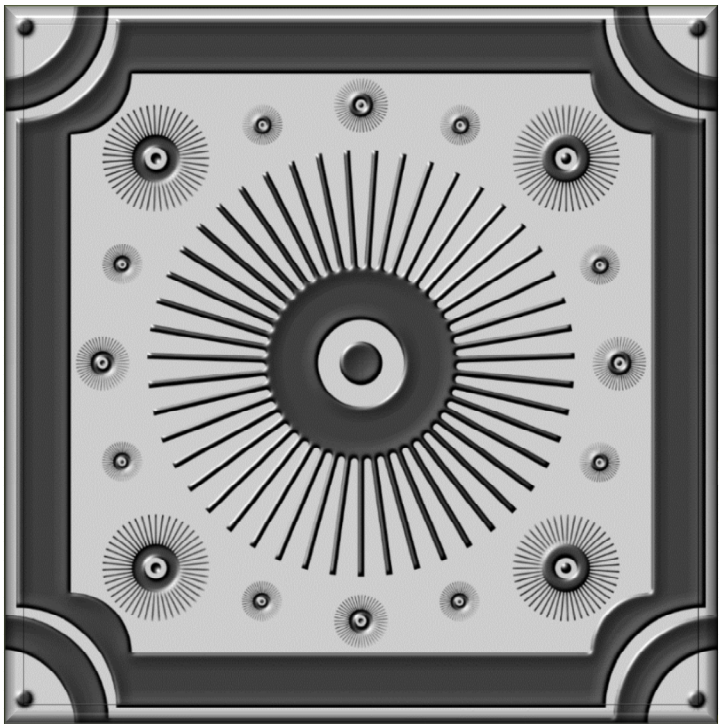
Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Elaboración Plan de Implementación de la ISO 27001-SOC



(*)-Caja fuerte de pared con muchas ruedas de bloqueo para mayor seguridad (licencia Creative Commons-openclirtart)

Tabla de contenido

Tabla de ilustraciones

1. SITUACIÓN ACTUAL. CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1. Introducción

El desarrollo del presente TFM tiene como objetivo la realización de un **Plan Director de Seguridad** tomando como referencia un modelo de empresa real.

Como punto de arranque, se recoge la definición de Plan Director de Seguridad-PDS (***INCIBE-Plan Director de Seguridad***) *:*

1.2 ¿Qué es un Plan Director de Seguridad?
« Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. *Es fundamental para la realización de un buen Plan Director de Seguridad, en adelante PDS, que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboren con ésta. »*

1-Tabla-INCIBE-PDS

Para ello nos vamos a centrar en cuatro aspectos fundamentales :

- **El Conocimiento de la situación actual de la organización desde el punto de vista de la Seguridad de la Información.**
- **El Conocimiento de las estrategias y objetivos de la Organización.**
- **La Elaboración de las propuestas de los Proyectos a acometer y su planificación, en los aspectos de Seguridad, como consecuencia de los resultados obtenidos en base a la aplicación de los puntos anteriores.**
- **La evaluación del estado actual de la Seguridad estableciendo el nivel de madurez de cumplimiento de la Seguridad por parte de la organización.**

Si profundizamos en base a los aspectos señalados:

- **El conocimiento de la Situación actual pasa por la realización de un proceso de análisis y valoración de la Seguridad que se desglosa en las siguientes actividades:**
  - El Establecimiento de una estructura organizativa de Seguridad de la Información.
  - La definición y establecimiento de las Políticas de Seguridad en la organización.
  - La existencia de procesos y procedimientos de gestión que posibiliten el control y seguimiento de todos los aspectos relacionados con la Gestión de la Seguridad.
  - La existencia de un inventario de activos soportado por la organización, así como su valoración.
  - Identificación de las amenazas las que están expuestos los activos de la organización.
  - Las medidas y controles de Seguridad ya establecidos en la organización; considerando su efectividad y grado de implantación.
  - La existencia y aplicación de una metodología de Análisis de Riesgos como base para determinar el nivel y grado de exposición los activos de la organización.

- Y como consecuencia de todo lo anterior, elaborar un diagnóstico de seguridad; estableciendo las estrategias encaminadas a la Eliminación y/o la mitigación del riesgo detectado.

- **El conocimiento de las Estrategias y Objetivos de la organización en base a la consideración de aspectos tales como:**
  - Los proyectos de crecimiento y/o expansión de las actividades de la organización.
  - Los cambios de los procesos y/o reorientación de los procesos de Negocio.
  - La reingeniería de los procesos soportados por la organización.
  - La adecuación de las organizaciones para el cumplimiento, garantizando el cumplimiento de los requisitos legales, contractuales, y los requisitos establecidos por las Partes interesadas (clientes, entidades gubernamentales, proveedores, etc.).
  - Las puestas en marchas de estrategias de Centralización, reorientación y/o externalización de Servicios IT.
  - El Portfolio de proyectos en curso y proyectos a abordar en el futuro próximo, etc.

- **La elaboración de las propuestas de los Proyectos a acometer y su planificación, en los aspectos de Seguridad, como consecuencia de los resultados obtenidos en base a la aplicación de los puntos anteriores.**
  - Recopilación de todas las iniciativas, en base a proyectos a considerar en base a los resultados obtenidos:
    - La revisión de la Seguridad de la organización.
    - Los riesgos detectados en el proceso de Análisis de Riesgos, que ha decidido la organización su tratamiento.
    - Los resultantes del desarrollo de las estrategias y objetivos del negocio.
  - Definición de la estrategia para la puesta en marcha de los Proyectos a través de:
    - La categorización, la priorización, la asignación de responsabilidades, el establecimiento de tiempos de ejecución, la dotación presupuestaria y de recursos, los mecanismos de seguimiento y de control de consecución de objetivos.
- **La evaluación del estado actual de la Seguridad estableciendo el nivel de madurez de cumplimiento de la Seguridad por parte de la organización.**
  - Evaluación de la madurez de la Seguridad, en base un referencial, para poder establecer el punto de situación de la organización en cuanto al nivel de cumplimiento en materia de Seguridad.

1.2. Metodología

Se ha establecido como base metodológica para poder abordar el PDS tomando como referencia los siguientes elementos:

- **La UNE-ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información-Requisitos (UNE-ISO/IEC 27001-Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información (SGSI)-Requisitos)**
  - Es la base que se va a usar en el PDS a desarrollar para establecer los requisitos para poder valorar la existencia y el grado de implantación de un sistema de Gestión de Seguridad de la Información.

1 Objeto y campo de aplicación
Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza"

2-Tabla-ISO 27001-objeto.

- **La UNE-ISO/IEC 27002-Código de prácticas para os controles de Seguridad de la información (UNE-ISO/IEC 27002-Tecnología de la información-Técnicas de seguridad– Código de prácticas para los controles de seguridad de la información).**
  - Usándolo como referencial de los controles de seguridad de la información aplicables a una organización para poder establecer los controles a aplicar y poder tener el punto de referencia para ver el estado de madurez en la aplicación de dichos controles.

1 Objeto y campo de aplicación
Esta norma internacional establece directrices para la seguridad de la información en las organizaciones y prácticas de gestión de seguridad de la información incluyendo la selección, la implantación, y la gestión de los controles teniendo en consideración el entorno de riesgos de seguridad de la información de la organización. *Esta norma internacional está diseñada para ser utilizada en organizaciones que pretendan:* *a) seleccionar controles en el proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001[10];* *b) implantar controles de seguridad de la información comúnmente aceptados;* *c) desarrollar sus propias normas de seguridad de la información."*

3-Tabla-ISO 27002-objeto

- **MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-Libro I-Método), (MAGERIT-Libro II Catálogo de Elementos), (MAGERIT-Libro III Guía de Técnicas)**
  - Cómo base metodológica para abordar el proceso de Análisis de riesgos en base a los activos de la organización.

1.3. Gestión
… Magerit persigue los siguientes objetivos: Directos:
1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
4. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso…

4-Tabla-MAGERIT-objetivos

1.3. Contextualización

Para ello vamos a desarrollar un caso concreto aplicado a una empresa ficticia; en dónde vamos se va a describir el ámbito de actividad; se va a delimitar el alcance del PDSI dentro de esta organización; y en dónde se va a realizar el desarrollo completo del PDSI que tendrá como consecuencia:

1.3.1. La Compañía

GLOBALSOC (nombre de empresa ficticia) es una compañía internacional de seguridad informática, dedicada a las tecnologías de comunicaciones y TI, especializada en soluciones de seguridad y servicios en la nube. En la actualidad está operando en 10 Países repartidos entre 3 continentes (Europa, América y Asia).

1.3.2. La Visión.

Prestación de Servicios de seguridad gestionados y Servicios en la Nube anuestros clientes, como base de protección para grandes empresas, PYMES y Administración Pública.

Red de Centros de Operaciones de Seguridad (SOC) con profesionales altamente calificados con más de 09 años de experiencia en nuestro haber.

1.3.3. El Objetivo

Ofrecer servicios de alta seguridad y calidad, con un gran rendimiento y servicio adaptado a las necesidades de cada uno de nuestros clientes.

1.3.4. Recursos y Actividades

Contamos con un extenso equipo especilalizado de Colaboradores en los distintos SOCs repartidos por el mundo y desarrollamos una actividad intensa a diario en el desempeño de nuestros servicios a los clientes.

5-Ilustración-Actividad.

1.3.5. Servicios Prestados

A modo de resumen, el catálogo de servicios que cubre las problemáticas de Ciberseguridad para nuestros clientes aparece a continuación:

Catálogo de Servicios Prestados	
Servicios de Consultoría	Integrada por los Servicios de asesoramiento, cumplimiento y evaluación de la Seguridad usando métodos y herramientas estándares del mercado
Servicios de Protección de infraestructuras	Dedicados a la protección de Centros de Procesos de datos, redes y dispositivos de clientes. Se protege tanto la información (datos, sistemas, aplicaciones) como las infraestructuras de comunicaciones.
Servicios de Seguridad Cloud	Dirigidos a desplegar la infraestructura desplegada por el cliente en el Cloud. Se proporcionan servicios soportados en clouds globales, que reducen los costes y los tiempos de acceso al mercado.

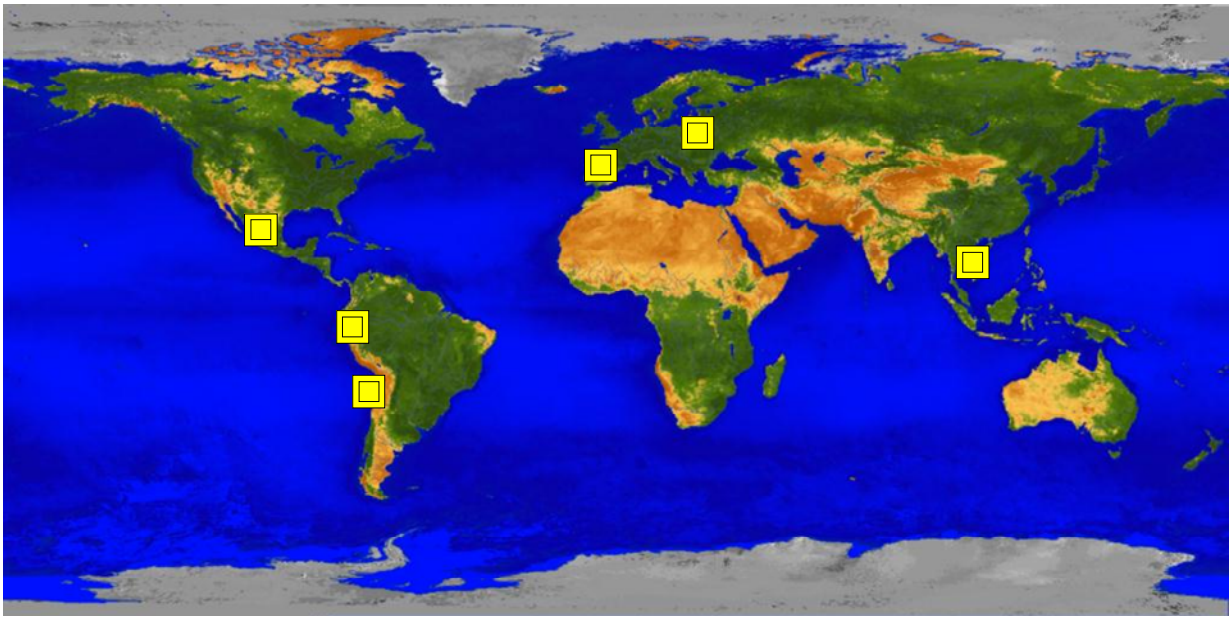
6-Tabla-Catálogo de Servicios.

1.3.6. Instalaciones e Infraestructuras

La empresa dispone de varios Centros de operaciones (SOCs) funcionalmente completos que operan en la modalidad 24x7x365.Los centros están ubicados en (Europa, América y Asia).

Tabla de Ubicaciones SOC	
Europa	• SOC-MADRID (Cubre el área de Madrid y los servicios a clientes de la mitad sur Peninsular (Castilla La Mancha, Levante, Andalucía) • SOC-BARCELONA (Cubre el área Metropolitana de Barcelona, Rsto de Cataluña, País Vasco y Galicia) • SOC-VARSOVIA (Servicios Prestados a Países Bajos, Noruega y Finlandia)
América	• SOC_MEXICO (Todos los clientes dentro de México) • SOC_COLOMBIA (Todos los clientes dentro de Colombia) • SOC_CHILE (Clientes de Chile y los nuevos clientes adquiridos en Argentina)
Asia	• SOC-SINGAPUR (Prestación de Servicios dedicados a Emiratos Árabes).

7-Tabla-Ubicaciones SOC



8-Tabla-Mapa SOC

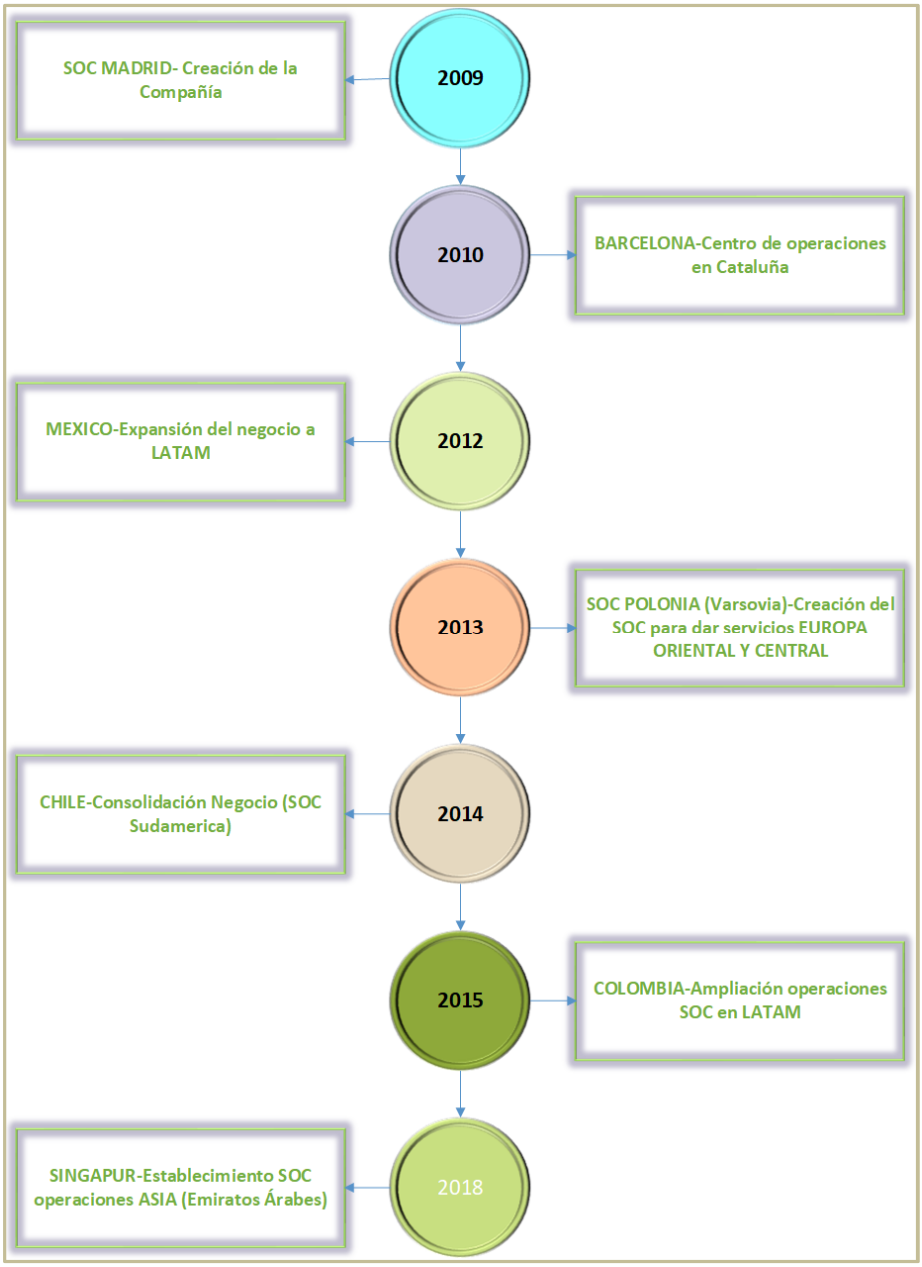
1.3.7. Antecedentes y evolución

La empresa de origen Español originalmente tenía constituido su foco de actividad en todo el Territorio Peninsular.

La compañía ha establecido su estrategia de crecimiento en base a la Internacionalización de sus servicios de Ciberseguridad, aportando proximidad en las necesidades de los clientes y, basada en una política de adquisiciones de empresas locales para reforzar los vínculos de proximidad y confianza.

Esto ha supuesto una expansión a nivel internacional y a un crecimiento continuo dentro del sector de la Ciberseguridad.

A continuación, se presenta una visión de la evolución histórica de la compañía.

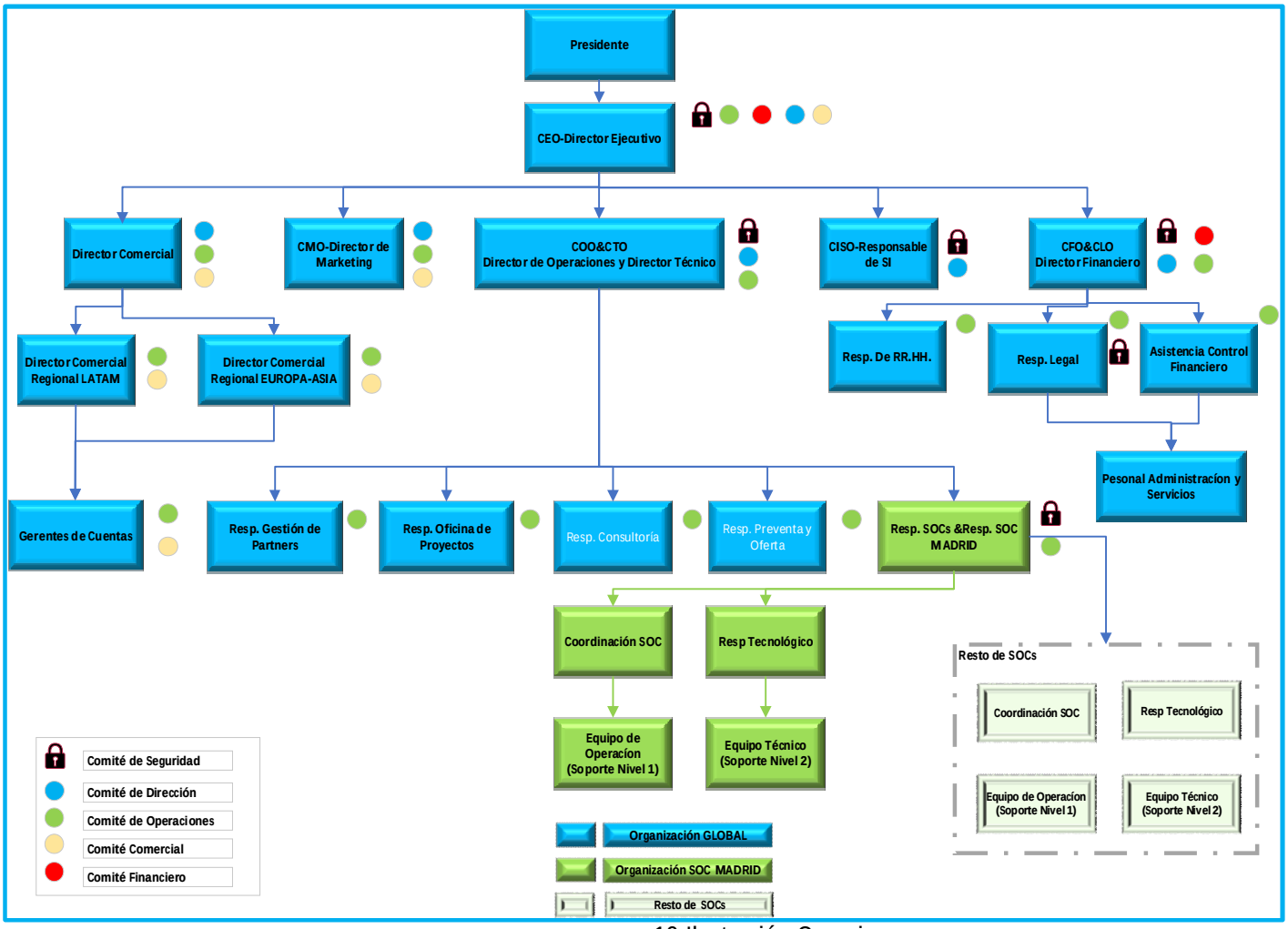


9-Ilustración-Historia

1.3.8. Organigrama de la Compañía

A continuación, se detalla la organización de la compañía (La figura del comité de Seguridad aparece representada, pero no se encuentra implementada en la actualidad).

En verde aparecen representadas las competencias específicas para la funciones del SOC de MADRID (objeto de nuestro alcance).



10-Ilustración-Organigrama

1.3.9. Roles y Responsabilidades en Seguridad de la Información

La descripción de los roles que aparecen declarados dentro de la organización en base a Seguridad de la Información se muestran con detalle en la tabla que aparece a continuación.

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN		
Rol	Tareas	Competencias
Director Ejecutivo (CEO)	• Revisar y aprobar la Declaración de política del SGSI. • Revisar y aprobar el Manual de Políticas del SGSI. • Revisar y aprobar las estrategias de continuidad de negocio.	N/A
Comité de Dirección	• Realizar la revisión por la Dirección. • Desarrollar un proceso de mejora continua - Establecer acciones de mejora.	N/A
Comité de Seguridad	• Realizar la revisión por la Dirección. • Evaluar y aprobar la Declaración de política del SGSI. • Evaluar y aprobar el Análisis de Riesgos y sus conclusiones. • Evaluar y aprobar el Plan de Tratamiento de Riesgos (PTR) de los riesgos detectados. • Evaluar y aprobar el Nivel de Riesgo Aceptable. • Evaluar y aprobar el Riesgo Residual. • Evaluar y aprobar los objetivos de seguridad de la información. • Analizar las incidencias. • Analizar los resultados de las auditorías internas e independientes. • Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad. • Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Coordinar aquellas funciones que le son propias, así como aquellas que le vengan indicadas por el Comité de Seguridad de la Información. • Dirigir y coordinar la respuesta a los incidentes de seguridad. • Elaborar informes periódicos del estado de la seguridad d ela información, para el Comité de Dirección, que incluyan los incidentes más relevantes de cada periodo o cualqueir otro punto reseñable.	N/A
CISO-Resp. de Seguridad	• Asegurar la puesta en marcha de las actividades de implantación y seguimiento del Sistema de Gestión de Seguridad de la Información. • Asegurarse de que se establecen, implementan y mantiene toda la documentación necesaria para el sistema de gestión. • Informar del funcionamiento del Sistema a la Dirección para su revisión y para la mejora del mismo. • Elaboración e implantación de mejoras continuas. • Efectuar el seguimiento del sistema de gestión. • Verificar y seguir el grado de cumplimiento con los objetivos establecidos. • Gestionar las comunicaciones internas y externas, en relación con la política y los objetivos. • Convocar las reuniones y revisiones de los sistemas por Dirección que se realicen para el buen funcionamiento	• Curso de ISO/IEC 27001. • Al menos 5 años de experiencia en relación a la seguridad. • Al menos 5 años de experiencia en relación a las TIC. • Conocimiento de procedimientos aplicables.

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN		
Rol	Tareas	Competencias
	del sistema, así como realizar un seguimiento de las acciones que se determinen. • Seguimiento de incidencias y no conformidades del sistema. • Cumplimiento de las normas y política de seguridad de la información. • Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad. • Promover la formación y concienciación en materia de la seguridad de la información dentro de su ámbito de responsabilidad. • Coordinar aquellas funciones que le son propias, así como aquellas que le vengan indicadas por el Comité de Seguridad de la Información. • Llevar a cabo tareas de inspección mediante la realización de auditorías y controles periódicos, para verificar el cumplimiento de las obligaciones en materia de seguridad de la información. • Dirigir y coordinar la respuesta a los incidentes de seguridad. • Elaborar informes periódicos del estado de la seguridad de la información, para el comité, que incluyan los incidentes más relevantes de cada período, o cualquier otro punto reseñable	
Director TI	• Revisión del Manual de Políticas del SGSI. • Actualización del Análisis de Riesgos (Incluyendo Contexto y Terceras partes). • Mantenimiento y Actualización del Inventario TIC. • Mantener actualización empresas y contratos con terceras partes • Informar sobre necesidades de formación. • Mantener actualizados accesos asignados por usuario. • Mantener actualizado el registro de mantenimiento de equipos y dispositivos cuando se produce alguna intervención de mantenimiento. • Realizar procedimiento de borrado seguro, cuando se elimina o se reutiliza un soporte que contiene datos. • Registrar cuando se produce una Entrada/Salida de soportes que contengan información. • Registrar cambios y aprobaciones. • Registrar cambios acordados y enviados a proveedores. • Realizar eventos y garantizar que se registran en los sistemas. • Realizar y comprobar realización de copias de seguridad. • Documentar y mantener requisitos de seguridad de las aplicaciones. • Registrar y mantener los accesos del personal. • Análisis de vulnerabilidades a máquinas. • Soluciones vulnerabilidades detectadas. • Registrar y Tratar incidentes. • Revisar BIAS. • Realizar pruebas del PCN y Contingencias. • Revisar y aprobar estrategias de continuidad. • Realizar planes de continuidad de negocio. • Llevar control de software y licencias. • Suministrar datos de indicadores. • Revisión y Actualización de Instrucciones Técnicas.	• Curso de Concienciación Seguridad de la información • Conocimiento de los procedimientos a Aplicables • Ingeniería Técnica Telecomunicaciones/informática • Experiencia en Dirección IT de al menos 7 años.

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN		
Rol	Tareas	Competencias
Dir. Área/Rep. Procesos de Negocio	• Revisión de cambios del alcance. • Revisión de contexto. • Solicitar alta de usuarios y permisos así como las bajas y las modificaciones de los mismos. • Revisar e incluir nuevos aspectos a regular (legislación y contractual). • Clasificación la información. • Informar sobre necesidades de formación. • Informar y autorizar cuando se produce una entrada/salida de soporte que contenga información. • Revisar BIAS. • Notificar y Tratar incidentes. • Colaborar en la realización de pruebas del PCN y Contingencias. • Realizar planes de continuidad de negocio. • Revisar y aprobar estrategias de continuidad de negocio. • Actualización del análisis de Riesgos incluyendo Contexto y Terceras Partes. • Suministrar datos de indicadores.	• Curso de Concienciación Seguridad de la información. • Conocimiento de los procedimientos a Aplicables.
Dir. RR.HH.	• Revisión de Declaración de Política del SGSI. • Actualización del Análisis de Riesgos. • Mantener actualizados los puestos y los perfiles exigidos. • Actualización de información y fichas del personal. • Actualización de listados del personal. • Actualización de curriculum. • Mantener actualizados la información de activos entregados. • Mantener actualizado un manual de bienvenida, y entregarlo a cada personal nuevo, incluyendo política de seguridad y normativa. • Garantizar que se piden y archivan todos los requisitos de selección de personal. • Tratar incidentes. • Realizar planes de continuidad de negocio. • Suministrar datos de indicadores. • Asegurar que se realizan las acciones formativas y de concienciación. • Realizar procedimiento de borrado seguro, cuando se elimina.	• Curso de Concienciación Seguridad de la información. • Conocimiento de los procedimientos a Aplicables.
Resp. Legal	• Revisar e incluir nuevos aspectos a regular (legistación y contractual). • Revisión del Manual de Políticas del SGSI. • Actualización del Análisis de Riesgos. • Notificar y Tratar incidentes. • Revisar e incluir nuevos aspectos a regular (legistación y contractual). • Actualización del Análisis de Riesgos. • Dar soporte al Responsable del SGSI sobre el cumplimiento. • Suministrar datos de indicadores. • Revisar e incluir nuevos aspectos a regular (legistación y contractual).	• Curso de Concienciación Seguridad de la información. • Conocimiento de los procedimientos a Aplicables.
Dir. Comercial	• Interlocución con los clientes. • Participación en la generación de la estrategia comercial de la organización.	• Curso de Concienciación Seguridad de la información.

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN		
Rol	Tareas	Competencias
	• Generación de la Preventa y realización de la oferta. • Seguimiento y apoyo en la gestión económica de los proyectos. • Participación en las reuniones de seguimiento y control de los proyectos dentro del ámbito táctico y estratégico.	• Conocimiento de los procedimientos a Aplicables.
Coordinador SOC	• Interlocución con el cliente. • Responsable de la Gestión de Incidencias • Responsables del seguimiento de cambios • Reporting actividad del Servicio. • Seguimiento del cumplimiento de los SLA's del servicio.	• Experiencia en coordinación de servicios al menos de 3 años. • Conocimientos de Seguridad lógica y física.
Responsable Tecnológico	• Referente tecnológico en Seguridad lógica. • Especialista tecnológico productos y soluciones de Seguridad. • Administración y configuración red y servicios de red. • Administrador de Sistemas (Linux, Windows, etc.). • Administración y gestión de soluciones de cifrado (certificados clave pública, firma electrónica, etc.). • Conocimientos y desarrollo de Scripting (powershell, bash, ksh, etc.).	• Licenciado y ingeniero técnico. • Experiencia de al menos 5 años. • Certificaciones de seguridad (CISSP, CEH , OSCP, CHFI, etc).
Técnico de Operación	• Manejo de entorno de usuario (windows, Linux). • Conocimiento de administración básica de sistemas operativos. • Manejo de herramientas de Service Desk, monitorización, IPS, SIEM, herr. de backup a nivel de explotación,etc.). • Soporte nivel 1 resolución de incidencias.	• Experiencia en operación de Servicios al menos de 2 años. • Conocimientos técnicos administración básica entornos Linux y Windows). • Conocimentos de herramientas de ofimática, her. Service Desk y de monitorización.
Técnico de Sistemas	• Administración y matenimiento de S.O. (bastionado, comf. Correo, conf. Backup). • Configuración y mantenimiento de Servicios de Red. • Configuración y mantenimiento de herramientas de seguridad (IPS, IDS, gestión de logs, SIEM, etc.). • Gestión de incidencias técnicas y de seguridad. • Mantenimiento de las plataformas e infraestructura IT. • Conocimientos y desarrollo de Scripting (powershell, bash, ksh, etc.).	• Ingeniero Técnico. • Experiencia de al menos 2 años en administración de Sistemas y gestión de Seguridad lógica. • Deseable certificaciones (CEH, Vmware, Red Hat, etc.)
Todo el Personal	• Comunicar incidentes. • Marcar la información. • Tratar la información según la normativa.	• Curso de Concienciación Seguridad de la información. • Conocimiento de los procedimientos a Aplicables.
Auditor Interno	• Realización de auditorías técnicas y de gestión enfocadas dentro de la Seguridad de la información dentro de la organización. • Planificación y seguimiento de las auditorías internas (técnicas y de gestión) a realizar en la organización.	• Conocimientos en Sistemas de Gestión (al menos 3 años). • Experiencia en implantación

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN		
Rol	Tareas	Competencias
	• Control y seguimiento de No Conformidades, observaciones y oportunidades de mejora resultantes de la realización de las auditorias.	y mantenimiento ISO 27001 (2 años). • Formación implantación y auditoría ISO 27001.

11-Tabla-Roles y Responsabilidades SI

1.3.10. Estrategias de la Organización

Nuestra Estrategia de cara a los próximos años se apoya en base a los siguientes elementos:

Estrategias de la Organización	
Crecimiento	Dentro de las áreas geográficas en las que ya estamos presentes: • Para los clientes en los que ya estamos presentes aumentando nuestro volumen de actividad y de Servicios prestados. • Incorporar nuevos Clientes en base a la calidad de nuestros servicios y el reconocimiento de marca y actividad en las áreas regionales en las que prestamos Servicios.
Política de Partner	• Seguir fomentando y potenciando las alianzas actuales con proveedores de Productos y Servicios de Ciberseguridad. • Mantener nuestro nivel de independencia respecto de productos y soluciones de Ciberseguridad (adaptándonos a las mejoras tecnologías existentes en cada caso y a las necesidades concretas de nuestros clientes.
Evolución infr. IT hacia la Nube	• Evolución de la infraestructura IT de nuestros SOC hacia la Nube que nos va a permitir la estandarización de recursos y servicios, la gestión del rendimiento y la capacidad.
Estandarización SOC	• Estandarización y homogeneización en el Delivery de nuestros servicios de SOC.

12-Tabla-ISO 27001-Estrategias

1.3.11. Alcance PDS

Considerando la Historia y la capacidad de operación del SOC de MADRID, siendo un punto de referencia vital dentro de la organización, se ha determinado que el alcance de nuestro PDS se va a centrar en:

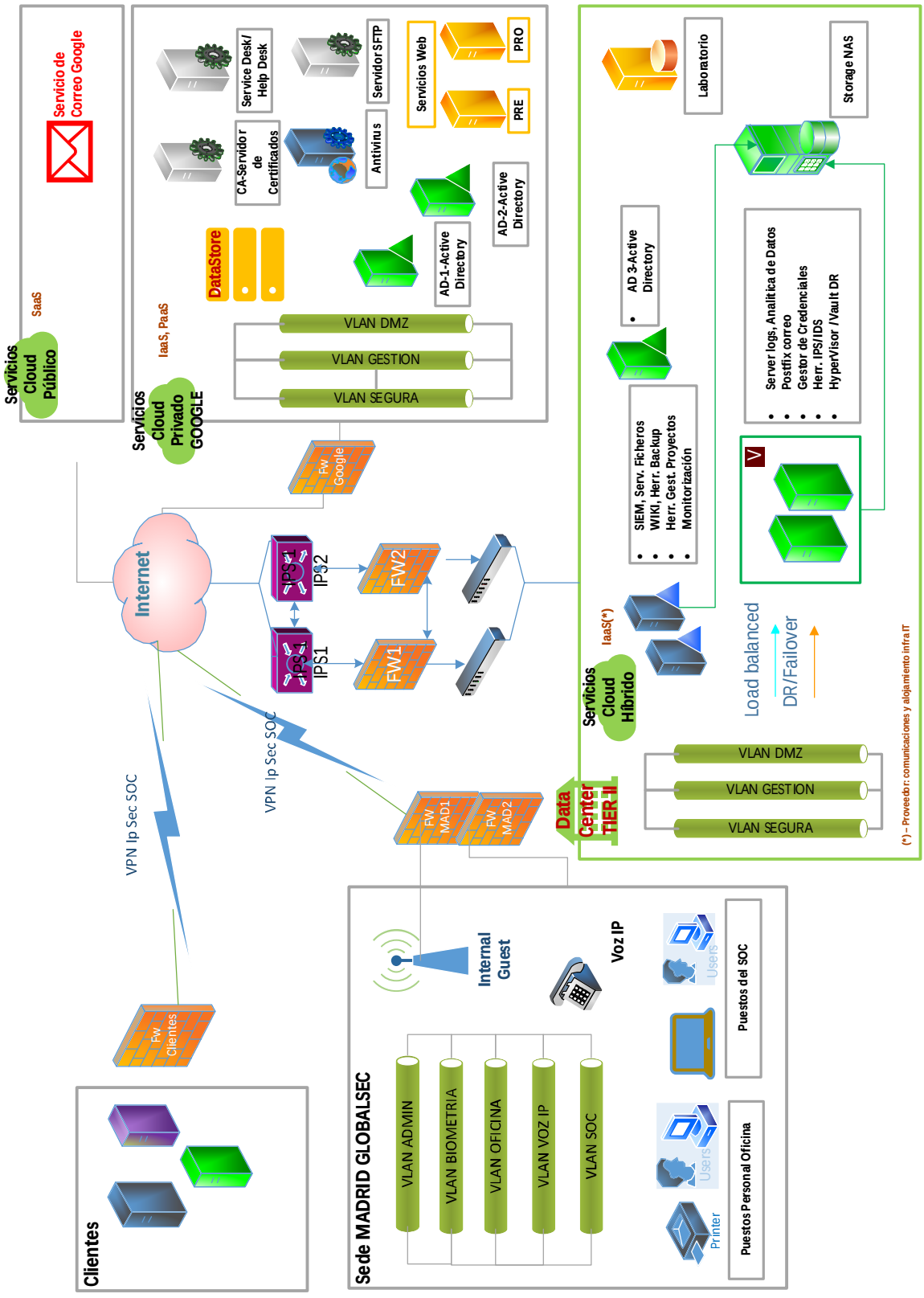
- **El Servicio de dispositivos gestionados a través del Centro de operaciones (SOC-MAD).**
  - Proporcionado a través de la realización de los procesos:
  - Gestión de Despliegue. Gestión de incidentes y Gestión de cambios.
  - Servicios Gestionados (*). Puesta en marcha y mantenimiento de las soluciones implantadas en los clientes desde el SOC, prestando servicios de implantación y soporte. Apoyándose para su realización en los siguientes procesos:

Alcance PDS-Servicios Gestionados	
SOC-MADRID	
Gest.Despliegue	• Abarca las tareas de implantación inicial y despliegue de los proyectos acordados con los clientes, en base al catálogo de servicios existente.
Gest.Incidencias	• Mecanismos de detección, prevención, atención y resolución de los incidentes que se puedan presentar sobre las soluciones y plataformas instaladas en los clientes.
Gest. Cambios	• Adecuación constante y mantenimiento continuado de la infraestructura y servicios que se usan por parte del SOC para la prestación de los servicios de los clientes.

13-Tabla-Alcance PDS

(*)- Servicios declarados en el Catálogo de Servicios Prestados (Tabla-Catálogo de Servicios): Servicios Protección Infraestructuras y Servicios de Seguridad Cloud.

1.3.12. Infraestructura del SOC MADRID



14-Ilustración-Infraestructura IT SOC-MADRID

1.4. Objetivos de la Organización

Los objetivos de la organización que están presentes en el PDS considerando las estrategias del Negocio se muestran en la siguiente tabla.

OBJETIVOS PLAN DIRECTOR DE SEGURIDAD										
Objetivos Organización		Objetivo Compañía Ofrecer servicios de alta seguridad y calidad, con un gran rendimiento y servicio adaptado a las necesidades de cada uno de nuestros clientes.				Estrategias de la Organización				Objetivo PDSI (S/N)
#	Descripción	Servicios de Alta Seguridad	Servicios de Alta Calidad	Gran rendimiento	Servicios adaptados a clientes	Crecimiento	Política de Partners	Evolución infraest. IT Nube	Estandarización de los SOC	
OBJ_ORG_1	Control de los requisitos de Seguridad de los Proveedores (partners)	X	X		X		X			S
OBJ_ORG_2	Construir una Arquitectura de Referencia para la infraestructura IT de los SOC en la nube	X	X	X	X	X		X	X	S
OBJ_ORG_3	Evaluación de nivel de Seguridad de los SOC existentes (piloto de base de valoración SOC-MAD)	X	X		X	X			X	S
OBJ_ORG_4	Establecimiento de SGSI para los SOC, estandarización de los Procesos de Gestión de la Seguridad	X	X	X		X		X	X	S
OBJ_ORG_5	Establecimiento de SGSI para los SOC, estandarización de los Procesos de Delivery	X	X	X	X	X			X	S
OBJ_ORG_6	Dotar a los SOC de Certificaciones de Seguridad y Certificaciones Técnicas	X	X			X	X		X	S
OBJ_ORG_7	Formación técnica especializada y extendida de manera uniforme a todos los SOCs	X	X		X	X	X		X	S
OBJ_ORG_8	Estandarización de los procesos de Operación IT de las infraestructuras de los SOCs	X	X	X		X			X	S

15-Tabla-Objetivos Organización

1.5. Análisis Diferencial

Se ha procedido a realizar una revisión del estado general de la Seguridad de la Información de la organización GLOBALSOC; como punto de arranque para poder realizar el proceso de evaluación del estado de la SI en la organización, y tomando como eje de referencia el SOC de Madrid se detalla a continuación.

Se procede a realizar un resumen del análisis diferencial realizado centrándonos en 2 grandes áreas:

- Presencia y profundidad de un Sistema de Gestión de la Seguridad de la Información (SGSI).
- La valoración de los controles de Seguridad existentes en la Organización basado en el referencial ISO 27002.

Consideraciones:

- A posteriori de la realización del presente Análisis Diferencial, se han desarrollado algunas políticas y procedimientos del SGSI de modo que ha quedado establecida la base para el desarrollo del PDSI de la organización (SISTEMA DE GESTIÓN DOCUMENTAL).
- Este trabajo ha sido tomado en consideración cuando se ha procedido a realizar el registro de la aplicabilidad SOA (TFM_Declaración de Aplicabilidad SOA.xlsx)

1.5.1. Existencia de Sistema de Gestión de la Seguridad de la Información (SGSI)

La organización tiene un **conocimiento claro acerca del contexto** (actividades, negocio, mercado, regulación etc.) en el que se encuentra ubicada su actividad y tiene identificados los elementos propios y los terceros con los que se relaciona en la realización de sus actividades (**Partes interesadas**).

No obstante, la organización no tiene **desarrollado procedimientos** de recopilación, análisis y evaluación sistemática de estos elementos para poder gestionarlo desde la perspectiva de la SI (relaciones, contexto, riesgos, evaluación, etc.).

Aunque su actividad está centrada en Temas de Seguridad, Ciberseguridad concretamente la organización no tiene de manera expresa establecida la política de seguridad, ni los mecanismos para el conocimiento y su cumplimiento dentro y fuera de la organización.

La organización tiene establecido un organigrama, en dónde se detallan las **funciones y competencias**; pero no los tiene expresamente adaptados y desarrollados para realizar una gestión eficiente de la Seguridad de la información.

Como consecuencia, no están establecidos unos **mecanismos de gestión de riesgos** y declaración expresa de objetivos de Seguridad.

En cuanto al conocimiento de las políticas y buenas prácticas en SI por parte de la organización.

- **Existe una clara concienciación y conocimiento de las buenas prácticas de seguridad (se hace notar el desarrollo de la actividad en ciberseguridad en la organización), sin embargo:**
  - No es un proceso que esté claramente, definido, articulado y sistematizado.
  - Aunque ya existen recursos que ya están desarrollados (manuales de buenas prácticas).

Hay establecidos dentro de la organización mecanismos de **Auditoría Interna.**

- Lo cual da fe de una cultura ya instalada de control en la organización; pero su aplicación se reduce a aspectos meramente técnicos (Pentesting y Análisis de Vulnerabilidades de sus Sistemas de Información.).

La función de **análisis y seguimiento de la Seguridad de la Información** no está implementada como proceso dentro de la organización (no existe la figura del comité de seguridad incluido dentro los distintos Comités ya existentes en la organización).

Tampoco está desarrollado en concepto de la **mejora continua** aplicada a la SI.

1.5.2. Estado de los controles

Hay que establecer los **roles específicos** en cuanto a Seguridad de la información dentro de la organización.

- La segregación de funciones está implementada dentro de la organización; pero hay que tener en consideración los siguientes aspectos:
  - Hay que revisar y mejorar las bases sobre las que está organizada la SI.
  - Hay que revisar la consistencia de las competencias y responsabilidades asociadas a las tareas de segregación (autorización, ejecución, validación, etc.).

Existe un bagaje en cuanto a los controles de Seguridad centrados en aspectos técnicos, de manera que que ya existen **políticas desarrolladas** y en uso para temas como:

- Políticas de uso Dispositivos móviles, Metodologías y herramientas para la Gestión de proyectos.
- Políticas de teletrabajo (como actividad normalizada dentro de la organización).

La **Gestión de RR.HH**. está correctamente definida y los procesos asociados con SI se encuentran ya implementados (Selección, contratación y gestión de recursos).

- Es necesario realizar los ajustes para que puedan garantizar el control y seguimiento; y que sea el eje central de información y concienciación en SI para la organización.

En cuanto a la **Gestión de la Activos** de la organización:

- No existen criterios adoptados para la tipificación, categorización, clasificación y gestión adecuada de los activos.
- No se parte de una base estable para poder desarrollar un proceso de seguimiento de los activos y gestión de los riesgos asociados.
- Los procedimientos de recogida, análisis y uso no están claramente definidos.
- Lo registros de activos existentes son parciales y no hay procedimientos para su mantenimiento y actualización (Infraestructura IT).

El **Control de Acceso** a los activos se encuentra desarrollado y en uso:

- Están declaradas e implementados políticas de control de accesos las aplicaciones y a los componentes de la infraestructura IT.
- Están implantados mecanismos de segregación de funciones.
- Se usan Herramientas de gestión para el control de acceso (SW de gestión de credenciales).
- Sin embargo, se requiere una revisión para ver si las políticas se cumplen globalmente y los procedimientos están correctamente definidos.
- En paralelo, no se están realizando revisiones periódicas del cumplimiento de las políticas establecidas.

Los **Controles Criptográficos** están desarrollados y en uso:

- Se echa en falta un inventario, control y seguimiento de los mismos (reglas de uso, mantenimiento de recursos asociados - P.e. ciclo de vida de los certificados -).

La **Seguridad Física** está bastante controlada:

- Se está aplicando de manera correcta el mecanismo de seguridad física por capas.
  - Controles de acceso físico al edificio, los controles de acceso físico a las oficinas y
  - Controles de acceso físico al SOC.

- Existen procedimientos de control y cumplimiento del acceso físico.

Respecto a la **Seguridad de las Operaciones** hay que hacer notar que este grupo de controles ya está gestionado por la organización.

Requiere ciertas mejoras y ajustes, pero los procesos ya existen y son usados con normalidad.

Para la **Seguridad de las Comunicaciones** se cumple estrictamente con los controles de seguridad en cuanto a arquitecturas, topologías y segmentación de redes.

- Quedan pendientes por desarrollar y ajustar todos los aspectos relacionados con:
  - Los acuerdos de intercambios de información (en base a la tipificación de los activos y su uso) y la Gestión derivada del uso de la mensajería electrónica.

En cuanto a la **Adquisición Desarrollo y Mantenimiento de Sistemas** no están establecidos y documentados los mecanismos de captación, evaluación y aprobación de los activos adquiridos por la organización que afectan SI.

No hay establecida una **Política de Desarrollo Seguro**, sin ser la actividad principal objeto del SOC); sí que existe la necesidad de la existencia y uso de la misma.

En la **Relación con los Proveedores** no hay controles establecidos, dentro de la organización, para la gestión de la seguridad de los proveedores.

La **Gestión de Incidentes** es un proceso ya implantado en la organización y se aprecia madurez en base a la ejecución de las actividades del SOC.

- La gestión de incidencias está ya implantada y en uso; faltaría realizar las adaptaciones necesarias para recoger los incidentes de seguridad de manera clara, y poder realizar la gestión de los mismos reajustando los procedimientos, herramientas y flujos ya existentes.

En cuanto a la **Continuidad del Negocio** no ha habido una evaluación previa de los Procesos gestionados y Servicios prestados para tener conciencia del grado de criticidad de los mismos (Análisis de Impacto de Negocio-BIAs).

- De modo que no se han podido determinar de manera precisa las necesidades de la organización en cuanto a Continuidad de Negocio.
- No obstante, si están presentes en la infraestructura IT consideraciones de arquitecturas de Redundancia y disponibilidad.

En el aspecto de **Cumplimiento**, salvo en el caso concreto de la privacidad (cono consecuencia del desarrollo en paralelo, dentro de la organización, del proyecto de adecuación al RGPD).

- No existe una gestión procedimentada y ordenada de los aspectos de cumplimiento en la organización, con especial énfasis a los que afectan a SI.

El análisis diferencial detallado se encuentra en el documento (TFM_Informe_Analisis_Diferencial.pdf)

2. SISTEMA DE GESTIÓN DOCUMENTAL

2.1. Introducción

Como consecuencia del Análisis diferencial realizado sobre la organización y considerando el alcance establecido (**Alcance PDS**) se han desarrollado la documentación de base del SGSI, en base a la referencia de la **ISO/IEC 27001**:

Esta documentación está cubriendo los siguientes aspectos:

- **Política de Seguridad**: Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.
  - TFM_Politica de Seguridad.pdf 
- **Procedimiento de Auditorías Internas**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.
  - TFM_PROC_Procedimiento de Auditorias Internas.pdf 
- **Gestión de Indicadores**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.
  - TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf 
- **Procedimiento Revisión por Dirección**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
  - TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf 
- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.
  - TFM_PROC_Procesos, Roles y Responsabilidades.pdf 
    - **Metodología de Análisis de Riesgos**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

- TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf

- **Declaración de Aplicabilidad**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.
  - TFM_Declaración de Aplicabilidad SOA.xlsx

Y se está apoyando en la existencia de Registros de apoyo sobre los documentos desarrollados:

- **Registro Acciones**: Acciones a realizar en el SGSI como consecuencia de la Gestión de los Riesgos detectados, las oportunidades de mejora halladas, la gestión de las No Conformidades aparecidas, etc.
  - TFM_REG_Acciones.xlsx

- **Registro de No conformidades y Acciones correctivas**: Como consecuencia de las acciones de auditoría desarrolladas.
  - TFM_REG_NC y Acciones Correctivas.xlsx

- **Registro para la Medición de los objetivos del SGSI, creación y seguimiento de indicadores**.
  - TFM_REG_Medición de Objetivos.xlsx

- **Registros de Roles, Responsabilidades y Competencias** que afectan al Seguridad de la Información dentro de la organización.
  - TFM_REG_Roles Responsabilidades y Competencias.xlsx

- **Registro de apoyo para la Gestión de las Auditorías** en el SGSI.
  - TFM_REG_Programa de Auditoria.xls
  - TFM_REG_Plan de Auditoría.xlsx

2.2. Esquema Documental

A continuación, se detallan los Documentos y registros de base desarrollados para construir las bases del SGSI en la organización **GLOBALSOC**, en base al alcance establecido (SOC MADRID) y su relación con el SGSI.

MAPA DE DOCUMENTACIÓN DESARROLLADA DEL SGSI- (Según el referencial de ISO27001 - PLAN / DO / CHECK / ACT)					
#	**Dominio**	**Control #**	**Descripción del Control**	**Documentación Desarrollada**	**Registros**
4. CONTEXTO DE LA ORGANIZACIÓN					
		Cláusula 4.1.	**4.1 Comprensión de la organización y de su contexto**	**TFM_plan de implementación ISO 27001-SOC.pdf**	
		Cláusula 4.2.	**4.2 Comprensión de las necesidades y expectativas de las partes interesadas**	**TFM_plan de implementación ISO 27001-SOC.pdf**	
		Cláusula 4.3.	**4.3 Determinación del alcance del sistema de gestión de seguridad de la información**	**TFM_plan de implementación ISO 27001-SOC.pdf**	
		Cláusula 4.4.	**4.4 Sistema de gestión de seguridad de la información**		
5. LIDERAZGO					
		Cláusula 5.1	**5.1 Liderazgo y compromiso**		
		Cláusula 5.2	**5.2 Política**	**TFM_Politica de Seguridad.pdf**	
		Cláusula 5.3	**5.3 Roles, responsabilidades y autoridades en la organización**	**TFM_plan de implementación ISO 27001-SOC.pdf TFM_PROC_Procesos, Roles y Responsabilidades.pdf**	**TFM_REG_Roles Responsabilidades y Competencias.xls**
6. PLANIFICACION					
		Cláusula 6.1.1	**6.1.1. Acciones para tratar los riesgos y oportunidades. Consideraciones generales**	**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf**	**TFM_REG_Acciones.xls**
		Cláusula 6.1.2	**6.1.2 Apreciación de riesgos de seguridad de la información**		
		Cláusula 6.1.3	**6.1.3 Tratamiento de los riesgos de seguridad de la información**		
		Cláusula 6.2	**6.2 Objetivos de seguridad de la información y planificación para su consecución**	**TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf**	**TFM_REG_Medición de Objetivos.xls**
7. SOPORTE					
		Cláusula 7.1	**7.1 Recursos**		
		Cláusula	**7.2 Competencia**		

MAPA DE DOCUMENTACIÓN DESARROLLADA DEL SGSI- (Según el referencial de ISO27001 - PLAN / DO / CHECK / ACT)					
#	Dominio	Control #	Descripción del Control	Documentación Desarrollada	Registros
		7.2			
		Cláusula 7.3	7.3 Concienciación		
		Cláusula 7.4	7.4 Comunicación		
		Cláusula 7.5	7.5 Información documentada		
8. OPERACIÓN					
		Cláusula 8.1	8.1 Planificación y control operacional		
		Cláusula 8.2	8.2 Apreciación de los riesgos de seguridad de información	TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf	
		Cláusula 8.3	8.3 Tratamiento de los riesgos de seguridad de información	TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf	
9. EVALUACION DEL DESEMPEÑO					
		Cláusula 9.1	9.1 Seguimiento, medición, análisis y evaluación	TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf	
		Cláusula 9.2	9.2 Auditoría interna	TFM_PROC_Procedimiento de Auditorias Internas.pdf	TFM_REG_Programa de Auditoria.xls TFM_REG_Plan de Auditoría.xls TFM_REG_Acciones.xls TFM_REG_NC y Acciones Correctivas.xls
		Cláusula 9.3	9.3 Revisión por la dirección	TFM_PROC_Objetivos de Seguridad, Indicadores y Métrica.pdf (3.6. Seguimiento y medición de métricas y objetivos de seguridad)	TFM_REG_Acciones.xls TFM_REG_NC y Acciones Correctivas.xls
10. MEJORA					

MAPA DE DOCUMENTACIÓN DESARROLLADA DEL SGSI- (Según el referencial de ISO27002 -Controles de Seguridad-Aplicabilidad SOA	
Descripción	Registros
APLICABILIDAD SOA	TFM_Declaración de Aplicabilidad SOA.xls

16-Tabla-Documentos SGSI

3. ANÁLISIS DE RIESGOS

3.1. Introducción

Teniendo en consideración los procesos y activos que forman parte del alcance del SGSI, incluyendo elementos tales como las personas, los sistemas de información, la información, los edificios y dependencias y, cualquier otro que sea necesario para garantizar la disponibilidad de los servicios esenciales se va a acometer el análisis del riesgo de dichos activos en base a la aplicación de la Metodología de Análisis y Gestión de Riesgos de la Seguridad de la Información.

- TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf

  De manera resumida para realizar el proceso de Análisis, valoración y Análisis de riesgos a los que están sometidos los activos de información se va a acometer de la siguiente forma:

En primer lugar, realizaremos el proceso de la obtención del **Inventario de los Activos** organizados y clasificados en base a un referencial de categorización (tal y como se muestra en la siguiente tabla).

Activos (Tipos)
▪ **Información y Servicios de Negocio (B)** ▪ **Servicios** ➢ Internos (SI), Externos (SE) ▪ **Sistemas de Información (SI)** ➢ Hardware (HW), Software (SW) ▪ **Comunicaciones (COM)** ▪ **Proveedores (SS)** ➢ Servicios esenciales, IT (Datacenter, otros), Otros ▪ **Personal (P)** ➢ Interno, Externo ▪ **Instalaciones y ubicaciones (L)** ➢ Dependencias, Salas técnicas, Edificios, Otras

17-Tabla-Categoría de activos

En segundo lugar, se considerarán las **Dependencias existentes entre los activos** declarados; dado que los activos están relacionados entre sí en cuanto a uso, su operación, su soporte, su tratamiento, etc. Una vez establecidas las relaciones entre los mismos vamos a poder explotar las consecuencias y afectaciones de unos activos respecto a otros y establecer el grado de influencia desde la perspectiva de la Seguridad de la información.

En tercer lugar, se realizará una **Valoración de los activos** en base a la consideración de la valoración de la criticidad de los activos desde la perspectiva de la degradación y o pérdida de los mismos en base al concepto de

Dimensiones de Seguridad (MAGERIT-Libro II Catálogo de Elementos, s.f.)

- **Disponibilidad**: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad**: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Y se establecerá una gradación para cada una de las dimensiones en base a la siguiente tabla:

Gradación Impacto-Dimensiones de Seguridad
• **Muy alto (9-10)** • **Alto (7-8)** • **Medio (4-6)** • **Bajo (2-3)** • **Muy bajo (0-1)**

18-Tabla-Gradación impacto DS

En cuarto lugar, se **Identificarán y evaluarán las Amenazas** para cada activo afectado y se valorará en términos de la frecuencia/probabilidad que se materialice la amenaza, así como el Porcentaje de degradación del activo si la amenaza declarada se llegara a materializar.

Como consecuencia de todo lo anterior obtendremos el **Riesgo Potencial** como la consecuencia Directa del impacto provocado por la materialización de las amenazas sobre os activos afectados.

A continuación, se realiza el desarrollo del proceso.

3.2. Inventario de activos

A continuación, se muestra la relación de Activos agrupada en base a los criterios de Categorización (**17-Tabla-Categoría de activos**).

INVENTARIO DE ACTIVOS-GLOBAL SOC		
Ámbito	**Clasificación**	**Activo**
[B] Activos esenciales	**[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES**	**[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS**
		[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)
		[B_D_SG_DES_TEC] Información Técnica de los Proyectos
		[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto
	[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS	**[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)**
		[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación

INVENTARIO DE ACTIVOS-GLOBAL SOC		
Ámbito	**Clasificación**	**Activo**
		[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)
	[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS	[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación
		[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)
		[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)
		[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)
		[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes
		[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES
		[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC
		[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC
		[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES
[SRV] Servicios	[SRVI] Servicios Internos	
	[SRVI_IT] SERVICIOS GESTIONADOS IT	[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE
		[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS
		[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS
	[SRVI_ADMIN] Servicios Corporativos	[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización
		[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales
		[SRVI_CORP_OPERACIONES] OPERACIONES
		[SRVI_CORP_RRHH] Área de RR.HH.
		[SRV_CORP_OPER] Dirección de Operaciones
	[SRVE] Servicios Externos	[SRVE_CORREO] Servicio de Correo (GOOGLE)
		[SRVE_DATACENTER] Servicio de CPD y Comunicaciones
		[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage
[SI] Sistema de Información	[HW] Hardware	
	[SI_HW_CLOUD_GOOGLE]	[SI_HW_SERV_DA] Servidores de DA
		[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus
		[SI_HW_SD_HD] Servidor Service Desk/Help Desk
		[SI_HW_SFTP] Servidor Servicio de transferencia ficheros
		[SI_HW_DATASTORE] Almacenamiento y Backup
		[SI_HW_WEB_CORP] Servidores Web Corporativa
		[SI_HW_CERTIF] Servidor de Certificados
	[SI_HW_DATACENTER]	[SI_HW_SIEM] Servidor SIEM
		[SI_HW_AD_3] Servidor Controlador DominIo (AD)
		[SI_HW_MONITOR] Servidor de Monitorización
		[SI_HW_GEST_PROY] Servidor Gestión de Proyectos

INVENTARIO DE ACTIVOS-GLOBAL SOC		
Ámbito	**Clasificación**	**Activo**
		[SI_HW_WIKI] Servidor de la Wiki
		[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup
		[SI_HW_CORREO] Relay del Correo
	[SI_HW_VIRTUAL] Plataforma Virtualización	[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)
		[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS
		[SI_HW_VM_CREDEN] Servidores Credenciales
		[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos
		[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos
		[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo
		[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos
		[SI_HW_NAS] Servidor de Almacenamiento NAS
		[SI_HW_VM_MONITOR] Sistema de Monitorización
		[SI_HW_SERV_LAB] Servidores laboratorio
	[SI_HW_GLOBALSOC_Sede_MADRID]	[SI_HW_PC] PC de Sobremesa
		[SI_HW_TFNO_MOVIL] Teléfono Móvil
		[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP
		[SI_HW_IMPRES] Equipos de Impresión
	[SI_HW_SOC_MAD] Hardware SOC de MADRID	[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD
		[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid
	[SW] Software	[SI_SW_Windows] S.O. Puesto de Trabajo
		[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos
		[SI_SW_Office] S.O. Puesto de Trabajo (Office)
		[SI_SW_ANTIVIRUS] Software Antivirus
		[SI_SW_ALM_NUBE] Google Drive
		[SI_SW_WINDOWS] Windows Server
		[SI_SW_LINUX] Software Linux
	[SI_SW_CLOUD_GOOGLE]	[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)
		[SI_SW_SERVICE DESK] Service Desk-Help Desk
		[SI_SW_SFTP] Servicios SFTP
		[SI_SW_CERTIFICADOS] Servicios Certificados
		[SI_SW_BACKUP] Servicios de Storage (DataStore)
		[SI_SW_WEB] Servicios Web Corporativos
		[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus
	[SI_SW_DATACENTER]	[SI_SW_SIEM] Software SIEM
		[SI_SW_HYPERVISOR] Software Virtualización
		[SI_SW_IPS] Software IPS
		[SI_SW_ANAL_DATA] Software Analítica de Datos
		[SI_SW_IDS] Software IDS
		[SI_SW_MONITOR] Software de Monitorización
		[SI_SW_SERV_FICH] Software de Servicio de Ficheros
		[SI_SW_WIKI] Software Wiki
		[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs
		[SI_SW_CREDENCIALES] Software Gest. Credenciales
		[SI_SW_RELAY CORREO] POSTFIX
[COM] Comunicacion	[COM_RED GOOGLE] Segmentación red	[COM_LAN_GOOGLE] Red GOOGLE
		[COM_FW_GOOGLE] Firewall Google

INVENTARIO DE ACTIVOS-GLOBAL SOC		
Ámbito	**Clasificación**	**Activo**
es	**(DMZ, cloud-mz, default, SHARED-XPN)**	**[COM_SWT_GOOGLE] Switches GOOGLE**
	[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)	**[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE**
		[COM_LAN_DATACENTER] Red DATACENTER
		[COM_SWT_DATACENTER] Switches DATACENTER
		[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)
	[COM_RED_GLOBALSOC_Sede_MADRID] Segmentación Red (oficina, Voz Ip,BiometrÍa, Dispositivos, SOC)	**[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid**
		[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid
		[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER
		[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD
		[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)
[SS] Proveedores	**[SS_ES] Servicios Esenciales**	**[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)**
		[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC
		[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)
	[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)	**[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5**
		[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7
	[SS_OT] Otros	**[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC**
		[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita
[P] Personal	**[P_I] Personal Interno**	**[P_I_SOC] Personal Interno del SOC MAD**
		[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID
		[P_I_FIN_LEG] Personal Resp. Financiero y Legal
		[P_I_RRHH] Personal Resp. RR.HH.
		[P_I_Comercial] Personal Área Comercial y Marketing
	[P_E] Personal Externo	**[P_E_MTO] Personal de Limpieza y Mantenimiento**
[L] Instalaciones y Ubicaciones	**[LD] Dependencias**	**[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid**
		[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
		[LD_GOOGLE_CLOUD] Cpd de GOOGLE
		[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID
	[LS] Salas Técnicas	**[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones**
	[LO] Otros	
	[LE] Edificios	**[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid**

19-Tabla-Inventario de activos

3.3. Dependencias de Activos

En base a las relaciones y dependencias existentes entre los distintos a activos, se establece un mapa de dependencias.

Cuando realicemos la valoración del impacto sobre los activos tendremos en cuenta estas dependencias para calcular el impacto resultante.

Una vez establecida las dependencias entre los distintos activos que configuran el mapa de activos; que nos va a posibilitar el poder considerar el grado de afectación en el impacto, respecto a las Dimensiones de Seguridad, de unos activos respecto a otros; se estará preparado para poder realizar la valoración de los activos.

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
[B] Activos esenciales	[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	[SRVI_IT_DESPL] , [SRVI_IT_INCID], [SRVI_IT_CAMB] , [SRVI_CORP_COMERCIAL] , [SRVI_CORP_FINAN&LEGAL]
		[SRVI_CORP_OPERACIONES], [SRVI_CORP_RRHH] , [SRV_CORP_OPER] , [SRVE_DATACENTER] , [SRVE_CLOUD_GOOGLE]
	[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES	
	[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	[SI_SW_GEST-PROY]
	[B_D_SG_DES_TEC] Información Técnica de los Proyectos	[SI_SW_ALM_NUBE]
	[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	[SI_SW_ALM_NUBE]
	[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS	
	[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	
	[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	
	[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	
	[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS	
	[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	
	[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	
	[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	
	[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	[SI_HW_VM_CREDEN] , [SI_HW_VM_IPS] , [SI_HW_VM_IDS] , [SI_HW_VM_POSTFIX_CORREO] , [SI_HW_VM_ANAL_DATA]
	[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	[SI_SW_ALM_NUBE]
	[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	[SI_SW_ALM_NUBE]
	[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	[SI_SW_ALM_NUBE]
	[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	[SI_SW_ALM_NUBE]
	[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	[SI_SW_ALM_NUBE]
[SRV] Servicios	[SRVI] Servicios Internos	
	[SRVI_IT] SERVICIOS GESTIONADOS IT	
	[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	[B_D_SG_DES_PROYECTOS], [B_D_SG_DES_TEC] , [B_D_SG_DES_CLI] , [B_D_SG_DES_CRED] , [B_D_SG_CAM_CONTRATOS_CLIENTES] , [SRVE_CLOUD_GOOGLE] ,[SRVE_DATACENTER] , [SI_HW_PC] , [SI_HW_PC_SOC_MAD] , [SI_HW_PORTATIL_SOC_MAD] , [SI_SW_Windows], [SI_SW_GEST-PROY] , [SI_SW_LINUX]

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
		[B_D_SG_CONF_CLIENTES] , [B_D_SG_CONF_GLOBALSOC] , [B_D_SG_CAM_ARQ-SIS-GLOBALSOC], [B_D_SG_CAM_ARQ-SIS-CLIENTES], [SRVE_CORREO] ,[SI_SW_SERV_FICH] , [SI_SW_CREDENCIALES] ,[COM_VPN_DATACENTER] ,[COM_LAN_DATACENTER] ,[COM_SWT_DATACENTER] ,[COM_FW_DATACENTER] ,[P_I_SOC]
	[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	[B_D_SG_INC_Incidencias],[B_D_SG_INC_DOC],[B_D_SG_INC_ BBDD del Conocimiento], [B_D_SG_DES_CRED],[B_D_SG_CAM_CONTRATOS_CLIENTES], [B_D_SG_CONF_CLIENTES], [B_D_SG_CONF_GLOBALSOC], [B_D_SG_CAM_ARQ-SIS-GLOBALSOC], [B_D_SG_CAM_ARQ-SIS-CLIENTES], [SRVE_CORREO], [SI_SW_Windows], [SI_SW_GEST-PROY], [SI_SW_Office], [SI_SW_ANTIVIRUS], [SI_SW_ALM_NUBE],[SI_SW_LINUX], [SI_SW_DA], [SI_SW_SERVICE DESK],[SI_SW_SFTP], [SI_SW_CERTIFICADOS], [SI_SW_BACKUP], [SI_SW_WEB],[SI_SW_CONSOLA_ANTIVIRUS],[SI_SW_SIEM], [SI_SW_HYPERVISOR], [SI_SW_IPS],[SI_SW_ANAL_DATA],[SI_SW_IDS], [SI_SW_MONITOR], [SI_SW_SERV_FICH],[SI_SW_RECOLECTOR], [SI_SW_CREDENCIALES], [SI_SW_RELAY CORREO], [COM_LAN_GOOGLE], [COM_VPN_DATACENTER],[COM_LAN_DATACENTER], [P_I_SOC]
	[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	[B_D_SG_CAM_PROC],[B_D_SG_CAM_RFC], [B_D_SG_CAM_PETICIONES],[B_D_SG_DES_CRED], [B_D_SG_CAM_CONTRATOS_CLIENTES],[B_D_SG_CONF_CLIENTES], [B_D_SG_CONF_GLOBALSOC], [B_D_SG_CAM_ARQ-SIS-GLOBALSOC], [B_D_SG_CAM_ARQ-SIS-CLIENTES], [SRVE_CORREO], [SI_SW_Windows], [SI_SW_Office],[SI_SW_ALM_NUBE], [SI_SW_LINUX], [SI_SW_DA], [SI_SW_CERTIFICADOS], [SI_SW_BACKUP], [SI_SW_IPS],[SI_SW_ANAL_DATA], [SI_SW_IDS], [SI_SW_WIKI],[SI_SW_RELAY CORREO],[COM_LAN_GOOGLE], [COM_VPN_DATACENTER], [COM_LAN_DATACENTER], [P_I_SOC]
	[SRVI_ADMIN] Servicios Corporativos	
	[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	[P_I_Comercial]
	[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	[P_I_OFI] , [P_I_FIN_LEG] , [P_I_RRHH]
	[SRVI_CORP_OPERACIONES] OPERACIONES	[SS_ES_ADMIN_EDIFICIO],[SS_ES_BIOMETRIA_SOC],[SS_ES_WIFI],[P_I_OFI],[P_I_FIN_LEG],[P_I_RRHH]
	[SRVI_CORP_RRHH] Área de RR.HH.	[P_I_OFI], [P_I_FIN_LEG], [P_I_RRHH]
	[SRV_CORP_OPER] Dirección de Operaciones	[P_I_OFI], [P_I_FIN_LEG], [P_I_RRHH], [SI_SW_Windows], [SI_SW_Office], [COM_RED_GLOBALSOC_Sede_MADRID]
	[SRVE] Servicios Externos	
	[SRVE_CORREO] Servicio de Correo (GOOGLE)	[COM_RED DATACENTER],[SS_IT_SG_PROVEEDORES_24*7]
	[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	[COM_RED DATACENTER],[SS_IT_SG_PROVEEDORES_24*7]
	[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	[COM_RED GOOGLE,[SS_IT_SG_PROVEEDORES_24*7
[SI] Sistema de Información	[HW] Hardware	
	[SI_HW_CLOUD_GOOGLE]	
	[SI_HW_SERV_DA] Servidores de DA	[SI_SW_WINDOWS, [SI_SW_DA], [P_I_SOC] ,[LD_GOOGLE_CLOUD]
	[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	[SI_SW_WINDOWS], [SI_SW_CONSOLA_ANTIVIRUS], [P_I_SOC],[LD_GOOGLE_CLOUD]
	[SI_HW_SD_HD] Servidor Service Desk/Help Desk	[SI_SW_LINUX], [SI_SW_SERVICE DESK], [SI_SW_SFTP], [SI_SW_CERTIFICADOS], [P_I_SOC], [LD_GOOGLE_CLOUD],
	[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	[SI_SW_LINUX], [SI_SW_SERVICE DESK], [SI_SW_SFTP], [SI_SW_CERTIFICADOS],[P_I_SOC], [LD_GOOGLE_CLOUD]

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
	[SI_HW_DATASTORE] Almacenamiento y Backup	[SI_HW_CONSOLA_ANTIVIRUS],[SI_SW_LINUX], [SI_SW_BACKUP], [P_I_SOC], [LD_GOOGLE_CLOUD]
	[SI_HW_WEB_CORP] Servidores Web Corporativa	[SI_SW_LINUX], [SI_SW_WEB], [SI_SW_CONSOLA_ANTIVIRUS], [P_I_SOC], [LD_GOOGLE_CLOUD],
	[SI_HW_CERTIF] Servidor de Certificados	[SI_SW_WINDOWS], [P_I_SOC], [LD_GOOGLE_CLOUD], [SRVE_CLOUD_GOOGLE]
	[SI_HW_DATACENTER]	
	[SI_HW_SIEM] Servidor SIEM	[SI_SW_LINUX],[SI_SW_SIEM],[SI_SW_HYPERVISOR],[SI_SW_IPS], [SI_SW_ANAL_DATA], [SI_SW_IDS], [P_I_SOC]
	[SI_HW_AD_3] Servidor Controlador DominIo (AD)	[SI_SW_LINUX],[SI_SW_SIEM],[SI_SW_HYPERVISOR],[SI_SW_IPS],[SI_SW_ANAL_DATA],[SI_SW_IDS],[P_I_SOC]
	[SI_HW_MONITOR] Servidor de Monitorización	[SI_SW_LINUX], [SI_SW_MONITOR], [SI_SW_SERV_FICH], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	[SI_SW_LINUX], [SI_SW_MONITOR], [SI_SW_SERV_FICH], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_WIKI] Servidor de la Wiki	[SI_SW_LINUX], [SI_SW_WIKI], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	[SI_SW_LINUX], [SI_SW_WIKI], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_CORREO] Relay del Correo	[SI_SW_LINUX], [SI_SW_RELAY CORREO], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_VIRTUAL] Plataforma Virtualización	
	[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	
	[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	[SI_SW_LINUX], [SI_SW_RECOLECTOR], [P_I_SOC], [LD_DATACENTER],
	[SI_HW_VM_CREDEN] Servidores Credenciales	[SI_SW_WINDOWS], [SI_SW_CREDENCIALES], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	[SI_SW_WINDOWS], [SI_SW_CREDENCIALES], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	[SI_SW_WINDOWS], [SI_SW_CREDENCIALES], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	[SI_SW_WINDOWS], [SI_SW_CREDENCIALES], [P_I_SOC], [LD_DATACENTER]
	[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	[SI_SW_WINDOWS],[SI_SW_CREDENCIALES],[P_I_SOC],[LD_DATACENTER],
	[SI_HW_NAS] Servidor de Almacenamiento NAS	
	[SI_HW_VM_MONITOR] Sistema de Monitorización	
	[SI_HW_SERV_LAB] Servidores laboratorio	[SI_SW_WINDOWS] Windows Server,[SI_SW_LINUX] Software Linux,[P_I_SOC] Personal Interno del SOC MAD,[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid,[SRVE_DATACENTER] Servicio de CPD y Comunicaciones
	[SI_HW_GLOBALSOC_Sede_MADRID]	
	[SI_HW_PC] PC de Sobremesa	[SI_SW_Windows] S.O. Puesto de Trabajo,[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos,[SI_SW_Office] S.O. Puesto de Trabajo (Office),[SI_SW_ANTIVIRUS] Software Antivirus,SI_SW_ALM_NUBE] Google Drive,[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID,[P_I_FIN_LEG] Personal Resp. Financiero y Legal,[P_I_RRHH] Personal Resp. RR.HH., [P_I_Comercial] Personal Área Comercial y Marketing,[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[SI_HW_TFNO_MOVIL] Teléfono Móvil	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC,[P_I_SOC] Personal Interno del SOC MAD,[P_I_Comercial] Personal Área Comercial y Marketing
	[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita,[P_I_SOC] Personal Interno del SOC MAD,[P_I_Comercial] Personal Área Comercial y Marketing
	[SI_HW_IMPRES] Equipos de Impresión	[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID,[P_I_FIN_LEG] Personal Resp. Financiero y Legal, [P_I_RRHH] Personal Resp. RR.HH.,[P_I_Comercial] Personal Área Comercial y Marketing,[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[SI_HW_SOC_MAD] Hardware SOC de MADRID	

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
	[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	[SI_SW_Windows] S.O. Puesto de Trabajo,[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos,[SI_SW_Office] S.O. Puesto de Trabajo (Office),[SI_SW_ANTIVIRUS] Software Antivirus, [SI_SW_ALM_NUBE] Google Drive,[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID,[P_I_FIN_LEG] Personal Resp. Financiero y Legal,[P_I_RRHH] Personal Resp. RR.HH., [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	[SI_SW_Windows] S.O. Puesto de Trabajo,[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos,[SI_SW_Office] S.O. Puesto de Trabajo (Office),[SI_SW_ANTIVIRUS] Software Antivirus, [SI_SW_ALM_NUBE] Google Drive,[P_I_SOC] Personal Interno del SOC MAD,[P_I_Comercial] Personal Área Comercial y Marketing,[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID, [SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5
	[SW] Software	
	[SI_SW_Windows] S.O. Puesto de Trabajo	[SI_HW_PC] PC de Sobremesa,[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD,[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid
	[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	[SI_HW_GEST_PROY] Servidor Gestión de Proyectos
	[SI_SW_Office] S.O. Puesto de Trabajo (Office)	[SI_HW_PC] PC de Sobremesa,[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD,[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid
	[SI_SW_ANTIVIRUS] Software Antivirus	[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus
	[SI_SW_ALM_NUBE] Google Drive	[SI_HW_DATASTORE] Almacenamiento y Backup
	[SI_SW_WINDOWS] Windows Server	[SI_HW_SERV_DA] Servidores de DA,[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus,[SI_HW_SD_HD] Servidor Service Desk/Help Desk,[SI_HW_SFTP] Servidor Servicio de transferencia ficheros, [SI_HW_CERTIF] Servidor de Certificados,[SI_HW_AD_3] Servidor Controlador DominIo (AD),[SI_HW_MONITOR] Servidor de Monitorización,[SI_HW_GEST_PROY] Servidor Gestión de Proyectos, [SI_HW_WIKI] Servidor de la Wiki,[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup,[SI_HW_VIRTUAL] Plataforma Virtualización
	[SI_SW_LINUX] Software Linux	[SI_HW_CERTIF] Servidor de Certificados,[SI_HW_WIKI] Servidor de la Wiki,[SI_HW_CORREO] Relay del Correo,[SI_HW_VM_MONITOR] Sistema de Monitorización,[SI_HW_SERV_LAB] Servidores laboratorio
	[SI_SW_CLOUD_GOOGLE]	
	[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	[SI_HW_SERV_DA] Servidores de DA
	[SI_SW_SERVICE DESK] Service Desk-Help Desk	[SI_HW_SD_HD] Servidor Service Desk/Help Desk
	[SI_SW_SFTP] Servicios SFTP	[SI_HW_SFTP] Servidor Servicio de transferencia ficheros
	[SI_SW_CERTIFICADOS] Servicios Certificados	[SI_HW_CERTIF] Servidor de Certificados
	[SI_SW_BACKUP] Servicios de Storage (DataStore)	[SI_HW_DATASTORE] Almacenamiento y Backup
	[SI_SW_WEB] Servicios Web Corporativos	[SI_HW_WEB_CORP] Servidores Web Corporativa
	[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus
	[SI_SW_DATACENTER]	
	[SI_SW_SIEM] Software SIEM	[SI_HW_SIEM] Servidor SIEM
	[SI_SW_HYPERVISOR] Software Virtualización	[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)
	[SI_SW_IPS] Software IPS	[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos
	[SI_SW_ANAL_DATA] Software Analítica de Datos	[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos, [SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos
	[SI_SW_IDS] Software IDS	[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos
	[SI_SW_MONITOR] Software de Monitorización	[SI_HW_MONITOR] Servidor de Monitorización,[SI_HW_VM_MONITOR] Sistema de Monitorización
	[SI_SW_SERV_FICH] Software de Servicio de	[SI_HW_NAS] Servidor de Almacenamiento NAS

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
	Ficheros	
	[SI_SW_WIKI] Software Wiki	[SI_HW_WIKI] Servidor de la Wiki
	[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs	[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS
	[SI_SW_CREDENCIALES] Software Gest. Credenciales	[SI_HW_VM_CREDEN] Servidores Credenciales
	[SI_SW_RELAY CORREO] POSTFIX	[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo
	[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)	
	[COM_LAN_GOOGLE] Red GOOGLE	[COM_FW_GOOGLE] Firewall Google,[COM_SWT_GOOGLE] Switches GOOGLE,[P_I_SOC] Personal Interno del SOC MAD,[LD_GOOGLE_CLOUD] Cpd de GOOGLE
	[COM_FW_GOOGLE] Firewall Google	
	[COM_SWT_GOOGLE] Switches GOOGLE	
	[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)	
	[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	
	[COM_LAN_DATACENTER] Red DATACENTER	[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE,[COM_SWT_DATACENTER] Switches DATACENTER,[COM_FW_DATACENTER] Firewall Datacenter (Redundancia),[P_I_SOC] Personal Interno del SOC MAD,[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID
	[COM_SWT_DATACENTER] Switches DATACENTER	
	[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	
	[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)	
	[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER,[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD,[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia),[P_I_SOC] Personal Interno del SOC MAD,[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER
	[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	
	[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	
	[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	
	[SS_ES] Servicios Esenciales	
	[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	
	[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	
	[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	
	[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)	
	[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	
	[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	
	[SS_OT] Otros	
	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC	
	[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	
[P] Personal		
	[P_I] Personal Interno	

Dependencias entre los Activos		
Ámbito	**Activos**	**Dependencias**
	[P_I_SOC] Personal Interno del SOC MAD	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC,[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid
	[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC, [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[P_I_FIN_LEG] Personal Resp. Financiero y Legal	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC, [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
		[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC, [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[P_I_RRHH] Personal Resp. RR.HH.	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC, [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[P_I_Comercial] Personal Área Comercial y Marketing	[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC, [LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[P_E] Personal Externo	
	[P_E_MTO] Personal de Limpieza y Mantenimiento	
[L] Instalaciones y Ubicaciones		
	[LD] Dependencias	
	[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC,[P_I_SOC] Personal Interno del SOC MAD,[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC,[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA),[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid
	[LD_GOOGLE_CLOUD] Cpd de GOOGLE	[COM_LAN_GOOGLE] Red GOOGLE,[COM_FW_GOOGLE] Firewall Google,[COM_SWT_GOOGLE] Switches GOOGLE,[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE
	[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD),[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE,[COM_LAN_DATACENTER] Red DATACENTER,[COM_SWT_DATACENTER] Switches DATACENTER,[COM_FW_DATACENTER] Firewall Datacenter (Redundancia),[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7
	[LS] Salas Técnicas	
	[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid,[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD,[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia),[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID
	[LO] Otros	
	[LE] Edificios	
	[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)

20-Tabla-Mapa dependencia entre activos

3.3.1. Mapa resumen Dependencias de Activos

A continuación, se muestra el resumen de las dependencias entre los distintos activos declarados en el inventario.

Dependencias Activos	Activos a los que afecta		Activos por los que es afectado	
	Directa	Total	Directa	Total
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	0	0	10	103

Dependencias Activos	Activos a los que afecta		Activos por los que es afectado	
	Directa	Total	Directa	Total
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	1	2	1	59
[B_D_SG_DES_TEC] Información Técnica de los Proyectos	1	2	1	61
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	1	2	1	61
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	1	2	0	0
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	1	2	0	0
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	1	2	0	0
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	1	2	0	0
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	1	2	0	0
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	1	2	0	0
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	3	4	5	58
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	3	4	1	61
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	3	4	1	61
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	3	4	1	61
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	3	4	1	61
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	3	4	1	61
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	1	1	25	85
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	1	1	37	86
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	1	1	26	82
[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	1	1	1	7
[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	1	1	3	9
[SRVI_CORP_OPERACIONES] OPERACIONES	1	1	6	9
[SRVI_CORP_RRHH] Área de RR.HH.	1	1	3	9
[SRV_CORP_OPER] Dirección de Operaciones	1	1	3	9
[SRVE_CORREO] Servicio de Correo (GOOGLE)	3	4	2	2
[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	3	3	2	2
[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	3	3	2	2
[SI_HW_SERV_DA] Servidores de DA	2	61	4	58
[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	4	61	4	58
[SI_HW_SD_HD] Servidor Service Desk/Help Desk	2	61	6	58
[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	2	61	6	58
[SI_HW_DATASTORE] Almacenamiento y Backup	2	20	5	60
[SI_HW_WEB_CORP] Servidores Web Corporativa	1	4	5	60
[SI_HW_CERTIF] Servidor de Certificados	3	61	3	58

Dependencias Activos	Activos a los que afecta		Activos por los que es afectado	
	Directa	Total	Directa	Total
[SI_HW_SIEM] Servidor SIEM	1	61	8	58
[SI_HW_AD_3] Servidor Controlador DominIo (AD)	1	61	8	58
[SI_HW_MONITOR] Servidor de Monitorización	2	61	5	58
[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	2	61	5	58
[SI_HW_WIKI] Servidor de la Wiki	3	61	4	58
[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	1	61	4	58
[SI_HW_CORREO] Relay del Correo	1	61	4	58
[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	1	62	0	0
[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	1	4	4	60
[SI_HW_VM_CREDEN] Servidores Credenciales	2	61	4	58
[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	3	61	4	58
[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	2	61	4	58
[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	2	61	4	58
[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	2	61	4	58
[SI_HW_NAS] Servidor de Almacenamiento NAS	1	62	0	0
[SI_HW_VM_MONITOR] Sistema de Monitorización	2	61	0	0
[SI_HW_SERV_LAB] Servidores laboratorio	1	61	4	58
[SI_HW_PC] PC de Sobremesa	3	10	10	72
[SI_HW_TFNO_MOVIL] Teléfono Móvil	0	0	3	9
[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	0	0	3	10
[SI_HW_IMPRES] Equipos de Impresión	0	0	5	10
[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	3	10	9	72
[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	3	10	8	72
[SI_SW_Windows] S.O. Puesto de Trabajo	7	10	3	72
[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	6	11	1	58
[SI_SW_Office] S.O. Puesto de Trabajo (Office)	6	10	3	72
[SI_SW_ANTIVIRUS] Software Antivirus	4	10	1	58
[SI_SW_ALM_NUBE] Google Drive	12	17	1	60
[SI_SW_WINDOWS] Windows Server	9	61	11	58
[SI_SW_LINUX] Software Linux	16	61	5	58
[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	3	61	1	58
[SI_SW_SERVICE DESK] Service Desk-Help Desk	3	61	1	58
[SI_SW_SFTP] Servicios SFTP	3	61	1	58
[SI_SW_CERTIFICADOS] Servicios Certificados	4	61	1	58
[SI_SW_BACKUP] Servicios de Storage (DataStore)	3	20	1	60
[SI_SW_WEB] Servicios Web Corporativos	2	4	1	60
[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	3	61	1	58
[SI_SW_SIEM] Software SIEM	3	61	1	58
[SI_SW_HYPERVISOR] Software Virtualización	3	61	1	1
[SI_SW_IPS] Software IPS	4	61	1	58

Dependencias Activos	Activos a los que afecta		Activos por los que es afectado	
	Directa	Total	Directa	Total
[SI_SW_ANAL_DATA] Software Analítica de Datos	4	61	2	58
[SI_SW_IDS] Software IDS	4	61	1	58
[SI_SW_MONITOR] Software de Monitorización	3	61	2	58
[SI_SW_SERV_FICH] Software de Servicio de Ficheros	4	61	1	1
[SI_SW_WIKI] Software Wiki	3	61	1	58
[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs	2	4	1	60
[SI_SW_CREDENCIALES] Software Gest. Credenciales	7	61	1	58
[SI_SW_RELAY CORREO] POSTFIX	3	61	1	58
[COM_LAN_GOOGLE] Red GOOGLE	3	63	4	13
[COM_FW_GOOGLE] Firewall Google	2	63	0	0
[COM_SWT_GOOGLE] Switches GOOGLE	2	63	0	0
[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	6	65	0	0
[COM_LAN_DATACENTER] Red DATACENTER	4	63	5	15
[COM_SWT_DATACENTER] Switches DATACENTER	3	63	0	0
[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	3	63	0	0
[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	0	0	5	11
[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	1	1	1	1
[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	2	3	0	0
[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	2	2	0	0
[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	2	2	0	0
[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	2	83	0	0
[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	3	82	0	0
[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	2	82	0	0
[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	1	1	0	0
[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	4	68	0	0
[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC	6	80	0	0
[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	1	1	0	0
[P_I_SOC] Personal Interno del SOC MAD	31	70	2	8
[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	7	15	2	6
[P_I_FIN_LEG] Personal Resp. Financiero y Legal	7	15	2	6
[P_I_RRHH] Personal Resp. RR.HH.	7	15	2	6
[P_I_Comercial] Personal Área Comercial y Marketing	6	14	2	6
[P_E_MTO] Personal de Limpieza y Mantenimiento	0	0	0	0
[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	2	70	3	8
[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	11	81	3	4
[LD_GOOGLE_CLOUD] Cpd de GOOGLE	8	63	4	13
[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	14	63	6	15
[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	0	0	3	4

Dependencias Activos	Activos a los que afecta		Activos por los que es afectado	
	Directa	Total	Directa	Total
[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	**1**	**82**	**1**	**1**

21-Tabla-Resumen dependencia activos

3.4. Valoración de los activos

Una vez establecido el inventario de los activos y las dependencias existentes entre los mismos, se va a proceder a realizar la valoración de los activos. Para poder realizar este ejercicio se establecen los criterios en base a los cuales se va a poder realizar.

3.4.1. Criterios de valoración

La valoración de los activos se realiza en base a los criterios establecidos en la metodología de Análisis de Riesgos (**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf**).

Considerando cada uno de los activos establecidos en el inventario de activos y en base a las dimensiones de seguridad afectadas (Disponibilidad, Integridad, Confidencialidad); y tomando como base a la afectación de los criterios establecidos (**tabla Valoración de activos-criterios**), dándole una valoración comprendida dentro del rango entre 1-10.

Valoración de Activos-criterios	
Criterio	**Desglose**
Obligaciones Legales	[ ] [lro] Obligaciones legales: [ ] [9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación [ ] [7.lro] probablemente cause un incumplimiento grave de una ley o regulación [ ] [5.lro] probablemente sea causa de incumplimiento de una ley o regulación [ ] [3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación [ ] [1.lro] pudiera causar el incumplimiento leve o técnico de una ley o regulación
Seguridad	[ ] [si] Seguridad: [ ] [10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios [ ] [9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios [ ] [7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [ ] [3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente [ ] [1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
Intereses comerciales	[ ] [cei] Intereses Comerciales / Económicos: [ ] [9.cei] Nivel 9 [ ] [a] de enorme interés para la competencia [ ] [b] de muy elevado valor comercial [ ] [c] causa de pérdidas económicas excepcionalmente elevadas [ ] [d] causa de muy significativas ganancias o ventajas para individuos u organizaciones [ ] [e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros [ ] [f] causa de unos costes excepcionalmente elevados de reemplazamiento [ ] [7.cei] Nivel 7 [ ] [5.cei] Nivel 5 [ ] [3.cei] Nivel 3 [ ] [2.cei] Nivel 2 [ ] [1.cei] Nivel 1 [ ] [0.3] supondría pérdidas económicas mínimas

Valoración de Activos-criterios	
Criterio	**Desglose**
Interrupción del Servicio	[ ] [da] Interrupción del servicio: [ ] [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [ ] [9.da2] Probablemente tenga un serio impacto en otras organizaciones [ ] [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones [ ] [7.da2] Probablemente tenga un gran impacto en otras organizaciones [ ] [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones [ ] [5.da2] Probablemente cause un cierto impacto en otras organizaciones [ ] [3.da] Probablemente cause la interrupción de actividades propias de la Organización [ ] [1.da] Pudiera causar la interrupción de actividades propias de la Organización
Orden público	[ ] [po] Orden Público: [ ] [9.po] Alteración seria del orden público [ ] [6.po] Probablemente cause manifestaciones, o presiones significativas [ ] [5.po] Puede causar un significativo malestar público [ ] [4.po] Puede causar malestar público [ ] [3.po] Causa de protestas puntuales [ ] [1.po] Pudiera causar protestas puntuales
Operaciones	[ ] [olm] Operaciones: [ ] [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística [ ] [9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística [ ] [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística [ ] [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local [ ] [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local) [ ] [1.olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
Administración y Gestión	[ ] [adm] Administración y Gestión: [ ] [9.adm] probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre [ ] [7.adm] probablemente impediría la operación efectiva de la Organización [ ] [5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización [ ] [3.adm] probablemente impediría la operación efectiva de una parte de la Organización [ ] [1.adm] pudiera impedir la operación efectiva de una parte de la Organización
Pérdida de confianza (Reputación)	[ ] [lg] Pérdida de Confianza (Reputación): [ ] [9.lg] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones ... [ ] [7.lg] Probablemente causaría una publicidad negativa generalizada [ ] [5.lg] Probablemente sea causa una cierta publicidad negativa [ ] [3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización [ ] [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización [ ] [1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización [ ] [0.4] no supondría daño a la reputación o buena imagen de las personas u organizaciones
Persecución de Delitos	[ ] [crm] Persecución de Delitos: [ ] [8.crm] Impida la investigación de delitos graves o facilite su comisión [ ] [4.crm] Dificulte la investigación o facilite la comisión de delitos
Tiempo de	

Valoración de Activos-criterios	
Criterio	**Desglose**
recuperación del Servicio	[ ] [rto] Tiempo de Recuperación del Servicio: [ ] [7.rto] RTO < 4 horas [ ] [4.rto] 4 horas < RTO < 1 día [ ] [1.rto] 1 día < RTO < 5 días [ ] [0.rto] 5 días < RTO

22-Tabla-Criterios de Valoración de activos

3.4.2. Resultado de la valoración de los activos

En la siguiente tabla se presenta la valoración de los activos de la organización GLOBALSOC (ya está considerando afectación repercutida en base a las dependencias establecidas entre los distintos activos).

Esto implica que a la hora de valorar los activos en base a cada una de las dimensiones de seguridad afectadas; ya se está considerando las dependencias establecidas entre los distintos activos (en base al mapa de dependencias que ya se ha establecido).

VALORACION DE ACTIVOS								
Ámbito	**Clasificación**	**Activo**	**Valoración**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[B] Activos esenciales		**[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS**	**Muy Alto**	**[9]**				
	[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES	**[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)**	**Muy Alto**	**[9]**	**[3]**	**[2]**	**[3]**	**[3]**
		B_D_SG_DES_TEC] Información Técnica de los Proyectos	**Muy Alto**	**[9]**	**[7]**	**[7]**	**[7]**	**[6]**
		[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	**Muy Alto**	**[9]**	**[3]**	**[2]**	**[3]**	**[3]**
	[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS	**[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)**	**Muy Alto**	**[9]**	**[7]**	**[7]**	**[7]**	**[5]**
		[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	**Muy Alto**	**[9]**	**[3]**	**[3]**	**[3]**	**[2]**
		[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	**Muy Alto**	**[9]**	**[7]**	**[7]**	**[7]**	**[2]**
	[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS	**[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación**	**Muy Alto**	**[9]**	**[3]**	**[3]**	**[3]**	**[2]**
		[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	**Muy Alto**	**[9]**	**[7]**	**[5]**	**[7]**	**[4]**
		[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	**Muy Alto**	**[9]**	**[7]**	**[3]**	**[7]**	**[6]**
		[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	**Muy Alto**	**[9]**	**[9]**	**[9]**	**[7]**	**[7]**

VALORACION DE ACTIVOS								
Ámbito	Clasificación	Activo	Valoración	[D]	[I]	[C]	[A]	[T]
		[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	Muy Alto	[9]	[5]	[3]	[5]	[4]
		[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	Muy Alto	[9]	[7]	[7]	[7]	[7]
		[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	Muy Alto	[9]	[7]	[7]	[7]	[7]
		[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	Muy Alto	[9]	[5]	[6]	[5]	[3]
		[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	Muy Alto	[9]	[7]	[7]	[7]	[2]
[SRV] Servicios	[SRVI] Servicios Internos							
	[SRVI_IT] SERVICIOS GESTIONADOS IT	[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	Muy Alto	[9]				
		[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	Muy Alto	[9]				
		[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	Muy Alto	[9]				
	[SRVI_ADMIN] Servicios Corporativos	[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	Muy Alto	[9]				
		[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	Muy Alto	[9]				
		[SRVI_CORP_OPERACIONES] OPERACIONES	Muy Alto	[9]				
		[SRVI_CORP_RRHH] Área de RR.HH.	Muy Alto	[9]				
		[SRV_CORP_OPER] Dirección de Operaciones	Muy Alto	[9]				
	[SRVE] Servicios Externos		Muy Alto					
		[SRVE_CORREO] Servicio de Correo (GOOGLE)	Muy Alto	[9]				
		[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	Muy Alto	[9]				
		[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	Muy Alto	[9]				
[SI] Sistema de Información	[HW] Hardware	[SI_HW_SERV_DA] Servidores de DA	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[SI_HW_CLOUD_GOOGLE]	[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_SD_HD] Servidor Service Desk/Help Desk	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_DATASTORE] Almacenamiento y Backup	Muy Alto	[9]	[7]	[7]	[7]	[7]
		[SI_HW_WEB_CORP] Servidores Web Corporativa	Muy Alto	[9]	[6]	[4]	[7]	[4]

VALORACION DE ACTIVOS								
Ámbito	Clasificación	Activo	Valoración	[D]	[I]	[C]	[A]	[T]
		[SI_HW_CERTIF] Servidor de Certificados	Muy Alto	[9]	[9]	[9]	[9]	[8]
	[SI_HW_DATACENTER]	[SI_HW_SIEM] Servidor SIEM	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_AD_3] Servidor Controlador DominIo (AD)	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_MONITOR] Servidor de Monitorización	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_WIKI] Servidor de la Wiki	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_CORREO] Relay del Correo	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[SI_HW_VIRTUAL] Plataforma Virtualización	[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	Muy Alto	[9]	[8]	[4]	[8]	[8]
		[SI_HW_VM_CREDEN] Servidores Credenciales	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_NAS] Servidor de Almacenamiento NAS	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_VM_MONITOR] Sistema de Monitorización	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_HW_SERV_LAB] Servidores laboratorio	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[SI_HW_GLOBALSOC_Sede_MADRID]	[SI_HW_PC] PC de Sobremesa	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_HW_TFNO_MOVIL] Teléfono Móvil	Muy Alto	[2]				
		[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	Muy Alto	[4]				
		[SI_HW_IMPRES] Equipos de Impresión	Muy Alto	[2]				
	[SI_HW_SOC_MAD] Hardware SOC de MADRID	[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	Muy Alto	[9]	[7]	[2]	[7]	[7]
	[SW] Software	[SI_SW_Windows] S.O. Puesto de Trabajo	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_SW_Office] S.O. Puesto de Trabajo (Office)	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_SW_ANTIVIRUS] Software Antivirus	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[SI_SW_ALM_NUBE] Google Drive	Muy Alto	[9]	[7]	[7]	[7]	[7]
		[SI_SW_WINDOWS] Windows Server	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_LINUX] Software Linux	Muy Alto	[9]	[9]	[9]	[8]	[8]

VALORACION DE ACTIVOS								
Ámbito	Clasificación	Activo	Valoración	[D]	[I]	[C]	[A]	[T]
	[SI_SW_CLOUD_GOOGLE]	[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_SERVICE DESK] Service Desk-Help Desk	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_SFTP] Servicios SFTP	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_CERTIFICADOS] Servicios Certificados	Muy Alto	[9]	[8]	[9]	[9]	[7]
		[SI_SW_BACKUP] Servicios de Storage (DataStore)	Muy Alto	[9]	[7]	[7]	[7]	[7]
		[SI_SW_WEB] Servicios Web Corporativos	Muy Alto	[9]	[6]	[4]	[7]	[4]
		[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[SI_SW_DATACENTER]	[SI_SW_SIEM] Software SIEM	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_HYPERVISOR] Software Virtualización	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_IPS] Software IPS	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_ANAL_DATA] Software Analítica de Datos	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_IDS] Software IDS	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_MONITOR] Software de Monitorización	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_SERV_FICH] Software de Servicio de Ficheros	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_WIKI] Software Wiki	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_RECOLECTOR] Software de Recolección y Gestión de Logs	Muy Alto	[9]	[8]	[4]	[8]	[8]
		[SI_SW_CREDENCIALES] Software Gest. Credenciales	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[SI_SW_RELAY CORREO] POSTFIX	Muy Alto	[9]	[9]	[9]	[8]	[8]
[COM] Comunicaciones	[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)	[COM_LAN_GOOGLE] Red GOOGLE	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[COM_FW_GOOGLE] Firewall Google	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[COM_SWT_GOOGLE] Switches GOOGLE	Muy Alto	[9]	[9]	[9]	[9]	[8]
	[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)	[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[COM_LAN_DATACENTER] Red DATACENTER	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[COM_SWT_DATACENTER] Switches DATACENTER	Muy Alto	[9]	[9]	[9]	[8]	[8]
		[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)	[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	Muy Alto	[5]				
		[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	Muy Alto	[5]				

VALORACION DE ACTIVOS								
Ámbito	Clasificación	Activo	Valoración	[D]	[I]	[C]	[A]	[T]
		[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	Muy Alto	[5]				
		[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	Muy Alto	[5]				
		[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	Muy Alto	[5]				
[SS] Proveedores	[SS_ES] Servicios Esenciales	[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	Muy Alto	[9]	[9]	[9]	[9]	[8]
	[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)	[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	Alto	[6]				
		[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[SS_OT] Otros	[SS_OT_TFNO_MOVIL] Teléfonos Móviles SOC	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	Medio	[5]				
[P] Personal	[P_I] Personal Interno	[P_I_SOC] Personal Interno del SOC MAD	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[P_I_FIN_LEG] Personal Resp. Financiero y Legal	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[P_I_RRHH] Personal Resp. RR.HH.	Muy Alto	[9]	[7]	[2]	[7]	[7]
		[P_I_Comercial] Personal Área Comercial y Marketing	Muy Alto	[9]	[7]	[2]	[7]	[7]
	[P_E] Personal Externo	[P_E_MTO] Personal de Limpieza y Mantenimiento	Bajo	[3]				
[L] Instalaciones y Ubicaciones	[LD] Dependencias	[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[LD_GOOGLE_CLOUD] Cpd de GOOGLE	Muy Alto	[9]	[9]	[9]	[9]	[8]
		[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	Muy Alto	[9]	[9]	[9]	[8]	[8]
	[LS] Salas Técnicas	[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	Medio	[3]				
	[LO] Otros							
	[LE] Edificios	[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	Muy Alto	[9]	[9]	[9]	[9]	[8]

23-Tabla-Valoración de activos

3.5. Catálogo de Amenazas

El catálogo de amenazas que se ha usado como base para la realización del análisis de las amenazas sobre los activos de información de GLOBAL es el que se presenta en la tabla que aparece a continuación.

Este catálogo se ha extraído tomando como referencia el declarado para Magerit V.3 ((MAGERIT-Libro II Catálogo de Elementos, s.f.).

CATÁLOGO DE AMENAZAS								
Amenazas	**Activos Afectados**		**Dimensiones de Seguridad afectadas**					
			[D] Disponibilidad	**[I] Integridad**	**[C] Confidencialidad**	**[T] Trazabilidad**	**[A] Autenticidad**
[N] Desastres naturales	**[N.*] Desastres naturales**	**[HW] equipos informáticos (hardware)**	X				
		[Media] soportes de información	X				
		[AUX] equipamiento auxiliar	X				
		[L] instalaciones	X				
[I] De origen industrial	**[I.*] Desastres industriales**						
		[HW] equipos informáticos (hardware)	X				
		[Media] soportes de información	X				
		[AUX] equipamiento auxiliar	X				
		[L] instalaciones	X				
[E] Errores y fallos no intencionados	**[E.1] Errores de los usuarios**	**[D] datos / información**	X	X	X		
		[keys] claves criptográficas	X	X	X		
		[S] servicios	X	X	X		
		[SW] aplicaciones (software)	X	X	X		
		[Media] soportes de información	X	X	X		
	[E.4] Errores de configuración	**[D.conf] datos de configuración**		X			
	[E.7] Deficiencias en la organización	**[P] personal**	X				
	[E.18] Destrucción de información	**[D] datos / información**	X				
		[keys] claves criptográficas	X				
		[S] servicios	X				
		[SW] aplicaciones (SW)	X				
		[COM] comunicaciones (tránsito)	X				
		[Media] soportes de información	X				
		[L] instalaciones	X				
	[E.19] Fugas de información	**[D] datos / información**			X		
		[keys] claves criptográficas			X		
		[S] servicios			X		
		[SW] aplicaciones (SW)			X		

CATÁLOGO DE AMENAZAS							
Amenazas	Activos Afectados		Dimensiones de Seguridad afectadas				
			[D] Disponibilidad	[I] Integridad	[C] Confidencialidad	[T] Trazabilidad	[A] Autenticidad
		[COM] comunicaciones (tránsito)			X		
		[Media] soportes de información			X		
		[L] instalaciones			X		
		[P] personal (revelación)			X		
	[E.20] Vulnerabilidades de los programas (software)	[SW] aplicaciones (software)	X	X	X		
	[E.21] Errores de mantenimiento / actualización de programas (software)	[SW] aplicaciones (software)	X	X			
	[E.24] Caída del sistema por agotamiento de recursos	[S] servicios	X				
		[HW] equipos informáticos (hardware)	X				
		[COM] redes de comunicaciones	X				
	[E.28] Indisponibilidad del personal	[P] personal interno	X				
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	[D.log] registros de actividad		X		X	
	[A.4] Manipulación de la configuración	[D.log] registros de actividad		X	X	X	
	[A.5] Suplantación de la identidad del usuario	[D] datos / información		X	X		X
		[keys] claves criptográficas		X	X		X
		[S] servicios		X	X		X
		[SW] aplicaciones (software)		X	X		X
		[COM] redes de comunicaciones		X	X		X
	[A.6] Abuso de privilegios de acceso	[D] datos / información	X	X	X		
		[keys] claves criptográficas	X	X	X		
		[S] servicios	X	X	X		
		[SW] aplicaciones (software)	X	X	X		
		[HW] equipos informáticos (hardware)	X	X	X		
		[COM] redes de comunicaciones	X	X	X		
	[A.8] Difusión de software dañino	[SW] aplicaciones (software)	X	X	X		
	[A.11] Acceso no autorizado	[D] datos / información		X	X		
		[keys] claves criptográficas		X	X		
		[S] servicios		X	X		

CATÁLOGO DE AMENAZAS							
Amenazas	**Activos Afectados**		**Dimensiones de Seguridad afectadas**				
			[D] Disponibilidad	**[I] Integridad**	**[C] Confidencialidad**	**[T] Trazabilidad**	**[A] Autenticidad**
		[SW] aplicaciones (software)		X	X		
		[HW] equipos informáticos (hardware)		X	X		
		[COM] redes de comunicaciones		X	X		
		[Media] soportes de información		X	X		
		[AUX] equipamiento auxiliar		X	X		
		[L] instalaciones		X	X		
	[A.15] Modificación deliberada de la información	[D] datos / información		X			
		[keys] claves criptográficas		X			
		[S] servicios (acceso)		X			
		[SW] aplicaciones (SW)		X			
		[COM] comunicaciones (tránsito)		X			
		[Media] soportes de información		X			
		[L] instalaciones		X			
	[A.18] Destrucción de información	[D] datos / información	X				
		[keys] claves criptográficas	X				
		[S] servicios	X				
		[SW] aplicaciones (SW)	X				
		[Media] soportes de información	X				
		[L] instalaciones	X				
	[A.24] Denegación de servicio	[S] servicios	X				
		[HW] equipos informáticos (hardware)	X				
		[COM] redes de comunicaciones	X				
	[A.28] Indisponibilidad del personal	[P] personal interno	X				

24-Tabla-Catálogo de amenazas

3.6. Valoración Activos-Amenazas

Una vez establecida las amenazas aplicables sobre los activos de información, en base al catálogo de referencia de amenazas establecido**,** se determina para cada uno de los activos y su amenaza asociada la probabilidad de ocurrencia estimada de materialización de la amenaza y el % de impacto (estimación de degradación del activo) para la Dimensiones de Seguridad afectadas por la Amenaza.

Está recogido dentro de la metodología de riesgos de la Organización (**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf**).

Probabilidad	Valor	Descripción	Descripción
MA	**100**	muy frecuente	a diario
A	**10**	frecuente	mensualmente
M	**1**	normal	una vez al año
B	**1/10 (0,1)**	poco frecuente	cada varios años
MB	**1/100 (0,01)**	muy poco frecuente	siglos

25-Tabla-Probabilidad amenazas

La valoración de los activos en base a las amenazas identificadas se detalla en la tabla que aparece a continuación:

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	**Frecuencia**	**[D]**	**[I]**	**[C]**
[B] Activos esenciales				
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS				
[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES				
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)		**0,7**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**0,1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,7**		
[E.19] Fugas de información	**0,1**		**0,15**	
[B_D_SG_DES_TEC] Información Técnica de los Proyectos		**0,7**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**0,1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,7**		
[E.19] Fugas de información	**0,1**		**0,15**	
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto		**0,7**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**0,1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,7**		
[E.19] Fugas de información	**0,1**		**0,15**	
[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS				
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)		**0,7**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**0,1**	**0,15**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,2**		
[E.18] Destrucción de la información	**0,1**	**0,7**		
[E.19] Fugas de información	**0,1**		**0,1**	
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación		**0,5**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**0,1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,5**		
[E.19] Fugas de información	**0,1**		**0,15**	
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)		**0,5**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,5**		
[E.19] Fugas de información	**0,1**		**0,15**	
[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS				
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación		**0,7**	**0,3**	**0,1**
[E.1] Errores de los usuarios	**1**	**0,1**	**0,3**	**0,1**
[E.7] Deficiencias en la organización	**0,1**	**0,1**		
[E.18] Destrucción de la información	**0,1**	**0,7**		

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[E.19] Fugas de información	0,1		0,15	
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)		0,3	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.7] Deficiencias en la organización	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,3		
[E.19] Fugas de información	0,1		0,15	
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)		0,3	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.7] Deficiencias en la organización	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,3		
[E.19] Fugas de información	0,1		0,15	
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)		0,85	0,8	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.7] Deficiencias en la organización	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,85		
[E.19] Fugas de información	0,1		0,8	
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes		0,3	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.7] Deficiencias en la organización	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,3		
[E.19] Fugas de información	0,1		0,15	
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES		0,45	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.4] Errores de configuración	0,1	0,1		
[E.7] Deficiencias en la organización	0,1	0,45		
[E.18] Destrucción de la información	0,1		0,15	
[E.19] Fugas de información	0,1	0,1		
[A.4] Manipulación de los ficheros de configuración	0,1	0,1	0,1	0,1
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC		0,6	0,3	0,1
[E.4] Errores de configuración	0,1	0,1	0,3	0,1
[E.18] Destrucción de la información	0,1	0,1		
[A.4] Manipulación de los ficheros de configuración	0,1	0,6		
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC		0,7	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.15] Alteración de la información	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,7		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1		0,15	
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES		0,15	0,3	0,1
[E.1] Errores de los usuarios	0,1	0,1	0,3	0,1
[E.15] Alteración de la información	0,1	0,1		
[E.18] Destrucción de la información	0,1	0,15		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1		0,15	
[SRV] Servicios				
[SRVI] Servicios Internos				
[SRVI_IT] SERVICIOS GESTIONADOS IT				
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE		0,3		0,2
[E.18] Destrucción de la información	0,1	0,3		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,3		
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS		0,8		0,2
[E.18] Destrucción de la información	0,1	0,3		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,8		
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS		0,5		0,2
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,5		
[SRVI_ADMIN] Servicios Corporativos				
[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización		0,15		0,15
[E.18] Destrucción de la información	0,1	0,15		
[E.19] Fugas de información	0,1			0,15

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales		0,8		0,4
[E.18] Destrucción de la información	0,1	0,8		
[E.19] Fugas de información	0,1			0,4
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,3		
[SRVI_CORP_OPERACIONES] OPERACIONES		0,8		0,15
[E.18] Destrucción de la información	0,1	0,8		
[E.19] Fugas de información	0,1			0,15
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,8		
[SRVI_CORP_RRHH] Área de RR.HH.		0,6		0,4
[E.18] Destrucción de la información	0,1	0,6		
[E.19] Fugas de información	0,1			0,4
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,15		
[SRV_CORP_OPER] Dirección de Operaciones		0,4		0,2
[E.18] Destrucción de la información	0,1	0,4		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[SRVE] Servicios Externos				
[SRVE_CORREO] Servicio de Correo (GOOGLE)		0,85		0,35
[E.18] Destrucción de la información	0,1	0,8		
[E.19] Fugas de información	0,1			0,35
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,85		
[SRVE_DATACENTER] Servicio de CPD y Comunicaciones		0,85		0,4
[E.18] Destrucción de la información	0,1	0,85		
[E.19] Fugas de información	0,1			0,4
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage		0,8		0,45
[E.18] Destrucción de la información	0,1	0,8		
[E.19] Fugas de información	0,1			0,45
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,8		
[SI] Sistema de Información				
[HW] Hardware				
[SI_HW_CLOUD_GOOGLE]				
[SI_HW_SERV_DA] Servidores de DA		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,15		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,3		
[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,3		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,2		
[SI_HW_SD_HD] Servidor Service Desk/Help Desk		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_SFTP] Servidor Servicio de transferencia ficheros		0,5	0,4	0,3
[I.*] Desastres industriales	0,01	0,5		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,4	0,1
[A.11] Acceso no autorizado	0,1		0,2	0,3
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_DATASTORE] Almacenamiento y Backup		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_WEB_CORP] Servidores Web Corporativa		0,85	0,1	0,1
[I.*] Desastres industriales	0,01	0,85		

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_CERTIF] Servidor de Certificados		0,85	0,4	0,4
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,4	0,4	0,4
[A.11] Acceso no autorizado	0,1		0,4	0,4
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_DATACENTER]				
[SI_HW_SIEM] Servidor SIEM		0,3	0,2	0,15
[I.*] Desastres industriales	0,01	0,3		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,2		
[A.6] Abuso de privilegios de acceso	0,1	0,2	0,2	0,1
[A.11] Acceso no autorizado	0,1		0,2	0,15
[A.24] Denegación de servicio	0,1	0,2		
[SI_HW_AD_3] Servidor Controlador DominIo (AD)		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_MONITOR] Servidor de Monitorización		0,4	0,4	0,1
[I.*] Desastres industriales	0,01	0,4		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,3		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,4	0,1
[A.11] Acceso no autorizado	0,1		0,4	0,1
[A.24] Denegación de servicio	0,1	0,15		
[SI_HW_GEST_PROY] Servidor Gestión de Proyectos		0,4	0,1	0,1
[I.*] Desastres industriales	0,01	0,3		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_WIKI] Servidor de la Wiki		0,4	0,1	0,1
[I.*] Desastres industriales	0,01	0,15		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,15		
[A.6] Abuso de privilegios de acceso	0,1	0,15	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup		0,85	0,5	0,5
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,6		
[A.6] Abuso de privilegios de acceso	0,1	0,4	0,5	0,5
[A.11] Acceso no autorizado	0,1		0,5	0,5
[A.24] Denegación de servicio	0,1	0,3		
[SI_HW_CORREO] Relay del Correo		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,4	0,3	0,3
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VIRTUAL] Plataforma Virtualización				
[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,7	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,7		
[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VM_CREDEN] Servidores Credenciales		0,85	0,8	0,85
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,8		
[A.6] Abuso de privilegios de acceso	0,1	0,8	0,8	0,85
[A.11] Acceso no autorizado	0,1		0,8	0,85
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo		0,3	0,1	0,1
[I.*] Desastres industriales	0,01	0,3		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,25		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,3		
[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos		0,6	0,3	0,3
[I.*] Desastres industriales	0,01	0,6		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,2		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,3	0,3
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_NAS] Servidor de Almacenamiento NAS		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_VM_MONITOR] Sistema de Monitorización		0,85	0,3	0,3
[I.*] Desastres industriales	0,01	0,85		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,1
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_SERV_LAB] Servidores laboratorio		0,15	0,1	0,1
[I.*] Desastres industriales	0,01	0,15		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_GLOBALSOC_Sede_MADRID]				
[SI_HW_PC] PC de Sobremesa		0,1	0,1	0,1
[I.*] Desastres industriales	0,01	0,1		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_TFNO_MOVIL] Teléfono Móvil		0,2	0,1	0,1
[I.*] Desastres industriales	0,01	0,2		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP		0,4	0,1	0,1
[I.*] Desastres industriales	0,01	0,1		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,4		
[SI_HW_IMPRES] Equipos de Impresión		0,1	0,1	0,1
[I.*] Desastres industriales	0,01	0,1		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_SOC_MAD] Hardware SOC de MADRID				
[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD		0,1	0,1	0,1
[I.*] Desastres industriales	0,01	0,1		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.6] Abuso de privilegios de acceso	0,1	0,1	0,1	0,1
[A.11] Acceso no autorizado	0,1		0,1	0,1
[A.24] Denegación de servicio	0,1	0,1		
[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid		0,3	0,3	0,3
[I.*] Desastres industriales	0,01	0,1		
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,2		
[A.6] Abuso de privilegios de acceso	0,1	0,3	0,3	0,2
[A.11] Acceso no autorizado	0,1		0,3	0,3
[A.24] Denegación de servicio	0,1	0,15		
[SW] Software				
[SI_SW_Windows] S.O. Puesto de Trabajo		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos		0,15	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,1	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,1	0,1	
[SI_SW_Office] S.O. Puesto de Trabajo (Office)		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_ANTIVIRUS] Software Antivirus		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_ALM_NUBE] Google Drive		0,3	0,3	0,4
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,4
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,4
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,3	
[SI_SW_WINDOWS] Windows Server		0,3	0,3	0,3
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,3
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_LINUX] Software Linux		0,3	0,3	0,3
[E.1] Errores de los usuarios	0,1	0,2	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,3
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[SI_SW_CLOUD_GOOGLE]				
[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)		0,2	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,2	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,1	
[SI_SW_SERVICE DESK] Service Desk-Help Desk		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_SFTP] Servicios SFTP		0,15	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,1	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,1	0,1	
[SI_SW_CERTIFICADOS] Servicios Certificados		0,3	0,45	0,5
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,5
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,4	0,5
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,45	
[SI_SW_BACKUP] Servicios de Storage (DataStore)		0,3	0,4	0,4
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,4
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,4	0,4
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,4	
[SI_SW_WEB] Servicios Web Corporativos		0,2	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,1	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,1	0,1	
[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_DATACENTER]				
[SI_SW_SIEM] Software SIEM		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_HYPERVISOR] Software Virtualización		0,5	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,25	0,15	0,15
[E.18] Destrucción de la información	0,1	0,5		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,4	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,3	0,2	
[SI_SW_IPS] Software IPS		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_ANAL_DATA] Software Analítica de Datos		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_IDS] Software IDS		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_MONITOR] Software de Monitorización		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_SERV_FICH] Software de Servicio de Ficheros		0,3	0,3	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,3	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,2	
[SI_SW_WIKI] Software Wiki		0,15	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,1	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,1	0,1	
[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs		0,3	0,7	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,7	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,7	
[SI_SW_CREDENCIALES] Software Gest. Credenciales		0,3	0,7	0,7
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,7
[E.20] Vulnerabilidades de los programas (software)	0,1	0,3	0,7	0,7
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,2	0,7	
[SI_SW_RELAY CORREO] POSTFIX		0,15	0,15	0,15
[E.1] Errores de los usuarios	0,1	0,15	0,15	0,15
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,1
[E.20] Vulnerabilidades de los programas (software)	0,1	0,1	0,1	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,1	0,1	0,1	
[COM] Comunicaciones				
[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)				
[COM_LAN_GOOGLE] Red GOOGLE		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_FW_GOOGLE] Firewall Google		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_SWT_GOOGLE] Switches GOOGLE		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)				
[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_LAN_DATACENTER] Red DATACENTER		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_SWT_DATACENTER] Switches DATACENTER		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)				
[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)		0,7	0,4	0,3
[E.18] Destrucción de la información	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,4	0,2
[A.24] Denegación de servicio	0,1	0,7		
[SS] Proveedores				
[SS_ES] Servicios Esenciales				
[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)		0,1	0,1	0,2
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC		0,1	0,1	0,2

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)		0,1	0,1	0,2
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)				
[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5		0,1	0,1	0,2
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7		0,4	0,4	0,3
[E.18] Destrucción de la información	0,1	0,4		
[E.19] Fugas de información	0,1			0,3
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,4		
[A.11] Acceso no autorizado	0,1		0,4	0,3
[SS_OT] Otros				
[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC		0,1	0,1	0,2
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita		0,1	0,1	0,2
[E.18] Destrucción de la información	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.24] Caída del sistema por agotamiento de recursos	0,1	0,1		
[A.11] Acceso no autorizado	0,1		0,1	0,2
[P] Personal				
[P_I] Personal Interno				
[P_I_SOC] Personal Interno del SOC MAD		0,4		0,4
[E.7] Deficiencias en la organización	0,1	0,3		
[E.19] Fugas de información	0,1			0,4
[E.28] Indisponibilidad del personal	0,1	0,4		
[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID		0,2		0,2
[E.7] Deficiencias en la organización	0,1	0,2		
[E.19] Fugas de información	0,1			0,2
[E.28] Indisponibilidad del personal	0,1	0,2		
[P_I_FIN_LEG] Personal Resp. Financiero y Legal		0,4		0,4
[E.7] Deficiencias en la organización	0,1	0,3		
[E.19] Fugas de información	0,1			0,4
[E.28] Indisponibilidad del personal	0,1	0,4		
[P_I_RRHH] Personal Resp. RR.HH.		0,4		0,4
[E.7] Deficiencias en la organización	0,1	0,3		
[E.19] Fugas de información	0,1			0,4
[E.28] Indisponibilidad del personal	0,1	0,4		
[P_I_Comercial] Personal Área Comercial y Marketing		0,2		0,3
[E.7] Deficiencias en la organización	0,1	0,2		
[E.19] Fugas de información	0,1			0,3
[E.28] Indisponibilidad del personal	0,1	0,2		
[P_E] Personal Externo				
[P_E_MTO] Personal de Limpieza y Mantenimiento		0,1		0,2
[E.7] Deficiencias en la organización	0,1	0,1		
[E.19] Fugas de información	0,1			0,2
[E.28] Indisponibilidad del personal	0,1	0,1		
[L] Instalaciones y Ubicaciones				
[LD] Dependencias				
[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid		0,2	0,3	0,35
[N.*] Desastres naturales	0,01	0,2		
[I.*] Desastres industriales	0,01	0,2		
[E.18] Destrucción de la información	0,1	0,15		
[A.11] Acceso no autorizado	0,1		0,3	0,35

VALORACIÓN ACTIVOS-AMENAZAS				
ACTIVOS	Frecuencia	[D]	[I]	[C]
[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID		0,2	0,3	0,35
[N.*] Desastres naturales	0,01	0,2		
[I.*] Desastres industriales	0,01	0,2		
[E.18] Destrucción de la información	0,1	0,15		
[A.11] Acceso no autorizado	0,1		0,3	0,35
[LD_GOOGLE_CLOUD] Cpd de GOOGLE		0,7	0,3	0,35
[N.*] Desastres naturales	0,01	0,7		
[I.*] Desastres industriales	0,01	0,7		
[E.18] Destrucción de la información	0,1	0,7		
[A.11] Acceso no autorizado	0,1		0,3	0,35
[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID		0,85	0,3	0,35
[N.*] Desastres naturales	0,01	0,8		
[I.*] Desastres industriales	0,01	0,8		
[E.18] Destrucción de la información	0,1	0,85		
[A.11] Acceso no autorizado	0,1		0,3	0,35
[LS] Salas Técnicas				
[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones		0,2	0,3	0,35
[N.*] Desastres naturales	0,01	0,2		
[I.*] Desastres industriales	0,01	0,2		
[E.18] Destrucción de la información	0,1	0,15		
[A.11] Acceso no autorizado	0,1		0,3	0,35
[LO] Otros				
[LE] Edificios				
[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid		0,2	0,3	0,35
[N.*] Desastres naturales	0,01	0,2		
[I.*] Desastres industriales	0,01	0,2		
[E.18] Destrucción de la información	0,1	0,15		
[A.11] Acceso no autorizado	0,1		0,3	0,35

26-Tabla-Valoración Activos-amenazas

3.7. Riesgo Potencial y Riesgo Actual

Como consecuencia de la valoración de las amenazas sobre los activos (**Valoración Activos-Amenazas**) se calcula el **Riesgo Potencial** (los riesgos a los que quedan expuestos los activos desde un punto de visto teórico sin haber todavía considerado los controles de Seguridad que ya tiene establecidos la organización) de los activos de **GLOBALSOC**.

La formula para obtener el cálculo del riesgo potencial se describe en la siguiente tabla:

Cálculo del Riesgo Potencial	
Riesgo Potencial=((D|I|C)* Valoración)/10)* frecuencia*100	
En donde:	
D|I|C	Es el % de impacto (estimación de degradación del activo) para la Dimensiones de Seguridad afectadas por la Amenaza.
Valoración	Valoración del impacto del activo
Frecuencia	Es la probabilidad de que materialice la amenaza.

27-Tabla-Cálculo Riesgo Potencial

Además, se ha calculado el **Riesgo Actual**, como consecuencia de la valoración de los controles seguridad existentes en la organización tomando como base al referencial de controles de la **ISO 27002**.

- Para realizar el cálculo del Riesgo Actual, se han considerado los siguientes elementos:
  - El Análisis Diferencial de valoración del estado de situación de la Seguridad de la información en la organización (Análisis Diferencial).
  - La Documentación generada del SGSI como contribución que ya se ha realizado para constituir el SGSI a través de los documentos (políticas y procedimientos) y registros asociados (SISTEMA DE GESTIÓN DOCUMENTAL).
  - Como consecuencia de lo anterior se ha elaborado el informe de Aplicabilidad SOA (TFM_Declaración de Aplicabilidad SOA.xlsx) y La Evaluación del grado actual de madurez de los controles basado en el modelo de madurez de capacidad CMM (niveles desde L0-L5) (**Ilustración 39- Modelo de Evaluación Nivel de Madurez-CMM**).
  - Se ha recalculado el riesgo actual; teniendo en cuanto la atenuación del impacto resultante de la valoración de las amenazas considerando los mecanismos de control que pueden actuar sobre ellas (reduciendo, mitigando y/o eliminando el riesgo asociado).
  - Para ello se ha establecido una relación de la relación de amenazas que afectan a los activos de información, determinado los controles que la aplican para poder gestionar el riesgo asociado.
  - En base al promedio de madurez sobre los controles aplicables sobre cada amenaza, se calcula el factor de atenuación del riesgo (**tabla-49-Amenazas&Atenuación controles ISO 27002**)

Amenazas-Atenuación		
Amenaza	**Promedio madurez controles aplicables**	**Coeficiente Reducción/Atenuación del Riesgo**
[A.11] Acceso no autorizado	**1,73**	**0,31**
[A.24] Denegación de servicio	**2,43**	**0,44**
[A.4] Manipulación de los ficheros de configuración	**1,60**	**0,29**
[A.6] Abuso de privilegios de acceso	**1,64**	**0,29**
[E.1] Errores de los usuarios	**1,36**	**0,25**

Amenazas-Atenuación		
Amenaza	**Promedio madurez controles aplicables**	**Coeficiente Reducción/Atenuación del Riesgo**
[E.15] Alteración de la información	**1,65**	**0,30**
[E.18] Destrucción de la información	**1,65**	**0,30**
[E.19] Fugas de información	**1,73**	**0,31**
[E.20] Vulnerabilidades de los programas (software)	**1,75**	**0,32**
[E.21] Errores de mantenimiento / actualización de programas (software)	**2,14**	**0,39**
[E.24] Caída del sistema por agotamiento de recursos	**2,43**	**0,44**
[E.28] Indisponibilidad del personal	**1,38**	**0,25**
[E.4] Errores de configuración	**1,73**	**0,31**
[E.7] Deficiencias en la organización	**1,47**	**0,27**
[I.*] Desastres industriales	**0,57**	**0,10**
[N.*] Desastres naturales	**0,57**	**0,10**

28-Tabla-Coefiente atenuación Amenaza

- Dicho factor se aplica a continuación sobre los riesgos potenciales ya calculados para obtener los Riesgos actuales.

El cálculo del coeficiente de atenuación se muestra en la siguiente tabla:

Cálculo de la atenuación sobre Riesgo Potencial
(1)-Coeficiente_reduccion/Atenuación riesgo=90* ((Promedio_madurez actual (**Asociación Amenazas & Atenuación controles**)/5)*0,01)

29-Cálculo estimación atenuación sobre el Riesgo potencial

La formula para obtener el cálculo del riesgo potencial se describe en la siguiente tabla:

Cálculo del Riesgo Actual	
Riesgo Actual = Riesgo potencial - (Riesgo Potencial*Coeficiente Reducción/atenuación del riesgo)	
En donde:	
Riesgo Potencial	Es el riesgo calculado en (**27-Tabla-Cálculo Riesgo Potencial**)
Coeficiente Reducción/atenuación del riesgo)	Coeficiente de atenuación por amenaza en (**28-Tabla-Coefiente atenuación Amenaza**)

30-Cálculo del Riesgo Actual

El resultado en detalle se muestra en la tabla que aparece a continuación:

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[B] Activos esenciales						
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	6,3	0	0	4,4	0,0	0,0
[E.1] Errores de los usuarios	0,9	0,0	0,0	0,7	0,0	0,0
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES						
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	5,6	0,9	0,2	3,9	0,7	0,2
[E.1] Errores de los usuarios	0,8	0,9	0,2	0,6	0,7	0,2
[E.7] Deficiencias en la organización	0,8	0,0	0,0	0,6	0,0	0,0
[E.18] Destrucción de la información	5,6	0,0	0,0	3,9	0,0	0,0
[E.19] Fugas de información	0	0,5	0,0	0,0	0,3	0,0
[B_D_SG_DES_TEC] Información Técnica de los Proyectos	4,9	2,1	0,7	3,4	1,6	0,5
[E.1] Errores de los usuarios	0,7	2,1	0,7	0,5	1,6	0,5
[E.7] Deficiencias en la organización	0,7	0,0	0,0	0,5	0,0	0,0
[E.18] Destrucción de la información	4,9	0,0	0,0	3,4	0,0	0,0
[E.19] Fugas de información	0	1,1	0,0	0,0	0,7	0,0
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	4,9	2,1	0,7	3,4	1,6	0,5
[E.1] Errores de los usuarios	0,7	2,1	0,7	0,5	1,6	0,5
[E.7] Deficiencias en la organización	0,7	0,0	0,0	0,5	0,0	0,0
[E.18] Destrucción de la información	4,9	0,0	0,0	3,4	0,0	0,0
[E.19] Fugas de información	0	1,1	0,0	0,0	0,7	0,0
[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS						
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	6,3	2,1	0,7	4,4	1,6	0,5
[E.1] Errores de los usuarios	1,35	2,1	0,7	1,0	1,6	0,5
[E.7] Deficiencias en la organización	1,8	0,0	0,0	1,3	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0
[E.19] Fugas de información	0	0,7	0,0	0,0	0,5	0,0
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	4,5	0,9	0,3	3,2	0,7	0,2
[E.1] Errores de los usuarios	0,9	0,9	0,3	0,7	0,7	0,2
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	4,5	0,0	0,0	3,2	0,0	0,0
[E.19] Fugas de información	0	0,5	0,0	0,0	0,3	0,0
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	4,5	2,1	0,7	3,2	1,6	0,5
[E.1] Errores de los usuarios	0,9	2,1	0,7	0,7	1,6	0,5
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	4,5	0,0	0,0	3,2	0,0	0,0
[E.19] Fugas de información	0	1,1	0,0	0,0	0,7	0,0
[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS						
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	6,3	0,9	0,3	4,4	0,7	0,2
[E.1] Errores de los usuarios	0,9	0,9	0,3	0,7	0,7	0,2
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.19] Fugas de información	0	0,5	0,0	0,0	0,3	0,0
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	2,7	2,1	0,5	1,9	1,6	0,4
[E.1] Errores de los usuarios	0,9	2,1	0,5	0,7	1,6	0,4
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	2,7	0,0	0,0	1,9	0,0	0,0
[E.19] Fugas de información	0	1,1	0,0	0,0	0,7	0,0
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	2,7	2,1	0,3	1,9	1,6	0,2
[E.1] Errores de los usuarios	0,9	2,1	0,3	0,7	1,6	0,2
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	2,7	0,0	0,0	1,9	0,0	0,0
[E.19] Fugas de información	0	1,1	0,0	0,0	0,7	0,0
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	6,3	6,3	0,9	4,4	4,3	0,7
[E.1] Errores de los usuarios	0,9	2,7	0,9	0,7	2,0	0,7
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0
[E.19] Fugas de información	0	6,3	0,0	0,0	4,3	0,0
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	2,7	1,5	0,3	1,9	1,1	0,2
[E.1] Errores de los usuarios	0,9	1,5	0,3	0,7	1,1	0,2
[E.7] Deficiencias en la organización	0,9	0,0	0,0	0,7	0,0	0,0
[E.18] Destrucción de la información	2,7	0,0	0,0	1,9	0,0	0,0
[E.19] Fugas de información	0	0,8	0,0	0,0	0,5	0,0
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	4,05	2,1	0,7	3,0	1,6	0,5
[E.1] Errores de los usuarios	0,9	2,1	0,7	0,7	1,6	0,5
[E.4] Errores de configuración	0,9	0,0	0,0	0,6	0,0	0,0
[E.7] Deficiencias en la organización	4,05	0,0	0,0	3,0	0,0	0,0
[E.18] Destrucción de la información	0	1,1	0,0	0,0	0,7	0,0
[E.19] Fugas de información	0,9	0,0	0,0	0,6	0,0	0,0
[A.4] Manipulación de los ficheros de configuración	0,9	0,7	0,7	0,6	0,5	0,5
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	5,4	2,1	0,7	3,8	1,4	0,5
[E.4] Errores de configuración	0,9	2,1	0,7	0,6	1,4	0,5
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[A.4] Manipulación de los ficheros de configuración	5,4	0,0	0,0	3,8	0,0	0,0
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	5,4	1,5	0,6	3,8	1,1	0,5
[E.1] Errores de los usuarios	0,9	1,5	0,6	0,7	1,1	0,5
[E.15] Alteración de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0	0,8	0,0	0,0	0,8	0,0
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	1,35	2,1	0,7	0,9	1,6	0,5
[E.1] Errores de los usuarios	0,9	2,1	0,7	0,7	1,6	0,5
[E.15] Alteración de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.18] Destrucción de la información	1,35	0,0	0,0	0,9	0,0	0,0
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0	1,1	0,0	0,0	1,1	0,0
[SRV] Servicios						
[SRVI] Servicios Internos						
[SRVI_IT] SERVICIOS GESTIONADOS IT						
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	2,7	0,0	0,0	1,9	0,0	0,0
[E.18] Destrucción de la información	2,7	0,0	0,0	1,9	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.24] Caída del sistema por agotamiento de recursos	2,7	0,0	0,0	1,5	0,0	0,0
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	6,3	0,0	0,0	3,5	0,0	0,0
[E.18] Destrucción de la información	2,7	0,0	0,0	1,9	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	6,3	0,0	0,0	3,5	0,0	0,0
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	4,5	0,0	0,0	2,5	0,0	0,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	4,5	0,0	0,0	2,5	0,0	0,0
[SRVI_ADMIN] Servicios Corporativos						
[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	1,35	0,0	0,0	0,9	0,0	0,0
[E.18] Destrucción de la información	1,35	0,0	0,0	0,9	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	5,4	0,0	0,0	3,8	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2,7	0,0	0,0	1,5	0,0	0,0
[SRVI_CORP_OPERACIONES] OPERACIONES	5,4	0,0	0,0	3,8	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	4,5	0,0	0,0	2,5	0,0	0,0
[SRVI_CORP_RRHH] Área de RR.HH.	5,4	0,0	0,0	3,8	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,35	0,0	0,0	0,8	0,0	0,0
[SRV_CORP_OPER] Dirección de Operaciones	3,6	0,0	0,0	2,5	0,0	0,0
[E.18] Destrucción de la información	3,6	0,0	0,0	2,5	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[SRVE] Servicios Externos	0	0,0	0,0	0,0	0,0	0,0
[SRVE_CORREO] Servicio de Correo (GOOGLE)	5,4	0,0	0,0	3,8	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	4,5	0,0	0,0	2,5	0,0	0,0
[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	6,3	0,0	0,0	4,4	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	6,3	0,0	0,0	3,5	0,0	0,0
[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	6,3	0,0	0,0	4,4	0,0	0,0
[E.18] Destrucción de la información	6,3	0,0	0,0	4,4	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	6,3	0,0	0,0	3,5	0,0	0,0
[SI] Sistema de Información						
[HW] Hardware						
[SI_HW_CLOUD_GOOGLE]						
[SI_HW_SERV_DA] Servidores de DA	2,7	2,7	2,7	1,9	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,35	0,0	0,0	0,8	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	2,7	0,0	0,0	1,5	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	2,7	2,7	2,7	1,9	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2,7	0,0	0,0	1,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	1,8	0,0	0,0	1,0	0,0	0,0
[SI_HW_SD_HD] Servidor Service Desk/Help Desk	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	0,9	3,6	2,7	0,6	2,5	1,9
[I.*] Desastres industriales	0,45	0,0	0,0	0,4	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	3,6	0,9	0,6	2,5	0,6
[A.11] Acceso no autorizado	0	1,8	2,7	0,0	1,2	1,9
[A.24] Denegación de servicio	0,9	0,0	0,0	0,5	0,0	0,0
[SI_HW_DATASTORE] Almacenamiento y Backup	3,6	2,1	2,1	2,0	1,5	1,4
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,1	0,7	1,9	1,5	0,5
[A.11] Acceso no autorizado	0	2,1	2,1	0,0	1,4	1,4
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_WEB_CORP] Servidores Web Corporativa	3,6	0,6	0,4	2,0	0,4	0,3
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	0,6	0,4	0,6	0,4	0,3
[A.11] Acceso no autorizado	0	0,6	0,4	0,0	0,4	0,3
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_CERTIF] Servidor de Certificados	3,6	3,6	3,6	2,5	2,5	2,5
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	3,6	3,6	3,6	2,5	2,5	2,5
[A.11] Acceso no autorizado	0	3,6	3,6	0,0	2,5	2,5
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_DATACENTER]						
[SI_HW_SIEM] Servidor SIEM	1,8	1,8	1,4	1,3	1,3	0,9
[I.*] Desastres industriales	0,27	0,0	0,0	0,2	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,8	0,0	0,0	1,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	1,8	1,8	0,9	1,3	1,3	0,6
[A.11] Acceso no autorizado	0	1,8	1,4	0,0	1,2	0,9
[A.24] Denegación de servicio	1,8	0,0	0,0	1,0	0,0	0,0
[SI_HW_AD_3] Servidor Controlador DominIo (AD)	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_MONITOR] Servidor de Monitorización	2,7	3,6	0,9	1,9	2,5	0,6
[I.*] Desastres industriales	0,36	0,0	0,0	0,3	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2,7	0,0	0,0	1,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	3,6	0,9	1,9	2,5	0,6
[A.11] Acceso no autorizado	0	3,6	0,9	0,0	2,5	0,6
[A.24] Denegación de servicio	1,35	0,0	0,0	0,8	0,0	0,0
[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	3,6	0,9	0,9	2,0	0,6	0,6
[I.*] Desastres industriales	0,27	0,0	0,0	0,2	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	0,9	0,9	0,6	0,6	0,6
[A.11] Acceso no autorizado	0	0,9	0,9	0,0	0,6	0,6
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_WIKI] Servidor de la Wiki	3,6	0,9	0,9	2,0	0,6	0,6
[I.*] Desastres industriales	0,135	0,0	0,0	0,1	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,35	0,0	0,0	0,8	0,0	0,0
[A.6] Abuso de privilegios de acceso	1,35	0,9	0,9	1,0	0,6	0,6
[A.11] Acceso no autorizado	0	0,9	0,9	0,0	0,6	0,6
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	5,4	4,5	4,5	3,0	3,2	3,2
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	5,4	0,0	0,0	3,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	3,6	4,5	4,5	2,5	3,2	3,2
[A.11] Acceso no autorizado	0	4,5	4,5	0,0	3,1	3,1
[A.24] Denegación de servicio	2,7	0,0	0,0	1,5	0,0	0,0
[SI_HW_CORREO] Relay del Correo	3,6	2,7	2,7	2,5	1,9	1,9
[I.*] Desastres industriales	0,45	0,0	0,0	0,4	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	3,6	2,7	2,7	2,5	1,9	1,9
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_VIRTUAL] Plataforma Virtualización				0,0	0,0	0,0
[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	5,4	2,7	2,7	3,2	1,9	1,9
[I.*] Desastres industriales	0,63	0,0	0,0	0,6	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	4,5	2,7	0,9	3,2	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	5,4	0,0	0,0	3,0	0,0	0,0
[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	3,6	2,4	1,2	2,0	1,7	0,8
[I.*] Desastres industriales	0,54	0,0	0,0	0,5	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,4	0,4	1,9	1,7	0,3
[A.11] Acceso no autorizado	0	2,4	1,2	0,0	1,7	0,8
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_VM_CREDEN] Servidores Credenciales	6,3	5,4	5,4	4,4	3,8	3,8
[I.*] Desastres industriales	0,63	0,0	0,0	0,6	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	6,3	0,0	0,0	3,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	6,3	5,4	5,4	4,4	3,8	3,8
[A.11] Acceso no autorizado	0	5,4	5,4	0,0	3,7	3,7
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,54	0,0	0,0	0,5	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,54	0,0	0,0	0,5	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	2,7	0,9	0,9	1,9	0,6	0,6
[I.*] Desastres industriales	0,27	0,0	0,0	0,2	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2,25	0,0	0,0	1,3	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	0,9	0,9	1,9	0,6	0,6
[A.11] Acceso no autorizado	0	0,9	0,9	0,0	0,6	0,6
[A.24] Denegación de servicio	2,7	0,0	0,0	1,5	0,0	0,0
[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,54	0,0	0,0	0,5	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,8	0,0	0,0	1,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	2,7	2,7	0,6	1,9	1,9
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_NAS] Servidor de Almacenamiento NAS	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_VM_MONITOR] Sistema de Monitorización	3,6	2,7	2,7	2,0	1,9	1,9
[I.*] Desastres industriales	0,765	0,0	0,0	0,7	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,7	0,9	1,9	1,9	0,6
[A.11] Acceso no autorizado	0	2,7	2,7	0,0	1,9	1,9
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[SI_HW_SERV_LAB] Servidores laboratorio	0,9	0,9	0,9	0,6	0,6	0,6
[I.*] Desastres industriales	0,135	0,0	0,0	0,1	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	0,9	0,9	0,6	0,6	0,6
[A.11] Acceso no autorizado	0	0,9	0,9	0,0	0,6	0,6
[A.24] Denegación de servicio	0,9	0,0	0,0	0,5	0,0	0,0
[SI_HW_GLOBALSOC_Sede_MADRID]						
[SI_HW_PC] PC de Sobremesa	0,9	0,7	0,2	0,6	0,5	0,1
[I.*] Desastres industriales	0,09	0,0	0,0	0,1	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	0,7	0,2	0,6	0,5	0,1
[A.11] Acceso no autorizado	0	0,7	0,2	0,0	0,5	0,1
[A.24] Denegación de servicio	0,9	0,0	0,0	0,5	0,0	0,0
[SI_HW_TFNO_MOVIL] Teléfono Móvil	0,2	0,0	0,0	0,1	0,0	0,0
[I.*] Desastres industriales	0,04	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,2	0,0	0,0	0,1	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,2	0,0	0,0	0,1	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	0,2	0,0	0,0	0,1	0,0	0,0
[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	1,6	0,0	0,0	0,9	0,0	0,0
[I.*] Desastres industriales	0,04	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,4	0,0	0,0	0,2	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,4	0,0	0,0	0,3	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	1,6	0,0	0,0	0,9	0,0	0,0
[SI_HW_IMPRES] Equipos de Impresión	0,2	0,0	0,0	0,1	0,0	0,0
[I.*] Desastres industriales	0,02	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,2	0,0	0,0	0,1	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,2	0,0	0,0	0,1	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	0,2	0,0	0,0	0,1	0,0	0,0
[SI_HW_SOC_MAD] Hardware SOC de MADRID						

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	0,9	0,7	0,2	0,6	0,5	0,1
[I.*] Desastres industriales	0,09	0,0	0,0	0,1	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.6] Abuso de privilegios de acceso	0,9	0,7	0,2	0,6	0,5	0,1
[A.11] Acceso no autorizado	0	0,7	0,2	0,0	0,5	0,1
[A.24] Denegación de servicio	0,9	0,0	0,0	0,5	0,0	0,0
[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	2,7	2,1	0,6	1,9	1,5	0,4
[I.*] Desastres industriales	0,09	0,0	0,0	0,1	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,8	0,0	0,0	1,0	0,0	0,0
[A.6] Abuso de privilegios de acceso	2,7	2,1	0,4	1,9	1,5	0,3
[A.11] Acceso no autorizado	0	2,1	0,6	0,0	1,4	0,4
[A.24] Denegación de servicio	1,35	0,0	0,0	0,8	0,0	0,0
[SW] Software						
[SI_SW_Windows] S.O. Puesto de Trabajo	2,7	2,1	0,3	1,8	1,4	0,2
[E.1] Errores de los usuarios	1,35	1,1	0,3	1,0	0,8	0,2
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,2	0,0	0,0	0,1
[E.20] Vulnerabilidades de los programas (software)	2,7	2,1	0,2	1,8	1,4	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,4	0,0	1,1	0,9	0,0
[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	1,35	1,1	0,3	1,0	0,8	0,2
[E.1] Errores de los usuarios	1,35	1,1	0,3	1,0	0,8	0,2
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	0,2	0,0	0,0	0,1
[E.20] Vulnerabilidades de los programas (software)	0,9	0,7	0,2	0,6	0,5	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	0,9	0,7	0,0	0,6	0,4	0,0
[SI_SW_Office] S.O. Puesto de Trabajo (Office)	2,7	2,1	0,3	1,8	1,4	0,2
[E.1] Errores de los usuarios	1,35	1,1	0,3	1,0	0,8	0,2
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,2	0,0	0,0	0,1
[E.20] Vulnerabilidades de los programas (software)	2,7	2,1	0,2	1,8	1,4	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,4	0,0	1,1	0,9	0,0
[SI_SW_ANTIVIRUS] Software Antivirus	2,7	2,1	0,3	1,8	1,4	0,2
[E.1] Errores de los usuarios	1,35	1,1	0,3	1,0	0,8	0,2
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,2	0,0	0,0	0,1
[E.20] Vulnerabilidades de los programas (software)	2,7	2,1	0,2	1,8	1,4	0,1
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,4	0,0	1,1	0,9	0,0
[SI_SW_ALM_NUBE] Google Drive	2,7	2,1	2,8	1,8	1,4	1,9
[E.1] Errores de los usuarios	1,35	1,1	1,1	1,0	0,8	0,8
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,8	0,0	0,0	1,9
[E.20] Vulnerabilidades de los programas (software)	2,7	2,1	2,8	1,8	1,4	1,9
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	2,1	0,0	1,1	1,3	0,0
[SI_SW_WINDOWS] Windows Server	2,7	2,7	2,7	1,8	1,8	1,9
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	2,7	1,8	1,8	1,8
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_LINUX] Software Linux	2,7	2,7	2,7	1,8	1,8	1,9

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.1] Errores de los usuarios	1,8	1,4	1,4	1,4	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	2,7	1,8	1,8	1,8
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_CLOUD_GOOGLE]						
[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	1,8	1,4	1,4	1,3	1,0	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	1,8	0,9	0,9	1,2	0,6	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	0,9	0,0	1,1	0,6	0,0
[SI_SW_SERVICE DESK] Service Desk-Help Desk	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_SFTP] Servicios SFTP	1,35	1,4	1,4	1,0	1,0	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	0,9	0,9	0,9	0,6	0,6	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	0,9	0,9	0,0	0,6	0,6	0,0
[SI_SW_CERTIFICADOS] Servicios Certificados	2,7	3,6	4,5	1,8	2,2	3,1
[E.1] Errores de los usuarios	1,35	1,2	1,4	1,0	0,9	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	4,5	0,0	0,0	3,1
[E.20] Vulnerabilidades de los programas (software)	2,7	3,2	4,5	1,8	2,2	3,1
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	3,6	0,0	1,1	2,2	0,0
[SI_SW_BACKUP] Servicios de Storage (DataStore)	2,7	2,8	2,8	1,8	1,9	1,9
[E.1] Errores de los usuarios	1,35	1,1	1,1	1,0	0,8	0,8
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,8	0,0	0,0	1,9
[E.20] Vulnerabilidades de los programas (software)	2,7	2,8	2,8	1,8	1,9	1,9
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	2,8	0,0	1,1	1,7	0,0
[SI_SW_WEB] Servicios Web Corporativos	1,8	0,9	0,6	1,3	0,7	0,5
[E.1] Errores de los usuarios	1,35	0,9	0,6	1,0	0,7	0,5
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,4	0,0	0,0	0,3
[E.20] Vulnerabilidades de los programas (software)	0,9	0,6	0,4	0,6	0,4	0,3
[E.21] Errores de mantenimiento / actualización de programas (software)	0,9	0,6	0,0	0,6	0,4	0,0
[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_DATACENTER]						
[SI_SW_SIEM] Software SIEM	2,7	2,7	1,4	1,8	1,8	1,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_HYPERVISOR] Software Virtualización	4,5	2,7	1,4	3,2	1,8	1,0
[E.1] Errores de los usuarios	2,25	1,4	1,4	1,7	1,0	1,0
[E.18] Destrucción de la información	4,5	0,0	0,0	3,2	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	3,6	2,7	0,9	2,5	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	2,7	1,8	0,0	1,7	1,1	0,0
[SI_SW_IPS] Software IPS	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_ANAL_DATA] Software Analítica de Datos	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_IDS] Software IDS	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_MONITOR] Software de Monitorización	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_SERV_FICH] Software de Servicio de Ficheros	2,7	2,7	1,4	1,8	1,8	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	2,7	2,7	0,9	1,8	1,8	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	1,8	0,0	1,1	1,1	0,0
[SI_SW_WIKI] Software Wiki	1,35	1,4	1,4	1,0	1,0	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	0,9	0,9	0,9	0,6	0,6	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	0,9	0,9	0,0	0,6	0,6	0,0
[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs	2,7	5,6	0,6	1,8	3,8	0,5
[E.1] Errores de los usuarios	1,35	1,2	0,6	1,0	0,9	0,5

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,4	0,0	0,0	0,3
[E.20] Vulnerabilidades de los programas (software)	2,7	5,6	0,4	1,8	3,8	0,3
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	5,6	0,0	1,1	3,4	0,0
[SI_SW_CREDENCIALES] Software Gest. Credenciales	2,7	6,3	6,3	1,8	4,3	4,3
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	6,3	0,0	0,0	4,3
[E.20] Vulnerabilidades de los programas (software)	2,7	6,3	6,3	1,8	4,3	4,3
[E.21] Errores de mantenimiento / actualización de programas (software)	1,8	6,3	0,0	1,1	3,9	0,0
[SI_SW_RELAY CORREO] POSTFIX	1,35	1,4	1,4	1,0	1,0	1,0
[E.1] Errores de los usuarios	1,35	1,4	1,4	1,0	1,0	1,0
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	0,9	0,0	0,0	0,6
[E.20] Vulnerabilidades de los programas (software)	0,9	0,9	0,9	0,6	0,6	0,6
[E.21] Errores de mantenimiento / actualización de programas (software)	0,9	0,9	0,0	0,6	0,6	0,0
[COM] Comunicaciones						
[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)						
[COM_LAN_GOOGLE] Red GOOGLE	4,5	3,6	2,7	2,5	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	4,5	0,0	0,0	2,5	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	4,5	0,0	0,0	2,5	0,0	0,0
[COM_FW_GOOGLE] Firewall Google	4,5	3,6	2,7	2,5	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	4,5	0,0	0,0	2,5	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_SWT_GOOGLE] Switches GOOGLE	3,6	3,6	2,7	2,0	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)						
[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	3,6	3,6	2,7	2,0	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_LAN_DATACENTER] Red DATACENTER	3,6	3,6	2,7	2,0	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_SWT_DATACENTER] Switches DATACENTER	3,6	3,6	2,7	2,0	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	3,6	3,6	2,7	2,0	2,5	1,9
[E.18] Destrucción de la información	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	1,8	0,0	2,5	1,2
[A.24] Denegación de servicio	3,6	0,0	0,0	2,0	0,0	0,0
[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)						
[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	1,5	0,0	0,0	0,8	0,0	0,0
[E.18] Destrucción de la información	1	0,0	0,0	0,7	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,5	0,0	0,0	0,8	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	1,5	0,0	0,0	0,8	0,0	0,0
[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	1,5	0,0	0,0	0,8	0,0	0,0
[E.18] Destrucción de la información	1	0,0	0,0	0,7	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,5	0,0	0,0	0,8	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	1,5	0,0	0,0	0,8	0,0	0,0
[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	2	0,0	0,0	1,1	0,0	0,0
[E.18] Destrucción de la información	1	0,0	0,0	0,7	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2	0,0	0,0	1,1	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	2	0,0	0,0	1,1	0,0	0,0
[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	1,5	0,0	0,0	0,8	0,0	0,0
[E.18] Destrucción de la información	1	0,0	0,0	0,7	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	1,5	0,0	0,0	0,8	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	1,5	0,0	0,0	0,8	0,0	0,0
[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	2	0,0	0,0	1,1	0,0	0,0
[E.18] Destrucción de la información	1	0,0	0,0	0,7	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	2	0,0	0,0	1,1	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[A.24] Denegación de servicio	2	0,0	0,0	1,1	0,0	0,0
[SS] Proveedores						
[SS_ES] Servicios Esenciales						
[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	0,9	0,9	1,8	0,6	0,6	1,2
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	1,8	0,0	0,0	1,2
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.11] Acceso no autorizado	0	0,9	1,8	0,0	0,6	1,2
[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	0,9	0,9	1,8	0,6	0,6	1,2
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	1,8	0,0	0,0	1,2
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[A.11] Acceso no autorizado	0	0,9	1,8	0,0	0,6	1,2
[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	0,9	0,9	1,8	0,6	0,6	1,2
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	1,8	0,0	0,0	1,2
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.11] Acceso no autorizado	0	0,9	1,8	0,0	0,6	1,2
[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)						
[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	0,6	0,0	0,0	0,4	0,0	0,0
[E.18] Destrucción de la información	0,6	0,0	0,0	0,4	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,6	0,0	0,0	0,3	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	3,6	3,6	2,7	2,5	2,5	1,9
[E.18] Destrucción de la información	3,6	0,0	0,0	2,5	0,0	0,0
[E.19] Fugas de información	0	0,0	2,7	0,0	0,0	1,9
[E.24] Caída del sistema por agotamiento de recursos	3,6	0,0	0,0	2,0	0,0	0,0
[A.11] Acceso no autorizado	0	3,6	2,7	0,0	2,5	1,9
[SS_OT] Otros						
[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC	0,9	0,9	1,8	0,6	0,6	1,2
[E.18] Destrucción de la información	0,9	0,0	0,0	0,6	0,0	0,0
[E.19] Fugas de información	0	0,0	1,8	0,0	0,0	1,2
[E.24] Caída del sistema por agotamiento de recursos	0,9	0,0	0,0	0,5	0,0	0,0
[A.11] Acceso no autorizado	0	0,9	1,8	0,0	0,6	1,2
[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	0,5	0,0	0,0	0,4	0,0	0,0
[E.18] Destrucción de la información	0,5	0,0	0,0	0,4	0,0	0,0
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.24] Caída del sistema por agotamiento de recursos	0,5	0,0	0,0	0,3	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[P] Personal						
[P_I] Personal Interno						
[P_I_SOC] Personal Interno del SOC MAD	3,6	0,0	3,6	2,7	0,0	2,5
[E.7] Deficiencias en la organización	2,7	0,0	0,0	2,0	0,0	0,0
[E.19] Fugas de información	0	0,0	3,6	0,0	0,0	2,5
[E.28] Indisponibilidad del personal	3,6	0,0	0,0	2,7	0,0	0,0
[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	1,8	0,0	0,4	1,4	0,0	0,3
[E.7] Deficiencias en la organización	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,4	0,0	0,0	0,3
[E.28] Indisponibilidad del personal	1,8	0,0	0,0	1,4	0,0	0,0
[P_I_FIN_LEG] Personal Resp. Financiero y Legal	3,6	0,0	0,8	2,7	0,0	0,6
[E.7] Deficiencias en la organización	2,7	0,0	0,0	2,0	0,0	0,0
[E.19] Fugas de información	0	0,0	0,8	0,0	0,0	0,6
[E.28] Indisponibilidad del personal	3,6	0,0	0,0	2,7	0,0	0,0
[P_I_RRHH] Personal Resp. RR.HH.	3,6	0,0	0,8	2,7	0,0	0,6
[E.7] Deficiencias en la organización	2,7	0,0	0,0	2,0	0,0	0,0
[E.19] Fugas de información	0	0,0	0,8	0,0	0,0	0,6
[E.28] Indisponibilidad del personal	3,6	0,0	0,0	2,7	0,0	0,0
[P_I_Comercial] Personal Área Comercial y Marketing	1,8	0,0	0,6	1,4	0,0	0,4
[E.7] Deficiencias en la organización	1,8	0,0	0,0	1,3	0,0	0,0
[E.19] Fugas de información	0	0,0	0,6	0,0	0,0	0,4
[E.28] Indisponibilidad del personal	1,8	0,0	0,0	1,4	0,0	0,0
[P_E] Personal Externo						
[P_E_MTO] Personal de Limpieza y Mantenimiento	0,3	0,0	0,0	0,2	0,0	0,0
[E.7] Deficiencias en la organización	0,3	0,0	0,0	0,2	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	Riesgo Potencial			Riesgo Actual		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[E.19] Fugas de información	0	0,0	0,0	0,0	0,0	0,0
[E.28] Indisponibilidad del personal	0,3	0,0	0,0	0,2	0,0	0,0
[L] Instalaciones y Ubicaciones						
[LD] Dependencias						
[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	1,35	2,7	3,2	0,9	1,9	2,2
[N.*] Desastres naturales	0,18	0,0	0,0	0,2	0,0	0,0
[I.*] Desastres industriales	0,18	0,0	0,0	0,2	0,0	0,0
[E.18] Destrucción de la información	1,35	0,0	0,0	0,9	0,0	0,0
[A.11] Acceso no autorizado	0	2,7	3,2	0,0	1,9	2,2
[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	1,35	2,7	3,2	0,9	1,9	2,2
[N.*] Desastres naturales	0,18	0,0	0,0	0,2	0,0	0,0
[I.*] Desastres industriales	0,18	0,0	0,0	0,2	0,0	0,0
[E.18] Destrucción de la información	1,35	0,0	0,0	0,9	0,0	0,0
[A.11] Acceso no autorizado	0	2,7	3,2	0,0	1,9	2,2
[LD_GOOGLE_CLOUD] Cpd de GOOGLE	4,5	2,7	3,2	3,2	1,9	2,2
[N.*] Desastres naturales	0,36	0,0	0,0	0,3	0,0	0,0
[I.*] Desastres industriales	0,36	0,0	0,0	0,3	0,0	0,0
[E.18] Destrucción de la información	4,5	0,0	0,0	3,2	0,0	0,0
[A.11] Acceso no autorizado	0	2,7	3,2	0,0	1,9	2,2
[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	5,4	2,7	3,2	3,8	1,9	2,2
[N.*] Desastres naturales	0,54	0,0	0,0	0,5	0,0	0,0
[I.*] Desastres industriales	0,54	0,0	0,0	0,5	0,0	0,0
[E.18] Destrucción de la información	5,4	0,0	0,0	3,8	0,0	0,0
[A.11] Acceso no autorizado	0	2,7	3,2	0,0	1,9	2,2
[LS] Salas Técnicas						
[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	0,45	0,0	0,0	0,3	0,0	0,0
[N.*] Desastres naturales	0,06	0,0	0,0	0,1	0,0	0,0
[I.*] Desastres industriales	0,06	0,0	0,0	0,1	0,0	0,0
[E.18] Destrucción de la información	0,45	0,0	0,0	0,3	0,0	0,0
[A.11] Acceso no autorizado	0	0,0	0,0	0,0	0,0	0,0
[LO] Otros						
[LE] Edificios						
[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	1,35	2,7	3,2	0,9	1,9	2,2
[N.*] Desastres naturales	0,18	0,0	0,0	0,2	0,0	0,0
[I.*] Desastres industriales	0,18	0,0	0,0	0,2	0,0	0,0
[E.18] Destrucción de la información	1,35	0,0	0,0	0,9	0,0	0,0
[A.11] Acceso no autorizado	0	2,7	3,2	0,0	1,9	2,2

31-Tabla-Detalle Valoración Riesgos Potenciales/Actuales

El resultado resumido sobre los riesgos asociados al inventario de activos se presenta en la siguiente tabla:

VALORACIÓN ACTIVOS-AMENAZAS	RIESGO POTENCIAL (Valor)			Riesgo Actual (Valor)		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[B] Activos esenciales						
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	6,3	0	0	4,3	0,0	0,0
[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES						
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	5,6	0,9	0,2	3,9	0,6	0,1
[B_D_SG_DES_TEC] Información Técnica de los Proyectos	4,9	2,1	0,7	3,4	1,5	0,5
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	4,9	2,1	0,7	3,4	1,5	0,5
[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS						
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	6,3	2,1	0,7	4,3	1,5	0,5
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	4,5	0,9	0,3	3,1	0,6	0,2
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	4,5	2,1	0,7	3,1	1,5	0,5
[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS						
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	6,3	0,9	0,3	4,3	0,6	0,2
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	2,7	2,1	0,5	1,9	1,5	0,4
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	2,7	2,1	0,3	1,9	1,5	0,2
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	6,3	6,3	0,9	4,3	4,3	0,6
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	2,7	1,5	0,3	1,9	1,1	0,2
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	4,05	2,1	0,7	3,6	1,5	0,5
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	5,4	2,1	0,7	3,8	1,5	0,5
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	5,4	1,5	0,6	3,7	1,1	0,4
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	1,35	2,1	0,7	0,9	1,5	0,5
[SRV] Servicios						
[SRVI] Servicios Internos						
[SRVI_IT] SERVICIOS GESTIONADOS IT						
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	2,7	0,0	0,0	2,0	0,0	0,0
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	6,3	0,0	0,0	4,7	0,0	0,0
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	4,5	0,0	0,0	3,4	0,0	0,0
[SRVI_ADMIN] Servicios Corporativos						
[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	1,35	0,0	0,0	0,9	0,0	0,0
[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	5,4	0,0	0,0	3,7	0,0	0,0
[SRVI_CORP_OPERACIONES] OPERACIONES	5,4	0,0	0,0	3,7	0,0	0,0
[SRVI_CORP_RRHH] Área de RR.HH.	5,4	0,0	0,0	3,7	0,0	0,0
[SRV_CORP_OPER] Dirección de Operaciones	3,6	0,0	0,0	2,7	0,0	0,0
[SRVE] Servicios Externos	0	0,0	0,0	0,0	0,0	0,0
[SRVE_CORREO] Servicio de Correo (GOOGLE)	5,4	0,0	0,0	3,7	0,0	0,0
[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	6,3	0,0	0,0	4,7	0,0	0,0

VALORACIÓN ACTIVOS-AMENAZAS	RIESGO POTENCIAL (Valor)			Riesgo Actual (Valor)		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	6,3	0,0	0,0	4,7	0,0	0,0
[SI] Sistema de Información						
[HW] Hardware						
[SI_HW_CLOUD_GOOGLE]						
[SI_HW_SERV_DA] Servidores de DA	2,7	2,7	2,7	2,0	2,0	1,5
[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	2,7	2,7	2,7	2,0	2,0	1,5
[SI_HW_SD_HD] Servidor Service Desk/Help Desk	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	0,9	3,6	2,7	0,7	2,7	1,5
[SI_HW_DATASTORE] Almacenamiento y Backup	3,6	2,1	2,1	2,7	1,6	1,2
[SI_HW_WEB_CORP] Servidores Web Corporativa	3,6	0,6	0,4	2,6	0,5	0,3
[SI_HW_CERTIF] Servidor de Certificados	3,6	3,6	3,6	2,7	2,7	2,7
[SI_HW_DATACENTER]						
[SI_HW_SIEM] Servidor SIEM	1,8	1,8	1,4	1,4	1,4	0,8
[SI_HW_AD_3] Servidor Controlador DominIo (AD)	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_MONITOR] Servidor de Monitorización	2,7	3,6	0,9	2,0	2,7	0,7
[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	3,6	0,9	0,9	2,6	0,7	0,7
[SI_HW_WIKI] Servidor de la Wiki	3,6	0,9	0,9	2,6	0,7	0,7
[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	5,4	4,5	4,5	4,1	3,4	3,4
[SI_HW_CORREO] Relay del Correo	3,6	2,7	2,7	2,7	2,0	2,0
[SI_HW_VIRTUAL] Plataforma Virtualización				0,0	0,0	0,0
[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	5,4	2,7	2,7	3,8	2,0	1,5
[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	3,6	2,4	1,2	2,7	1,8	0,7
[SI_HW_VM_CREDEN] Servidores Credenciales	6,3	5,4	5,4	4,8	4,1	4,1
[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	2,7	0,9	0,9	2,0	0,7	0,7
[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	3,6	2,7	2,7	2,6	2,0	2,0
[SI_HW_NAS] Servidor de Almacenamiento NAS	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_VM_MONITOR] Sistema de Monitorización	3,6	2,7	2,7	2,7	2,0	1,5
[SI_HW_SERV_LAB] Servidores laboratorio	0,9	0,9	0,9	0,7	0,7	0,7
[SI_HW_GLOBALSOC_Sede_MADRID]						
[SI_HW_PC] PC de Sobremesa	0,9	0,7	0,2	0,7	0,5	0,2
[SI_HW_TFNO_MOVIL] Teléfono Móvil	0,2	0,0	0,0	0,2	0,0	0,0
[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	1,6	0,0	0,0	1,1	0,0	0,0
[SI_HW_IMPRES] Equipos de Impresión	0,2	0,0	0,0	0,2	0,0	0,0
[SI_HW_SOC_MAD] Hardware SOC de MADRID						
[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	0,9	0,7	0,2	0,7	0,5	0,2
[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	2,7	2,1	0,6	2,0	1,6	0,3
[SW] Software						
[SI_SW_Windows] S.O. Puesto de Trabajo	2,7	2,1	0,3	1,7	1,3	0,2
[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	1,35	1,1	0,3	0,9	0,7	0,2
[SI_SW_Office] S.O. Puesto de Trabajo (Office)	2,7	2,1	0,3	1,7	1,3	0,2
[SI_SW_ANTIVIRUS] Software Antivirus	2,7	2,1	0,3	1,7	1,3	0,2
[SI_SW_ALM_NUBE] Google Drive	2,7	2,1	2,8	1,7	1,3	1,9
[SI_SW_WINDOWS] Windows Server	2,7	2,7	2,7	1,7	1,7	1,8
[SI_SW_LINUX] Software Linux	2,7	2,7	2,7	1,7	1,7	1,8
[SI_SW_CLOUD_GOOGLE]						
[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	1,8	1,4	1,4	1,2	0,9	0,9
[SI_SW_SERVICE DESK] Service Desk-Help Desk	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_SFTP] Servicios SFTP	1,35	1,4	1,4	0,9	0,9	0,9
[SI_SW_CERTIFICADOS] Servicios Certificados	2,7	3,6	4,5	1,7	2,0	3,1
[SI_SW_BACKUP] Servicios de Storage (DataStore)	2,7	2,8	2,8	1,7	1,7	1,9

VALORACIÓN ACTIVOS-AMENAZAS	RIESGO POTENCIAL (Valor)			Riesgo Actual (Valor)		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI_SW_WEB] Servicios Web Corporativos	1,8	0,9	0,6	1,2	0,6	0,4
[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_DATACENTER]						
[SI_SW_SIEM] Software SIEM	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_HYPERVISOR] Software Virtualización	4,5	2,7	1,4	3,1	1,7	0,9
[SI_SW_IPS] Software IPS	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_ANAL_DATA] Software Analítica de Datos	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_IDS] Software IDS	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_MONITOR] Software de Monitorización	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_SERV_FICH] Software de Servicio de Ficheros	2,7	2,7	1,4	1,7	1,7	0,9
[SI_SW_WIKI] Software Wiki	1,35	1,4	1,4	0,9	0,9	0,9
[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs	2,7	5,6	0,6	1,7	3,4	0,4
[SI_SW_CREDENCIALES] Software Gest. Credenciales	2,7	6,3	6,3	1,7	3,9	4,3
[SI_SW_RELAY CORREO] POSTFIX	1,35	1,4	1,4	0,9	0,9	0,9
[COM] Comunicaciones						
[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)						
[COM_LAN_GOOGLE] Red GOOGLE	4,5	3,6	2,7	3,4	2,0	1,8
[COM_FW_GOOGLE] Firewall Google	4,5	3,6	2,7	3,4	2,0	1,8
[COM_SWT_GOOGLE] Switches GOOGLE	3,6	3,6	2,7	2,7	2,0	1,8
[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)						
[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	3,6	3,6	2,7	2,7	2,0	1,8
[COM_LAN_DATACENTER] Red DATACENTER	3,6	3,6	2,7	2,7	2,0	1,8
[COM_SWT_DATACENTER] Switches DATACENTER	3,6	3,6	2,7	2,7	2,0	1,8
[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	3,6	3,6	2,7	2,7	2,0	1,8
[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)						
[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	1,5	0,0	0,0	1,1	0,0	0,0
[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	1,5	0,0	0,0	1,1	0,0	0,0
[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	2	0,0	0,0	1,5	0,0	0,0
[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	1,5	0,0	0,0	1,1	0,0	0,0
[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	2	0,0	0,0	1,5	0,0	0,0
[SS] Proveedores						
[SS_ES] Servicios Esenciales						
[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	0,9	0,9	1,8	0,7	0,5	1,2
[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	0,9	0,9	1,8	0,7	0,5	1,2
[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	0,9	0,9	1,8	0,7	0,5	1,2
[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)						
[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	0,6	0,0	0,0	0,5	0,0	0,0
[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	3,6	3,6	2,7	2,7	2,0	1,8
[SS_OT] Otros						
[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC	0,9	0,9	1,8	0,7	0,5	1,2
[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	0,5	0,0	0,0	0,4	0,0	0,0
[P] Personal						
[P_I] Personal Interno						
[P_I_SOC] Personal Interno del SOC MAD	3,6	0,0	3,6	2,5	0,0	2,5
[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	1,8	0,0	0,4	1,6	0,0	0,3
[P_I_FIN_LEG] Personal Resp. Financiero y Legal	3,6	0,0	0,8	2,5	0,0	0,5
[P_I_RRHH] Personal Resp. RR.HH.	3,6	0,0	0,8	2,5	0,0	0,5

VALORACIÓN ACTIVOS-AMENAZAS	RIESGO POTENCIAL (Valor)			Riesgo Actual (Valor)		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[P_I_Comercial] Personal Área Comercial y Marketing	1,8	0,0	0,6	1,6	0,0	0,4
[P_E] Personal Externo						
[P_E_MTO] Personal de Limpieza y Mantenimiento	0,3	0,0	0,0	0,3	0,0	0,0
[L] Instalaciones y Ubicaciones						
[LD] Dependencias						
[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	1,35	2,7	3,2	0,9	1,5	1,8
[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	1,35	2,7	3,2	0,9	1,5	1,8
[LD_GOOGLE_CLOUD] Cpd de GOOGLE	4,5	2,7	3,2	3,1	1,5	1,8
[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	5,4	2,7	3,2	3,7	1,5	1,8
[LS] Salas Técnicas						
[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	0,45	0,0	0,0	0,3	0,0	0,0
[LO] Otros						
[LE] Edificios						
[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	0	0,0	0,0	1,4	2,7	3,2

32-Tabla-Resumen Valoración Riesgos Potenciales/Actuales

3.8. Nivel de Riesgo Aceptable

En base a la metodología de Análisis de riesgo que se ha establecido en la organización (**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf**) una vez calculado los riesgos se establecen las reglas en cuanto a la Gestión de los mismos:

Todo riesgo que afecte a cualquier activo tendrá un propietario que asumirá dicho riesgo, y propondrá las medidas para tratarlo.

- Está permitido asignar más de un propietario para un riesgo, para el caso del Comité de Dirección.
- Se han establecido los siguientes criterios:
  - Riesgos por encima de 3/10. El propietario del riesgo para todos los activos será el Comité de Dirección (Seguridad).
  - Riesgos por debajo o igual a 3/10. El propietario del riesgo será el responsable del activo.

NIVEL	RIESGO	CONDICIÓN	TRATAMIENTO	PROPIETARIO	REVISIÓN
>7-10	EXTREMO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>3,0-7	SIGNIFICATIVO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>2-3,0	APRECIABLE	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	TRIMESTRAL
>1-2	BAJO	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	ANUAL
0-1	DESPRECIABLE	ACEPTABLE	NO	PROPIETARIO DEL RIESGO	ANUAL

33-Tabla-Nivel de Riesgo Aceptable

4. PROPUESTAS DE PROYECTOS

En base al análisis realizado en GLOBALSOC se establecido una bateria acciones ejecutar con la vista puesta en el aseguramiento y la mejora de la Seguridad de la Información de la Organización.

Como elementos se a la hora de determinar las acciones ejecutar se han considerado tanto la realización de análisis diferencial y el proceso acometido de Análisis de Riesgos sobre los activos de la Organización.

4.1. Relación de Proyectos

Las acciones a ejecutar se han agrupado en Proyectos, en base a criterios de afinidad y vinculación a los controles de Seguridad sobre los que afectan.

Las proyectos se han agrupado y tipificado en base a criterios tales como :

- **La tipología de proyecto**: El tipo de acciones a realizar.
- **La categoría**: En base a la casuística de tareas (técnicas y/o gestión resultante).
- **Responsable**: Se ha establecido los responsables finales de la ejecución de los proyectos.
- **Prioridad**: El nivel de importancia en cuanto al peso de mejora de la Seguridad en la organización.

En la tabla que aparece a continuación, se muestra el detalle de los proyectos resultantes.

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	**Tipo de Proyecto**	**Categoría**	**Nombre**	**Descripción**	**Actividades**	**Responsable**	**Prioridad**
PRY_01	**Implementación y Desarrollo**	**Gestión**	**Conocimiento y Difusión de la Política de Seguridad de la Organización**	**Mecanismo de conocimiento y difusión Política de Seguridad (Interna y Externamente a las partes interesadas)**	**Establecer mecanismos de difusión regulares Internos y Externos. Aseguramiento del conocimiento de las políticas (organización y proveedores).**	**CEO**	**Alta**
PRY_02	**Implementación y Desarrollo**	**Gestión**	**Constitución y Puesta en funcionamiento del Comité de Seguridad**	**Establecer oficialmente el Comité de Seguridad.**	**Establecer oficialmente el Comité de Seguridad. Entender las competencias. Establecer las funciones. Incorporarlo dentro del ciclo de Gestión de la Organización. Empezar a operar con normalidad (reunión, toma de decisiones, elaboración de actas).**	**Comité de Dirección**	**Alta**
PRY_03	**Desarrollo**	**Gestión**	**Definir en detalle las competencias, funciones y responsabilidades de todos los actores que intervienen en SI.**	**Definir en detalle las competencias, funciones y responsabilidades de todos los actores que intervienen en SI.**	**En base a los perfiles de Seguridad declarados dejar establecido en detalle: - Competencias técnicas y funcionales necesarias. - Roles y responsabilidades en SI.**	**CEO**	**Alta**
PRY_04	**Identificación y Registro**	**Gestión**	**Segregación de funciones**	**Establecer en Detalle las responsabilidades sobre los activos (propietarios) y los mecanismos de Autorización y validación de los accesos. Establecer mecanismos de registro y control.**	**Establecer en Detalle las responsabilidades sobre los activos (propietarios) y los mecanismos de Autorización y validación de los accesos. Establecer mecanismos de registro y control.**	**Resp. SGSI**	**Alta**

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	Tipo de Proyecto	Categoría	Nombre	Descripción	Actividades	Responsable	Prioridad
PRY_05	Implementación y Desarrollo	Gestión	Establecer un Plan de Comunicación para SI	Establecer/integrar en la organización un plan de Comunicación para poder gestionar las notificaciones en relación con la SI.	Verificar la existencia previa de un Plan de Comunicación Global a nivel de la organización. Establecer/integrar las necesidades de comunicación en SI. - Autoridades a Notificar. - Responsables. - Mecanismos y medios. - Incidencias. Difundirlo para el conocimiento de las Partes interesadas/afectadas.	Comité de Dirección	Alta
PRY_06	Definir y Desarrollar	Gestión	Revisión y Desarrollo de la Seguridad en los RR.HH.	Existe un Departamento dedicado a la gestión de RR.HH. Dentro de la Organización que centraliza todas las funciones de gestión de RR.HH (Selección, contratación , seguimiento del personal, y Baja). Tiene de Base las siguientes carencias: - La asunción, control y seguimiento de las necesidades en cuanto a formación (tanto en aspectos competenciales, funcionales y de seguridad). - Establecimiento de los mecanismos adecuados de aseguramiento de la Seguridad de los empleados en el momento de su contratación: - Acuerdos de Confidencialidad, protección de Datos personales, registro de entregas de equipamiento, políticas de Seguridad, etc.	Desarrollo Política de Capacitación y formación de los RR.HH. (relacionados con SI). Control y Seguimiento de los RR.HH. En cuanto a capacitación en SI. Planificación de la formación y/o concienciación en SI de todo el personal de la organización. Aseguramiento de la notificación y conocimiento de las Políticas de Seguridad de la información. TFM_PLAN_DE _SEGURIDAD_DE_LA_INFORMACION (apartado RR.HH.).pdf Creación registros asociados control Personal: - Recepción y devolución de activos de la organización. - Cláusulado de SI (confidencialidad, derechos de propiedad intelectual, Privacidad, etc.).	Dir. RR.HH.	Alta
PRY_07	Implementación y Desarrollo	Gestión y Tecnología (Mixto)	Políticas de Gestión y uso de los activos	Determinar las políticas a ampliar en el ciclo de vida de uso de los activos: - Mantenimiento de los registros de inventario (propiedad). - Prestamos y uso. - Manipulación y borrado de la información.	Determinar las políticas a ampliar en el ciclo de vida de uso de los activos: - Mantenimiento de los registros de inventario (propiedad). - Prestamos y uso. - Manipulación y borrado de la información.	CEO	Alta
PRY_08	Implementación y Desarrollo	Gestión	Establecer los criterios de Clasificación de la información y su uso	Establecer los criterios de clasificación de la información en base a la necesidad de seguridad de la organización:	Establecer los criterios de clasificación de la información en base a la necesidad de seguridad de la organización: - Tipificación de los criterios (Pública, Interna, Confidencial, Secreta). - Necesidades de etiquetado y reconocimiento del criterio. - Mecanismos de uso y tratamiento. Plan de implantación de la clasificación en toda la organización n base a las directrices establecidas. Entendimiento, conocimiento y uso en toda la Organización.	CEO	Alta

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	**Tipo de Proyecto**	**Categoría**	**Nombre**	**Descripción**	**Actividades**	**Responsable**	**Prioridad**
PRY_09	**Identificación evidencias existentes**	**Gestión**	**Revisión de los mecanismos de control de acceso ya existentes**	**Existe una política de control de acceso a los recursos de Red (habría que revisar si cumple con la Segregación de funciones ya que puede haber incoherencias).**	**Verificación de los criterios de Autorización y validación del acceso. Verificación de la existencia de registros. Verificación de la realización periódica de auditorías de comprobación de acceso.**	**Director IT**	**Alta**
PRY_10	**Definir y Registrar**	**Gestión y Tecnología (Mixto)**	**Establecer procedimiento de mecanismos y uso del Cifrado en la Organización**	**Establecer procedimiento de mecanismos y uso del Cifrado en la Organización**	**Establecer los mecanismos de cifrado necesarios y existentes, justificando su uso. Establecer registros de localización, configuración y gestión de los recursos asociados (Certificados, registros, caducidades, roles autorizados, etc.). PLAN_DE_SEGURIDAD_LA_INFORMACION (apartado cifrado).pdf registros de mantenimiento y Control.**	**Director IT**	**Media**
PRY_11	**Definir y Desarrollar**	**Gestión**	**Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)**	**No existe un procedimiento documentado que determine como se realiza la retirada de materiales en la organización y en especial si afecta a Seguridad de la Información.**	**Describir el procedimiento de retirada de materiales. Especificar si hay presencia de terceros; delimitando su actividades y responsabilidades. Establecer los mecanismos de salvaguarda, custodia y destrucción (en el caso que proceda). Especificar políticas de seguridad , roles y responsabilidades. Aseguramiento ante la intervención de terceros que cumplan con el procedimiento descrito y establecer compromisos de cumplimiento entre las partes. PLAN_DE_SEGURIDAD_DE_LA_INFORMACION.pdf (Retirada y custodia de materiales)**	**CEO**	**Media**
PRY_12	**Implementación y Desarrollo**	**Gestión**	**Revisar y Documentar las prácticas en Reutilización y Eliminación Segura de Equipos**	**Revisar las prácticas de reutilización y eliminación de equipos (centrándose en el aspecto de la posible información almacenada).**	**Revisión de las prácticas actuales. Desarrollo de procedimiento teniendo especial consideración en: - La presencia y/o ausencia de información en los equipos afectados. - Técnicas de aseguramiento del borrado físico de la información. - Roles y responsabilidades. - Necesidades de establecer mecanismos de custodia. SEGURIDAD_FISICA_Y_DEL_ENTORNO_pdf (desarrollar aquí los contenidos descritos).**		
PRY_13	**Identificación y Registro**	**Gestión**	**Revisión y aseguramiento de la documentación Técnica del área de Operación**	**Revisión de la IT's Técnicas existentes puestas a disposición del área de Operación. Calidad de los procedimientos, conocimiento, uso, mantenimiento y accesibilidad. Roles y responsabilidades sobre el mantenimiento de dichos documentos en el SOC.**	**Revisión de la IT's Técnicas existentes puestas a disposición del área de Operación. Calidad de los procedimientos, conocimiento, uso, mantenimiento y accesibilidad. Roles y responsabilidades sobre el mantenimiento de dichos documentos en el SOC.**	**Responsable SOC**	**Media**

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	**Tipo de Proyecto**	**Categoría**	**Nombre**	**Descripción**	**Actividades**	**Responsable**	**Prioridad**
PRY_14	**Identificación evidencias existentes**	**Gestión**	**Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia infraestructura del SOC**	**No se constata el uso del Service Desk para los cambios de la infraestructura IT del SOC.**	**Analizar la configuración de la Herramienta. Establecer los mecanismos de uso: registro, control y seguimiento de los cambios. Establecer Roles y Responsabilidades. Incluir la Gestión de Cambios en los reportes de Seguridad.**	**Director de Operaciones**	**Alta**
PRY_15	**Identificación y Registro**	**Gestión**	**Gestión de la Capacidad del SOC**	**Establecer los mecanismos para la Gestión de la Capacidad en base a: - La gestión del comportamiento de la infraestructura TI. - Los RR.HH. Afectados por el alcance (SOC). - La gestión del presupuesto en base a estrategia de negocio y necesidades del Servicio.**	**Revisión y Valoración de los mecanismos de monitorización existentes sobre la infraestructura IT. Aseguramiento del uso de los reportes de la monitorización para anticipar problemas de capacidad y/o rendimiento de la IT. Establecer mecanismos para anticipar las necesidades en los RR.HH. , con preferencia la equipo del SOC (en base a crecimiento de negocio, necesidad de nuevas competencias funcionales y/o técnicas, etc.). Realizar un registro formal de las necesidades presupuestarios del SOC. Como consecuencia de lo anterior se desarrolla: - Aseguramiento de la monitorización de IT (mecanismos de alerta y reporting). - Informes de monitorización con análisis de tendencias y seguimientos. - Informes de Comité de Operaciones (Carga de trabajo en Proyecto y Necesidades SOC). - Registro Previsión Presupuestos SOC**	**Director de Operaciones**	**Alta**
PRY_16	**Implementación y Desarrollo**	**Gestión**	**Separación de entornos**	**Establecer y normalizar una infraestructura diferenciada para gestionar de manera separada entornos de Desarrollo y Producción.**	**Establecer una Infraestructura diferenciada para tener entornos de Desarrollo y Producción, centrándose en los siguientes aspectos: - Ordenación y normalización en el uso de la Infraestructura de Laboratorio. - Establecer la Plataforma de Virtualización para su uso dentro del entorno de desarrollo. - Procedimentar el uso de los entornos, las garantías en el uso de los datos provenientes de la Producción. - Establecer los Roles y responsabilidades en cuanto a Mantenimiento y uso de los entornos. PLAN_DE_SEGURIDAD_DE_LA_NFORMACION.pdf (Separación de Entornos)**	**Responsable SOC**	**Alta**

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	Tipo de Proyecto	Categoría	Nombre	Descripción	Actividades	Responsable	Prioridad
PRY_17	Identificación y Registro	Gestión	Copias de Seguridad de la Información	Revisar y documentar las prácticas en la organización en la realización de los backups	Recopilación y revisión de los backups que se realizan en la organización. Documentación y registro de los backups realizados (tipos, periodicidad, retención, almacenamiento y custodia, recuperación, etc.) Documentación de la política backup y generación de los ajustes necesarios en base a la aplicación de dicha política. - Backup en base a los criterios de Clasificación. - Permanencia, retención, custodia y borrado. - Gestión de logs. - Pruebas de recuperación de backups, etc. POLITICA_DE_BACKUP.pdf IT_Documenta_Backup.pdf IT_BACKUPS_SERVICIOS_Registros.xls	Director de Operaciones	
PRY_18	Definir y Desarrollar	Gestión	Registro de eventos	Revisión de la gestión y control de los registros de eventos. Establecer el procedimiento de revisión y uso.	Revisión de la gestión y control de los registros de eventos. Establecer el procedimiento de revisión y uso. - Asegurar las fuentes de emisión de los logs (para ver si la recolección es adecuada). - Declaración de Roles y Responsabilidades. - Aseguramiento de los mecanismos de autorización y acceso. - Desarrollo del procedimiento de uso y mantenimiento de los registros de logs.	Director de Operaciones	Alta
PRY_19	Identificar evidencias existentes y añadir nuevas	Gestión	Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas encontradas)	Revisión y planificación de auditorías Regulares de Gestión de Accesos. Seguimiento de las vulnerabilidades encontradas en las auditorías técnicas halladas.	En base a las políticas de Acceso realizar revisiones periódicas de acceso: Establecer mecanismos de control y seguimiento en base a los hallazgos encontrados.	Director de Operaciones	Media
PRY_20	Implementación y Desarrollo	Gestión	Adquisición, desarrollo y mantenimiento de los sistemas de información	Análisis de requisitos y especificaciones de seguridad de la información	Establecer un procedimiento que contemple los Requisitos de seguridad a los proveedores que abarquen el ciclo de vida de Adquisición, desarrollo y Mantenimiento de los Sistemas de Información. Generar los siguientes recursos : - TFM_PROC_Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.pdf - Existencia de Herramienta para la Gestión de Proyectos (No está institucionalizado su uso para proyectos del SOC). - TFM_PROC_Gestión de riesgos en Proyectos.pdf - TFM_REG_Análisis de Riesgos en Proyectos.xls	CEO	Alta
PRY_21	Implementación y Desarrollo	Gestión y Tecnología (Mixto)	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	Generar procedimiento de Buenas práctica de Desarrollo: - Focalizado al desarrollo realizado (Scripting) PRACTICAS_DESARROLLO_DE_CODIGO.pdf Y establecer la tipificación y realización de pruebas funciones y de sistemas. Tratar los aspectos derivados del uso de Datos de producción en entornos de Desarrollo.	Director de Operaciones	Media

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	**Tipo de Proyecto**	**Categoría**	**Nombre**	**Descripción**	**Actividades**	**Responsable**	**Prioridad**
PRY_22	**Implementación y Desarrollo**	**Gestión**	**Relaciones con Proveedores**	**La gestión de los proveedores no está procedimentada y documentada. No se están realizando formalmente procesos de evaluación y revisión de los proveedores.**	**Desarrollar un procedimiento para establecer y determinar los requisitos de Seguridad con los Proveedores. Establecer, usar y mantener un registro de Proveedores. Realizar evaluaciones de cumplimiento de los requisitos de Seguridad. - PROC_Relaciones con Proveedores.pdf - REG_Relación y Evaluación Proveedores.xls**	**CEO**	**Alta**
PRY_23	**Identificación y Registro**	**Gestión y Tecnología (Mixto)**	**Gestión de incidentes de seguridad de la información**	**La organización tiene implantado un proceso de gestión de Incidentes que aplica tanto para la operativa de los Servicios a los Clientes; como para gestionar las incidencias específicas del SOC. cuenta con herramientas, tienen establecidos las categorizaciones, tratamiento, flujos y mecanismos de escalado. No existe una tipificación de los incidentes de seguridad (pero son adaptables dentro de los procesos de incidencias ya existentes).**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**Director de Operaciones**	**Alta**
PRY_24	**Implementación y Desarrollo**	**Gestión**	**CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**	**Determinar los Servicios Críticos de la Organización en base a la realización de los BIAs (Análisis de Impacto de Negocio). Establecer un plan de continuidad de negocio para afrontar la recuperación de Servicios Críticos detectados. Establecer Un plan de pruebas para chequear y mejorar la Continuidad implementada.**	**Determinar los Servicios Críticos de la Organización en base a la realización de los BIAs: - Generación de los BIAs en Base a los Servicios de Negocio/Soporte existentes en la organización. - Metodología de Análisis de Impacto en el Negocio.pdf PROC_Gestión de la Continuidad de Negocio.pdf REG_Planificación Escenarios de Contingencia.xls REG_Bitácora Prueba Escenarios de Contingencia .xls REG_BIA y Estrategias_GESTION DE CAMBIOS.xls REG_BIA y Estrategias_GESTION DE DESPLIEGUES.xls REG_BIA y Estrategias_GESTION DE INCIDENCIAS.xls Roles, Responsabilidades y Competencias del PCN.xls REG_ DRT y Contactos.xls Establecer un Plan de Continuidad focalizado en los Servicios Críticos . prestando especila atención al DRP. Metodología de Análisis de Impacto en el Negocio.pdf IT_Plan de Contingencia.pdf REG_PLAN_DE_PRUEBAS**	**CEO**	**Alta**

Propuesta de Proyectos para mejorar la madurez sobre ISO 27002							
Proyecto	Tipo de Proyecto	Categoría	Nombre	Descripción	Actividades	Responsable	Prioridad
PRY_25	Identificación y Registro	Gestión	CONFORMIDAD CON LOS REQUISITOS LEGALES	Competencia delegada al Área Jurídica. El enfoque está contemplado parcialmente; pero no existe una unificación de los criterios y sobre todo un mecanismo de aplicación y control.	TFM_PROC_Plan de Seguridad de la Información.pdf (Revisión) TFM_PROC_Cumplimiento Legal y Normativo.pdf (Centralizar los requisitos)	Dir. RR.HH.	Alta
PRY_26	Implementación y Desarrollo	Gestión	DOCUMENTACIÓN PARTES INTERESADAS	Análisis, Registro y matenimiento de las partes interesadas que son relevantes para la Organización y la SI,	Análisis, Registro y matenimiento de las partes interesadas que son relevantes para la Organización y la SI,	Dir. RR.HH.	Media
PRY_27	Implementación y Desarrollo	Gestión	DOCUMENTACIÓN DE LOS PROCESOS DE LA ORGANIZACIÓN	Establecer los procesos de Negocio y Soporte de la organización: - Funciones, activiades y roles - Flujos de información y dependencias	Establecer los procesos de Negocio y Soporte de la organización: - Funciones, activiades y roles - Flujos de información y dependencias	Comité de Dirección	Media

34-Propuesta de Proyectos

4.1.1. Asociación Proyectos&Cláusulas ISO 27001&Controles ISO 27002

Es importante también, dejar establecida la relación de los proyectos y la afectación en base a :

- **Las cláusulas establecidas en el SGISI (establecidos en base a la ISO 27001).**
- **Los controles de Seguridad (asociados en base a la ISO 27002).**

Nos permitirá, más adelante, poder medir la mejora en cuanto a la evolución del nivel de madurez de la SI e interaccionar con los riesgos resultantes como consecuencia de la realización del proceso Análisis de Riesgos para calcular la mitigación, reduccción y/ eliminación sobre los riesgos actuales.

En la siguiente tabla, se muestra en detalle la implicación de los proyectos a ejecutar respecto de los controles de Seguridad.

Asociación Proyectos-Controles ISO 27002&ISO 27001			
Cod. Proyecto	**Tipo de proyecto**	**Nombre**	**Cláusulas ISO 27001& Controles ISO 27002 asociados**
PRY_01	**Implementación y Desarrollo**	**Conocimiento y Difusión de la Política de Seguridad de la Organización**	**A.5.1.1, A.5.1.2**
PRY_02	**Implementación y Desarrollo**	**Constitución y Puesta en funcionamiento del Comité de Seguridad**	**A.5.1.2**
PRY_03	**Desarrollo**	**Definir en detalle las competencias, funciones y responsabilidades de todos los actores que intervienen en SI.**	**A.6.1.1**
PRY_04	**Identificación y Registro**	**Segregación de funciones**	**A.6.1.2**
PRY_05	**Implementación y Desarrollo**	**Establecer un Plan de Comunicación para SI**	**A.6.1.3, A.6.1.4, C.7.4**
PRY_06	**Definir y Desarrollar**	**Revisión y Desarrollo de la Seguridad en los RR.HH.**	**A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, C.7.1, C.7.2, C.7.3**
PRY_07	**Implementación y Desarrollo**	**Políticas de Gestión y uso de los activos**	**A.8.1.1, A.8.1.2, A.8.1.3**
PRY_08	**Implementación y Desarrollo**	**Establecer los criterios de Clasificación de la información y su uso**	**A.8.2.1, A.8.2.2, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3**
PRY_09	**Identificación evidencias existentes**	**Revisión de los mecanismos de control de acceso ya existentes**	**A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, 9.2.5, A.9.4.1, A.9.4.4, A.9.4.5**
PRY_10	**Definir y Registrar**	**Establecer procedimiento de mecanismos y uso del Cifrado en la Organización**	**A.9.10.1, A.9.10.2**
PRY_11	**Definir y Desarrollar**	**Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)**	**A.11.2.5**
PRY_12	**Implementación y Desarrollo**	**Revisar y Documentar las prácticas en Reutilización y Eliminación Segura de Equipos**	**A.11.2.7**
PRY_13	**Identificación y Registro**	**Revisión y aseguramiento de la documentación Técnica del área de Operación**	**A.12.1.1**
PRY_14	**Identificación evidencias existentes**	**Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia infraestructura del SOC**	**A.12.1.2**
PRY_15	**Identificación y Registro**	**Gestión de la Capacidad del SOC**	**A.12.1.3**
PRY_16	**Implementación y Desarrollo**	**Separación de entornos**	**A.12.1.4**
PRY_17	**Identificación y Registro**	**Copias de Seguridad de la Información**	**A.12.3.1**
PRY_18	**Definir y Desarrollar**	**Registro de eventos**	**A.12.4.1**
PRY_19	**Identificar evidencias existentes y añadir nuevas**	**Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas encontradas)**	**A.12.7.1**
PRY_20	**Implementación y Desarrollo**	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4**
PRY_21	**Implementación y Desarrollo**	**Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas**	**A.14.2.1, A.14.2.8, A.14.2.9**

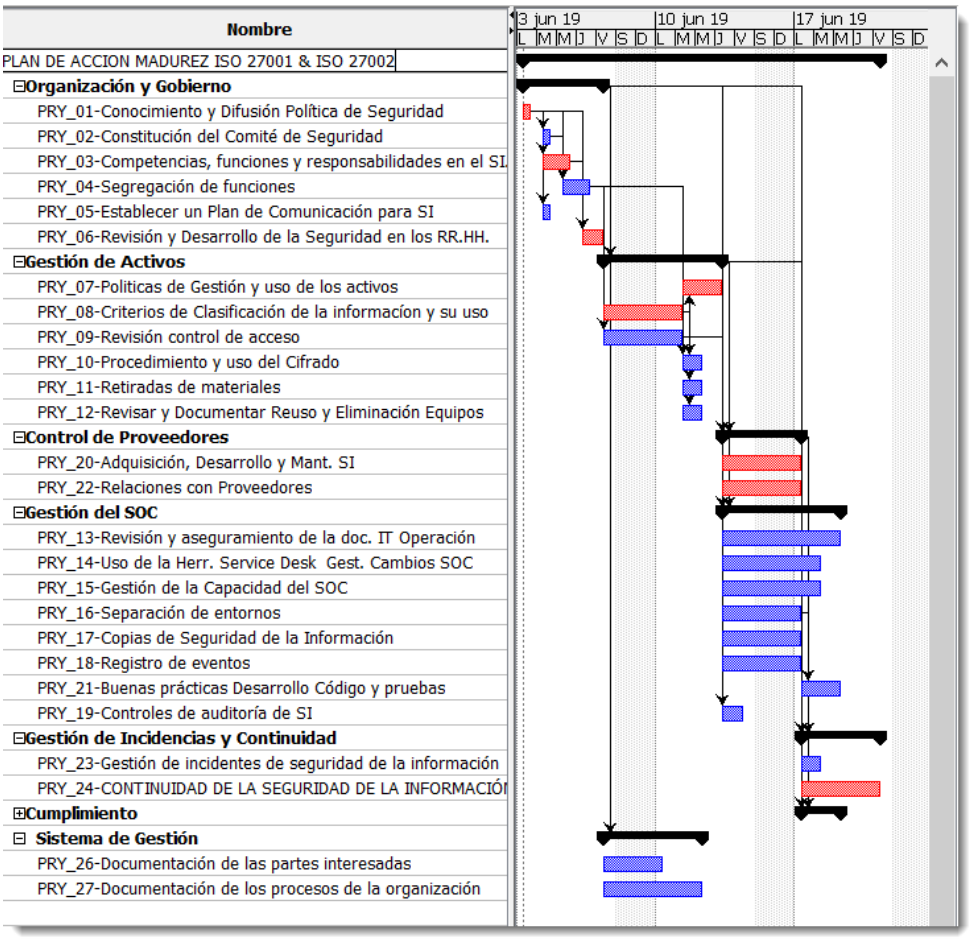
Asociación Proyectos-Controles ISO 27002&ISO 27001			
Cod. Proyecto	Tipo de proyecto	Nombre	Cláusulas ISO 27001& Controles ISO 27002 asociados
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.1.1,A.15.1.2,A.15.1.3,A.15.2.1,A.15.2.2
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.1, .16.1.2,A.16.1.3,A.16.1.4,A.16.1.5,A.16.1.6
PRY_24	Implementación y Desarrollo	CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	A.17.1.1, A.17.1.2,A.17.1.3
PRY_25	Identificación y Registro	Conformidad con los requisitos legales	A.18.1.2,A.18.1.3,A.18.1.5
PRY_26	Implementación y Desarrollo	Documentación de las partes interesadas	C.4.2
PRY_27	Implementación y Desarrollo	Documentación de los procesos de la organización	C.4.3, C.5.3

35-Asociación Proyectos&Cláusulas ISO 27001&Controles ISO 27002

4.1.2. Planificación del Proyecto

La forma propuesta para acometer la ejecución global de los Proyectos descritos, agrupados en base a áreas de contenidos afines, dependencias de información y agrupación por áreas de responsabilidad dentro de la organización.

Como resultado de todo lo anterior, este sería el plan de Proyecto propuesto:



36-Planificacion del Proyecto

4.1.3. Planificación del esfuerzo en el Proyecto

La valoración del esfuerzo por cada uno de los proyectos detectados, así como el grado de intervención y participación de la organización en los mismos, se muestra en la tabla siguiente:

Planificación de Esfuerzo en Proyectos			
Cod. Proyecto	**Nombre**	**Tiempo estimado (jornadas)**	**Recursos& Participación**
PRY_01	**Conocimiento y Difusión de la Política de Seguridad de la Organización**	**2**	**CEO- 50%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25% DIR. OPERACIONES-25%, CISO-100%**
PRY_02	**Constitución y Puesta en funcionamiento del Comité de Seguridad**	**2**	**CEO- 10%,DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25% DIR. OPERACIONES-25%, CISO-100%**
PRY_03	**Definir en detalle las competencia, funciones y responsabilidades de todos los actores que intervienen en SI.**	**5**	**DIR. RR.HH. (CFO/CIO) 100%,RESP. LEGAL-15% DIR. OPERACIONES-50%, DIR. AREA-50% CISO-100%,RESP. SOC-100%**
PRY_04	**Segregación de funciones**	**6**	**DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15% DIR. OPERACIONES-50%, DIR. AREA-50% CISO-100%, RESP. SOC-100%**
PRY_05	**Establecer un Plan de Comunicación para SI**	**2**	**CEO-50%, DIR. MARKETING-100% DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50% DIR. OPERACIONES-50%, DIR. AREA-50% CISO-100%, RESP. SOC-15%**
PRY_06	**Revisión y Desarrollo de la Seguridad en los RR.HH.**	**4**	**DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-25% DIR. OPERACIONES-25%, CISO-100%**
PRY_07	**Políticas de Gestión y uso de los activos**	**7**	**CEO-10%, DIR. RR.HH. (CFO/CIO) 100% RESP. LEGAL-10%, DIR. OPERACIONES/DIR IT-50% DIR. AREA-50%, CISO-100%, RESP. SOC-15%**
PRY_08	**Establecer los criterios de Clasificación de la información y su uso**	**7**	**CEO-10%, DIR. RR.HH. (CFO/CIO) 100% RESP. LEGAL-10%, DIR. OPERACIONES/DIR. IT-50% DIR. AREA-50%, CISO-100%, RESP. SOC-15%**
PRY_09	**Revisión de los mecanismos de control de acceso ya existentes**	**3**	**CEO-10%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-10% DIR. OPERACIONES/DIR. IT-50%, DIR. AREA-50% CISO-100%, RESP. SOC-15%**
PRY_10	**Establecer procedimiento de mecanismos y uso del Cifrado en la Organización**	**3**	**DIR. OPERACIONES/DIR. IT-50%, CISO-100%, RESP. SOC-15%**
PRY_11	**Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)**	**3**	**DIR. RR.HH. (CFO/CIO) 25%, RESP. LEGAL-10% DIR. OPERACIONES/DIR. IT-50%, DIR. AREA-50% CISO-100%, RESP. SOC-35%**
PRY_12	**Revisar y Documentar las prácticas en Reutilización y Eliminación Segura de Equipos**	**10**	**DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10% DIR. OPERACIONES/DIR. IT-50%, CISO-100% RESP. SOC-35%**
PRY_13	**Revisión y aseguramiento de la documentación Técnica del área de Operación**	**8**	**DIR. OPERACIONES/DIR. IT-50%, CISO-30%, RESP. SOC-100%**

Planificación de Esfuerzo en Proyectos			
Cod. Proyecto	Nombre	Tiempo estimado (jornadas)	Recursos& Participación
PRY_14	Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia infraestructura del SOC	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_15	Gestión de la Capacidad del SOC	8	DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10%, DIR. OPERACIONES/DIR. IT-50%, CISO-100%, RESP. SOC-35%
PRY_16	Separación de entornos	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_17	Copias de Seguridad de la Información	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_18	Registro de eventos	8	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_19	Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas encontradas)	3	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_20	Adquisición, desarrollo y mantenimiento de los sistemas de información	9	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50% DIR. OPERACIONES/DIR. IT-30%, CISO-100%, RESP. SOC-25%
PRY_21	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	5	DIR. OPERACIONES/DIR. IT-50%, CISO-10%, RESP. SOC-100%
PRY_22	Relaciones con Proveedores	7	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-50%, DIR. OPERACIONES/DIR. IT-30%, CISO-100%, RESP. SOC-25%
PRY_23	Gestión de incidentes de seguridad de la información	4	DIR. RR.HH. (CFO/CIO) 10%, RESP. LEGAL-10% DIR. OPERACIONES/DIR. IT-50%, CISO-50%, RESP. SOC-100%
PRY_24	Continuidad de la Seguridad de la Información	12	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15% DIR. OPERACIONES-50%, DIR. AREA-50%, CISO-100% RESP. SOC-100%
PRY_25	Conformidad con los requisitos legales	6	DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-100%, CISO-50%
PRY_26	Documentación de las partes interesadas	5	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15% DIR. OPERACIONES-50%, DIR. AREA-50%, CISO-100% RESP. SOC-100%
PRY_27	Documentación de los procesos de la organización	12	CEO-15%, DIR. RR.HH. (CFO/CIO) 100%, RESP. LEGAL-15% DIR. OPERACIONES-50%, DIR. AREA-50%, CISO-100% RESP. SOC-100%

37-Planificación del Proyecto-Esfuerzo y Participación

4.1.4. Proyectos-Incremento de la Madurez ISO 27001&ISO 27002 estimada

La estimación de la mejora en la madurez de cláusulas y controles una vez ejecutados los proyectos planteados se muestra en la siguiente tabla :

Controles-Proyectos (INCREMENTO DE LA MADUREZ estimada)				
Cod. Proyecto	**Tipo de proyecto**	**Nombre**	**Cláusulas ISO 27001& Controles ISO 27002 Asociados**	**Incremento Madurez control**
PRY_01	Implementación y Desarrollo	Conocimiento y Difusión de la Política de Seguridad de la Organización	A.5.1.1	0,75
PRY_01	Implementación y Desarrollo	Conocimiento y Difusión de la Política de Seguridad de la Organización	A.5.1.2	0,75
PRY_02	Implementación y Desarrollo	Constitución y Puesta en funcionamiento del Comité de Seguridad	A.5.1.2	0,5
PRY_03	Desarrollo	Definir en detalle las competencias, funciones y responsabilidades de todos los actores que intervienen en SI.	A.6.1.1	0,75
PRY_04	Identificación y Registro	Segregación de funciones	A.6.1.2	1
PRY_05	Implementación y Desarrollo	Establecer un Plan de Comunicación para SI	A.6.1.3	1
PRY_05	Implementación y Desarrollo	Establecer un Plan de Comunicación para SI	A.6.1.4	0,25
PRY_05	Implementación y Desarrollo	Establecer un Plan de Comunicación para SI	C.7.4	1
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	A.7.1.1	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	A.7.1.2	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	A.7.2.1	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	A.7.2.2	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	C.7.1	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	C.7.2	0,75
PRY_06	Definir y Desarrollar	Revisión y Desarrollo de la Seguridad en los RR.HH.	C.7.3	0,75
PRY_07	Implementación y Desarrollo	Políticas de Gestión y uso de los activos	A.8.1.1	1
PRY_07	Implementación y Desarrollo	Políticas de Gestión y uso de los activos	A.8.1.2	1
PRY_07	Implementación y Desarrollo	Políticas de Gestión y uso de los activos	A.8.1.3	1
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.2.1	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.2.2	1,5
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.2.3	1,5
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.13.2.1	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.13.2.2	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.13.2.3	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.3.1	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.3.2	1,25
PRY_08	Implementación y Desarrollo	Establecer los criterios de Clasificación de la información y su uso	A.8.3.3	1,25
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.1.1	0,5
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.1.2	0,5

Controles-Proyectos (INCREMENTO DE LA MADUREZ estimada)				
Cod. Proyecto	Tipo de proyecto	Nombre	Cláusulas ISO 27001& Controles ISO 27002 Asociados	Incremento Madurez control
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.2.1	0,75
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.2.2	0,75
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.2.3	0,75
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.2.5	1
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.4.1	1
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.4.4	1,25
PRY_09	Identificación evidencias existentes	Revisión de los mecanismos de control de acceso ya existentes	A.9.4.5	1,25
PRY_10	Definir y Registrar	Establecer procedimiento de mecanismos y uso del Cifrado en la Organización	A.10.1.1	0,5
PRY_10	Definir y Registrar	Establecer procedimiento de mecanismos y uso del Cifrado en la Organización	A.10.1.2	1
PRY_11	Definir y Desarrollar	Retiradas de materiales propiedad de la empresa (Susceptibles de contener la Información)	A.11.2.5	0,5
PRY_12	Implementación y Desarrollo	Revisar y Documentar las prácticas en Reutilizacíon y Eliminación Segura de Equipos	A.11.2.7	0,75
PRY_13	Identificación y Registro	Revisión y aseguramiento de la documentación Técnica del área de Operación	A.12.1.1	0,75
PRY_14	Identificación evidencias existentes	Uso de la Herramienta de Service Desk para la Gestión de Cambios de la propia infraestructura del SOC	A.12.1.2	1
PRY_15	Identificación y Registro	Gestión de la Capacidad del SOC	A.12.1.3	0,75
PRY_16	Implementación y Desarrollo	Separación de entornos	A.12.1.4	1
PRY_17	Identificación y Registro	Copias de Seguridad de la Información	A.12.3.1	0,75
PRY_18	Definir y Desarrollar	Registro de eventos	A.12.4.1	0,75
PRY_19	Identificar evidencias existentes y añadir nuevas	Controles de auditoría de SI (Revisión de los accesos y vulnerabilidades técnicas encontradas)	A.12.7.1	0,75
PRY_20	Implementación y Desarrollo	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.1.1	1,25
PRY_20	Implementación y Desarrollo	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.2.2	0,75
PRY_20	Implementación y Desarrollo	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.2.3	0,75
PRY_20	Implementación y Desarrollo	Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.2.4	0,75
PRY_21	Implementación y Desarrollo	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	A.14.2.1	1,25
PRY_21	Implementación y Desarrollo	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	A.14.2.8	1
PRY_21	Implementación y Desarrollo	Buenas prácticas de Desarrollo de Código y tipificación pruebas funcionales y de Sistemas	A.14.2.9	0,75
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.1.1	1
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.1.2	1
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.1.3	0,75
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.2.1	1,25
PRY_22	Implementación y Desarrollo	Relaciones con Proveedores	A.15.2.2	1,25
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.1	0,75

Controles-Proyectos (INCREMENTO DE LA MADUREZ estimada)				
Cod. Proyecto	Tipo de proyecto	Nombre	Cláusulas ISO 27001& Controles ISO 27002 Asociados	Incremento Madurez control
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.2	0,75
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.3	0,75
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.4	0,75
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.5	0,75
PRY_23	Identificación y Registro	Gestión de incidentes de seguridad de la información	A.16.1.6	0,5
PRY_24	Implementación y Desarrollo	Continuidad de la Seguridad de la Información	A.17.1.1	1,25
PRY_24	Implementación y Desarrollo	Continuidad de la Seguridad de la Información	A.17.1.2	1,25
PRY_24	Implementación y Desarrollo	Continuidad de la Seguridad de la Información	A.17.1.3	1,25
PRY_25	Identificación y Registro	Conformidad con los requisitos legales	A.18.1.2	1,25
PRY_25	Identificación y Registro	Conformidad con los requisitos legales	A.18.1.3	1,25
PRY_25	Identificación y Registro	Conformidad con los requisitos legales	A.18.1.5	1,25
PRY_25	Identificación y Registro	Conformidad con los requisitos legales	A.18.2.2	1,25
PRY_26	Implementación y Desarrollo	Documentación de las partes interesadas	C.4.2	1,25
PRY_27	Implementación y Desarrollo	Documentación de los procesos de la organización	C.4.3	1
PRY_27	Implementación y Desarrollo	Documentación de los procesos de la organización	C.5.3	1

38-Incremento de madurez por proyectos

5. AUDITORÍA DE CUMPLIMIENTO

5.1. Introducción

Tomado como marco de referencia :

- **El referencial del SGSI UNE-ISO/IEC 27001--Sistemas de Gestión de Seguridad de la Información-Requisitos**
- **El referencial de Controles de Seguridad UNE-ISO/IEC 27002-Código de prácticas para los controles de Seguridad de la información.**

Los requisitos desarrollados en UNE-ISO/IEC 27001 se resumen en el cumplimiento en las siguientes áreas:

ISO 27001-Requisitos
• C.4- CONTEXTO DE LA ORGANIZACIÓN
• C.5- LIDERAZGO
• C.6- PLANIFICACION
• C.7- SOPORTE
• C.8- OPERACIÓN
• C.9- EVALUACION DEL DESEMPEÑO
• C.10- MEJORA

39-ISO 27001-Requisitos

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control.

ISO 27002-Dominios de Control
• A.5 Políticas de seguridad de la información
• A.6 Organización de la seguridad de la información
• A.7 Seguridad relativa a los recursos humanos
• A.8 Gestión de activos
• A.9 Control de acceso
• A.10 Criptografía
• A.11 Seguridad física y del entorno
• A.12 Seguridad de las operaciones
• A.13 Seguridad de las comunicaciones
• A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información
• A.15 Relación con proveedores
• A.16 Gestión de incidentes de seguridad de la información

ISO 27002-Dominios de Control
• **A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio**
• **A.18 Cumplimiento**

40-ISO 27002-Dominios de Control

Sobre este marco de referencia, se ha realizado un análisis del estado de situación de los controles de Seguridad existente en la organización y, a partir de dicho análisis se ha realizado una valoración del nivel de madurez actual en cuanto al grado de cumplimiento de los controles de seguridad.

- El análisis detallado de cada uno de los controles en dónde se determinan si ya han sido desarrollados mecanismos para abordar los controles, o bien no han sido abordados; y en todo caso, cuales son las posibles carencias de base que no han sido consideradas por la organización. Igualmente, se han valorado aquellos controles que no van a ser usados (no aplican), en base a los criterios de que sirven para controlar aspectos de la seguridad que quedan fuera del ámbito de las actividades dentro de nuestro alcance.
    - La realización de éste ejercicio ha quedado reflejado a través del Análisis Diferencial (**1.5-Análisis Diferencial**); habiendo obtenido como resultados :
        - **8.1**-TFM_Informe_Analisis_Diferencial.pdf
        - **8.2**-TFM_Declaración de Aplicabilidad SOA.xlsx
    - Se ha realizado el ejercicio de acometer el desarrollo de base del SGSI generando la documentación y registros para configurar un sistema de Gestión sobre el que sustentar la SI de la organización.
        - 2-**SISTEMA DE GESTIÓN DOCUMENTAL**
    - Asimismo, la lista de controles ISO 27002 no aplicados se resumen en la siguiente tabla:

Lista de Controles ISO 27002 excluidos			
Dominio	**Control**	**Descripción**	**Justificación**
A.11	**A.11.1.6**	**A.11.1.6 Áreas de carga y descarga**	**No existen áreas físicas de Carga y Descarga**
A.11	**A.11.2.8**	**A.11.2.8 Equipo del usuario desatendido**	**Servidor que muestra las pantallas (pero se encuentra ubicado dentro de la sala tecnica).**
A.14	**A.14.1.2**	**A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas**	**No existen éstos servicios dentro de nuestro alcance**
A.14	**A.14.1.3**	**A.14.1.3 Protección de las transacciones de servicios de aplicaciones**	**No existen éstos servicios dentro de nuestro alcance**
A.14	**A.14.2.7**	**A.14.2.7 Externalización del desarrollo de software**	**El sotfware desarrollado es internamente (Shell scripting)**

41-Lista de controles Excluidos

- La valoración del nivel de madurez se aborda aplicando sobre el resultado del análisis obtenido el basa en el Modelo de Madurez de la Capacidad-CMM (**ilustración-42- Modelo de Evaluación Nivel de Madurez-CMM**) y para ello se desarrolla en base a una metodología, en dónde quedan establecidos los pasos a realizar para obtener la valoración; obteniendo como resultado la valoración del nivel de madurez actual de la Seguridad en la Organización.

- La realización de este ejercicio ha quedado reflejado a través de la evaluación de la madurez actual de la seguridad en la organización.

5.2. Metodología

La metodología desarrollada para poder realizar la valoración de la madurez en Seguridad de la Información nuestra organización se expone a continuación.

5.2.1. Base Metodológica

Se toma como base para desarrollar la metodología de evaluación de la madurez el modelo de madurez de Capacidad-CMM que aparece detallado en la siguiente tabla :

Modelo de Evaluación Nivel de Madurez-CMM				
Efectividad	**Rango de valor (0-5)**	**CMM**	**Significado**	**Descripción**
0%	**0**	**L0**	**Inexistente**	• **Carencia completa de cualquier proceso reconocible.** • **No se ha reconocido siquiera que existe un problema a resolver.**
10%	**>0 & <1**	**L1**	**Inicial / Ad-hoc**	• **Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.** • **Los procedimientos son inexistentes o localizados en áreas concretas.**
50%	**>1 & <2**	**L2**	**Reproducible, pero intuitivo**	• **Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.** • **Se normalizan las buenas prácticas en base a la experiencia y al método.** • **No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.** • **Se depende del grado de conocimiento de cada individuo.**
90%	**>2 & <3**	**L3**	**Proceso definido**	• **La organización entera participa en el proceso.** • **Los procesos están implantados, documentados y comunicados mediante entrenamiento.**
95%	**>3 & < 4**	**L4**	**Gestionable y medible**	• **Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.** • **Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.**
100%	**≥4 & <=5**	**L5**	**Optimizado**	• **Los procesos están bajo constante mejora.** • **En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.**

42- Modelo de Evaluación Nivel de Madurez-CMM

Quedan establecidos los siguientes elementos de referencia :

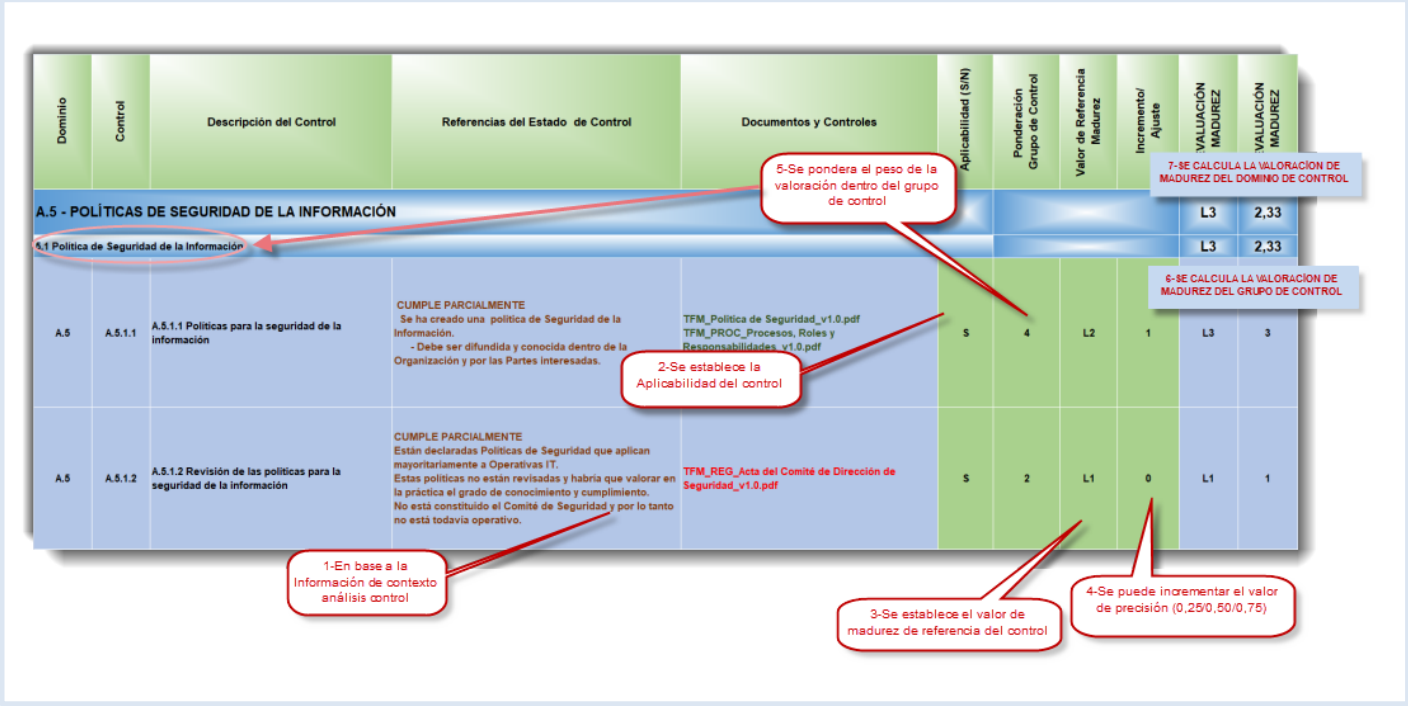
- El nivel de madurez **CMM** queda establecido para los valores comprendidos entre L0-L5; en dónde se describen las condiciones de base de cumplimiento y estado sobre los controles aplicados.
  - Viene a representar una escala que nace con la inexistencia de mecanismos de control (L0) hasta llegar a un grado máximo (L5) de aseguramiento y mejora constante de la efectividad del control aplicado sobre la organización.
- La medición por cada nivel, en base % del grado de **efectividad** del control en base al avance de la madurez de los controles (CMM).
  - Con un rango de recorrido desde el 0% al 100%.

- El **Rango de valor** permite una cuantificación más exacta del nivel de madurez, considerando siempre desde la referencia del CMM; dejando establecido un rango de precisión dentro de cada nivel.
    - Sobre un recorrido de rango comprendido entre 0-5.
- El **Significado** y la **Descripción** asociada muestran las condiciones a cumplir y el grado de progresión en el nivel de madurez en base a la no existencia, implantación, documentación y registro, medición, seguimiento y control, y optimización sobre los controles de seguridad.

5.2.2. Valoración de la madurez de los controles

La valoración de la madurez se aplica sobre cada uno de los controles del catálogo de controles de la ISO 27002, excluyendo aquellos controles que no aplican (**Tabla-41-Lista de controles Excluidos**).

Se realiza la valoración de la madurez para cada control siguiendo los pasos del 1-7 que se encuentran descritos en el siguiente gráfico.



43- Valoración de control-Nivel de Madurez

El detalle acerca de los valores de entrada y los cálculos asociados para obtener la valoración se desarrollan en la siguiente tabla:

Consideraciones-Valoración de los Controles		
Concepto	**Valores**	**Descripción**
Aplicabilidad	**S, N**	**Si el control es considerado dentro de la evaluación**
Valor de Referencia de Madurez	**L0, L1, L2, L3, L4, L5**	**Valor de Referencia de base de la Valoración del Control (L0-L5)** **El valor numérico entero que lleva asociado para cada uno de los niveles de Rango de Valor (L0=0, L1-=1, L2=>2, L3-=3,L4=>,L5=5)**

Consideraciones-Valoración de los Controles		
Concepto	**Valores**	**Descripción**
Incremento/Ajuste	**0/0,25/0,50/0,75/1**	**Mecanismo para establecer la precisión deseada en el valor de rango de control**
Ponderación Grupo de control	**1-Baja, 2-Media, 4-Alta**	**Peso específico en el grado de cumplimiento del control dentro del grupo de Control al que pertenece.**
EVALUACIÓN MADUREZ (Rango de Valor)	**0-5**	**Valor decimal calculado** • **Sobre Grupo de Control:** o **El sumatorio de la valoración de los controles en base al peso específico declarado para cada uno de ellos dividido entre el conjunto de controles aplicables dentro del grupo de control.** • **Sobre Dominio:** o **El promedio de la Valoración del conjunto de grupos de control asociados al Dominio.**
EVALUACIÓN MADUREZ (CMM)	**L0, L1, L2, L3, L4, L5**	**En base a EVALUACIÓN MADUREZ (Rango de Control) resultante** **=SI($O4>4;"L5";SI($O4>3;"L4";SI($O4>2;"L3";SI($O4>1;"L2";SI($O4>0;"L1";"L0")))))**

44- Consideraciones-valoración de las cláusulas y los controles

Tal y como ya se ha comentado, una vez realizada esta tarea para el conjunto de controles afectados se habrá obtenido la valoración global de madurez en base a al cláusulado de la **ISO 27001** y del referencial del Catálogo de controles de la **ISO 27002**.

5.3. Evaluación de la madurez ISO 27001

A continuación se muestra el detalla de la valoración de la madurez actual en cuanto al estado y grado de cumplimiento de las cláusulas basadas en la metodología anteriormente descrita.

Valoración Madurez-Cláusulas ISO 27001									
Dominio	**Cláusula**	**Descripción del Control**	**Referencias del Estado Cláusula**	**Documentos y Controles**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
C.4- CONTEXTO DE LA ORGANIZACIÓN								**L3**	**2,25**
4-Contexto de la Organización								**L3**	**2,25**
C.4	**C.4.1**	**4.1 Comprensión de la organización y de su contexto**	**La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.**	**CUMPLE** **Existe un conocimiento expreso del Contexto de la Organización y las Partes interesadas:** **- Existe documentación sobre conocimiento de Mercado, estrategias de la organización y una valoración de riesgos existentes dentro del mercado de la Ciberseguridad.** **TFM_plan de implementación ISO 27001-SOC (1.3. Contextualización)**	**4**	**L3**	**0**	**L3**	**3**
C.4	**C.4.2**	**4.2 Comprensión de las necesidades y expectativas de las partes interesadas**	**las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;** **los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.**	**NO CUMPLE** **Se tiene conocimentos de cuales son las partes interesadas y sus necesidades.** **No están recogidas de manera exhaustiva los requisitos; ni consIderada la valoración de su cumplimiento.**	**4**	**L1**	**0**	**L1**	**1**
C.4	**C.4.3**	**4.3 Determinación del alcance del sistema de gestión de seguridad de la información**	**a) las cuestiones externas e internas referidas en el apartado 4.1;** **b) los requisitos referidos en el apartado 4.2;** **c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.**	**CUMPLE PARCIALMENTE** **En consideración a los apartados 4.1. (ver)** **En consideración al apartado 4.2. (ver)** **Esta perfectamente delimitado el alcance en base a que se considera el SOC-MADRID y sus actividades y procesos gestionados.** **Falta por documentar los procesos de negocio y soporte de la organización (Funciones, actividades y roles)**	**4**	**L2**	**0**	**L2**	**2**

Valoración Madurez-Cláusulas ISO 27001										
Dominio	**Cláusula**	**Descripción del Control**	**Referencias del Estado Cláusula**		**Documentos y Controles**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
C.4	**C.4.4**	**4.4 Sistema de gestión de seguridad de la información**	**La organización debe establecer, implementar, mantener y mejorar de manera continúa un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional.**	**CUMPLE PARCIALMENTE En el proceso de análisis se ha implantado un sistema de Gestión como base para aplicarlo en la organización y empezar a gestionar el SGSI y la Mejora continua (TFM_plan de implementación ISO 27001-SOC (2. SISTEMA DE GESTIÓN DOCUMENTAL)**		**4**	**L3**	**0**	**L3**	**3**
C.5- LIDERAZGO									**L2**	**2,00**
5-Liderazgo									**L2**	**2,00**
C.5	**C.5.1**	**5.1 Liderazgo y compromiso**	**a) asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización; b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización; c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles; d) comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de seguridad de la información; e) asegurando que el sistema de gestión de seguridad de la información consigue los resultados previstos; f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de seguridad de la información; g) promoviendo la mejora continua; y h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de**		**CUMPLE PARCIALMENTE Se ha establecido un SGSI contemplando los apartados reseñados (TFM_plan de implementación ISO 27001-SOC (2. SISTEMA DE GESTIÓN DOCUMENTAL). El proceso debe de ser asumido por toda la organización y coge experiencia en el mismo.**	**4**	**L2**	**0**	**L2**	**2**

Valoración Madurez-Cláusulas ISO 27001									
Dominio	Cláusula	Descripción del Control	Referencias del Estado Cláusula	Documentos y Controles	Ponderación Grupo de Control	Valor de Referencia Madurez	Incremento/ Ajuste	EVALUACIÓN MADUREZ	EVALUACIÓN MADUREZ
			responsabilidad.						
C.5	C.5.2	5.2 Política	CUMPLE PARCIALMENTE Se ha creado una política de Seguridad de la Información. - Debe ser difundida y conocida dentro de la Organización y por las Partes interesadas.	TFM_Politica de Seguridad_v1.0.pdf TFM_PROC_Procesos, Roles y Responsabilidades_v1.0.pdf	4	L2	0	L2	2
C.5	C.5.3	5.3 Roles, responsabilidades y autoridades en la organización	CUMPLE PARCIALMENTE Los roles relacionados con SI están declarados dentro de la organización. Resto Ver C.4.3	(TFM_plan de implementación ISO 27001-SOC (1.3.9. Roles y Responsabilidades en Seguridad de la Información).	4	L2	0	L2	2
C.6- PLANIFICACION								L3	2,50

Valoración Madurez-Cláusulas ISO 27001									
Dominio	**Cláusula**	**Descripción del Control**	**Referencias del Estado Cláusula**	**Documentos y Controles**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
6.1-Contexto de la Organización								**L3**	**3,00**
C.6	**C.6.1.1**	**6.1.1. Acciones para tratar los riesgos y oportunidades. Consideraciones generales**	**CUMPLE** **Se ha establecido una metodología de Gestión de Riesgos en dónde se incoporan todos los requisitos reseñados en la Claúsuala 6.** **Se ha desarrollado un proceso formal de Análisis de Riesgos en la Organización.** **El proceso está puesto en marcha, hay que esperar que se gestiona de manera regular dentro del SGSI en el futuro.**	**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf (TFM_plan de implementación ISO 27001-SOC (3. ANÁLISIS DE RIESGOS).**	**4**	**L3**	**0**	**L3**	**3**
C.6	**C.6.1.2**	**6.1.2 Apreciación de riesgos de seguridad de la información**	**CUMPLE** **Ver C.6.1.1**		**4**	**L3**	**0**	**L3**	**3**
C.6	**C.6.1.3**	**6.1.3 Tratamiento de los riesgos de seguridad de la información**	**CUMPLE** **Ver C.6.1.2**		**4**	**L3**	**0**	**L3**	**3**
6.2-Objetivos de seguridad de la información y planificación para su consecución								**L2**	**2,00**
C.6	**C.6.2**	**6.2 Objetivos de seguridad de la información y planificación para su consecución**	**CUMPLE PARCIALMENTE** **Están definidas Estrategias y formulados objetivos dentro de la organización)** **Están establecidos objetivos para la SI** **Hay que desarrollarlos y realizar un seguimiento regular en el SGSI.**	**(TFM_plan de implementación ISO 27001-SOC (1.3.10. Estrategias de la Organización, 1.4. Objetivos del Plan Director). TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf**	**4**	**L2**	**0**	**L2**	**2**
C.7- SOPORTE								**L2**	**1,80**
7-Soporte								**L2**	**1,80**

Valoración Madurez-Cláusulas ISO 27001										
Dominio	**Cláusula**	**Descripción del Control**		**Referencias del Estado Cláusula**	**Documentos y Controles**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
C.7		**C.7.1**	**7.1 Recursos**	**La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.**	**CUMPLE PARCIALMENTE Dentro de la Capa Operativa de los servicios del SOC existen recursos establecidos con competencias específicas en SI; pero a nivel de gestión no hay una implementación efectiva; con lo cual existe un modelo incompleto.**	**4**	**L2**	**0**	**L2**	**2**
C.7		**C.7.2**	**7.2 Competencia**	**a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas; c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y d) conservar la información documentada apropiada, como evidencia de la competencia.**	**CUMPLE PARCIALMENTE Hay una preocupación y prioridad a nivel de la organización por mantener el nivel de formación adecuado a las necesidades para los perfiles técnicos. Sin embargo no se basa en un proceso definido, registrado y controlado**	**4**	**L2**	**0**	**L2**	**2**
C.7		**C.7.3**	**7.3 Concienciación**	**Las personas que trabajan bajo el control de la organización deben ser conscientes de: a) la política de la seguridad de la información; b) su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; c) las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información.**	**CUMPLE PARCIALMENTE La conciencación en SI está presente en la Organización. Existen iniciativas esporádicas; sin que haya una planificación y seguimiento; y sin que se marquen objetivos y alcance definidos.**	**4**	**L2**	**0**	**L2**	**2**

Valoración Madurez-Cláusulas ISO 27001										
Dominio	**Cláusula**	**Descripción del Control**		**Referencias del Estado Cláusula**	**Documentos y Controles**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
C.7	**C.7.4**	**7.4 Comunicación**		**La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información, que incluyan: a) el contenido de la comunicación; b) cuándo comunicar; c) a quién comunicar; d) quién debe comunicar; e) los procesos por los que debe efectuarse la comunicación.**	**NO CUMPLE No están desarrolladas. La comunicación y como comunicar se establece en el momento en el que surge la necesidad.**	**4**	**L1**	**0**	**L1**	**1**
C.7	**C.7.5**	**7.5 Información documentada**		**El sistema de gestión de seguridad de la información de la organización debe incluir: a) la información documentada requerida por esta norma internacional; b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de seguridad de la información.**	**CUMPLE PARCIALMENTE Está establecido un modelo para la Gestión de la Documentación en la Organización; que no está revisado y no se usa de manera normalizada**	**4**	**L2**	**0**	**L2**	**2**
C.8- OPERACIÓN									**L2**	**2,00**
8-Operación									**L2**	**2,00**
C.8	**C.8.1**	**8.1 Planificación y control operacional**		**CUMPLE PARCIALMENTE Se ha establecido un SGSI contemplando los apartados reseñados. El proceso debe de ser asumido por toda la organización y coge experiencia en el mismo.**	**TFM_plan de implementación ISO 27001-SOC (2. SISTEMA DE GESTIÓN DOCUMENTAL)**	**4**	**L2**	**0**	**L2**	**2**
C.8	**C.8.2**	**8.2 Apreciación de los riesgos de seguridad de información**		**CUMPLE Ver C.6.1, C.6.2**		**4**	**L2**	**0**	**L2**	**2**

Valoración Madurez-Cláusulas ISO 27001										
Dominio	Cláusula	Descripción del Control		Referencias del Estado Cláusula	Documentos y Controles	Ponderación Grupo de Control	Valor de Referencia Madurez	Incremento/ Ajuste	EVALUACIÓN MADUREZ	EVALUACIÓN MADUREZ
C.8	C.8.3	8.3 Tratamiento de los riesgos de seguridad de información		CUMPLE Ver C.6.1, C.6.3		4	L2	0	L2	2
C.9- EVALUACION DEL DESEMPEÑO									L3	2,33
9-Evaluación del desempeño									L3	2,33
C.9	C.9.1	9.1 Seguimiento, Medición, Análisis y Evaluación		CUMPLE PARCIALMENTE Están definidas Estrategias y formulados objetivos dentro de la organización) Están establecidos objetivos para la SI Hay que desarrollarlos y realizar un seguimiento regular en el SGSI.	(TFM_plan de implementación ISO 27001-SOC (1.3.10. Estrategias de la Organización, 1.4. Objetivos del Plan Director). TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf	4	L2	0	L2	2
C.9	C.9.2	9.2 Auditoría Interna		CUMPLE La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de seguridad de la información. - Existe en la organización actividad regular de Auditorías Técnicas y seguimiento de las no conformidades. Se ha formalizado un procedimiento de Auditoría en el SGSI desarrollado para unificar criterios.	Este proceso esta desarrollado dado que el SOC está periódicamente sometido a Auditorías técnicas (Pentesting, Análisis de Vulnerabilidades, etc). Contempla la planificación de las auditoríoas, suejcución y el seguimiento de las no conformidades y acciones correctivas. Habría que hacerlo más extensivo para cubrir auditorías desde la óptica de	4	L3	0	L3	3

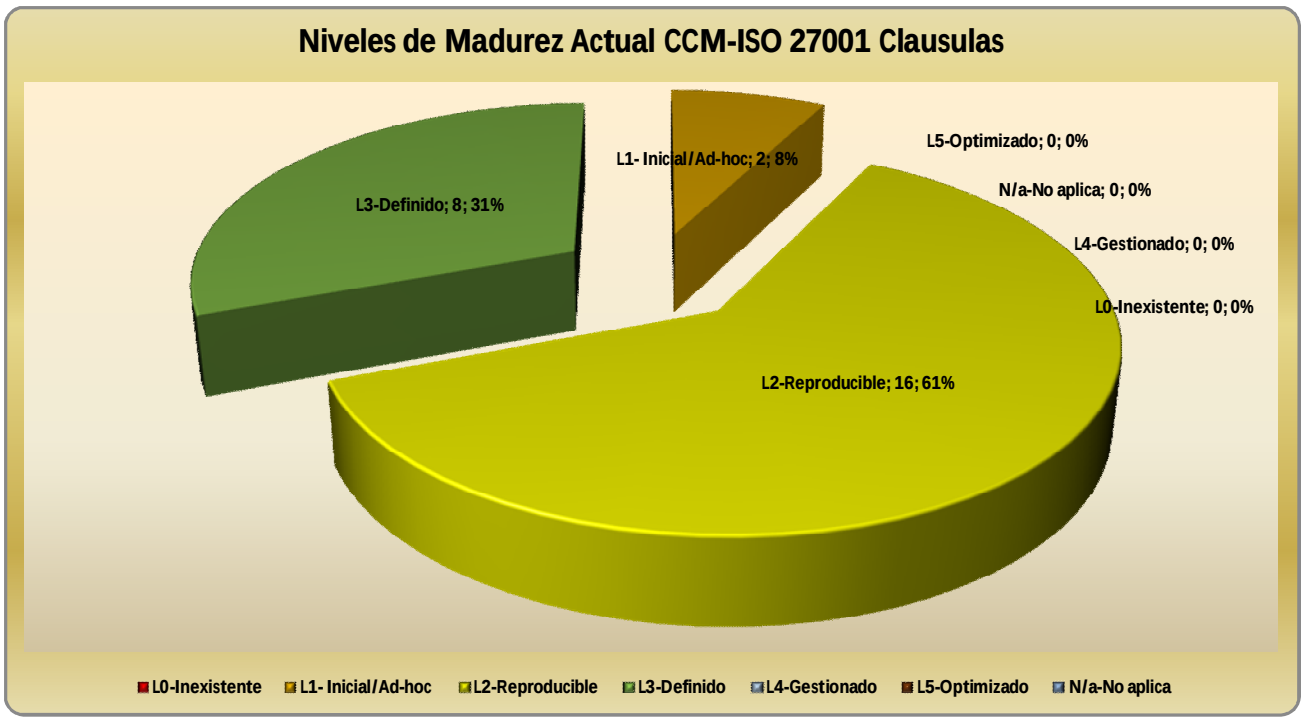
Valoración Madurez-Cláusulas ISO 27001									
Dominio	Cláusula	Descripción del Control	Referencias del Estado Cláusula	Documentos y Controles	Ponderación Grupo de Control	Valor de Referencia Madurez	Incremento/ Ajuste	EVALUACIÓN MADUREZ	EVALUACIÓN MADUREZ
				un sistema de Gestión. TFM_PROC_Procedimiento de Auditorias Internas.pdf					
C.9	C.9.3	9.3 Revisión por la Dirección	CUMPLE PARCIALMENTE Se ha formalizado un procedimiento de Auditoría en el SGSI desarrollado para unificar criterios.	TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf	4	L2	0	L2	2
C.10- MEJORA								L2	2,00
10-Mejora								L2	2,00
C.10	C.10.1	10.1 No conformidad y acciones correctivas	CUMPLE (Ver C.9.2.)		4	L2	0	L2	2

Valoración Madurez-Cláusulas ISO 27001										
Dominio	Cláusula	Descripción del Control		Referencias del Estado Cláusula		Documentos y Controles	Ponderación Grupo de Control	Valor de Referencia Madurez	Incremento/ Ajuste	EVALUACIÓN MADUREZ	EVALUACIÓN MADUREZ
C.10		C.10.2	10.2 Mejora continua	CUMPLE PARCIALMENTE Han quedado establecidas las bases del SGSI en la organización. El proceso de mejora que se realiza en la organizacíon hasta ahora se realizaba de manera intuitiva y no coordinada, La organización debe mejorar de manera continúa la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información. Ya depende de la organización su puesta en marcha regularmente.		(TFM_plan de implementación ISO 27001-SOC (2. SISTEMA DE GESTIÓN DOCUMENTAL) TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf TFM_PROC_Procedimiento de Auditorias Internas.pdf	4	L2	0	L2	2

45-Evaluación madurez actual ISO 27001

5.3.1. Mapa de Madurez actual sobre modelo CMM-ISO 27001

La visión resumida de la situación actual del nivel de madurez de las cláusulas de Seguridad de la información agrupado en base a los valores de madurez se muestran en el siguiente gráfico.



46-Modelo de madurez actual ISO 27001

En base al gráfico, una vez revisado, destacamos los siguientes puntos:

Dado que la organización no tenía previamente establecido un Sistema de Gestión, para haber sido tomado como palanca para construir el SGSI, se ha partido de una situación de arranque desde abajo.

A lo largo del proyecto de análisis se ha realizado un desarrollo e implantación de un SGSI creando un sistema documental sobre el que se pueda establecer una gestión de la Seguridad de la Información (2-**SISTEMA DE GESTIÓN DOCUMENTAL**).

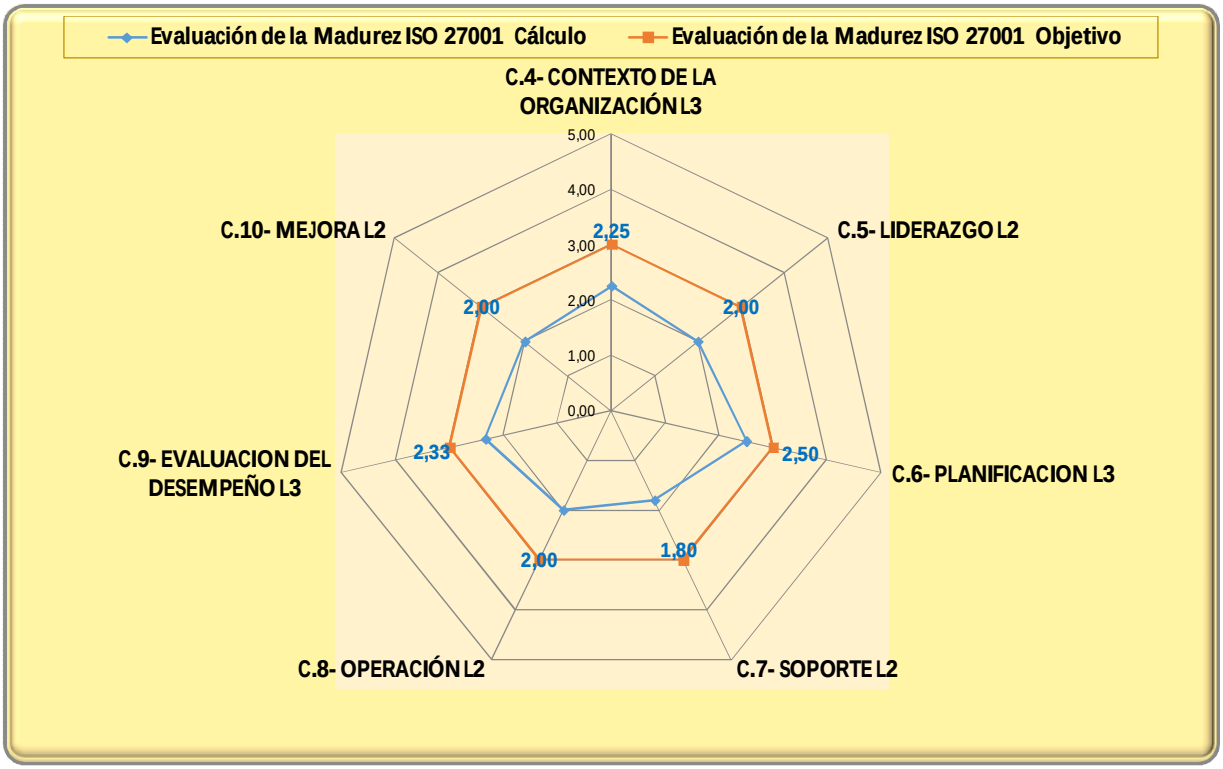
De modo que podemos decir, en términos generales que se han definido los procesos de Gestión del SGSI ; quedando reflejado en la evaluación de los niveles de madurez de las cláusulas de la ISO 27001, siendo mayoritaria la madurez para los niveles L2-L3.

- **L2 (61%) + L3 (31%).**

Recalcar que no es aspiración superar como valor objetivo el nivel L3 ; dado que estamos hablando de la instauración de SGSI nuevo ; sin que tengamos una experiencia constrastada sobre el funcionamiento del sistema durante un tiempo razonable dentro de la organización. Esto marca nuestro nivel objetivo de madurez, poniendo actualmente como techo lineal L3.

5.3.1. Nivel de cumplimiento por Cláusulas-ISO 27001

La visión del nivel de madurez vista desde la perspectiva de las cláusulas de ISO 27001 se muestra en el siguiente gráfico.



47- Nivel de cumplimiento actual en base a ISO 27001

En base al gráfico, una vez revisado, destacamos los siguientes puntos:

- No volver a insistir de nuevo sobre el diagnóstico, en base a la madurez. El diagrama revela la existencia de un sistema de Gestión puesto en marcha; que necesita ser conocido y rodado en la organización para poder seguir evolucionando en cuanto a madurez, adquiriendo aspectos tales como:
  - Capacidad de planificación, control, aplicación de la mejora y desarrollo del SGSI en base al mdelo PDCI (C.8, C9, C.10, C.6).
- Considerar de modo específico que desarrollar a través de los Proyectos de mejora (4.1.4-Proyectos-Incremento de la Madurez ISO 27001&ISO 27002 estimada) propiciar la mejora de la documentacíon del sistema y generar refuerzos en la madurez del SGSI (C.4,C.5,C.7)

5.4. Evaluación de la madurez ISO 27002

A continuación se muestra el detalla de la valoración de la madurez actual en cuanto al estado y grado de cumplimiento de los controles basados en la metodoogía anteriormente descrita.

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN									**L2**	**1,67**
5.1 Política de Seguridad de la Información									**L2**	**1,67**
A.5	**A.5.1.1**	**A.5.1.1 Políticas para la seguridad de la información**	**CUMPLE PARCIALMENTE** **Se ha creado una política de Seguridad de la Información.** **- Debe ser difundida y conocida dentro de la Organización y por las Partes interesadas.**	**TFM_Politica de Seguridad_v1.0.pdf** **TFM_PROC_Procesos, Roles y Responsabilidades_v1.0.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.5	**A.5.1.2**	**A.5.1.2 Revisión de las políticas para la seguridad de la información**	**CUMPLE PARCIALMENTE** **Están declaradas Políticas de Seguridad que aplican mayoritariamente a Operativas IT.** **Estas políticas no están revisadas y habría que valorar en la práctica el grado de conocimiento y cumplimiento.** **No está constituido el Comité de Seguridad y por lo tanto no está todavía operativo.**	**TFM_REG_Acta del Comité de Dirección de Seguridad_v1.0.pdf**	**S**	**2**	**L1**	**0**	**L1**	**1**
A.6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN									**L2**	**1,95**
6.1 Organización Interna									**L2**	**1,91**

SOA-Valoración Madurez - Controles ISO 27002									
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.6	A.6.1.1	A.6.1.1 Roles y responsabilidades en seguridad de la información	NO CUMPLE No están claramente establecidas en la organización los Roles y Responsabilidades asociadas a SI - Están establecidos los roles que interveniene en SI. - En base a la organización y el equipo del SOC afectado, hay que establecer las competencias y funciones que les afectan en cuanto a SI.	TFM_plan de implementación ISO 27001-SOC.pdf TFM_PROC_Procesos, Roles y Responsabilidades_SOC.pdf	S	4	L2	0	L2	2
A.6	A.6.1.2	A.6.1.2 Segregación de tareas Control	CUMPLE PARCIALMENTE En la operativa técnica están establecidos perfiles concretos que tienen responsabilidades y accesos sobre activos de TI concretos. No hay documentado un modelo global y no existen procedimientos que gestionen la Segregación de funciones.	TFM_PROC_Manual de Gestión de Seguridad de la Información.pdf TFM_PROC_PlaTFM_plan de implementación ISO 27001-SOC.pdf (Organigrama de la Organización) de la Seguridad de la Información.pdf	S	4	L2	0	L2	2
A.6	A.6.1.3	A.6.1.3 Contacto con las autoridades	NO CUMPLE Los contactos con las autoridades se realizan en base a cuando se da la necesidad en el momento concreto. No están documentados ni procedimentados.	TFM_plan de implementación ISO 27001-SOC.pdf (Organigrama de la Organización) TFM_PROC_Plan de Comunicación.pdf TFM_REG_Plan de Comunicación.xls	S	1	L1	0	L1	1
A.6	A.6.1.4	A.6.1.4 Contacto con grupos de interés especial	CUMPLE Dado el foco de Actividad en Ciberseguridad este punto está plenamente cubierto y forma parte del día a día Hay una colaboración y presencia directa en las organizaciones de Ciberseguridad.	Participación activa en grupos de Ciberseguridad. Pertenencia a organismos que gestionana Ciberseguridad	S	1	L2	0	L2	2
A.6	A.6.1.5	A.6.1.5 Seguridad de la información en la gestión de proyectos	CUMPLE Existe una Gestión de Proyectos que se usa tanto para los proyectos de los clientes como para los proyectos internos. Hay establecida una metodología de Gestión de	TFM_PROC_Gestión de riesgos en Proyectos.pdf TFM_REG_Análisis de Riesgos en Proyectos.xls (Herramienta)	S	1	L2	0	L2	2

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
			proyectos y se cuenta con herramientas.							
6.2 Dispositivos Móviles y Teletrabajo									**L2**	**2,00**
A.6	**A.6.2.1**	**A.6.2.1 Política de dispositivos móviles**	**CUMPLE** **Existe una política de Dispositivos móviles (política BYOD, buenas prácticas).** **Los smartphones de la organización son controlados por MDM, por lo tanto, están sujetos a la aplicación de una política de Seguridad.**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Dispositivos Móviles y Teletrabajo)** **TFM_PROC_Documentación para Personal.pdf**	**S**	**2**	**L2**	**0**	**L2**	**2**
A.6	**A.6.2.2**	**A.6.2.2 Teletrabajo**	**CUMPLE** **Está implantada una política de Teletrabajo centrada en los aspectos:** **Conexión Segura a través de VPN (INSTALACION Y MANTENIMIENTO DE CERTIFICADOS).** **Normas de seguridad de los puestos de Trabajo.**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Dispositivos Móviles y Teletrabajo)** **TFM_PROC_Documentación para Personal.pdf**	**S**	**2**	**L2**	**0**	**L2**	**2**
A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS									**L2**	**1,93**
7.1 Previa a la Contratación									**L2**	**2,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.7	A.7.1.1	A.7.1.1 Investigación de antecedentes	CUMPLE PARCIALMENTE Existe un Departamento dedicado a la gestión de RR.HH. dentro de la Organización que centraliza todas las funciones de gestión de RR.HH (Selección, contratación, seguimiento del personal, y Baja). Tiene de Base las siguientes carencias: - La asunción, control y seguimiento de las necesidades en cuanto a formación (tanto en aspectos competenciales, funcionales y de seguridad). - Establecimiento de los mecanismos adecuados de aseguramiento de la Seguridad de los empleados en el momento de su contratación: - Acuerdos de Confidencialidad, Protección de Datos personales, registro de entregas de equipamiento, políticas de Seguridad, etc.	TFM_PROC_Plan de Seguridad de la Información.pdf (están contemplados los procesos para recabar información acerca de los perfiles dentro de las normativas vigentes).	S	4	L2	0	L2	2
A.7	A.7.1.2	A.7.1.2 Términos y condiciones del empleo	CUMPLE PARCIALMENTE Ver A.7.1.1	TFM_PROC_Código de Conducta y Buenas Prácticas.pdf TFM_REG_DOCUMENTO FIRMA EMPLEADOS.pdf TFM_PROC_Plan de Seguridad de la Información.pdf	S	4	L2	0	L2	2
7.2 Durante el desempeño de funciones									L2	1,80
A.7	A.7.2.1	A.7.2.1 Responsabilidades de gestión	CUMPLE PARCIALMENTE Ver A.7.1.2	TFM_PROC_Plan de Seguridad de la Información.pdf (Pdte de Desarrollar) TFM_PROC_Código de Conducta y Buenas Prácticas.pdf	S	4	L2		L2	2

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.7	A.7.2.2	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información	CUMPLE PARCIALMENTE Ver A.7.1.3	Formación (Planes, temarios, registros, etc) TFM_PROC_FORMACION.pdf TFM_REG_PLAN DE FORMACIÓN.pdf TFM_PROC_Código de Conducta y Buenas Prácticas.pdf TFM_PROC_Plan de Seguridad de la Información.pdf (Cumplimentar los requisitos)	S	2	L1		L1	1
A.7	A.7.2.3	A.7.2.3 Proceso disciplinario	CUMPLE PARCIALMENTE Ver A.7.1.1	Se basa en el convenio colectivo y estatuto de los trabajadores (está cubierto).	S	4	L2		L2	2
7.3 Final del contrato o cambio de funciones									L2	2,00
A.7	A.7.3.1	A.7.3.1 Responsabilidades ante la finalización o cambio	Ver A.7.1.1	TFM_PROC_Plan de Seguridad de la Información.pdf TFM_PROC_Código de Conducta y Buenas Prácticas.pdf	S	4	L2		L2	2
A.8 - GESTIÓN DE ACTIVOS									L1	0,67
8.1 Responsabilidad sobre los activos									L1	1,00

SOA-Valoración Madurez - Controles ISO 27002									
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.8	**A.8.1.1**	**A.8.1.1 Inventario de activos**	**CUMPLE PARCIALMENTE Existen inventarios de los activos de Soporte IT (no se encuentran actualizados y no existe un mecanismo para su mantenimiento)**	**TFM_PROC_Clasificación y uso de la Información y Gestión de Activos_v1.0.pdf TFM_REG_Inventario portatiles corporativos.xls TFM_REG_Inventario Sistemas.xls TFM_MAPA_ACTIVOS TFM_plan de implementación ISO 27001-SOC.pdf (MAPA DE RED/INFRAESTRUCTURA SOC) INVENTARIO DE ACTIVOS Y DEPENDENCIAS/ANÁLISIS Y GESTIÓN DE RIESGOS - HERRAMIENTA Análisis y Gestión de Riesgos**	**S**	**4**	**L1**	**0**	**L1**	**1**

SOA-Valoración Madurez - Controles ISO 27002									
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.8	**A.8.1.2**	**A.8.1.2 Propiedad de los activos**	**CUMPLE PARCIALMENTE** **Están declarados los propietarios de los activos de manera generalizada.**	**TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf** **INVENTARIO DE ACTIVOS Y DEPENDENCIAS/ANÁLISIS Y GESTIÓN DE RIESGOS - HERRAMIENTA Análisis y Gestión de Riesgos** **TFM_PROC_Clasificación y uso de la Información y Gestión de Activos.pdf** **TFM_REG_Inventario portatiles corporativos.xls** **TFM_REG_Inventario Sistemas_v1.0.xls** **TFM_MAPA_ACTIVOS.pdf** **TFM_plan de implementación ISO 27001-SOC.pdf (MAPA DE RED/INFRAESTRUCTURA SOC)**	**S**	**4**	**L1**	**0**	**L1**	**1**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.8	**A.8.1.3**	**A.8.1.3 Uso aceptable de los activos**	**NO CUMPLE** **Hay establecidas prácticas de uso sobre ciertos activos de información, pero no están documentadas ni difundidas.**	**TFM_PROC_Clasificación y uso de la Información y Gestión de Activos.pdf** **TFM_PROC_Instrucciones Personal Protección de Datos.pdf** **CONTRATO CON EL TRABAJADOR** **TFM_REG_DOCUMENTO FIRMA EMPLEADOS.pdf** **TFM_PROC_Plan de Seguridad de la Información.pdf - (obligaciones de los Usuarios)** **CONTRATO CON TERCEROS** **TFM_PROC_Relaciones con Proveedores.pdf** **TFM_PROC_Plan de Seguridad de la Información.pdf** **TFM_PROC_Código de Conducta y Buenas Prácticas.pdf (VISIBILIDAD CLASIFICACION ACTIVOS INFORMACION Y USO DE ACTIVOS)**	**S**	**2**	**L1**	**0**	**L1**	**1**
A.8	**A.8.1.4**	**A.8.1.4 Devolución de activos**	**NO CUMPLE** **Ver A 7.1.1.**	**TFM_PROC_Plan de Seguridad de la Información.pdf (ASEGURAMIENTO)** **TFM_REG_Inventario portatiles corporativos.xls**	**S**	**2**	**L1**	**0**	**L1**	**1**
8.2 Clasificación de la información									**L0**	**0,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.8	**A.8.2.1**	**A.8.2.1 Clasificación de la información**	**NO CUMPLE No están establecidos crirterios de Clasificación de los activos de información; así como las políticas de seguridad a aplicar en su almacenamiento, tránsito y soporte.**	**TFM_PROC_Clasificación y uso de la Información y Gestión de Activos.pdf**	**S**	**4**	**L0**	**0**	**L0**	**0**
A.8	**A.8.2.2**	**A.8.2.2 Etiquetado de la información**	**NO CUMPLE Ver A. 8.2.1**	**TFM_PROC_Clasificación y uso de la Información y Gestión de Activos.pdf**	**S**	**4**	**L0**	**0**	**L0**	**0**
A.8	**A.8.2.3**	**A.8.2.3 Manipulado de la información**	**NO CUMPLE Ver A. 8.2.1**	**TFM_PROC_Código de Conducta y Buenas Prácticas.pdf (VISIBILIDAD CLASIFICACION ACTIVOS INFORMACION Y USO DE ACTIVOS) TFM_PROC_Plan de Seguridad de la Información.pdf TFM_PROC_Clasificación y uso de la Información y Gestión de Activos.pdf**	**S**	**4**	**L0**	**0**	**L0**	**0**
8.3 Gestión de Soportes									**L1**	**1,00**
A.8	**A.8.3.1**	**A.8.3.1 Gestión de soportes extraíbles**	**CUMPLE Existe una política de gestión de soportes extraíbles (integrada en A.6.1.)**	**TFM_PROC_Plan de Seguridad de la Información.pdf**	**S**	**2**	**L1**	**0**	**L1**	**1**
A.8	**A.8.3.2**	**A.8.3.2 Eliminación de soportes**	**CUMPLE PARCIALMENTE Existe una política de eliminación de soportes (habría que revisar dado que no da garantías en cuanto a la trazabilidad y la garantía del borrado de la información).**	**TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf (ASEGURAMIENTO) TFM_PROC_Documentación para Personal_v1.0.pdf (ASEGURAMIENTO)**	**S**	**2**	**L1**	**0**	**L1**	**1**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.8	**A.8.3.3**	**A.8.3.3 Soportes físicos en tránsito**	**CUMPLE PARCIALMENTE La operativa está desarrollada pero no documentada**	**TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf (Documentar la práctica que se realiza)**	**S**	**1**	**L1**	**0**	**L1**	**1**
A.9 - CONTROL DE ACCESO									**L2**	**1,83**
9.1 Requisitos de Negocio para el control de Accesos									**L2**	**2,00**
A.9	**A.9.1.1**	**A.9.1.1 Política de control de acceso**	**CUMPLE PARCIALMENTE Existe una política de control de acceso a los recursos de Red (habría que revisar si cumple con la Segregación de funciones ya que puede haber incoherencias).**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Control de Acceso y Política de Contraseñas)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.9	**A.9.1.2**	**A.9.1.2 Acceso a las redes y a los servicios de red**	**CUMPLE PARCIALMENTE Existe una política de control de acceso a los recursos de Red (habría que revisar si cumple con la Segregación de funciones ya que puede haber incoherencias).**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Gestión de las Comunicaciones y Operaciones) TFM_plan de implementación ISO 27001-SOC (MAPAS DE DE RED) TFM_REG_Accesos Logicos, Fisicos y Recursos Asociados.xls**	**S**	**4**	**L2**	**0**	**L2**	**2**
9.2 Gestión de Acceso de usuario									**L2**	**2,00**
A.9	**A.9.2.1**	**A.9.2.1 Registro y baja de usuario**	**CUMPLE PARCIALMENTE Los accesos están centralizados a través DA. Existe un procedimiento de Alta y Baja de Usuarios. El procedimiento de solicitud desde el área de recursos humanos no se cumple estrictamente.**	**TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf (REVISION CUMPLIMENTO PROC)**	**S**	**4**	**L2**	**0**	**L2**	**2**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.9	A.9.2.2	A.9.2.2 Provisión de acceso de usuario	CUMPLE PARCIALMENTE Los recursos generales son directamente solicitados desde el área de RR.HH. Los accesos a recursos, aplicaciones y herramientas específicas son gestionados por los responsables de las distintas áreas técnicas. Habría que revisar perfiles, funciones, procedimientos y uso.	TFM_REG_Accesos Logicos, Fisicos y Recursos Asociados.xls (REVISION CUMPLIMENTO REG)	S	4	L2	0	L2	2
A.9	A.9.2.3	A.9.2.3 Gestión de privilegios de acceso	CUMPLE PARCIALMENTE Ver A.9.2.2.	TFM_PROC_Plan de Seguridad de la Información.pdf (REVISION CUMPLIMENTO PROC)	S	2	L2	0	L2	2
A.9	A.9.2.4	A.9.2.4 Gestión de la información secreta de autenticación de los usuarios	CUMPLE Existen Herramientas de Gestión de Credenciales para garantizar la aplicación de este control.	GESTION DE CREDENCIALES -> (mostrar la configuración).	S	2	L3	0	L3	3
A.9	A.9.2.5	A.9.2.5 Revisión de los derechos de acceso de usuario	NO CUMPLE Ver.A. 8.2.1.	TFM_PROC_Plan de Seguridad de la Información.pdf (REVISION CUMPLIMENTO PROC) TFM_REG_Accesos Logicos, Fisicos y Recursos Asociados.xls (REVISION CUMPLIMENTO REG)	S	2	L1	0	L1	1
A.9	A.9.2.6	A.9.2.6 Retirada o reasignación de los derechos de acceso	CUMPLE Ver A.9.2.2.	TFM_PROC_Plan de Seguridad de la Información.pdf (REVISION CUMPLIMENTO PROC)	S	2	L2	0	L2	2
9.3 Responsabilidades del usuario									L2	2,00

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.9	A.9.3.1	A.9.3.1 Uso de la información secreta de autenticación	CUMPLE VER A.9.2.4.	TFM_PROC_Plan de Seguridad de la Información.pdf (Control de Acceso y Política de Contraseñas) TFM_PROC_Código de Conducta y Buenas Prácticas.pdf TFM_PROC_Plan de Seguridad de la Información.pdf - (obligaciones de los Usuarios EN BASE A LOS CRITERIOS DE CLASIFICACIÓN Y USO ESTABLECIDOS)	S	4	L2	0	L2	2
9.4 Control de acceso al Sistema Operativo y las Aplicaciones									L2	1,33
A.9	A.9.4.1	A.9.4.1 Restricción del acceso a la información	NO CUMPLE VER A. 8.2.1., y A.9.2.2.	TFM_PROC_Plan de Seguridad de la Información.pdf (Revisión de los mecanismos de acceso y las restricciones).	S	4	L1	0	L1	1
A.9	A.9.4.2	A.9.4.2 Procedimientos seguros de inicio de sesión	CUMPLE Hay desarrollado y puesto en marcha un procedimiento de control de Acceso.	TFM_PROC_IT_USO VPN.pdf	S	4	L2	0	L2	2
A.9	A.9.4.3	A.9.4.3 Sistema de gestión de contraseñas	CUMPLE Está implementada una política de Contraseñas que está extendida a todas las Aplicaciones que requieren control de Acceso.	TFM_PROC_Plan de Seguridad de la Información.pdf (Control de Acceso y Política de Contraseñas)	S	4	L2	0	L2	2
A.9	A.9.4.4	A.9.4.4 Uso de utilidades con privilegios del sistema	NO CUMPLE No existe un inventario de Utililities; por lo tanto, no hay un control sobre este tema en cuanto a su uso y los privilegios de acceso a la información.	Uitlidades controladas y acceso restringido Herr. Gestión credenciales . TFM_REG_Inventario de Utilities y control de Acceso	S	2	L0	0	L0	0
A.9	A.9.4.5	A.9.4.5 Control de acceso al código fuente de los programas	NO CUMPLE El código desarrollado básicamente es scripting. No se están establecidos unos procedimientos de acceso y uso.	TFM_PROC_Practicas_Desarrollo_De_Codigo.pdf	S	1	L0	0	L0	0

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.10 - CRIPTOGRAFÍA									**L2**	**1,67**
A.10	**A.10.1.1**	**A.10.1.1 A Política de uso de los controles criptográficos**	**CUMPLE PARCIALMENTE Están implantados y se mantienen Certificados de Servidores, acceso web seguro (HPPTS/SSL), Acceso VPN/IP SEC, Gestión de credenciales, etc. Sin embargo no hay documentada una política de controles Criptográficos.**	**TFM_PROC_Plan de Seguridad de la Información.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.10	**A.10.1.2**	**A.10.1.2 Gestión de claves**	**NO CUMPLE A incluir dentro de la Política de Controles Criptográficos (Ver A.10.1.2)**	**GESTION DE CREDENCIALES -> Herramienta (mostrar la configuración). No están procedimentados las plantillas para el control de certificados, caducidades, etc.**	**S**	**2**	**L1**	**0**	**L1**	**1**
A.11 - SEGURIDAD FÍSICA Y DEL ENTORNO									**L3**	**2,88**
11.1 Áreas seguras									**L3**	**3,00**
A.11	**A.11.1.1**	**A.11.1.1 Perímetro de seguridad física**	**CUMPLE Existen 3 Perímetros de seguridad dentro de las instalaciones: - Control de Acceso Físico al Edificio (Nivel 1). - Control de Acceso Físico a las Instalaciones de la Compañía (en el edificio) - (Nivel 2). - Control de Acceso al SOC (Nivel 3).**	**TFM_PROC_Seguridad Física y del Entorno.pdf TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S. TFM_REG_Registros Seguridad CPD externos**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.11	**A.11.1.2**	**A.11.1.2 Controles físicos de entrada**	**CUMPLE - Nivel 1 (Personal de Seguridad y Tornos de acceso). - Nivel 2 (Acceso biométrico). - Nivel 3 (Acceso biométrico específico SOC)**	**TFM_PROC_Seguridad Física y del Entorno.pdf TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S. TFM_REG_Registros Seguridad CPD externos**	**S**	**4**	**L3**	**0**	**L3**	**3**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.11	**A.11.1.3**	**A.11.1.3 Seguridad de oficinas, despachos y recursos**	**CUMPLE** **Acceso a salas técnicas restringida (acceso por panel numérico -claves)** **Armarios con llaves distribuidos por las instalaciones custodiados por responsables.** **Cajas fuertes ignifugas (almacenamiento de backups y custodia forense).**	**TFM_PROC_Seguridad Física y del Entorno.pdf**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.11	**A.11.1.4**	**A.11.1.4 Protección contra las amenazas externas y ambientales**	**CUMPLE** **Acceso a salas técnicas restringida (acceso por panel numérico -claves)** **Armarios con llaves distribuidos por las instalaciones custodiados por responsables.** **Cajas fuertes ignifugas (almacenamiento de backups y custodia forense).**	**TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S.**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.11	**A.11.1.5**	**A.11.1.5 El trabajo en áreas seguras**	**CUMPLE** **Las derivadas de las normas de Seguridad en la construcción y diseño del edificio.** **Planes de Mantenimiento de las instalaciones/planes de Emergencia actualizados y operativos.**	**TFM_PROC_Seguridad Física y del Entorno.pdf** **TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S.** **TFM_REG_Registros Seguridad CPD externos**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.11	**A.11.1.6**	**A.11.1.6 Áreas de carga y descarga**	**No Aplica**		**N**	**1**	**N/A**	**0**	**N/A**	**0**
11.2 Seguridad del equipamiento									**L3**	**2,75**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.11	A.11.2.1	A.11.2.1 Emplazamiento y protección de equipos	CUMPLE El equipamiento asociado a la Electrónica de Red se encuentra ubicado en las Salas Técnicas (Ver A.11.1.1); cuenta con medida de protección (control de acceso, control de temperatura, control anti incendios, etc.). El resto del equipamiento se encuentra ubicado dentro del SOC (puestos clientes y laboratorio (servidores de pruebas). La infraestructura de Servidores está alojada en CPDs Homologados de proveedores externos.	TFM_PROC_Seguridad Física y del Entorno_v1.0.pdf TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S. TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf CONTRATOS CON PROVEEDORES DE Equipamientos y proveedores de Soporte Help Desk y Servidores CONTRATOS DE SOPORTE PROVEEDORES DE TELECOMUNICACIONES. CONTRATOS DE PROVEEDORES DE ALOJAMIENTO Y SERVICIOS EN LA NUBE (Saas, PaaS)	S	4	L3	0	L3	3
A.11	A.11.2.2	A.11.2.2 Instalaciones de suministro	CUMPLE Salas Técnicas-Electrónica de Red (Dotados de SAI local). Equipamiento del SOC (infraestructura de edificio - puntos de corriente seguros) y edificio dotado con grupo electrógeno	CONTRATOS CON PROVEEDORES DE Equipamientos y proveedores de Soporte Help Desk y Servidores TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S.	S	4	L3	0	L3	3
A.11	A.11.2.3	A.11.2.3 Seguridad del cableado	CUMPLE Cumple con las normativas de instalación y seguridad a nivel de las instalaciones en el edificio y las líneas de comunicaciones contratadas con los proveedores.	TFM_PROC_Seguridad Física y del Entorno.pdf TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S.	S	4	L3	0	L3	3

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.11	A.11.2.4	A.11.2.4 Mantenimiento de los equipos	CUMPLE Equipamiento de Red y Servidores (Contratos de Soporte y Mantenimiento con los fabricantes). Puestos de trabajo, Dispositivos móviles y periféricos (impresoras, faxes, etc) son gestionados directamente por Servicio de Soporte Externo (Firmware, Hardware, Software base)	TFM_PROC_Seguridad Física y del Entorno.pdf TFM_REG_Registros Seguridad Física EDIFICIO Y CPD'S. TFM_PROC_Plan de Seguridad de la Información.pdf CONTRATOS CON PROVEEDORES DE Equipamientos y proveedores de Soporte Help Desk y Servidores CONTRATOS DE SOPORTE PROVEEDORES DE TELECOMUNICACIONES.	S	4	L3	0	L3	3
A.11	A.11.2.5	A.11.2.5 Retirada de materiales propiedad de la empresa	CUMPLE PARCIALMENTE Existen prácticas de control, pero no están documentadas.	TFM_PROC_Plan de Seguridad de la Información.pdf (ASEGURAMIENTO)	S	2	L2	0	L2	2
A.11	A.11.2.6	A.11.2.6 Seguridad de los equipos fuera de las instalaciones	CUMPLE Para Servidores (Ubicación en CPDs homologados proveedores externos) Para el equipamiento móvil (Ver a 6.2.1).	TFM_PROC_Seguridad Física y del Entorno.pdf TFM_PROC_Plan de Seguridad de la Información.pdf TFM_PROC_Código de Conducta y Buenas Prácticas.pdf	S	2	L3	0	L3	3
A.11	A.11.2.7	A.11.2.7 Reutilización o eliminación segura de equipos	CUMPLE PARCIALMENTE Ver A.8.3.2.	TFM_PROC_Seguridad Física y del Entorno_v1.0.pdf	S	2	L2	0	L2	2
A.11	A.11.2.8	A.11.2.8 Equipo de usuario desatendido	No Aplica	Servidor que muestra las pantallas (pero se encuentra ubicado dentro de la sala tecnica).	N	1	N/A	0	N/A	0

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.11	**A.11.2.9**	**A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia**	**CUMPLE** **Existe una Política declarada, difundida y en uso dentro de la Organización.**	**TFM_PROC_Seguridad Física y del Entorno_v1.0.pdf** **TFM_PROC_Código de Conducta y Buenas Prácticas_v1.0.pdf** **TFM_REG_DOCUMENTO FIRMA EMPLEADOS_v1.0.pdf**	**S**	**2**	**L2**	**0**	**L2**	**2**
A.12 - SEGURIDAD DE LAS OPERACIONES									**L3**	**2,37**
12.1 Procedimientos y responsabilidades de Operación									**L2**	**1,83**
A.12	**A.12.1.1**	**A.12.1.1 Documentación de procedimientos de los operación**	**CUMPLE PARCIALMENTE** **Existe procedimientos de Operación dentro del SOC, que está delegados en su ejecución a los Técnicos de Nivel 1 (Revisar en profundidad).**	**TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf** **INSTRUCCIONES TÉCNICAS:** **TFM_IT_VPN Forticlient.pdf** **TFM_IT_Documento Backup.pdf** **TFM_IT_Plan de Contingencia.pdf** **TFM_IT_Procedimiento de Entrada y salida material SOC.pdf** **TFM_IT_Procedimientos SOC.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.12	**A.12.1.2**	**A.12.1.2 Gestión de cambios**	**CUMPLE PARCIALMENTE** **Existe Herramientas de Service Desk con el proceso de Gestión de Cambios implementado; no se usa de manera habitual para la Gestión de los Cambios del SOC.**	**Herramientas de Service Desk (Gestión de Incidencias, Gestión de Cambios)** **TFM_REG_Registro y Seguimiento de los Cambios**	**S**	**4**	**L2**	**0**	**L2**	**2**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.12	**A.12.1.3**	**A.12.1.3 Gestión de capacidades**	**CUMPLE PARCIALMENTE** **Se está realizando una monitorización continua de las infraestructuras del SOC (rendimiento, consumo, almacenamiento). Se emite y analiza el reporting de estado y necesidades en base a crecimiento infraestructura.** **La gestión de la Capacidad en Base a:** **- Recursos Humanos.** **- Necesidades de Negocio, etc** **no aparece contemplada.**	**Monitorización con HERR. de MONITORIZACION (generación de alertas).** **Informes de Monitorización con analisis de tendencias.** **Informes de comité de operaciones (Carga de trabajo en proyecto, uso de recursos y tendencias).** **Previsión de necesidades presupuestarias del SOC. (Director de Operaciones).**	**S**	**2**	**L2**	**0**	**L2**	**2**
A.12	**A.12.1.4**	**A.12.1.4 Separación de los recursos de desarrollo, prueba y operación**	**CUMPLE PARCIALMENTE** **En la Práctica no hay una infraestructura paralela que permita la realización de pruebas previas en entornos que no sean de Producción.** **La infraestructura de Laboratorio es usado para recrear entornos de Desarrollo y Pruebas, pero parcialmente.**	**Equipos de Laboratorio instalados en el SOC y en los CPDS de los PROVEEDORES para pruebas de desarrollo y pre-producción.** **TFM_PROC_Practicas_Desarrollo_De_Codigo.pdf**	**S**	**2**	**L1**	**0**	**L1**	**1**
12.2 Protección contra el Malware									**L3**	**3,00**
A.12	**A.12.2.1**	**A.12.2.1 Controles contra el código malicioso**	**CUMPLE** **Dentro del SOC se aplican los procedimientos que están desarrollados para los servicios que se prestan a los clientes.**	**TFM_PROC_Plan de Seguridad de la Información_v1.0.pdf**	**S**	**4**	**L3**	**0**	**L3**	**3**
12.3 Copia de Seguridad									**L2**	**2,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.12	**A.12.3.1**	**A.12.3.1 Copias de seguridad de la información**	**CUMPLE PARCIALMENTE** **Se realizan copias de Seguridad de los Sistemas Críticos.** **Están implementadas políticas de backup, pero no están documentadas.** **Sería necesario revisar la permanencia y retención de la información de la que se hace backup.** **No se realizan pruebas periódicas de recuperación para asegurar la Sanidad de los backups realizados.**	**TFM_PROC_Plan de Seguridad de la Información.pdf** **IT_Documento Backup.pdf** **IT_Backups Servicios.xlsx**	**S**	**4**	**L2**	**0**	**L2**	**2**
12.4 Logs y Monitorización									**L3**	**2,75**
A.12	**A.12.4.1**	**A.12.4.1 Registro de eventos**	**CUMPLE PARCIALMENTE** **Los eventos de los Servidores y de la electrónica de Red son registrados en Servidores con acceso restringido que son específicos para almacenar logs.** **No están siendo analizados regularmente; salvo que exista una incidencia y/o problema concreto.** **No están alimentando a ninguna herramienta SIEM.**	**Colectores de Logs de(herr. De gestion de logs) ya implementado.**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.12	**A.12.4.2**	**A.12.4.2 Protección de la información de registro**	**CUMPLE** **Política de Hardening de Servidores y dispositivos de Red.**	**TFM_PROC_Plan de Seguridad de la Información.pdf** **TFM_IT_HARDENING_SERVIDORES_ELCTRONICA DE RED.pdf**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.12	**A.12.4.3**	**A.12.4.3 Registros de administración y operación**	**CUMPLE** **Política de Hardening de Servidores y dispositivos de Red (Trazabilidad en la operación y administración).**	**Herramientas de Service Desk (Gestión de Incidencias, Gestión de Cambios)** **TFM_REG_Registro y Seguimiento de los Cambios**	**S**	**4**	**L3**	**0**	**L3**	**3**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.12	**A.12.4.4**	**A.12.4.4 Sincronización del reloj**	**CUMPLE** **Centralización del reloj de tiempo a través de la configuración sobre protocolo NTP contra servidores de tiempo externos.**	**Si está activo en NTP. Se usa NTP.HORA.ROA.ES**	**S**	**4**	**L3**	**0**	**L3**	**3**
12.5 Control del Software en explotación									**L2**	**2,00**
A.12	**A.12.5.1**	**A.12.5.1 Instalación del software en explotación**	**CUMPLE** **Existen procedimientos definidos para la instalación del SW en entornos de producción.**	**TFM_PROC_Gestión de Parches de Seguridad.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
12.6 Gestión de vulnerabilidades técnicas									**L3**	**3,00**
A.12	**A.12.6.1**	**A.12.6.1 Gestión de las vulnerabilidades técnicas**	**CUMPLE** **Se aplican los mismos procedimientos que los usados con los clientes.**	**TFM_PROC_Plan de Seguridad de la Información.pdf**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.12	**A.12.6.2**	**A.12.6.2 Restricción en la instalación de software**	**CUMPLE** **Existen procedimientos en el SOC que establecen y limitan la instalación de software**	**TFM_PROC_Plan de Seguridad de la Información.pdf** **TFM_PROC_Gestión de Parches de Seguridad.pdf**	**S**	**2**	**L3**	**0**	**L3**	**3**
12.7 Consideraciones acerca de la Auditoría de Sistemas									**L2**	**2,00**
A.12	**A.12.7.1**	**A.12.7.1 Controles de auditoría de sistemas de información**	**CUMPLE PARCIALMENTE** **El SOC está sometido a un proceso de monitorización continua.** **Periódicamente se practican auditorías para detectar vulnerabilidades a los Sistemas.** **No se están practicando con regularidad auditorías para verificar los mecanismos de acceso a los recursos.**	**HERR. DE SEGUIM. DE VULNERABILIDADES IMPLANTADA (Seguimiento de registro de auditoría).** **TFM_REG_Plan de revisiones de control de Acceso.** **TFM_INF_Auditorías de control de Acceso**	**S**	**2**	**L2**	**0**	**L2**	**2**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.13 - SEGURIDAD DE LAS COMUNICACIONES									**L2**	**1,79**
13.1 Gestión de la Seguiridad de Red									**L3**	**2,33**
A.13	**A.13.1.1**	**A.13.1.1 Controles de red**	**CUMPLE** **La arquitectura y diseño de red contempla la segmentación del acceso y el control de los mecanismos de acceso entre las distintas redes. Se usa la segmentación de redes basada en el establecimiento de distintas VLANs.**	**TFM_PROC_Plan de Seguridad de la Información.pdf** **TFM_plan de implementación ISO 27001-SOC .pdf (MAPAS DE RED).**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.13	**A.13.1.2**	**A.13.1.2 Seguridad de los servicios de red**	**CUMPLE** **Están gestionados por los propios equipos técnicos del SOC.** **Para la infraestructura de Red que se soporta por los activos que se encuentran ubicados en los CPD's se realiza a través de los mecanismos de soporte de los proveedores externos; con los que están suscritos compromisos de Disponibilidad y los niveles de Calidad de servicios de red QoS.**	**TFM_PROC_Plan de Seguridad de la Información.pdf**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.13	**A.13.1.3**	**A.13.1.3 Segregación en redes**	**CUMPLE** **Ver A.13.1.1** **La infraestructura expuesta en INTERNET está bajo una DMZ.**	**Mecanismos de segregación de redes.** **TFM_plan de implementación ISO 27001-SOC .pdf (MAPAS DE RED).**	**S**	**4**	**L2**	**0**	**L2**	**2**
13.2 Intercambios de información									**L2**	**1,25**
A.13	**A.13.2.1**	**A.13.2.1 Políticas y procedimientos de intercambio de información**	**NO CUMPLE** **Aunque existen prácticas en este sentido no están inventariadas, registradas y procedimentadas.**	**TFM_PROC_Clasificación de la Información y Gestión de Activos.pdf** **DOCUMENTO FIRMA EMPLEADOS.pdf** **TFM_PROC_Código de Conducta y**	**S**	**4**	**L1**	**0**	**L1**	**1**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
				Buenas Prácticas.pdf						
A.13	**A.13.2.2**	**A.13.2.2 Acuerdos de intercambio de información** Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	**NO CUMPLE Ver A.13.2.1.**	**TFM_PROC_Clasificación de la Información y Gestión de Activos.pdf TFM_PROC_Código de Conducta y Buenas Prácticas.pdf**	**S**	**4**	**L1**	**0**	**L1**	**1**
A.13	**A.13.2.3**	**A.13.2.3 Mensajería electrónica** La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	**NO CUMPLE A.8.2.1.**	**TFM_PROC_Clasificación de la Información y Gestión de Activos.pdf TFM_PROC_Código de Conducta y Buenas Prácticas.pdf**	**S**	**4**	**L1**	**0**	**L1**	**1**
A.13	**A.13.2.4**	**A.13.2.4 Acuerdos de confidencialidad o no revelación** Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación	**CUMPLE PARCIALMENTE Aunque se ha analizado la existencia de acuerdos de confidencialidad tanto para el personal interno como el externo; así como en los contratos existentes con los proveedores vinculados con la Organización; no se ha realizado una revisión exhaustiva y tampoco hay constancia de la existencia de procedimientos para asegurar el cumplimiento.**	**TFM_PROC_Código de Conducta y Buenas Prácticas.pdf DOCUMENTO FIRMA EMPLEADOS.pdf TFM_PROC_Gestion de Proveedores.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SSTEMAS DE INFORMACIÓN									**L1**	**0,69**
14.1 Requisitos de seguridad de los sistemas de información									**L1**	**1,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.14	A.14.1.1	A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	NO CUMPLE Se establecen requisitos de Seguridad ad-hoc en los procesos de contratación de algunos proveedores a través de la emisión de las correspondientes RFPs; sin embargo, no están tipificados y documentados los requisitos de seguridad de la organización hacia los proveedores de servicios.	TFM_PROC_Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.pdf Existencia de Herramienta para la Gestión de Proyectos (No está institucionalizado su uso para proyectos del SOC). TFM_PROC_Gestión de riesgos en Proyectos.pdf TFM_REG_Análisis de Riesgos en Proyectos.xls	S	4	L1	0	L1	1
A.14	A.14.1.2	A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas	No aplica		N	1	N/A	0	N/A	0
A.14	A.14.1.3	A.14.1.3 Protección de las transacciones de servicios de aplicaciones	No aplica		N	1	N/A	0	N/A	0
14.2 Seguridad en los procesos de Desarrollo y Soporte									L2	1,07
A.14	A.14.2.1	A.14.2.1 Política de desarrollo seguro	NO CUMPLE No hay establecida una política en la Organización.	TFM_PROC_Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.pdf	S	4	L0	0	L0	0
A.14	A.14.2.2	A.14.2.2 Procedimiento de control de cambios en sistemas	CUMPLE PARCIALMENTE Ver A.12.1.2 Habría que procedimentar el flujo y los mecanismos de revisión y aprobación de cambios.	Existe Herr. De Service (no se le está dando un uso para los cambios interos del SOC) TFM_PROC_Gestión del Cambio.pdf	S	2	L1	0	L1	1

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.14	A.14.2.3	A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	CUMPLE PARCIALMENTE Esta práctica se realiza habitualmente; pero no está ni procedimentada ni documentada.	TFM_PROC_Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.pdf	S	2	L1	0	L1	1
A.14	A.14.2.4	A.14.2.4 Restricciones a los cambios en los paquetes de software	CUMPLE PARCIALMENTE Idem a. 14.2.3.	TFM_PROC_Gestión de Parches de Seguridad.pdf	S	2	L2	0	L2	2
A.14	A.14.2.5	A.14.2.5 Principios de ingeniería de sistemas seguros	CUMPLE. Dentro de SOC se realizan las tareas de diseño de arquitecturas teniendo una competencia adecuado para ello.	Competencias existentes dentro del Equipo del SOC	S	2	L2	0	L2	2
A.14	A.14.2.6	A.14.2.6 Entorno de desarrollo seguro	CUMPLE Se está usando la infraestructura de Laboratorio del SOC para realizar estas actividades.	Equipos laboratorio (SOC y CPDs PROVEEDORES).	S	1	L2	0	L2	2
A.14	A.14.2.7	A.14.2.7 Externalización del desarrollo de software	No aplica		N	1	N/A	0	N/A	0
A.14	A.14.2.8	A.14.2.8 Pruebas funcionales de seguridad de sistemas	CUMPLE PARCIALMENTE Esta práctica se realiza; pero no está ni procedimentada ni documentada.	TFM_PROC_Practicas_Desarrollo_De_Codigo.pdf	S	1	L1	0	L1	1
A.14	A.14.2.9	A.14.2.9 Pruebas de aceptación de sistemas	CUMPLE PARCIALMENTE Esta práctica se realiza; pero no está ni procedimentada ni documentada.	TFM_PROC_Practicas_Desarrollo_De_Codigo.pdf	S	1	L1	0	L1	1
14.3 Datos de Prueba									**L0**	**0,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.14	A.14.3.1	A.14.3.1 Protección de los datos de prueba	NO CUMPLE No se están considerando los datos de Prueba con el mismo nivel de protección cuando su origen viene desde los entornos de producción.	TFM_PROC_Practicas_Desarrollo_De_Codigo.pdf	S	1	L0	0	L0	0
A.15 - RELACIÓN CON PROVEEDORES									L1	0,50
15.1 Seguridad de la Información en las Relaciones con proveedores									L1	1,00
A.15	A.15.1.1	A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores	NO CUMPLE Ver A.14.1.1	TFM_PROC_Relaciones con Proveedores.pdf TFM_REG_Relación y Evaluación Proveedores.xls	S	4	L1	0	L1	1
A.15	A.15.1.2	A.15.1.2 Requisitos de seguridad en contratos con terceros	NO CUMPLE Ver A.14.1.1	TFM_PROC_Relaciones con Proveedores.pdf	S	4	L1	0	L1	1
A.15	A.15.1.3	A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	CUMPLE PARCIALMENTE No están tipificados ni documentados. Se ha verificado la existencia de requisitos de seguridad para los proveedores más críticos, pero no se ha llegado a analizar el resto.	TFM_PROC_Relaciones con Proveedores.pdf (No hay conocimiento de existencia de cadena de suministro). TFM_REG_Relación y Evaluación Proveedores.xls	S	2	L1	0	L1	1
15.2 Gestión de la prestación de Servicios de Proveedor									L0	0,00
A.15	A.15.2.1	A.15.2.1 Control y revisión de la provisión de servicios del proveedor	NO CUMPLE. No hay implementado un mecanismo en la organización.	TFM_PROC_Relaciones con Proveedores.pdf	S	2	L0	0	L0	0
A.15	A.15.2.2	A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor	NO CUMPLE. No hay implementado un mecanismo en la organización.	TFM_PROC_Relaciones con Proveedores.pdf	S	2	L0	0	L0	0

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN									**L3**	**2,08**
16.1 GESTIÓN DE INCIDENCIAS Y MEJORAS DE LA SEGURIDAD DE LA INFORMACIÓN									**L3**	**2,08**
A.16	**A.16.1.1**	**A.16.1.1 Responsabilidades y procedimientos**	**CUMPLE PARCIALMENTE La organización tiene implantado un proceso de gestión de Incidentes que aplica tanto para la operativa de los Servicios a los Clientes; como para gestionar las incidencias específicas del SOC. cuenta con herramientas, tienen establecidos las categorizaciones, tratamiento, flujos y mecanismos de escalado. No existe una tipificación de los incidentes de seguridad (pero son adaptables dentro del procesos de incidencias ya existente).**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.16	**A.16.1.2**	**A.16.1.2 Notificación de los eventos de seguridad de la información**	**CUMPLE PARCIALMENTE Ver A. 16.1.2 y considerar la adaptación del flujo para adecuar las notificaciones de incidentes de seguridad dentro y fuera de la organización.**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.16	**A.16.1.3**	**A.16.1.3 Notificación de puntos débiles de la seguridad**	**CUMPLE PARCIALMENTE Estos mecanismos no están procedimentados y asegurados para todos los contratos con los proveedores.**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**4**	**L2**	**0**	**L2**	**2**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.16	**A.16.1.4**	**A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información**	**CUMPLE PARCIALMENTE A.16.1.1**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.16	**A.16.1.5**	**A.16.1.5 Respuesta a incidentes de seguridad de la información**	**CUMPLE PARCIALMENTE Ver A.16.1.2**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.16	**A.16.1.6**	**A.16.1.6 Aprendizaje de los incidentes de seguridad de la información**	**CUMPLE PARCIALMENTE El conocimiento está extendido de manera natural dentro de los equipos, pero no existen herramientas en las que apoyarse; ni se elaboran de manera habitual instrucciones técnicas para tipificar la resolución de los incidentes.**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**2**	**L2**	**0**	**L2**	**2**
A.16	**A.16.1.7**	**A.16.1.7 Recopilación de evidencias**	**CUMPLE Reutilización de los mecanismos y procedimientos del Análisis Forense que existen en la organización y que se usan habitualmente con los Servicios prestados a los clientes.**	**TFM_PROC_Gestión de Incidentes de Seguridad de la Información y Gestión de Crisis.pdf (Adecuar el procedimiento ya existente) Los incidentes de seguridad se vuelcan sobre herramienta de Service Desk (CONFIGURACÍON DE HERR. PARA INCIDENTES DE SEGURIDAD)**	**S**	**2**	**L3**	**0**	**L3**	**3**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO									**L2**	**1,25**
17.1 Continuidad de la seguridad de la Información									**L1**	**0,50**
A.17	**A.17.1.1**	**A.17.1.1 Planificación de la continuidad de la seguridad de la información**	**NO CUMPLE** **De manera natural la información crítica manejada por el SOC es conocida; pero no se han realizado de manera formal los BIA's para determinar el alcance y las necesidades.**	**TFM_PROC_Gestión de la Continuidad de Negocio.pdf** **TFM_REG_Planificación Escenarios de Contingencia.xls** **TFM_REG_Bitácora Prueba Escenarios de Contingencia .xls** **TFM_REG_BIA y Estrategias_GESTION DE CAMBIOS.xls** **TFM_REG_BIA y Estrategias_GESTION DE DESPLIEGUES.xls** **TFM_REG_BIA y Estrategias_GESTION DE INCIDENCIAS.xls** **TFM_REG_Roles, Responsabilidades y Competencias del PCN.xls** **TFM_REG_ DRT y Contactos.xls**	**S**	**4**	**L1**	**0**	**L1**	**1**
A.17	**A.17.1.2**	**A.17.1.2 Implementar la continuidad de la seguridad de la información**	**NO CUMPLE.** **No están documentados los procesos, procedimientos y controles para el nivel requerido que no ha sido calculado.**	**TFM_REG_Metodología de Análisis de Impacto en el Negocio.pdf** **TFM_IT_Plan de Contingencia.pdf**	**S**	**2**	**L0**	**0**	**L0**	**0**
A.17	**A.17.1.3**	**A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información**	**NO CUMPLE** **No se someten a revisiones y pruebas periódicas.**	**TFM_PROC_Gestión de la Continuidad de Negocio.pdf**	**S**	**2**	**L0**	**0**	**L0**	**0**
17.2 Redundancias									**L2**	**2,00**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.17	**A.17.2.1**	**A.17.2.1 Disponibilidad de los recursos de tratamiento de la información**	**CUMPLE PARCIALMENTE Existe redundancias en las infraestructuras que soportan la información desde el punto de vista del Almacenamiento, tratamiento y transferencia de la información; sin embargo, para ciertas informaciones críticas desde el punto de vista de la operativa del SOC no está garantizada esta redundancia (p.e. Gestión de credenciales).**	**TFM_PROC_Gestión de la Continuidad de Negocio.pdf TFM_IT_Plan de Contingencia.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.18 - CUMPLIMIENTO									**L2**	**1,83**
18.1 Conformidad con los requisitos Legales									**L2**	**1,67**
A.18	**A.18.1.1**	**A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales**	**CUMPLE PARCIALMENTE Competencia delegada al Área Jurídica. El enfoque está contemplado parcialmente; pero no existe una unificación de los criterios y sobre todo mecanismos de aplicación y control.**	**TFM_PROC_Cumplimiento Legal y Normativo.pdf (Centralizar los requisitos)**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.18	**A.18.1.2**	**A.18.1.2 Derechos de propiedad intelectual (DPI)**	**NO CUMPLE No están desarrollados los procedimientos pertinentes.**	**TFM_PROC_Cumplimiento Legal y Normativo.pdf (Centralizar los requisitos)**	**S**	**4**	**L1**	**0**	**L1**	**1**
A.18	**A.18.1.3**	**A.18.1.3 Protección de los registros de la organización**	**NO CUMPLE Ver A.8.1.2**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Revisión) TFM_PROC_Cumplimiento Legal y Normativo.pdf (Centralizar los requisitos) TFM_PROC_Clasificación de la Información y Gestión de Activos.pdf (Alinaemineto con la política creada)**	**S**	**4**	**L1**	**0**	**L1**	**1**

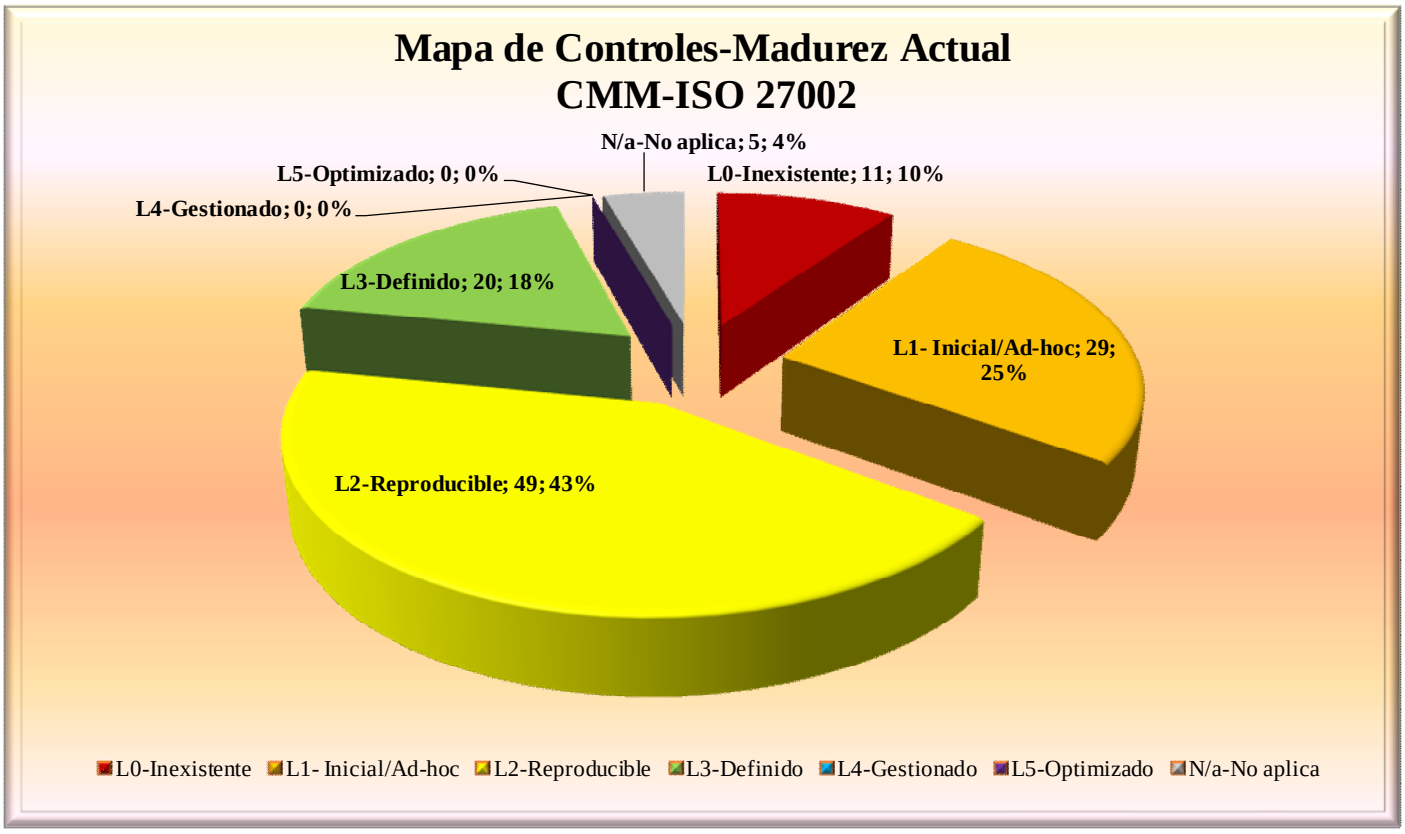
SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.18	**A.18.1.4**	**A.18.1.4 Protección y privacidad de la información de carácter personal**	**CUMPLE** **Dentro de la organización existe un Área Jurídica que tiene delegada esta responsablidad.** **Tiene puesta en marcha una adecuación al RGPD teniendo en consideración la Privacidad gestionada desde el SOC (el nivel de sensibilidad de la información personal manejada es bajo).**	**Alineamiento Área Jurídica (a través del RAT determinar los activos afectados dentro del alcance por la Privacidad, análisis de riesgos y contramedidas))**	**S**	**4**	**L3**	**0**	**L3**	**3**
A.18	**A.18.1.5**	**A.18.1.5 Regulación de los controles criptográficos**	**NO CUMPLE** **Ver. A.10.1.1, A.8.2.1 y A.8.2.3**	**TFM_PROC_Plan de Seguridad de la Información.pdf (Revisión)**	**S**	**2**	**L1**	**0**	**L1**	**1**
18.2 Revisiones de la Seguridad de la Información									**L2**	**2,00**
A.18	**A.18.2.1**	**A.18.2.1 Revisión independiente de la seguridad de la información**	**CUMPLE PARCIALMENTE** **No hay un sistema de Gestión de la Seguridad de la Información como tal ya implantado en la organización.** **Se han definido los procedimientos de Base para el control y seguimiento de Auditorías en la organizacíon para el SGSI.**	**TFM_PROC_Auditorías Internas.pdf** **TFM_PROC_Gestion de No Conformidades. Acciones Correctivas y de Mejora.pdf**	**S**	**4**	**L2**	**0**	**L2**	**2**
A.18	**A.18.2.2**	**A.18.2.2 Cumplimiento de las políticas y normas de seguridad**	**CUMPLE PARCIALMENTE** **Ver A.18.2.1**	**TFM_PROC_Auditorías Internas.pdf** **TFM_PROC_Gestion de No Conformidades. Acciones Correctivas y de Mejora.pdf** **TFM_PROC_Cumplimiento Legal y Normativo.pdf** **INFORMES DE AUDITORÍA**	**S**	**4**	**L2**	**0**	**L2**	**2**

SOA-Valoración Madurez - Controles ISO 27002										
Dominio	**Control**	**Descripción del Control**	**Referencias del Estado de Control**	**Documentos y Controles**	**Aplicabilidad (S/N)**	**Ponderación Grupo de Control**	**Valor de Referencia Madurez**	**Incremento/ Ajuste**	**EVALUACIÓN MADUREZ**	**EVALUACIÓN MADUREZ**
A.18	**A.18.2.3**	**A.18.2.3 Comprobación del cumplimiento técnico**	**CUMPLE PARCIALMENTE Ver A.18.2.1**	**TFM_PROC_Auditorías Internas.pdf TFM_PROC_Plan de Seguridad de la Información.pdf (Revisión)**	**S**	**4**	**L2**	**0**	**L2**	**2**

48-Evaluación madurez actual ISO 27002

5.4.1. Mapa de Madurez actual sobre modelo CMM-ISO 27002

La visión resumida de la situación actual del nivel de madurez de los controles de Seguridad agrupado en base a los valores de madurez se muestran en el siguiente gráfico.



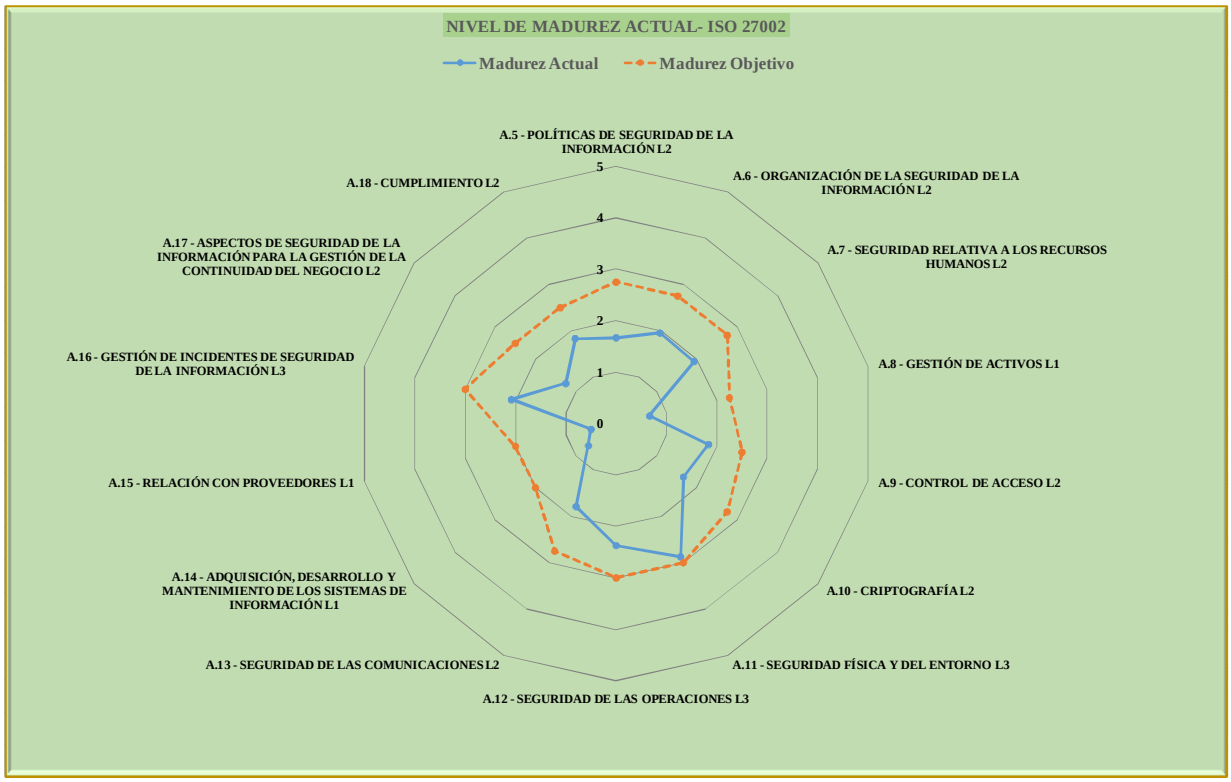
49-Modelo de madurez actual ISO 27002

En base al gráfico, una vez revisado, destacamos los siguientes puntos:

- La madurez de los controles de la organización están presentes sólo para los niveles comprendidos entre la L0-L3 y no hay valoración de madurez para los niveles L4-L5.
- Un alto porcentaje de la madurez de los controles se encuentra situada en el nivel L2 (43%) y otros tantos en el nivel L3 (18%); junto suman el 61% en grado de madurez sobre el total de los controles.
- El nivel de madurez L1 representa el 25% respecto del resto de valores (L0, L2 y L3).
- Como contrapartida, se observa la existencia de varios controles con valoración de madurez L0 (inexistente), que en porcentaje representan el 10% sobre el total.

5.4.2. Nivel de cumplimiento por Dominios de control-ISO 27002

La visión del nivel de madurez vista desde la perspectiva de los Dominios de control se muestra en el siguiente gráfico :



50-Nivel de cumplimiento actual por Dominios ISO 27002

En base al gráfico, una vez revisado, destacamos los siguientes puntos:

- **Destacar la disparidad, en cuanto a la valoración de madurez de los 14 dominios de control.**

Valoración Madurez-Dominios de Control (con Objetivos)				
Dominios	Actual		Objetivo	
	Madurez	Valor	Madurez	Valor
A.8 - GESTIÓN DE ACTIVOS	L1	0,7	L2	2,0
A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	L1	0,7	L2	2,0
A.15 - RELACIÓN CON PROVEEDORES	L1	0,5	L2	2,0
A.5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	L2	1,7	L3	2,8
A.6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	L2	2,0	L3	2,8
A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	L2	1,9	L3	2,8
A.9 - CONTROL DE ACCESO	L2	1,8	L3	2,5
A.10 - CRIPTOGRAFÍA	L2	1,7	L3	2,8
A.13 - SEGURIDAD DE LAS COMUNICACIONES	L2	1,8	L3	2,8

Valoración Madurez-Dominios de Control (con Objetivos)				
Dominios	Actual		Objetivo	
	Madurez	Valor	Madurez	Valor
A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L2	1,3	L2	2,0
A.18 - CUMPLIMIENTO	L2	1,8	L3	2,5
A.11 - SEGURIDAD FÍSICA Y DEL ENTORNO	L3	2,9	L3	3,0
A.12 - SEGURIDAD DE LAS OPERACIONES	L3	2,4	L3	3,0
A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L3	2,1	L3	3,0

51-Valoración Madurez-Dominios de Control (con Objetivos)

- Los dominios con nivel de madurez Inicial (**L1**) representa el **21%** sobre el total de los dominios de control evaluados.
- Los dominios con nivel de madurez (**L2**) representa el **57%** sobre el total de los dominios de control evaluados.
- Los dominios con nivel de madurez (**L3**) representa el **21%** sobre el total de los dominios de control evaluados.

Y se establecen las siguientes conclusiones:

- Con **carácter general la organización parte de la base de que actualmente ya tiene establecidos algunos controles de seguridad de manera no uniforme y con un grado de madurez predominante L2 (reproducible, pero intuitivo)** ; en dónde los controles establecidos están iniciados, son reproducibles y se gestionan de manera intuitiva y no se apoyan en un proceso ya definido (en dominios y controles concretos si existe un nivel mayor de madurez en dónde ya está puesto en marcha un proceso para su realización).
- Al mismo tiempo, se observa un **desequilibrio en ciertos grupos y dominios de control** dado que están declarados hasta 11 controles inexistentes; lo que conlleva la realización de un trabajo para establecer dichos controles ya que no se contemplan en la actualidad.
- En base a los elementos anteriores, hay que hacer notar que todavía **no están establecidas las bases de gestión en la Seguridad de la Información para esta organización que posibilite el poder intentar acometer y/o alcanzar un nivel de madurez que esté por encima del L3**.
- Como consecuencia de todo lo anterior, adelantaremos que cuando se establezcan los niveles objetivos de madurez de la organización, por muy ambiciosa que pueda ser la pretensión de la organización por incrementar de manera significativa el nivel de madurez, nuestro techo de objetivo no podría ir más allá de dejar los controles establecidos y definidos (aproximación al nivel de madurez **L3** con carácter general). Evidentemente, para aquellos controles de los que se parte desde el nivel de madurez **L0/L1**; nuestra pretensión de objetivos será empezar a desarrollarlos y adquirir experiencia dentro de la organización para más tarde constituirlos como proceso definidos.

- Sin haber establecido una base adecuada de gestión para los controles y haberla puesto en marcha en toda la organización, no es posible desarrollar iniciativas de medición, control, seguimiento y por supuesto optimización (niveles de madurez **L4-L5**).

6. EVALUACIÓN DE RESULTADOS

6.1. Introducción

A continuación, para a valorar los efectos de la realización del PDS y las consecuencias de la ejecución del Plan de Proyectos propuesto.

Consideraciones de partida

La organización partía de una situación en dónde ya existía un interés claro por considerar la Seguridad de la información como un elemento importante dentro del desarrollo de sus actividades ; pero no estaba ordena da la Seguridad como una función global.

- Parte de la carencia de base de no haberlo abordado como un proceso global que afecta a toda la organización.
- No haber establecido un sistema de gestión que no solamente ordene y organice de manera adecuada; sino que permitir que las prácticas establecidas se puedan mantener en el tiempo, se puedan llegar a medir; y exista una base sobre lo que que poder aplicar la mejora continua.

De forma que, en la organización hay ya implantadas prácticas de seguridad con un cierto grado de madurez, pero de forma específica, no homogenea, discontinua.

El conocimiento de esas prácticas no está en muchos casos documentado y difundido ; con lo cual se presenta el riesgo añadido de que caigan en el obstracismo y se pierdan.

Con lo cual, se ha abordado la tarea de establecer de principio un SGSI, para tener una plataforma desde la que poder desarrollar la Seguridad de la información en la Organización.

Análisis de Riesgos

En base a la implentación deun SGSI, se ha establecido una metodología de Análisis de riesgos, se ha aplicado sobre el conjunto de activos afectados por la SI en la organización y se ha obtenido como resultado la visión concreta de la evaluación de los riesgos que afectan a la SI.

- Este ejercicio nos permite establecer el foco de dónde tenemos que realizar el esfuerzo en cuanto a la aplicación de controles de seguridad para evitar sistuaciones y/o efectos no deseados.
- Este ejercicio, nos permite también alinear el foco de mejora de los controles de seguridad, de forma que los planes de proyectos construidos cumplen con 2 objetivos fundamentales:
    - Reducir/mitigar los riesgos detectados que vamos a gestionar.
    - Acrecentar/reforzar la madurez de los controles en base a las necesidades detectadas durante nuestra fase de análisis/diagnóstico de la Seguridad en a organización (**1.5-Análisis Diferencial**).

Mejora de los controles de Seguridad

Tal y como ya hemos comentado (apartado **Consideraciones de partida**) los controles de seguridad en la organización estaban desarrollados de manera heterogénea.

Con carácter general como citar se partía de la situación de que ciertos dominios de seguridad contaban con un nivel se seguridad alto y, en cambio en otros en el nivel de madurez era bastante bajo (**ver tabla-51-Valoración Madurez-Dominios de Control (con Objetivos)**).

Una vez realizado el análisis y diagnóstico de la Seguridad se han establecido las siguientes líneas de trabajo :

Para aquellos dominios de control que presentaban en nivel de madurez bajo, el objetivo es subir el nivel lo suficiente para poder dejar el proceso definido y establecido.

Para aquellos dominios de control que presentaban un cierto nivel de madurez, se ha buscado la consecución de varios objetivos :

- Reforzar los controles, sobre aquellas deficiencias y/o ajustes que se han evaluado como necesarios.
- Elevar el nivel de madurez de los controles, para tener la base suficiente para poder enfrentrarlo con capacidad de medición, revisión y mejora.

Queda pendiente realizar un ejercicio final que pasa por realizar la estimación como consecuencia de la aplicación de los proyectos de mejora que hemos dejado establecidos como consecuencia del Análisis y diagnóstico del estado de la Seguridad de la Información en la organización GLOBALSOC.

Elementos valorados

Tal y como se ha comentado, se va a considerar 3 aspectos:

- **Plan de Tratamiento de riesgos (PTR):** en base a los riesgos detectados, y según lo establecido en nuestra metodología; se va valorar la afectación sobre los riesgos actuales, como consecuencia de la ejecución del plan de proyectos Propuesto (4-**PROPUESTAS DE PROYECTOS**).
- **Mejora de la madurez, en referencia al Clausulado de la ISO 27001:** considerando las propuestas de proyectos **(**4-**PROPUESTAS DE PROYECTOS)** con acciones específicas para mejorar la madurez de las cláusulas de la ISO 27001, y a través de mejoras sobre los controles de la ISO 27002 que tienen también repercusión directa en la mejora de la madurez.
- **Mejora de la madurez de los controles de la ISO 27002:** a través de la ejecución de las propuestas de proyectos **(**4-**PROPUESTAS DE PROYECTOS)** con acciones específicas que repercuten en la mejora de la madurez de los controles de la ISO 27002.

6.1.2. Plan de Tratamiento Riesgos (Proyección mejora)

Como consecuencia de la ejecución de los Proyectos propuesto se producirá un incremento en la madurez de los controles de Seguridad.

Esta mejora debe de repercutir en la Valoración de los riesgos actuales dada la mejora en el grado de efectividad de los controles.

En base al catálogo de amenazas establecido como referencia para acometer el proceso de AR , estableciendo la asociación de los controles que interactuan contra las amenazas contribuyendo a su mitigación ,y realizando una valoración de la capacidad de mitigación de los riesgos actuales (**coeficiente de atenuación**) podemos proyectar la mejora en base a los riesgos actuales gestionados y provocar una reducción del riesgo (**Riesgo Previsto**).

Asociación Amenazas & Atenuación controles.

Asociación Amenazas/Controles aplicados reducción amenazas																					
Amenazas	Controles aplicados Reducción Amenazas																				
[A.11] Acceso no autorizado	A.6.1.1	A.6.1.2	A.8.1.1	A.8.1.3	A.8.2.1	A.9.1.1	A.9.1.2	A.9.2.1	A.9.2.3	A.9.4.3	A.11.1.2										
[A.24] Denegación de servicio	A.12.1.3	A.12.2.1	A.12.6.1	A.13.1.1	A.13.1.2	A.16.1.2	A.17.2.1														
[A.4] Manipulación de los ficheros de configuración	A.5.1.1	A.6.1.1	A.6.1.2	A.8.1.1	A.8.1.2	A.8.2.1	A.9.1.1	A.9.1.2	A.9.2.2	A.9.2.3	A.9.4.1	A.9.4.3	A.9.4.4	A.12.1.1	A.12.1.2	A.12.4.1	A.12.5.1	A.13.1.2	A.14.2.2	A.14.2.3	
[A.6] Abuso de privilegios de acceso	A.6.1.1	A.6.1.2	A.7.2.2	A.7.2.3	A.9.1.1	A.9.2.1	A.9.2.3	A.9.2.5	A.9.4.2	A.9.4.3	A.9.4.4										
[E.1] Errores de los usuarios	A.6.1.1	A.6.1.2	A.7.2.2	A.8.2.1	A.8.2.3	A.9.1.1	A.9.2.3	A.9.2.5	A.9.4.1	A.12.1.2	A.12.4.1										
[E.15] Alteración de la información	A.5.1.1	A.6.1.1	A.6.1.2	A.7.2.2	A.7.2.3	A.8.2.1	A.8.2.3	A.9.1.1	A.9.2.3	A.9.2.5	A.9.4.1	A.12.1.2	A.12.4.1	A.12.6.1	A.12.7.1	A.13.1.2	A.14.2.2				
[E.18] Destrucción de la información	A.5.1.1	A.6.1.1	A.6.1.2	A.7.2.2	A.7.2.3	A.8.2.1	A.8.2.3	A.9.1.1	A.9.2.3	A.9.2.5	A.9.4.1	A.12.1.2	A.12.4.1	A.12.6.1	A.12.7.1	A.13.1.2	A.14.2.2				
[E.19] Fugas de información	A.5.1.1	A.7.1.1	A.7.1.2	A.7.2.2	A.7.2.3	A.8.3.2	0	A.9.1.2	A.9.3.1	0	A.9.4.2	A.9.4.4	A.11.1.3	A.11.2.5							
[E.20] Vulnerabilidades de los programas (software)	A.5.1.1	A.6.1.1	A.6.1.2	A.12.2.1	A.12.4.1	A.12.6.1	A.12.6.2	A.14.1.1	A.14.2.1	A.14.2.8	A.15.1.1	A.15.1.2									
[E.21] Errores de mantenimiento / actualización de programas (software)	A.12.1.1	A.12.1.2	A.12.1.4	A.12.3.1	A.12.4.3	A.12.5.1	A.12.6.2														
[E.24] Caída del sistema por agotamiento de recursos	A.12.1.3	A.12.2.1	A.12.6.1	A.13.1.1	A.13.1.2	A.16.1.2	A.17.2.1														
[E.28] Indisponibilidad del personal	A.6.1.1	A.6.1.2	A.7.2.2	A.12.1.1	A.12.1.3	A.15.1.2	A.15.2.1	A.17.1.1													
[E.4] Errores de configuración	A.5.1.2	A.9.4.1	A.9.4.4	A.12.1.1	A.12.1.2	A.12.1.4	A.12.3.1	A.12.4.1	A.12.4.3	A.12.5.1	A.12.6.2										
[E.7] Deficiencias en la organización	A.5.1.1	A.5.1.2	A.6.1.2	A.7.1.1	A.7.1.2	A.7.2.1	A.7.2.2	A.7.3.1	A.8.2.1	A.9.3.1	A.13.2.1	A.14.1.1	A.15.1.2	A.15.2.2	A.16.1.5	A.17.1.1	A.18.1.1	A.18.2.1	A.18.2.3		
[I.*] Desastres industriales	A.15.1.1	A.15.1.3	A.15.1.2	A.15.2.1	A.17.1.1	A.17.1.2	A.17.1.3														
[N.*] Desastres naturales	A.15.1.1	A.15.1.3	A.15.1.2	A.15.2.1	A.17.1.1	A.17.1.2	A.17.1.3														

52-Amenazas&Atenuación controles ISO 27002

Coeficiente de atenuación

- Tomando como base la valoración de madurez **(EVALUACION MADUREZ**) actual para cada uno de los controles (**5.4-Evaluación de la madurez ISO 27002**) Aplicado en base a la valoración del riesgo actual **(4)**.
- También, tomando como referencia el incremento previsto en la madurez de los controles (**4.1.4-Proyectos-Incremento de la Madurez ISO 27001&ISO 27002 estimada)** como consecuencia de la ejecución de los proyectos planificados **(3)**.
- Y considerando el **Riesgo actual** calculado se estima la mitigación de los riesgos tras la aplicación del plan de ejecución de los proyectos en base a la siguiente fórmula.

Cálculo de la atenuación sobre Riesgo actual (Riesgo Previsto)
(1)-Coeficiente_actual=90* ((Promedio_madurez actual (**Asociación Amenazas & Atenuación controles**)/5)*0,01)
(5)- Coeficiente_prevision = 90*((Promedio_madurez_prevista (**Asociación Amenazas & Atenuación controles**)/5)*0,01)
(2)-Coeficiente_mejora= (Coeficiente_prevision - Coeficiente_actual)
Riesgo Estimado = Riesgo Actual – (Riesgo Actual * Coeficiente_mejora)

53-Cálculo estimación atenuación riesgo actual (por proyectos)

- El detalle de los coeficientes obtenidos para las amenazas se muestran en la siguiente tabla:

Amenaza	Promedio madurez Actual (4)	Coeficiente actual Reducción/atenuación del Riesgo (1)	Promedio Madurez Prevista (3)	Coeficiente Mejora (2)	Coeficiente previsión reducción mejora (5)
[A.11] Acceso no autorizado	1,73	0,31	2,37	0,12	0,43
[A.24] Denegación de servicio	2,43	0,44	2,58	0,03	0,47
[A.4] Manipulación de los ficheros de configuración	1,60	0,29	2,25	0,12	0,40
[A.6] Abuso de privilegios de acceso	1,64	0,29	2,43	0,14	0,44
[E.1] Errores de los usuarios	1,36	0,25	2,45	0,20	0,44
[E.15] Alteración de la información	1,65	0,30	2,36	0,13	0,43
[E.18] Destrucción de la información	1,65	0,30	2,36	0,13	0,43
[E.19] Fugas de información	1,73	0,31	2,39	0,12	0,43
[E.20] Vulnerabilidades de los programas (software)	1,75	0,32	2,32	0,10	0,42
[E.21] Errores de mantenimiento / actualización de programas (software)	2,14	0,39	2,71	0,10	0,49
[E.24] Caída del sistema por agotamiento de recursos	2,43	0,44	2,58	0,03	0,47
[E.28] Indisponibilidad del personal	1,38	0,25	2,36	0,18	0,42
[E.4] Errores de configuración	1,73	0,31	2,59	0,16	0,47
[E.7] Deficiencias en la organización	1,47	0,27	2,33	0,15	0,42
[I.*] Desastres industriales	0,57	0,10	1,78	0,22	0,32
[N.*] Desastres naturales	0,57	0,10	1,78	0,22	0,32

54-Detalle Amenazas/coeficientes de atenuación

Estimación de la reducción del riesgo en base al Riesgo actual (por ejecución de los Proyectos).

El resultado de la estimación queda reflejado en la siguiente tabla:

ESTIMACIÓN REDUCCIÓN RIESGO ACTUAL ACTIVOS-AMENAZAS	Riesgo Actual (Valor)			Riesgo Estimado		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[B] Activos esenciales						
[B_S_SG_SERVICIOS GESTIONADOS] SERVICIOS GESTIONADOS	4,3	0,0	0,0	3,8	0,0	0,0
[B_D_SG_GESTION DE DESPLIEGUES] GESTION DE DESPLIEGUES						
[B_D_SG_DES_PROYECTOS] Información de Desarrollo de los Proyectos (Herr. Proyectos)	3,9	0,6	0,1	3,4	0,5	0,1
[B_D_SG_DES_TEC] Información Técnica de los Proyectos	3,4	1,5	0,5	2,9	1,2	0,5
[B_D_SG_DES_CLI] Información de Clientes acerca del Proyecto	3,4	1,5	0,5	2,9	1,2	0,4
[B_D_SG_GESTION DE INCIDENCIAS] GESTION DE INCIDENCIAS						
[B_D_SG_INC_Incidencias] Registros de Incidencias (Herr. Service Desk)	4,3	1,5	0,5	3,8	1,2	0,4
[B_D_SG_INC_DOC] Documentación Interna del Proceso y Explotación	3,1	0,6	0,2	2,7	0,5	0,2
[B_D_SG_INC_BBDD del Conocimiento] Conocimiento Resolución Inc., Proced. Técnicos ,etc. (Wiki)	3,1	1,5	0,5	2,7	1,2	0,4
[B_D_SG_GESTION DE CAMBIOS] GESTION DE CAMBIOS						
[B_D_SG_CAM_PROC] Procedimientos, Documentación interna del Proceso y Explotación	4,3	0,6	0,2	3,8	0,5	0,2
[B_D_SG_CAM_RFC] Documentación RFC cambios (Service Desk)	1,9	1,5	0,4	1,6	1,2	0,3
[B_D_SG_CAM_PETICIONES] Registros de Cambios (Service Desk)	1,9	1,5	0,2	1,6	1,2	0,2
[B_D_SG_DES_CRED] Información de Credenciales (Gestor Credenciales)	4,3	4,3	0,6	3,8	3,8	0,5
[B_D_SG_CAM_CONTRATOS_CLIENTES] Registros de los Servicios Contratados con los Clientes	1,9	1,1	0,2	1,6	0,8	0,2
[B_D_SG_CONF_CLIENTES] Registros de las configuraciones componentes IT CLIENTES	3,6	1,5	0,5	3,1	1,2	0,4
[B_D_SG_CONF_GLOBALSOC] Registros de las configuraciones componentes IT GLOBALSOC	3,8	1,5	0,5	3,4	1,3	0,4
[B_D_SG_CAM_ARQ-SIS-GLOBALSOC] Documentación Arquitectura de Sistemas GLOBALSOC	3,7	1,1	0,4	3,2	0,8	0,3
[B_D_SG_CAM_ARQ-SIS-CLIENTES] Documentación Arquitectura Sistemas CLIENTES	0,9	1,5	0,5	0,8	1,2	0,4
[SRV] Servicios						
[SRVI] Servicios Internos						
[SRVI_IT] SERVICIOS GESTIONADOS IT						
[SRVI_IT_DESPL] SERVICIO DE GESTION DEL DESPLIEGUE	2,0	0,0	0,0	2,0	0,0	0,0
[SRVI_IT_INCID] SERVICIO DE GESTION DE INCIDENCIAS	4,7	0,0	0,0	4,6	0,0	0,0
[SRVI_IT_CAMB] SERVICIO DE GESTION DE CAMBIOS	3,4	0,0	0,0	3,3	0,0	0,0
[SRVI_ADMIN] Servicios Corporativos						
[SRVI_CORP_COMERCIAL] Área Comercial y Marketing de la Organización	0,9	0,0	0,0	0,8	0,0	0,0
[SRVI_CORP_FINAN&LEGAL] Servicios Financieros y Legales	3,7	0,0	0,0	3,2	0,0	0,0
[SRVI_CORP_OPERACIONES] OPERACIONES	3,7	0,0	0,0	3,3	0,0	0,0
[SRVI_CORP_RRHH] Área de RR.HH.	3,7	0,0	0,0	3,2	0,0	0,0
[SRV_CORP_OPER] Dirección de Operaciones	2,7	0,0	0,0	2,6	0,0	0,0
[SRVE] Servicios Externos	0,0	0,0	0,0	0,0	0,0	0,0
[SRVE_CORREO] Servicio de Correo (GOOGLE)	3,7	0,0	0,0	3,3	0,0	0,0
[SRVE_DATACENTER] Servicio de CPD y Comunicaciones	4,7	0,0	0,0	4,6	0,0	0,0
[SRVE_CLOUD_GOOGLE] Servicio Alojamiento Servidores y Storage	4,7	0,0	0,0	4,6	0,0	0,0

ESTIMACIÓN REDUCCIÓN RIESGO ACTUAL ACTIVOS-AMENAZAS	Riesgo Actual (Valor)			Riesgo Estimado		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI] Sistema de Información						
[HW] Hardware						
[SI_HW_CLOUD_GOOGLE]						
[SI_HW_SERV_DA] Servidores de DA	2,0	2,0	1,5	1,9	1,7	1,5
[SI_HW_CONSOLA_ANTIVIRUS] Consola Antivirus	2,0	2,0	1,5	2,0	1,7	1,5
[SI_HW_SD_HD] Servidor Service Desk/Help Desk	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_SFTP] Servidor Servicio de transferencia ficheros	0,7	2,7	1,5	0,7	2,3	1,5
[SI_HW_DATASTORE] Almacenamiento y Backup	2,7	1,6	1,2	2,6	1,4	1,2
[SI_HW_WEB_CORP] Servidores Web Corporativa	2,6	0,5	0,3	2,5	0,4	0,3
[SI_HW_CERTIF] Servidor de Certificados	2,7	2,7	2,7	2,6	2,3	2,3
[SI_HW_DATACENTER]						
[SI_HW_SIEM] Servidor SIEM	1,4	1,4	0,8	1,3	1,2	0,8
[SI_HW_AD_3] Servidor Controlador DominIo (AD)	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_MONITOR] Servidor de Monitorización	2,0	2,7	0,7	2,0	2,3	0,6
[SI_HW_GEST_PROY] Servidor Gestión de Proyectos	2,6	0,7	0,7	2,5	0,6	0,6
[SI_HW_WIKI] Servidor de la Wiki	2,6	0,7	0,7	2,5	0,6	0,6
[SI_HW_HERR_BACKUP] Servidor de la Herramienta de Backup	4,1	3,4	3,4	4,0	2,9	2,9
[SI_HW_CORREO] Relay del Correo	2,7	2,0	2,0	2,6	1,7	1,7
[SI_HW_VIRTUAL] Plataforma Virtualización	0,0	0,0	0,0	0,0	0,0	0,0
[HW_VIRTUAL_HYPER] Plataforma gestion Virtualizadora (Hypervisor)	3,8	2,0	1,5	3,7	1,7	1,5
[SI_HW_VM_LOGS] Servidores recolectores y concentradores LOGS	2,7	1,8	0,7	2,6	1,6	0,7
[SI_HW_VM_CREDEN] Servidores Credenciales	4,8	4,1	4,1	4,6	3,5	3,5
[SI_HW_VM_IPS] Servidores VM Sistema de Prevención Intrusos	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_VM_IDS] Servidores VM Sistema de Detección Intrusos	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_VM_POSTFIX_CORREO] Servidores VM Relay de Correo	2,0	0,7	0,7	1,9	0,6	0,6
[SI_HW_VM_ANAL_DATA] Servidores VM Analitica de Datos	2,6	2,0	2,0	2,5	1,7	1,7
[SI_HW_NAS] Servidor de Almacenamiento NAS	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_VM_MONITOR] Sistema de Monitorización	2,7	2,0	1,5	2,6	1,7	1,5
[SI_HW_SERV_LAB] Servidores laboratorio	0,7	0,7	0,7	0,7	0,6	0,6
[SI_HW_GLOBALSOC_Sede_MADRID]						
[SI_HW_PC] PC de Sobremesa	0,7	0,5	0,2	0,7	0,5	0,1
[SI_HW_TFNO_MOVIL] Teléfono Móvil	0,2	0,0	0,0	0,1	0,0	0,0
[SI_HW_TFNOS_CENTRALITA] Teléfonos Fijos IP	1,1	0,0	0,0	1,1	0,0	0,0
[SI_HW_IMPRES] Equipos de Impresión	0,2	0,0	0,0	0,1	0,0	0,0
[SI_HW_SOC_MAD] Hardware SOC de MADRID						
[SI_HW_PC_SOC_MAD] PC de Sobremesa del SOC MAD	0,7	0,5	0,2	0,7	0,5	0,1
[SI_HW_PORTATIL_SOC_MAD] Equipos Portátiles del SOC de Madrid	2,0	1,6	0,3	1,7	1,4	0,3
[SW] Software						
[SI_SW_Windows] S.O. Puesto de Trabajo	1,7	1,3	0,2	1,5	1,2	0,2
[SI_SW_GEST-PROY] Herramienta de Gestión de proyectos	0,9	0,7	0,2	0,8	0,6	0,2
[SI_SW_Office] S.O. Puesto de Trabajo (Office)	1,7	1,3	0,2	1,5	1,2	0,2
[SI_SW_ANTIVIRUS] Software Antivirus	1,7	1,3	0,2	1,5	1,2	0,2
[SI_SW_ALM_NUBE] Google Drive	1,7	1,3	1,9	1,5	1,2	1,7
[SI_SW_WINDOWS] Windows Server	1,7	1,7	1,8	1,5	1,5	1,6
[SI_SW_LINUX] Software Linux	1,7	1,7	1,8	1,5	1,5	1,6
[SI_SW_CLOUD_GOOGLE]						
[SI_SW_DA] Servicios de Directorio Activo (c/conector CLOUD)	1,2	0,9	0,9	1,1	0,8	0,8
[SI_SW_SERVICE DESK] Service Desk-Help Desk	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_SFTP] Servicios SFTP	0,9	0,9	0,9	0,8	0,8	0,8
[SI_SW_CERTIFICADOS] Servicios Certificados	1,7	2,0	3,1	1,5	1,8	2,7
[SI_SW_BACKUP] Servicios de Storage (DataStore)	1,7	1,7	1,9	1,5	1,5	1,7
[SI_SW_WEB] Servicios Web Corporativos	1,2	0,6	0,4	1,1	0,5	0,3
[SI_SW_CONSOLA_ANTIVIRUS] Servicios Antivirus	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_DATACENTER]						
[SI_SW_SIEM] Software SIEM	1,7	1,7	0,9	1,5	1,5	0,8

ESTIMACIÓN REDUCCIÓN RIESGO ACTUAL ACTIVOS-AMENAZAS	Riesgo Actual (Valor)			Riesgo Estimado		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[SI_SW_HYPERVISOR] Software Virtualización	3,1	1,7	0,9	2,7	1,5	0,8
[SI_SW_IPS] Software IPS	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_ANAL_DATA] Software Analítica de Datos	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_IDS] Software IDS	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_MONITOR] Software de Monitorización	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_SERV_FICH] Software de Servicio de Ficheros	1,7	1,7	0,9	1,5	1,5	0,8
[SI_SW_WIKI] Software Wiki	0,9	0,9	0,9	0,8	0,8	0,8
[SI_SW_RECOLECTOR] Sotware de Recolección y Gestión de Logs	1,7	3,4	0,4	1,5	3,1	0,3
[SI_SW_CREDENCIALES] Software Gest. Credenciales	1,7	3,9	4,3	1,5	3,5	3,8
[SI_SW_RELAY CORREO] POSTFIX	0,9	0,9	0,9	0,8	0,8	0,8
[COM] Comunicaciones						
[COM_RED GOOGLE] Segmentación red (DMZ, cloud-mz, default, SHARED-XPN)						
[COM_LAN_GOOGLE] Red GOOGLE	3,4	2,0	1,8	3,3	2,0	1,6
[COM_FW_GOOGLE] Firewall Google	3,4	2,0	1,8	3,3	2,0	1,6
[COM_SWT_GOOGLE] Switches GOOGLE	2,7	2,0	1,8	2,6	2,0	1,6
[COM_RED DATACENTER] Segmentacion Red (Redundancia acceso CPD)						
[COM_VPN_DATACENTER] TUNEL IPSEC DATACENTER-GOOGLE	2,7	2,0	1,8	2,6	2,0	1,6
[COM_LAN_DATACENTER] Red DATACENTER	2,7	2,0	1,8	2,6	2,0	1,6
[COM_SWT_DATACENTER] Switches DATACENTER	2,7	2,0	1,8	2,6	2,0	1,6
[COM_FW_DATACENTER] Firewall Datacenter (Redundancia)	2,7	2,0	1,8	2,6	2,0	1,6
[COM_RED_GLOBALSOC_Sede_MADRID] Segmentacion Red (oficina, Voz Ip,Biometria, Dispositivos, SOC)						
[COM_LAN_GLOBALSOC_Sede_MAD] Red Sede Madrid	1,1	0,0	0,0	1,1	0,0	0,0
[COM_RED WIFI_GLOBALSOC_Sede_MAD] Red Wifi Sede Madrid	1,1	0,0	0,0	1,1	0,0	0,0
[COM_VPN_GLOBALSOC_SOC_MAD] TUNEL IPSEC SOC-DATACENTER	1,5	0,0	0,0	1,5	0,0	0,0
[COM_SWT_GLOBASOC_Sede_MAD] Switches Sede MAD	1,1	0,0	0,0	1,1	0,0	0,0
[COM_FW_GLOBALSOC_Sede MAD] Firewall Sede MADRID (Redundancia)	1,5	0,0	0,0	1,5	0,0	0,0
[SS] Proveedores						
[SS_ES] Servicios Esenciales						
[SS_ES_ADMIN_EDIFICIO] Administración del Edificio Sede MADRID (Administrador externo)	0,7	0,5	1,2	0,7	0,5	1,1
[SS_ES_BIOMETRIA_SOC] Gestión Infr. Biometría del OFICINA Y SOC	0,7	0,5	1,2	0,7	0,5	1,1
[SS_ES_WIFI] Servicios de Comunicaciones Wifi (TELEFÓNICA)	0,7	0,5	1,2	0,7	0,5	1,1
[SS_IT_SG] Proveedores IT (SERVICIOS GESTIONADOS)						
[SS_IT_SG_PROVEEDORES_8*5] Proveedores Soporte 8*5	0,5	0,0	0,0	0,4	0,0	0,0
[SS_IT_SG_PROVEEDORES_24*7] Proveedores Soporte 24*7	2,7	2,0	1,8	2,6	2,0	1,6
[SS_OT] Otros						
[SS_OT_TFNO_MOVIL] Telefonos Móviles SOC	0,7	0,5	1,2	0,7	0,5	1,1
[SS_OT_CENTRALITA] Servicio de Telefonía Voz IP-Centralita	0,4	0,0	0,0	0,4	0,0	0,0
[P] Personal						
[P_I] Personal Interno						
[P_I_SOC] Personal Interno del SOC MAD	2,5	0,0	2,5	2,1	0,0	2,2
[P_I_OFI] Personal Administración y Servicios GLOBALSOC MADRID	1,6	0,0	0,3	1,4	0,0	0,2
[P_I_FIN_LEG] Personal Resp. Financiero y Legal	2,5	0,0	0,5	2,1	0,0	0,5
[P_I_RRHH] Personal Resp. RR.HH.	2,5	0,0	0,5	2,1	0,0	0,5
[P_I_Comercial] Personal Área Comercial y Marketing	1,6	0,0	0,4	1,4	0,0	0,4
[P_E] Personal Externo						
[P_E_MTO] Personal de Limpieza y Mantenimiento	0,3	0,0	0,0	0,2	0,0	0,0
[L] Instalaciones y Ubicaciones						
[LD] Dependencias						
[LD_GLOBALSOC_SOC_MAD] Sala de ubicación del SOC de Madrid	0,9	1,5	1,8	0,8	1,5	1,8

ESTIMACIÓN REDUCCIÓN RIESGO ACTUAL ACTIVOS-AMENAZAS	Riesgo Actual (Valor)			Riesgo Estimado		
ACTIVOS	[D]	[I]	[C]	[D]	[I]	[C]
[LD_SEDE GLOBALSOC_MAD] Oficina GLOBALSOC Sede MADRID	0,9	1,5	1,8	0,8	1,5	1,8
[LD_GOOGLE_CLOUD] Cpd de GOOGLE	3,1	1,5	1,8	2,7	1,5	1,8
[LD_DATACENTER] Datacenter usado por GLOBALSOC sede MADRID	3,7	1,5	1,8	3,2	1,5	1,8
[LS] Salas Técnicas						
[LS_COM_GLOBALSOC_SALA_COM] Sala Técnica Comunicaciones	0,3	0,0	0,0	0,3	0,0	0,0
[LO] Otros						
[LE] Edificios						
[LE_GLOBALSOC_MAD] Edificio Compartido Ubicación de GLOBALSOC en Madrid	1,4	2,7	3,2	0,9	2,7	3,2

55-Estimación Reducción riesgo actual (por ejecución de los proyectos)

6.1.3. Mejora madurez ISO 27001 (Proyección mejora)

En el siguiente diagrama de radar se representa la comparativa, en cuanto a la evolución de los requerimientos de las cláusulas del referencial de la ISO 27001, que de manera resumida viene a representar el establecimiento del Sistema de Gestión de la Seguridad de información en la Organización.

56-Estimación Mejora madurez ISO 27001

Valoración de la evolución

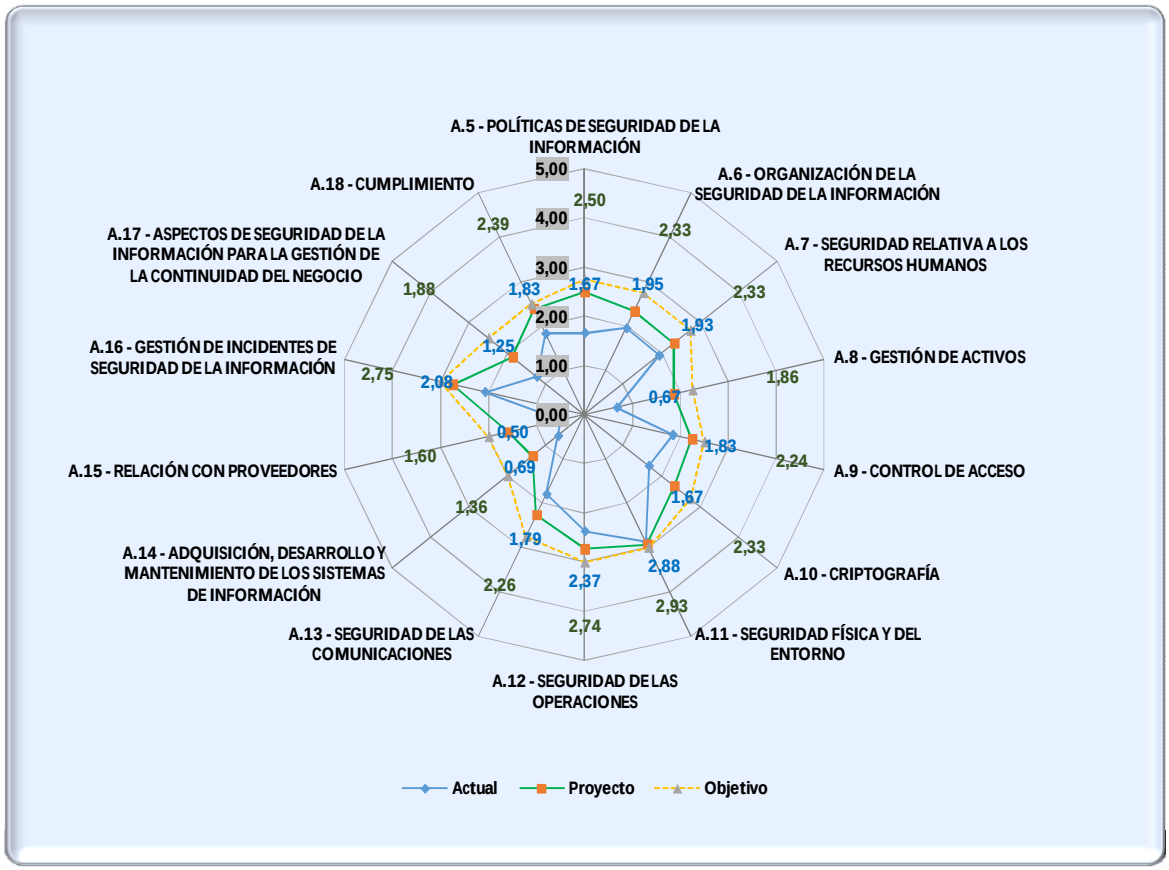
El estado **Actual** (representado en azul) es la consecuencia de la implantación del SGSI que hemos realizado durante el desarrollo del presente proyecto (**2-SISTEMA DE GESTIÓN DOCUMENTAL**) ; en donde hemos establecido los componentes de base para dota de un sistema de Gestión de la Seguridad de la Información en la organización.

El estado de Proyecto (representado en verde) es también la consecuencia de acometer algunas acciones de mejora/refuerzo del SGSI para asegurar ciertos aspectos concretos, en particular :

- Dejar establecido una visión completa de las Partes interesadas que afectan a la Seguridad de la información y dejar establecidos los mecanismos para su mantenimiento y control (**4-Contexto de la Organización-C.4.2**).
- Documentar los procesos y actividades que se realizan en la organización (que afectan a Seguridad de la información); estableciendo las dependencias, los flujos de información y las responsabilidades asociadas.
    - Lo cual nos va a aportar una visión detallada y ordenada de la organización para poder gestionar de manera eficiente los requisitos y controles de SI (**4-Contexto de la Organización-C.4.3**).
- Refuerzo del conocimiento en base a los roles y responsabilidades de la organización en base a la descripción de los procesos de la organización (C.4.3), que afectan de manera directa al refuerzo de la madurez en los requisitos del apartado **5-Liderazgo-C.5.3**.
- Desde la perspectiva del refuerzo de los requisitos de seguridad aplicados a la gestión de RR.HH. queda reforzado el cumplimiento de los requerimientos relacionados para **C.7-Soporte y C.9-Evaluación del desempeño**.
    - Planificación del proceso de concienciación y formación en SI dentro de la organización.
    - Valorar las necesidades en cuantos a competencias técnicas y funciones de los perfiles de la organización.
- El estado objetivo (representado en naranja) viene a representar el objetivo de madurez global al que se puede llegar en base al nivel de desarrollo, tiempo y experiencia en el SGSI del que parte la organización. Explicado de otra manera la aspiración debe ser establecer y poner en funcionamiento el sistema antes de aspirar a subir a cotas de madurez (L4-L5) que actualmente no se pueden plantear.

6.1.4. Mejora madurez ISO 27002 (Proyección mejora)

En el siguiente diagrama de radar se representa la comparativa, en cuanto a la evolución de los controles de Seguridad en base al referencial de la ISO 27002, que de manera resumida viene a representar el establecimiento del Sistema de Gestión de la Seguridad de información en la Organización.



57-Estimación Mejora madurez ISO 27002

Disparidad en cuanto al nivel de madurez en los distintos Dominios de Control tal y como aparecen detallados en la siguiente tabla.

Valoración Madurez-Dominios de Control (con Objetivos)				
Dominios	Actual		Objetivo	
	Madurez	Valor	Madurez	Valor
A.8 - GESTIÓN DE ACTIVOS	L1	0,7	L2	2,0
A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	L1	0,7	L2	2,0
A.15 - RELACIÓN CON PROVEEDORES	L1	0,5	L2	2,0
A.5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	L2	1,7	L3	2,8
A.6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	L2	2,0	L3	2,8
A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	L2	1,9	L3	2,8
A.9 - CONTROL DE ACCESO	L2	1,8	L3	2,5
A.10 - CRIPTOGRAFÍA	L2	1,7	L3	2,8
A.13 - SEGURIDAD DE LAS COMUNICACIONES	L2	1,8	L3	2,8
A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L2	1,3	L2	2,0
A.18 - CUMPLIMIENTO	L2	1,8	L3	2,5
A.11 - SEGURIDAD FÍSICA Y DEL ENTORNO	L3	2,9	L3	3,0
A.12 - SEGURIDAD DE LAS OPERACIONES	L3	2,4	L3	3,0
A.16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L3	2,1	L3	3,0

58-Evolución madurez Dominios de Control ISO 27002

Resaltar el aspecto del incremento de madurez sobre aquellos dominios con un nivel más bajo (**L1**).

- A destacar que el establecimiento de los criterios de clasificación de la información permitirá una gestión adecuada de la seguridad de la información y de dotarla de las medidas de Seguridad apropiadas de manera focalizada y eficaz (**A8.-Gestión de Activos**).
- El poder tener una gestión centralizada y ordenada de los activos de la organización permite poder tener un control sobre los activos y sus riesgos; con todo lo que esto implica en la mejora de Seguridad. (**A8.-Gestión de Activos**).
- El ciclo de adquisición, desarrollo y mantenimiento de Sistemas de información quedarán establecidas pautas y procedimientos para controlar la adquisición, evaluación y control de los Sistemas de Información (Aseguramiento de especificaciones, servicios, cumplimiento de normas de seguridad, gestión de derechos y licenciamiento, etc.) que están bajo el dominio de control (**A.14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN)**
- La gestión controlada de los proveedores permitirá tener un control sobre los mismos, sobre los servicios prestados, el cumplimiento de las especificaciones de seguridad, etc.), reflejados en el dominio (**A.15 - RELACIÓN CON PROVEEDORES**).

A destacar el aspecto del incremento de madurez sobre aquellos dominios con un nivel (**L2**), destacando especialmente.

- Sobre la Gestión de las comunicaciones en la organización, se mejoran los aspectos de documentación de las arquitecturas y topologías de red presentes en la organización y sobre todo dejar documentado, registrado y establecidos los mecanismos de transporte e intercambio de información para mantener los niveles de seguridad deseados (transporte, correo, notificaciones internas/externas, etc.). Que quedan reflejados a través del dominio (**A.13 - SEGURIDAD DE LAS COMUNICACIONES**).

- Sobre el conocimiento de los servicios críticos de la organización se tendrá una idea clara acerca de las afectaciones a negocio, de las necesidades y de los recursos necesarios para mantener la prestación de los servicios, de las necesidades de disponibilidad y de los tiempos de recuperación reales de los servicios. Es un proceso ya iniciado que habrá que seguir madurándolo progresivamente (**A.17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**).
- Reforzar los mecanismos de seguridad a través de la planificación y seguimiento, dentro de la organización, de los aspectos de concienciación y formación en Seguridad de la Información (**A.7 - SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS**).
- Mejora en la detección de anomalías y violaciones de Seguridad; recalcar la necesidad de tener contemplado como actividad regular dentro de la organización, la revisión periódica de los derechos de acceso a recursos y aplicaciones; como un elemento básico de detección de anomalías de Seguridad (**A.9 - CONTROL DE ACCESO**).

En cuanto a los dominios de control que parten de un nivel de madurez (**L3**), solamente decir.

- Los controles ya estaban gestionados por la organización, con lo cual se realizan algunos ajustes/mejoras para acrecentar su efectividad (**A11., A.12 Y A.16**).

El estado objetivo (representado en naranja) viene a representar el objetivo de madurez global al que se puede llegar en base al nivel de desarrollo, tiempo y experiencia en el uso de los controles de seguridad de los que parte la organización. Explicado de otra manera la aspiración debe ser establecer y poner en funcionamiento la batería de controles adecuados antes de aspirar a subir a cotas de madurez (L4-L5) que actualmente no se pueden plantear.

7. BIBLIOGRAFÍA

INCIBE-Plan Director de Seguridad. (s.f.). Obtenido de (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf).

MAGERIT-Libro II Catálogo de Elementos. (s.f.). Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XI6IEChKiDI

MAGERIT-Libro III Guía de Técnicas. (s.f.). Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XI6IEChKiDI

MAGERIT-Libro I-Método. (s.f.). *https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XI6IEChKiDI*.

UNE-ISO/IEC 27001-Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información (SGSI)-Requisitos. (s.f.).

UNE-ISO/IEC 27002-Tecnología de la información-Técnicas de seguridad– Código de prácticas para los controles de seguridad de la información. (s.f.).

8. REFERENCIAS

8.1. Documentos

8.1.1. TFM_Informe_Analisis_Diferencial.pdf

8.1.2. TFM_Metodología de Análisis y Gestión de Riesgos de SI.pdf

8.1.3. TFM_Politica de Seguridad.pdf

8.1.4. TFM_PROC_Gestion de No Conformidades. Acciones Correctivas y de Mejora.pdf

8.1.5. TFM_PROC_Objetivos de Seguridad, Indicadores y Métricas.pdf

8.1.6. TFM_PROC_Procedimiento de Auditorias Internas.pdf

8.1.7. TFM_PROC_Procesos, Roles y Responsabilidades.pdf

8.2. Registros

8.2.1. TFM_REG_Acciones.xlsx

8.2.2. TFM_REG_Medición de Objetivos.xlsx

8.2.3. TFM_REG_NC y Acciones Correctivas.xlsx

8.2.4. TFM_REG_Plan de Auditoría.xlsx

8.2.5. TFM_REG_Programa de Auditoria.xls

8.2.6. TFM_REG_Roles Responsabilidades y Competencias.xlsx

8.2.7. TFM_Declaración de Aplicabilidad SOA.xlsx

8.2.8. TFM_Evaluación_Madurez_Controles.xlsx