATIVA SISTEMA DE GESTION DE LA CALIDAD TÍTULO: PROCEDIMIENTO DE COORDINACIÓN Y RESPUESTA A CIBERINCIDENTES.”

[9] Iberdrola GEM, “GEM_ES_MG00_Manual de Gestión de Seguridad de la Información”.

[10] N. Española, “Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015),” 2017. [Online]. Available: www.aenor.com

[11] OEA-AWS, “chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf,” 2019.

[12] ARIS, “https://aris-process-mining.com/es/.”

[13] Iberdrola GEM, “GEM_Gestión de objetivos_SGSI”.

8 Anexo

8.1 Anexo A: Declaración de Aplicabilidad (SoA)

Declaración de Aplicabilidad (SoA)					
ID	**Control**	**Descripción del control**	**Nivel de madurez**	**Numérico**	**Documentación de soporte**
5	**A.5 Políticas de seguridad de la información**			**3**	
5.1	**Dirección de gestión de seguridad de la información**				**1.1.Politica_seguridad_corporativa. Consta de:** **politica_proteccion_datos** **Política de riesgos de ciberseguridad** **1.2. politica_general_control_riesgos** **1.3. Requisitos adicionales de Ciberseguridadv.1.ES** **2.Normativa Ciberseguridad GEM** **Framework de Seguridad Cloud (S4)** **Modelo de Gobierno cloud (S4)**
5.1.1	Políticas de seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	L3 - Definido (90%)	3	1.1. Politica_seguridad_corporativa. Consta de: politica_proteccion_datos Política de riesgos de ciberseguridad 1.2. politica_general_control_riesgos 1.3. Requisitos adicionales de Ciberseguridadv.1.ES 2.Normativa Ciberseguridad GEM Framework de Seguridad Cloud (S4) Modelo de Gobierno cloud (S4)
5.1.2	Revisión de las políticas de seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	L3 - Definido (90%)	3	1.1.Politica_seguridad_corporativa. Consta de: politica_proteccion_datos Política de riesgos de ciberseguridad 1.2. politica_general_control_riesgos 1.3.Requisitos adicionales de Ciberseguridadv.1.ES 2.Normativa Ciberseguridad GEM Framework de Seguridad Cloud (S4) Modelo de Gobierno cloud (S4)
6	**A.6 Organización de seguridad de la información**			**2,2857143**	
6.1	**Organización Interna**				**1.esquema_modelo_3_lineas_defensa_PDF** **2. GEM_GB_PG02_20_Organización_Organisation** **Manual del Sistema de Gestión SGSI**
6.1.1	Responsabilidades y roles de seguridad de la información	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	L2 - Reproducible (50%)	2	1.esquema_modelo_3_lineas_defensa_PDF 2. GEM_GB_PG02_20_Organización_Organisation Manual del Sistema de Gestión SGSI
6.1.2	Segregación de funciones	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no	L2 - Reproducible (50%)	2	1.esquema_modelo_3_lineas_defensa_PDF 2. GEM_GB_PG02_20_Organización_Organisation Manual del Sistema de Gestión SGSI

		intencionadas o usos indebidos de los activos de la organización.			
6.1.3	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.	L2 - Reproducible (50%)	2	1.esquema_modelo_3_lineas_defensa_PDF 2. GEM_GB_PG02_20_Organización_Organisation Manual del Sistema de Gestión SGSI
6.1.4	Contacto con grupos de interés especial	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	L2 - Reproducible (50%)	2	1.esquema_modelo_3_lineas_defensa_PDF 2. GEM_GB_PG02_20_Organización_Organisation Manual del Sistema de Gestión SGSI
6.1.5	Seguridad de la información en gestión de proyectos	La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	L2 - Reproducible (50%)	2	1.esquema_modelo_3_lineas_defensa_PDF 2. GEM_GB_PG02_20_Organización_Organisation Manual del Sistema de Gestión SGSI
6.2	**Teletrabajo y dispositivos móviles**				Norma global dispositivos portátiles
6.2.1	Política de dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	L3 - Definido (90%)	3	Norma global dispositivos portátiles
6.2.2	Teletrabajo	Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	L3 - Definido (90%)	3	0501NormativaTeletrabajo 0506GuiaBuenasPracticasTeletrabajo
7	**A.7 Seguridad de los recursos humanos**			**2,8333333**	**Codigo ético proveedor_sobre todo enfocado a la protección de datos NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola**
7.1	**Antes del empleo**				
7.1.1	Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	L3 - Definido (90%)	3	Si el auditor pide la evidencia se le proporcionará. Por confidencialidad no se proporcionan las evidencias en este momento.
7.1.2	Términos y condiciones de empleo	Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y	L3 - Definido (90%)	3	Contrato tipo.

		condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.			
7.2	**Durante el empleo**				
7.2.1	Responsabilidades de gestión	La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	L3 - Definido (90%)	3	Respecto a contratistas: Codigo ético proveedor_sobre todo enfocado a la protección de datos NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola
7.2.2	Capacitación, educación y concienciación de seguridad de información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	L2 - Reproducible (50%)	2	Plan de formación y concienciación.
7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	L3 - Definido (90%)	3	Convenio colectivo aplicable y Estatuto de los trabajadores.
7.3	**Terminación y cambio de empleo**				
7.3.1	Responsabilidades ante la finalización o cambio	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	L3 - Definido (90%)	3	Contrato tipo.
8	**A.8 Gestión de activos**			2,7	1.Norma global de uso aceptable de la ciber infraestructura del Grupo 1.NormaGlobalClasificacionCiberactivos 1.Norma Global para la Protección de la Información 2.GEM_ES_PG02_41_Control de la información documentada 2. Normativa de ciberseguridad de GEM
8.1	**Responsabilidad de activos**				
8.1.1	Inventario de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente	L3 - Definido (90%)	3	NormaGlobalClasificacionCiberactivos

		identificados y debe elaborarse y mantenerse un inventario.			
8.1.2	Propiedad de los activos	Todos los activos que figuran en el inventario deben tener un propietario.	L3 - Definido (90%)	3	NormaGlobalClasificacionCiberactivos
8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	L3 - Definido (90%)	3	Norma global de uso aceptable de la ciberinfraestructura del Grupo (NormaGlobalUtilizacionCiberinfraestructuraGrupo.pdf)
8.1.4	Devolución de los activos	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	L3 - Definido (90%)	3	Norma global de uso aceptable de la ciberinfraestructura del Grupo (NormaGlobalUtilizacionCiberinfraestructuraGrupo.pdf)
8.2	**Clasificación de información**				
8.2.1	Clasificación de la información	La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	L2 - Reproducible (50%)	2	Norma Global para la Protección de la Información; GEM_ES_PG02_41_Control de la información documentada 2. Normativa de ciberseguridad de GEM
8.2.2	Etiquetado de información	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	L2 - Reproducible (50%)	2	Norma Global para la Protección de la Información
8.2.3	Manipulado de la información	Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	L2 - Reproducible (50%)	2	Norma Global para la Protección de la Información
8.3	**Manipulación de los medios**				
8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	L3 - Definido (90%)	3	Norma Global para la Protección de la Información

8.3.2	Eliminación de soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	L3 - Definido (90%)	3	Norma Global para la Protección de la Información
8.3.3	Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	L3 - Definido (90%)	3	Norma Global para la Protección de la Información
9	**A.9 Control de acceso**			3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestion de usuarios (PEDIR A VIRGINIA)
9.1	**Requerimientos del negocio para el control de acceso**				
9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol ~~2. Gestion de usuarios (Virginia)~~
9.1.2	Acceso a redes y servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.2	**Gestión de acceso de usuario**				
9.2.1	Registro de usuario	Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.2.2	Aprovisionamiento de acceso de usuarios	Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.2.3	Gestión de privilegiados los derechos de acceso	La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.2.4	Gestión de la información secreta de autenticación de usuarios	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.2.5	Informe sobre los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)

9.2.6	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.3	**Responsabilidades del usuario**				
9.3.1	Uso de la información de autenticación secreta	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.4	**Aplicaciones y el sistema de control de acceso**				
9.4.1	Restricción de acceso de la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.4.2	Aseguramiento de los procedimientos del inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.4.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.4.4	Uso de programas de utilidad privilegiada	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
9.4.5	Control de acceso al código fuente del programa	Se debe restringir el acceso al código fuente de los programas.	L3 - Definido (90%)	3	1.Norma de Gobierno de Accesos 2.Normativa Ciberseguridad GEM 2.GEM_ES_611102_1_Gestion de usuarios y accesos al Sistema de Telecontrol 2. Gestión de usuarios (Virginia)
10	**A.10 Criptografía**			3	1.Adquisición certificados_v7 2.Normativa Ciberseguridad GEM
10.1	**Controles criptográficos**				

10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	L3 - Definido (90%)	3	1.Adquisición certificados_v7 2.Normativa Ciberseguridad GEM
10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	L3 - Definido (90%)	3	1.Adquisición certificados_v7 2.Normativa Ciberseguridad GEM
11	**A.11 Seguridad física y ambiental**			1	Pendiente (Virginia)
11.1	**Zonas seguras**				
11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	L1 - Inicial (10%)	1	
11.1.2	Controles de entrada física	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	L1 - Inicial (10%)	1	
11.1.3	Asegurar las oficinas, habitaciones e instalaciones	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	L1 - Inicial (10%)	1	
11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	L1 - Inicial (10%)	1	
11.1.5	Trabajando en zonas seguras	Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	L1 - Inicial (10%)	1	
11.1.6	Entrega y zonas de carga	Deben controlarse 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.	L1 - Inicial (10%)	1	
11.2	**Equipamiento**				

11.2.1	Ubicación y protección de equipos	Los equipos deben situarse o protegerse 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.	L1 - Inicial (10%)	1	
11.2.2	Utilidades de apoyo	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	L1 - Inicial (10%)	1	
11.2.3	Cableado de seguridad	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	L1 - Inicial (10%)	1	
11.2.4	Mantenimiento de equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	L1 - Inicial (10%)	1	
11.2.5	Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	L1 - Inicial (10%)	1	
11.2.6	Seguridad de equipos y activos fuera de los locales	Deben aplicarse 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.	L1 - Inicial (10%)	1	
11.2.7	Eliminación o reutilización de equipos segura	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	L1 - Inicial (10%)	1	
11.2.8	Equipo del usuario desatendido	Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	L1 - Inicial (10%)	1	
11.2.9	Política de mesas y pantallas limpias	Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	L1 - Inicial (10%)	1	

12	**A.12 Seguridad de las operaciones**			2,1428571	1.NormaGlobalSeguridadOperacionComunicacionesRed.pdf 2.Infra: GEM_ES_PH01_24_Actualización de software de infraestructura GEM_ES_PH01_22_Realizar pruebas operatividad sistemas informáticos (servidores y equipos de red) GEM_ES_611102_2_Procesos de Mantenimiento del Sistema de Telecontrol GEM_ES_612201_1_Pruebas operatividad sistemas informáticos GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra 2.Soluciones: Guía de puesta en producción de aplicaciones v2.4 GEM_ES_PH01_85_Paso entre entornos Normativa Ciberseguridad GEM
12.1	**Las responsabilidades y los procedimientos operacionales**				
12.1.1	Documentar los procedimientos de operación	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.	L3 - Definido (90%)	3	GEM_ES_612201_1_Pruebas operatividad sistemas informáticos GEM_ES_611102_2_Procesos de Mantenimiento del Sistema de Telecontrol GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra
12.1.2	Gestión del cambio	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.	L1 - Inicial (10%)	1	NormaGlobalSeguridadOperacionComunicacionesRed.pdf
12.1.3	Administración de la capacidad	Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	L3 - Definido (90%)	3	NormaGlobalSeguridadOperacionComunicacionesRed.pdf
12.1.4	Separación del desarrollo, entornos de pruebas y operacionales	Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	L2 - Reproducible (50%)	2	NormaGlobalSeguridadOperacionComunicacionesRed.pdf Guía de puesta en producción de aplicaciones v2.4 GEM_ES_PH01_85_Paso entre entornos
12.2	**Protección contra el software malicioso (malware)**				
12.2.1	Controles contra el código malicioso	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	L3 - Definido (90%)	3	NormaGlobalSeguridadOperacionComunicacionesRed.pdf Normativa Ciberseguridad GEM
12.3	**Copias de seguridad**				
12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política	L3 - Definido (90%)	3	GEM_ES_612101_2_Sistemas backup y restauración información

		de copias de seguridad acordada.			
12.4	**Registros y supervisión**				
12.4.1	Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	L1 - Inicial (10%)	1	
12.4.2	Protección de la información de registro	Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	L1 - Inicial (10%)	1	
12.4.3	Administrador y operación de registros	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	L1 - Inicial (10%)	1	
12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.	L1 - Inicial (10%)	1	
12.5	**Control de software operacional**				
12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación del software en explotación.	L2 - Reproducible (50%)	2	NormaGlobalSeguridadOperacionComunicacionesRed.pdf
12.6	**Gestión de las vulnerabilidades técnicas**				
12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	L3 - Definido (90%)	3	NormaGestionVulnerabilidades.pdf NormaGlobalSeguridadOperacionComunicacionesRed.pdf
12.6.2	Restricciones a la instalación del software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	L3 - Definido (90%)	3	NormaGlobalSeguridadOperacionComunicacionesRed.pdf

12.7	**Consideraciones de auditoría de sistemas de información**				
12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadOperacionComunicacionesRed.pdf 2. GEM_ES_PG02_30_Gestión de No Conformidades y Mejoras
13	**A.13 Seguridad en las comunicaciones**			2,55	1.GEM_ES_PH01_22_Realizar pruebas operatividad sistemas informáticos (servidores y equipos de red) 2.NormaGlobalSeguridadOperacionComunicacionesRed.pdf 2.proveedores_OS_ES_01.pdf
13.1	**Gestión de seguridad de red**				
13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	L3 - Definido (90%)	3	NormaGlobalSeguridadOperacionComunicacionesRed.pdf
13.1.2	Seguridad de servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	L3 - Definido (90%)	3	NormaGlobalSeguridadOperacionComunicacionesRed.pdf
13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	L3 - Definido (90%)	3	
13.2	**Transferencia de la información**				
13.2.1	Los procedimientos y las políticas de transferencia de información	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	L1 - Inicial (10%)	1	
13.2.2	Acuerdos sobre transferencia de información	Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	L1 - Inicial (10%)	1	

13.2.3	Mensajería electrónica	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	L1 - Inicial (10%)	1	
13.2.4	Acuerdos de confidencialidad o no divulgación	Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación	L1 - Inicial (10%)	1	proveedores_OS_ES_01.pdf
14	**A.14 Mantenimiento, desarrollo y adquisición del sistema**			2,9230769	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.1	**Requisitos de seguridad de sistemas de información**				
14.1.1	Especificación y análisis de requisitos de seguridad de información	Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.1.2	Asegurar servicios de aplicación en las redes públicas	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.1.3	Protegiendo las transacciones de servicios de aplicación	La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2	**Seguridad en los procesos de desarrollo y soporte**				

14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.2	Procedimientos de control de cambio de sistema	La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.3	Revisión técnica de las aplicaciones después de los cambios de la plataforma de funcionamiento	Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.4	Restricciones sobre los cambios en los paquetes de software	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.5	Garantizar los principios de ingeniería de sistema	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.7	Desarrollo subcontratado	El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.8	Pruebas de seguridad del sistema	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
14.2.9	Pruebas de aceptación del sistema	Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	L3 - Definido (90%)	3	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1

14.3	**Datos de prueba**				
14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	L2 - Reproducible (50%)	2	1.NormaGlobalSeguridadDesarrolloAdquisicionMantenimientoActivos Especificaciones de seguridad para Servicios en la Nube (Soluciones) Directrices de Construcción de Aplicaciones Seguras 2. GEM_ES_PH01_80_Procedimiento de gestión de proyectos (Digital) Normativa de ciberseguridad de GEM Creación de guías de Desarrollo Seguro (S5) Guía de Desarrollo de Software GEM (S5)- PEDIR A VIRGINIA Formaciones de desarrollo de código seguro (S5) Secure Applications Guidelines-ES v1.1
15	**A.15 Relaciones con los proveedores**			3	NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES COMPR-GECOM-PR-0001_ES
15.1	**Seguridad de la información en relaciones con los proveedores**				
15.1.1	Política de seguridad de la información para relaciones con los proveedores	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 deben acordarse con el proveedor y quedar documentados.	L3 - Definido (90%)	3	COMPR-GECOM-PR-0001_ES NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES
15.1.2	Abordar la seguridad dentro de los acuerdos de proveedor	Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.	L3 - Definido (90%)	3	COMPR-GECOM-PR-0001_ES NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES
15.1.3	Cadena de suministro de tecnología información y comunicación	Los acuerdos con proveedores deben incluir requisitos 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.	L3 - Definido (90%)	3	COMPR-GECOM-PR-0001_ES NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES
15.2	**Gestión de entrega de servicio de proveedores**				
15.2.1	Control y revisión de la provisión de servicios del proveedor	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	L3 - Definido (90%)	3	COMPR-GECOM-PR-0001_ES NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la	L3 - Definido (90%)	3	COMPR-GECOM-PR-0001_ES NormaGlobalGestionRiesgosCiberseguridadTercerasPartes Protocolo Subcontratación Servicios Iberdrola Requisitos adicionales de Ciberseguridadv.1.ES

		información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.			
16	**A.16 Gestión de incidentes de seguridad de información**			3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE; Manual GESTION EMERGENCIAS GENERICO; EN_Iberdrola Global Incident Response Framework; 2. Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1	**Gestión de incidentes de seguridad de la información y las mejoras**				
16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE;Manual GESTION EMERGENCIAS GENERICO;EN_Iberdrola Global Incident Response Framework; 2.Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.2	Notificación de eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE; Manual GESTION EMERGENCIAS GENERICO; EN_Iberdrola Global Incident Response Framework; 2. Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.3	Notificación de puntos débiles de la seguridad	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE; Manual GESTION EMERGENCIAS GENERICO; EN_Iberdrola Global Incident Response Framework; 2. Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE;Manual GESTION EMERGENCIAS GENERICO;EN_Iberdrola Global Incident Response Framework; 2.Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE;Manual GESTION EMERGENCIAS GENERICO;EN_Iberdrola Global Incident Response Framework; 2.Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE;Manual GESTION EMERGENCIAS GENERICO;EN_Iberdrola Global Incident Response Framework; 2.Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf
16.1.7	Recopilación de evidencias	La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.	L3 - Definido (90%)	3	1.FINAL_IBERDROLA_Plan de Gestión de Ciber Incidentes (PGCI)_v.1.1.0 POP-SESPA-PRC-01_rev4; ORE;Manual GESTION EMERGENCIAS GENERICO;EN_Iberdrola Global Incident Response Framework; 2.Iberdrola_DRAFT_Manual de Respuesta Técnica_Ransomware.V.0.0. ProcedimientoAnteAustraccionPerdidaMaterial.pdf

17	**A.17 Aspectos de seguridad de información de gestión de continuidad del negocio**			2,75	GEM_ES_PH01_25_Plan de recuperación ante desastres GEM_ES_612501_2_Instrucción recuperación Datos en Red GEM_ES_612502_1_Instrucción recuperación Base de Datos GEM_ES_612503_4_Instrucción de recuperación de máquinas virtuales GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra BIA_GEM_TELECONTROL 19102020_revisado BIA_GEM_INDES 04112020 INDES - Procedimiento Disaster Recovery_Iberdrola GEM_v1 TELECONTROL - Procedimiento Disaster Recovery_Iberdrola GEM_v2 Test DR para TELECONTROL- Dic20. Resultado OK Pruebas cada 3 meses. Test DR para INDES- Dic 20 (Pablo Cobreros- soluciones).
17.1	**Continuidad de seguridad de información**				
17.1.1	Planificación de continuidad de seguridad de información	La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	L3 - Definido (90%)	3	GEM_ES_PH01_25_Plan de recuperación ante desastres GEM_ES_612501_2_Instrucción recuperación Datos en Red GEM_ES_612502_1_Instrucción recuperación Base de Datos GEM_ES_612503_4_Instrucción de recuperación de máquinas virtuales GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra BIA_GEM_TELECONTROL 19102020_revisado BIA_GEM_INDES 04112020 INDES - Procedimiento Disaster Recovery_Iberdrola GEM_v1 TELECONTROL - Procedimiento Disaster Recovery_Iberdrola GEM_v2 Test DR para TELECONTROL- Dic20. Resultado OK Pruebas cada 3 meses. Test DR para INDES- Dic 20 (Pablo Cobreros- soluciones).
17.1.2	Implementación de continuidad de seguridad de información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	L3 - Definido (90%)	3	GEM_ES_PH01_25_Plan de recuperación ante desastres GEM_ES_612501_2_Instrucción recuperación Datos en Red GEM_ES_612502_1_Instrucción recuperación Base de Datos GEM_ES_612503_4_Instrucción de recuperación de máquinas virtuales GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra BIA_GEM_TELECONTROL 19102020_revisado BIA_GEM_INDES 04112020 INDES - Procedimiento Disaster Recovery_Iberdrola GEM_v1 TELECONTROL - Procedimiento Disaster Recovery_Iberdrola GEM_v2 Test DR para TELECONTROL- Dic20. Resultado OK Pruebas cada 3 meses. Test DR para INDES- Dic 20 (Pablo Cobreros- soluciones).
17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de información	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	L3 - Definido (90%)	3	GEM_ES_PH01_25_Plan de recuperación ante desastres GEM_ES_612501_2_Instrucción recuperación Datos en Red GEM_ES_612502_1_Instrucción recuperación Base de Datos GEM_ES_612503_4_Instrucción de recuperación de máquinas virtuales GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra BIA_GEM_TELECONTROL 19102020_revisado BIA_GEM_INDES 04112020 INDES - Procedimiento Disaster Recovery_Iberdrola GEM_v1 TELECONTROL - Procedimiento Disaster Recovery_Iberdrola GEM_v2 Test DR para TELECONTROL- Dic20. Resultado OK Pruebas cada 3 meses. Test DR para INDES- Dic 20 (Pablo Cobreros- soluciones).
17.2	**Redundancia**				
17.2.1	Disponibilidad de instalaciones de procesamiento de información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	L2 - Reproducible (50%)	2	GEM_ES_PH01_25_Plan de recuperación ante desastres GEM_ES_612501_2_Instrucción recuperación Datos en Red GEM_ES_612502_1_Instrucción recuperación Base de Datos GEM_ES_612503_4_Instrucción de recuperación de máquinas virtuales GEM_ES_612504_1_Instrucción aislamiento red Sistema Sombra BIA_GEM_TELECONTROL 19102020_revisado BIA_GEM_INDES 04112020 INDES - Procedimiento Disaster Recovery_Iberdrola GEM_v1 TELECONTROL - Procedimiento Disaster Recovery_Iberdrola GEM_v2 Test DR para TELECONTROL- Dic20. Resultado OK Pruebas cada 3 meses. Test DR para INDES- Dic 20 (Pablo Cobreros- soluciones).
18	**A.18 Cumplimiento de normas**			1,625	politica_proteccion_datos Programa para la prevención de la comisión de delitos (PDD)

18.1	**Cumplimiento de los requisitos legales y contractuales**				Iberdrola_FINAL_Procedimiento de Notificación a Autoridades_V.1.0.0
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	L3 - Definido (90%)	3	*No se adjunta como evidencia el PDD (Programa para la prevención de la comisión de delitos) por confidencialidad*
18.1.2	Derechos de propiedad intelectual	Deben implementarse 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.	L1 - Inicial (10%)	1	
18.1.3	Protección de registros	Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	L1 - Inicial (10%)	1	
18.1.4	Privacidad y protección de información personal identificable	Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	L3 - Definido (90%)	3	politica_proteccion_datos
18.1.5	Regulación de controles criptográficos	Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	L2 - Reproducible (50%)	2	
18.2	**Revisiones sobre seguridad de la información**				GEM_ES_PG02_50_Auditorías internas del SG
18.2.1	Revisión independiente de seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios	L1 - Inicial (10%)	1	

		significativos en la implantación de la seguridad.			
18.2.2	Cumplimiento de normas y políticas de seguridad	Los directivos deben asegurarse 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	L1 - Inicial (10%)	1	
18.2.3	Revisión del cumplimiento técnico	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	L1 - Inicial (10%)	1	

8.2 Anexo B: Captura de Pantalla de CM Madurez de los controles

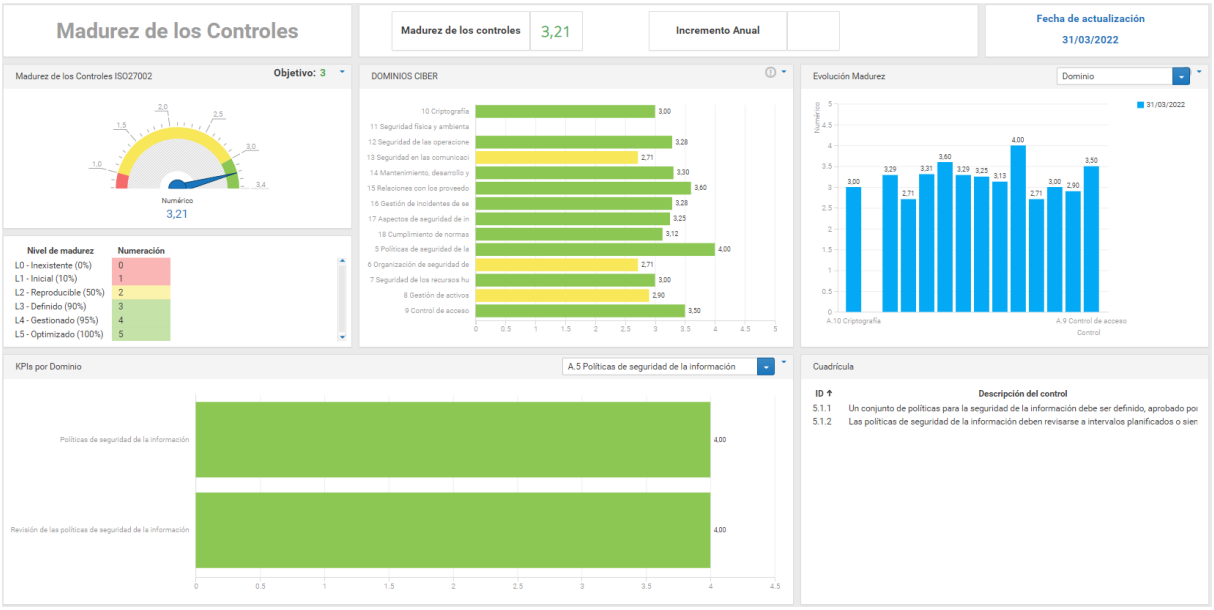


Ilustración 8.1 CM Madurez de los Controles Dominio 5: Política de Seguridad de la Información

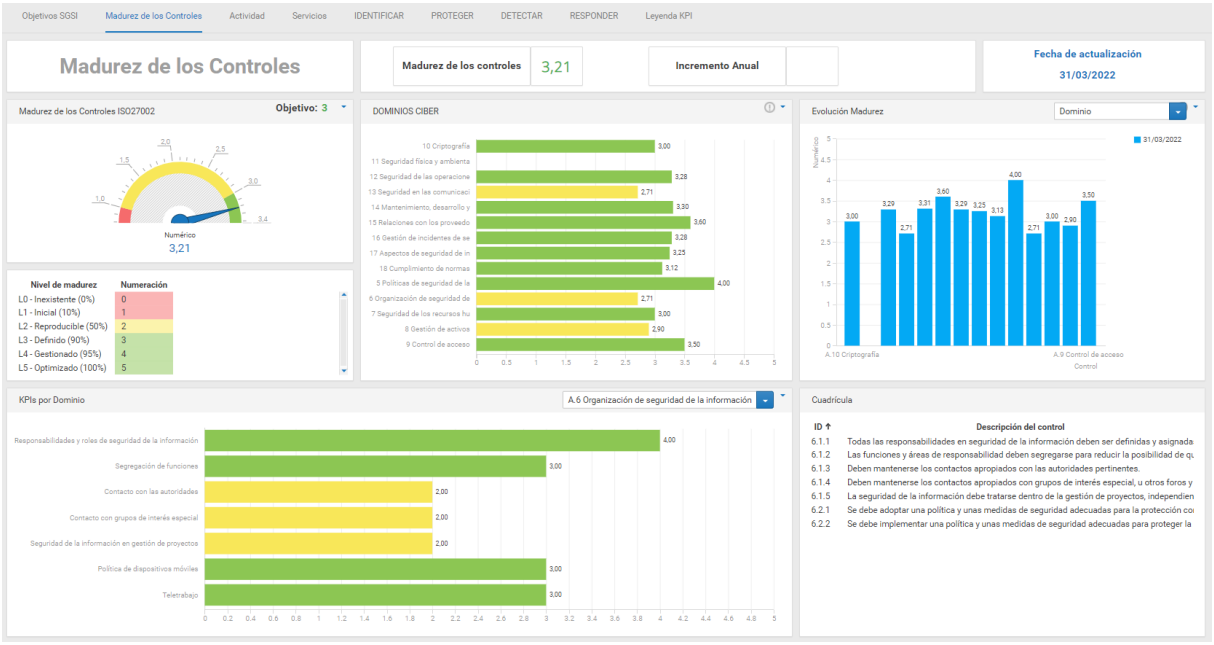


Ilustración 8.2 CM Madurez de los Controles Dominio 6: Organización de Seguridad de la Información

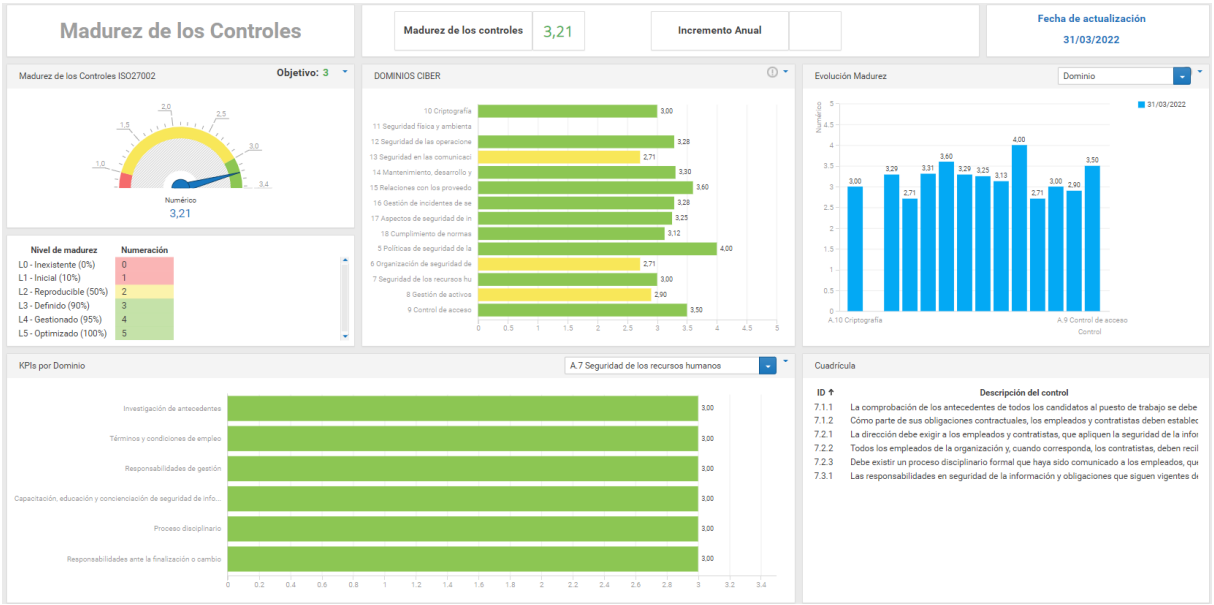


Ilustración 8.3 CM Madurez de los Controles Dominio 7: Seguridad de los Recursos Humanos

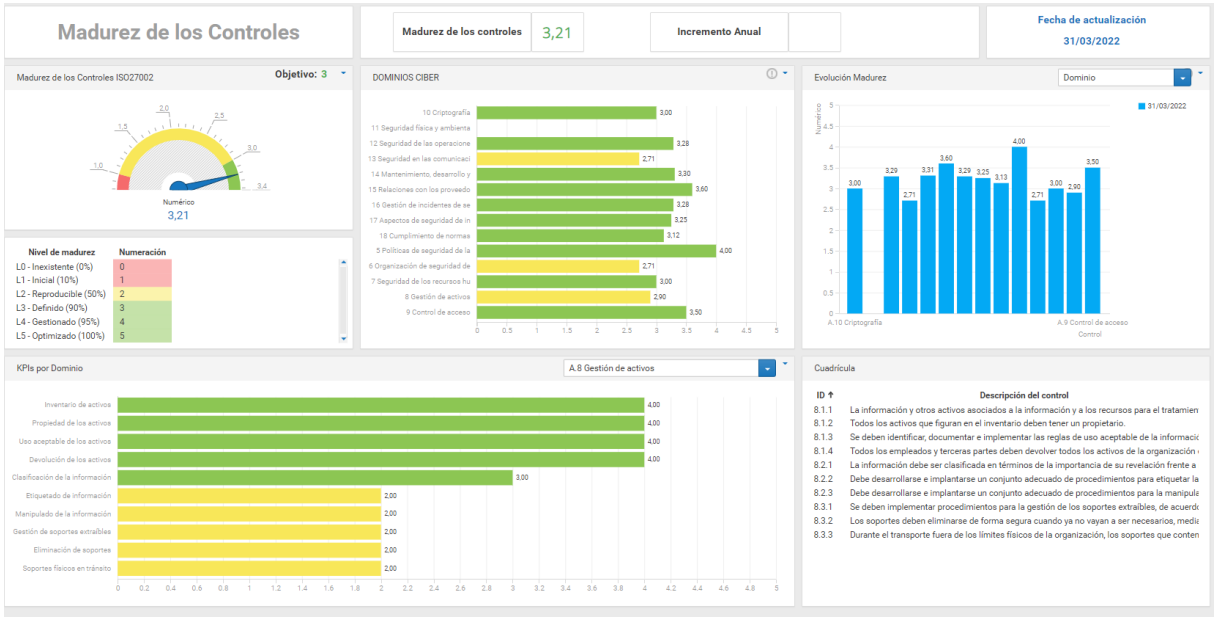


Ilustración 8.4 CM Madurez de los Controles Dominio 8: Gestión de activos

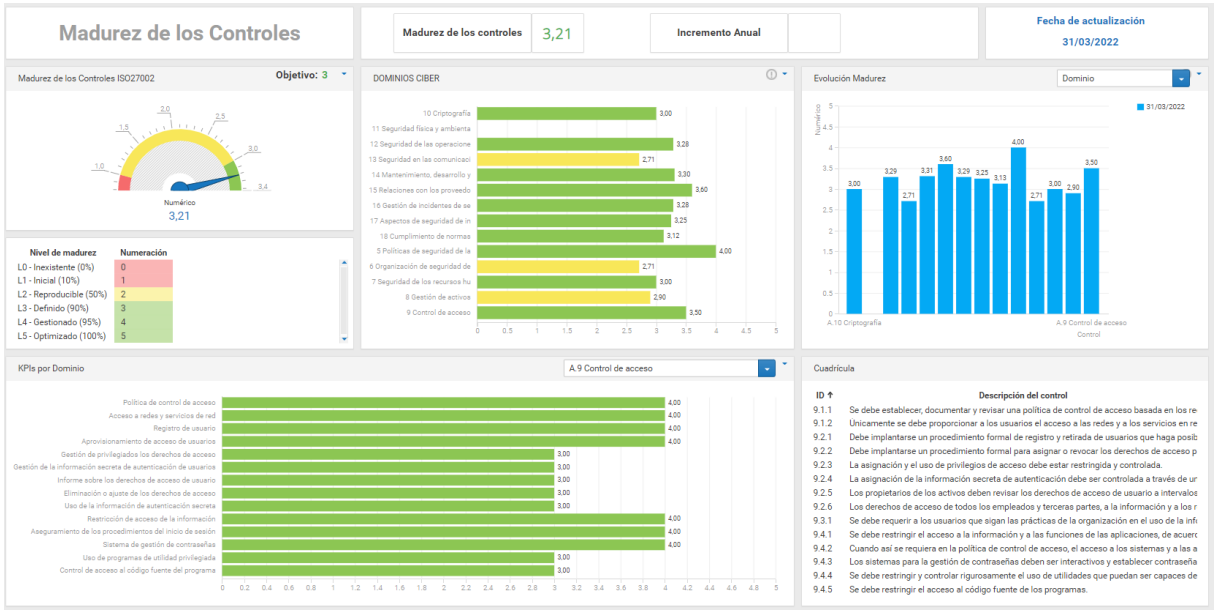


Ilustración 8.5 CM Madurez de los Controles Dominio 9: Control de acceso

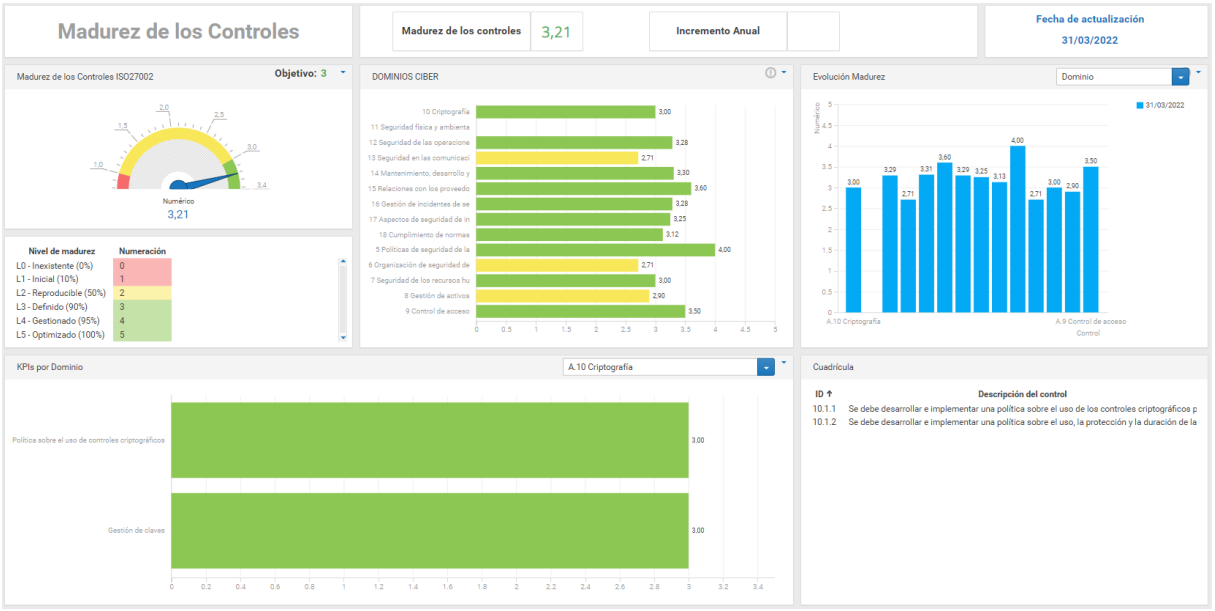


Ilustración 8.6 CM Madurez de los Controles Dominio 10: Criptografía

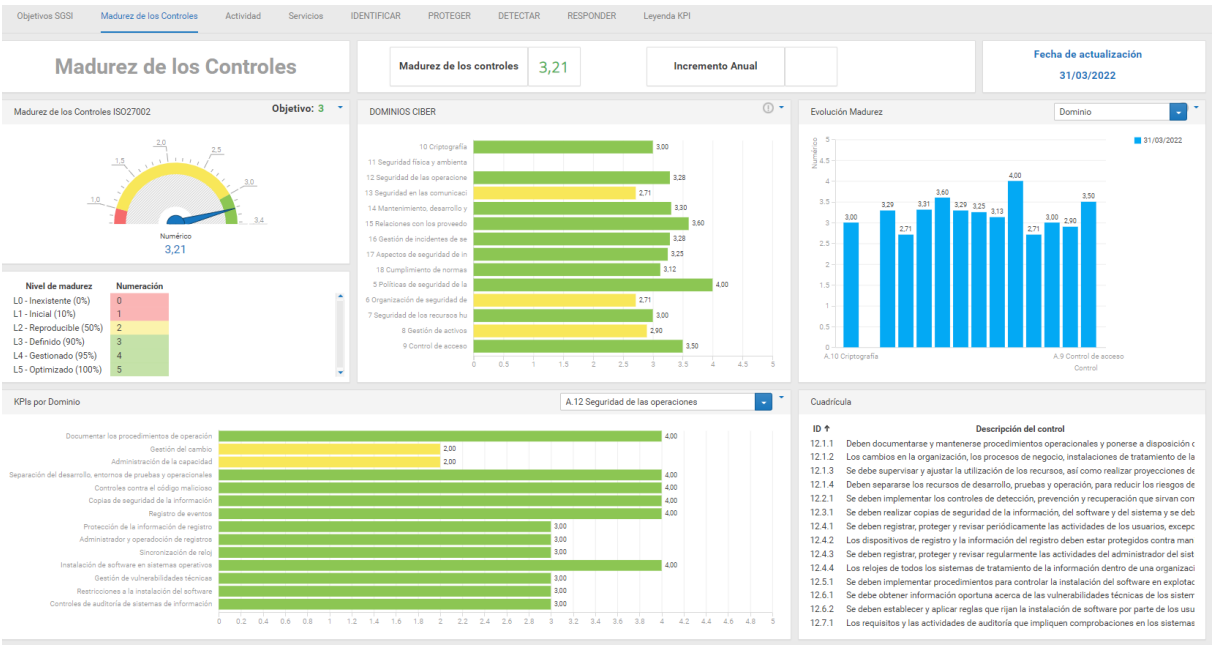


Ilustración 8.7 CM Madurez de los Controles Dominio 12: Seguridad de las operaciones

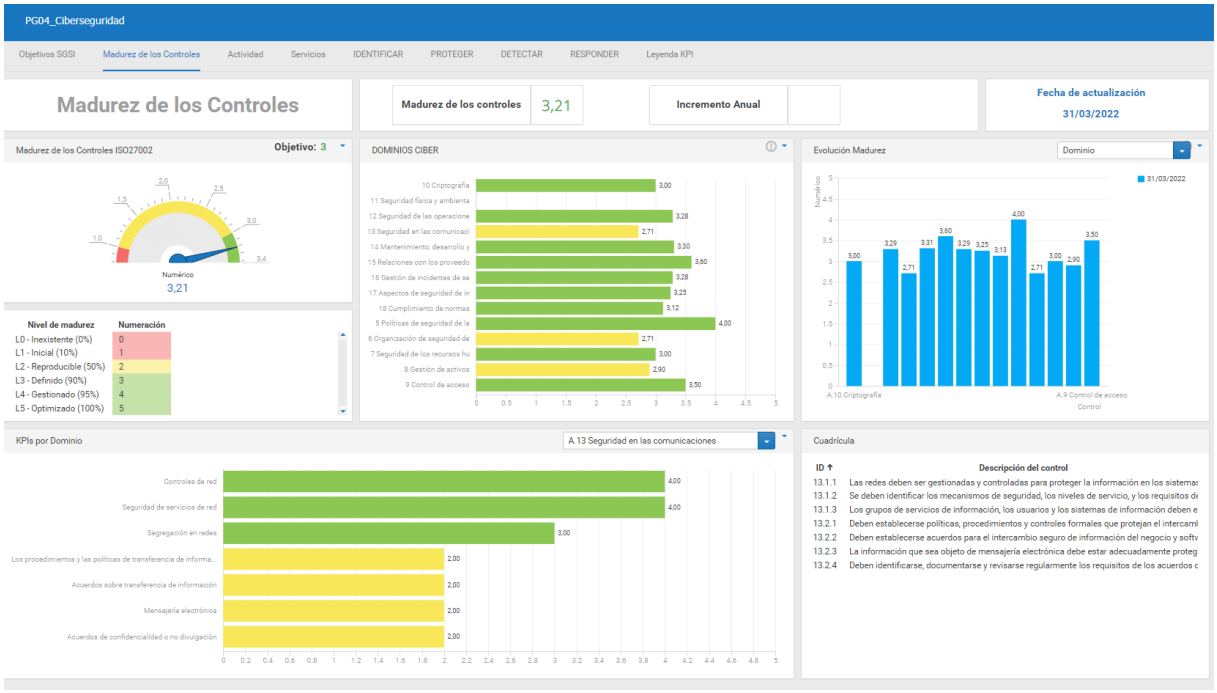


Ilustración 8.8 CM Madurez de los Controles Dominio 13 : Política de Seguridad de las comunicaciones

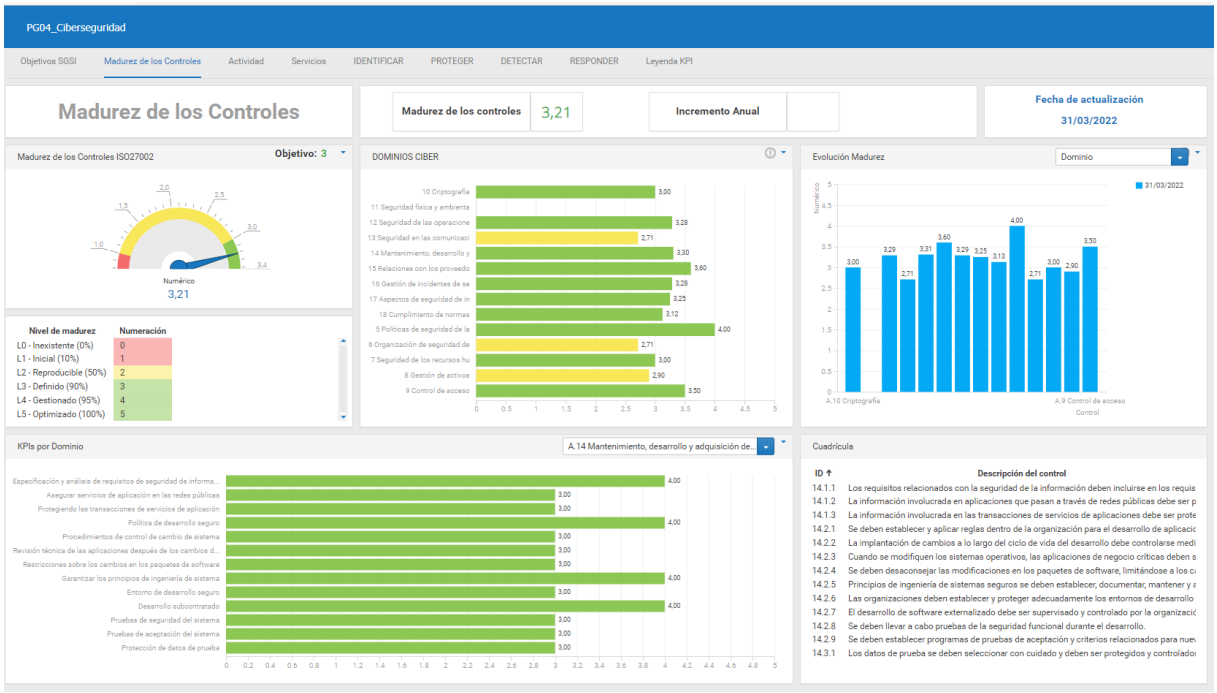


Ilustración 8.9 CM Madurez de los Controles Dominio 5: mantenimiento, desarrollo y adquisición del sistema

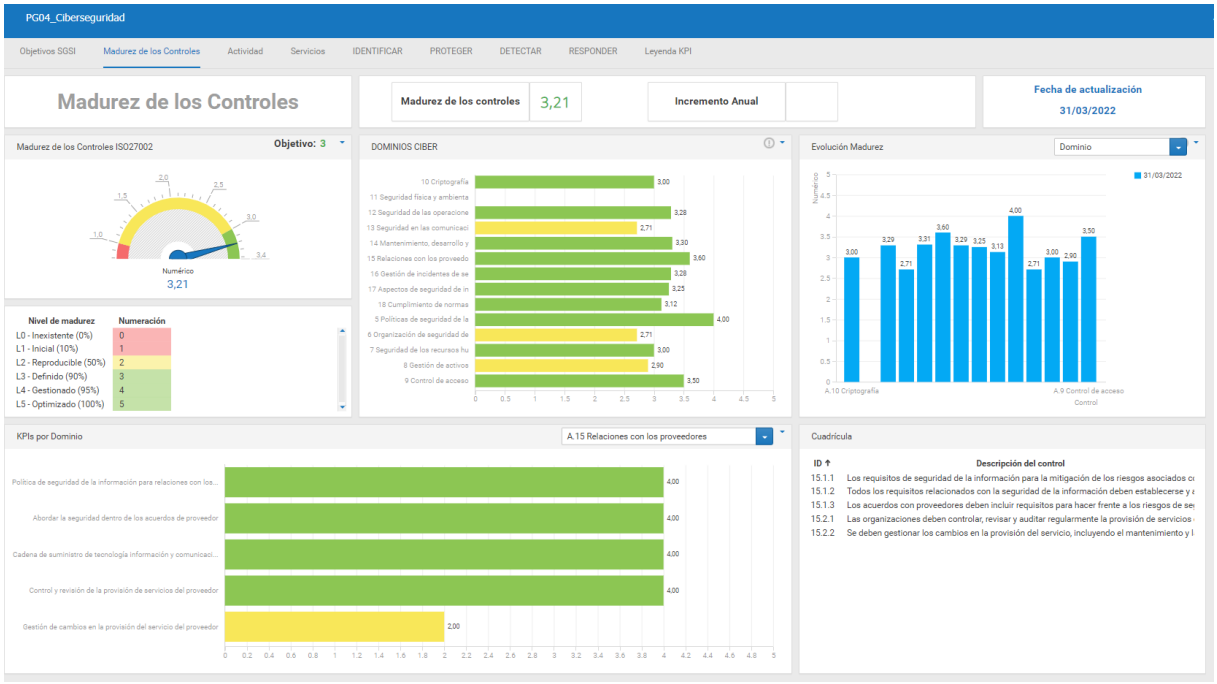


Ilustración 8.10 CM Madurez de los Controles Dominio 15: Relaciones con los proveedores

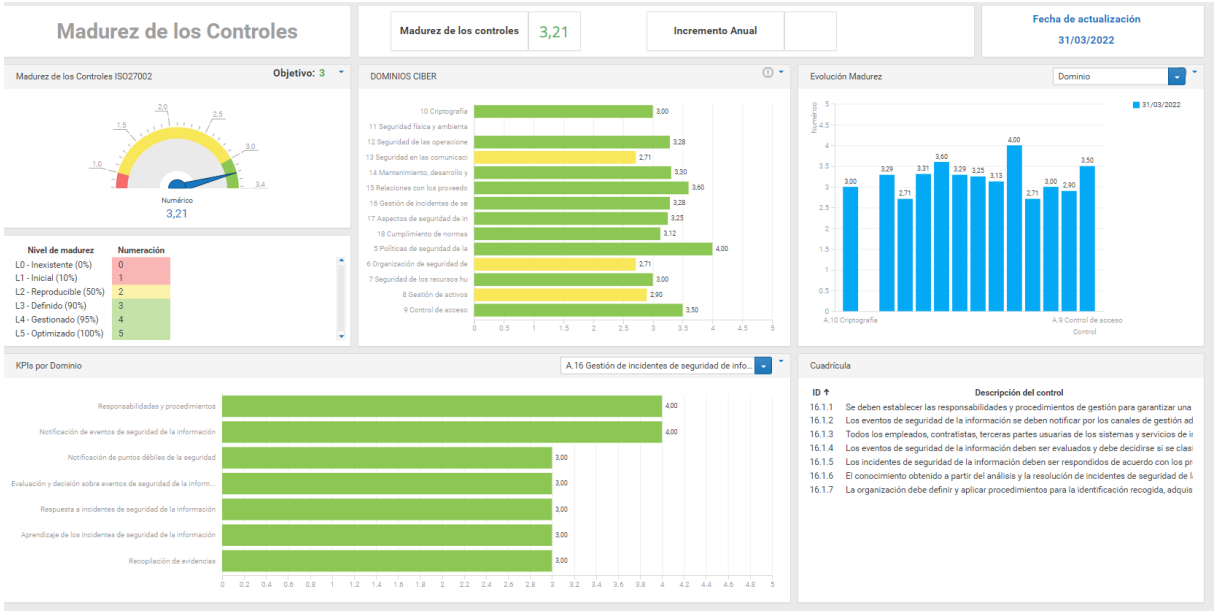


Ilustración 8.11 CM Madurez de los Controles Dominio 16: Gestión de incidentes de seguridad de la información

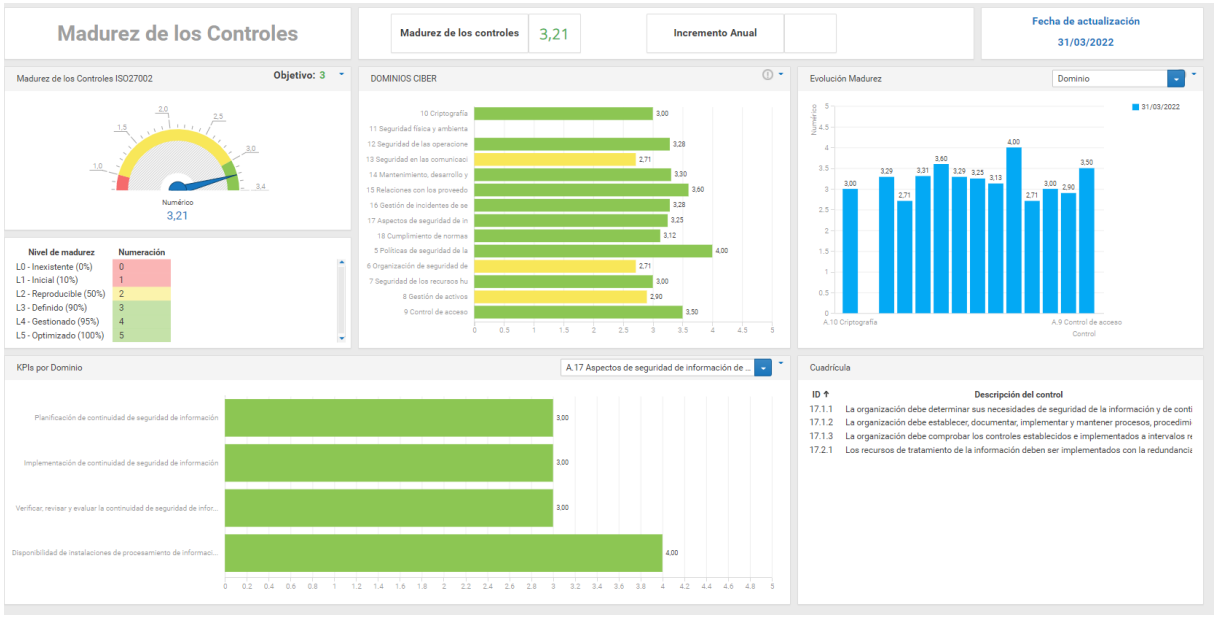


Ilustración 8.12 CM Madurez de los Controles Dominio 17: aspectos de seguridad de la Información

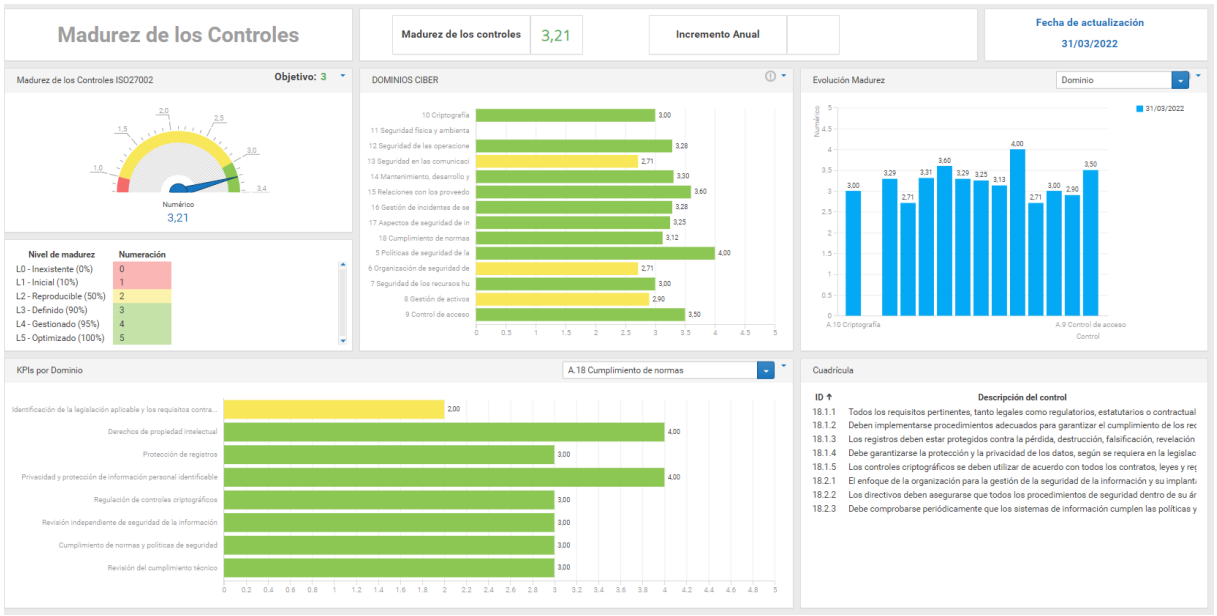


Ilustración 8.13 CM Madurez de los Controles Dominio 18: cumplimiento de normas

8.3 Anexo C: capturas de pantalla CM de Ciberseguridad Antiguo

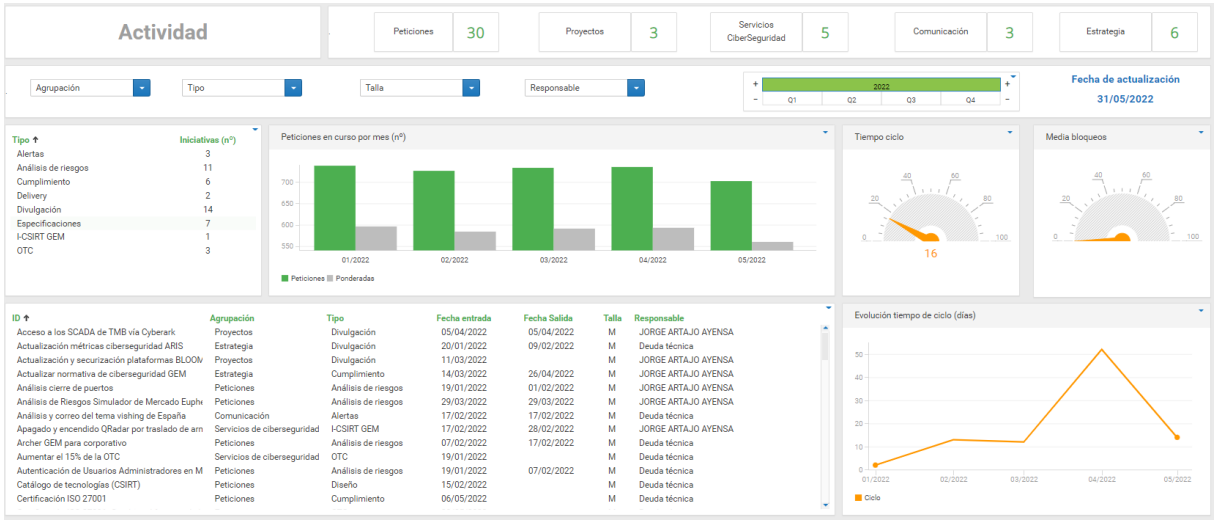


Ilustración 8.14 CM actividad ciberseguridad

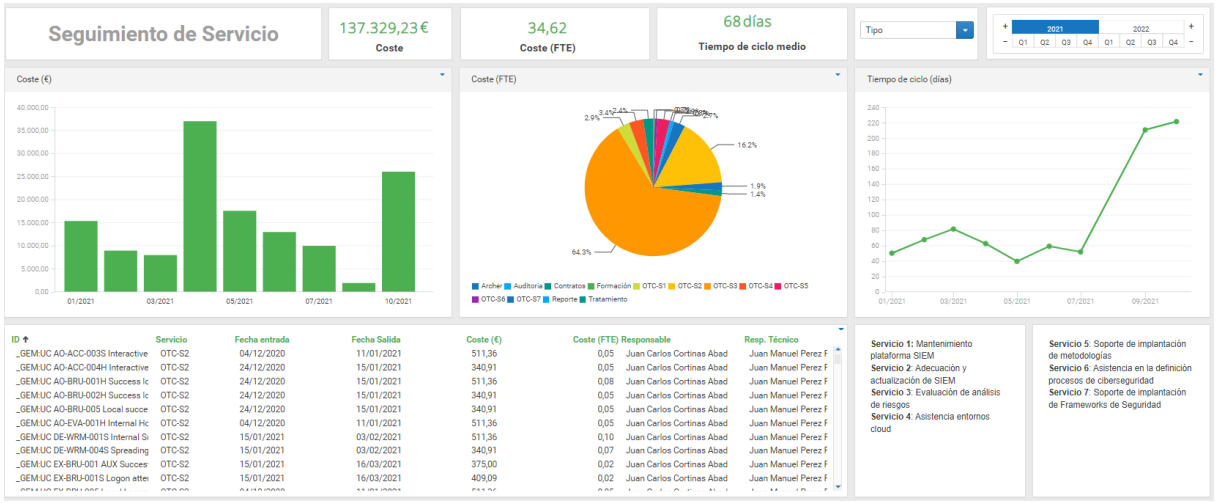


Ilustración 8.15 CM seguimiento de Servicio

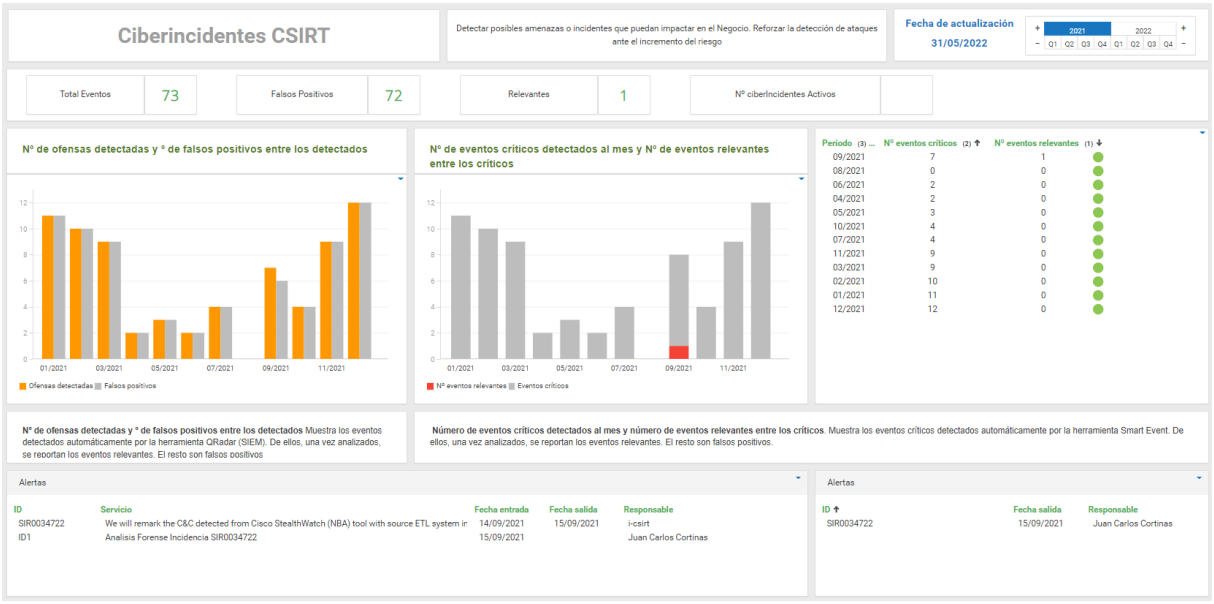


Ilustración 8.16 CM ciberincidentes