Trabajo Final de Master

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y la Comunicación (MISTIC)

ICARO

Título	**Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013**
Autor	Luis Rodríguez Conde
Dirección	Antonio José Segovia Henares
Fecha	Junio, 2017

Universitat Rovira i Virgili

Contenido

Índice de Ilustraciones

Índice de Tablas

0 Introducción

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El marco legal ha reflejado la importancia de la seguridad de la información. En los últimos años se han aprobado leyes que así lo demuestran.

Como ejemplo, a nivel de España nos encontramos las siguientes leyes relacionadas con la seguridad de la información:

- Ley15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD) y su desarrollo en el Real Decreto de 1720/2007, de 21 de diciembre
- Ley 11/2007 artículo 42: "Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad" y su desarrollo en el Real Decreto 3/2010, de 8 de enero.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Y no solo a nivel estatal, también cada vez más a nivel europeo se toman mayores medidas respecto a la seguridad de la información:

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS (Network and Information Security).
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, conocida como directiva GDPR (General Data Protection Regulation).

La seguridad no es por tanto un aspecto opcional, sino que debe ser inherente a las actividades de la propia empresa, y constituye un punto de partida ineludible para toda organización en la actualidad independientemente del sector en el que desarrolle su actividad.

El planteamiento del proyecto es, por tanto, sentar las bases de un Plan de Director de Seguridad para la empresa. Simplificado, el proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.

- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción.

Intencionadamente, la lista anterior no contempla aspectos organizativos, que, aun así, se introducen a lo largo del presente proyecto.

0.1 Conociendo la norma ISO/IEC 27001 y 27002

La información es un activo muy valioso capaz de impulsar o destruir una empresa. Su seguridad se ha consolidado como una parte cada vez más importante, y a la par también lo ha ido haciendo la metodología y las 'buenas prácticas' sobre seguridad de la información.

En este sentido organizaciones como ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) han elaborado conjuntamente la familia ISO/IEC 27000. Esta, es un conjunto de normas desarrolladas para proveer un marco en gestión de la seguridad de la información que sirva de aplicación en cualquier tipo de organización, ya sea pública o privada, grande o pequeña.

0.1.1 El origen de la norma

La primera entidad de normalización a nivel mundial relativa a la seguridad de la información que publicó un estándar ha sido la BSI (British Standars Intitution, institución británica de normalización) con la publicación en 1995 de la norma BS 7799. Esta norma se creó con el ánimo de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.

La norma de divide en dos partes. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas sin esquema de certificación. La segunda parte (BS 7799-2), publicada en 1998, establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999. La primera parte fue adoptada por ISO sin realizar cambios sustanciales como ISO/IEC 17799 en el año 2000. Posteriormente, en el año 2002 se revisó la BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión y en el año 2005 se publicó como estándar ISO/IEC 27001:2005. En ese mismo año, se revisó y se actualizó la ISO 17799 (basada en BS 7799-1) para convertirse en la ISO/IEC 17799:2005 y dos años más tarde se renombra como ISO/IEC 27002:2007 como parte de la reserva de numeración de la familia 27000.

La última versión de la norma es la ISO/IEC 27002:2013. En esta, se extiende la información de los anexos de la también última versión de la ISO/IEC 27001:2013 donde

básicamente se describen los dominios de control y los mecanismos de control que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001.

0.1.2 Relación entre las normas ISO/IEC 27001 y 27002

Ya que ambas nacen de la primitiva norma británica BS 7799 (Parte I y II), las normas ISO/IEC 27001 y 27002 no son normas diferentes, si no que son complementarias.

La 27001 es una norma que define como ejecutar un Sistema de Gestión de la Seguridad de la información (SGSI), indicando que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada. De estos hitos, se extraen una serie de objetivos para su cumplimiento y que están establecidos en la norma. Por lo tanto, la norma 27001 es una norma de certificación de cumplimiento de dichos objetivos.

En cambio, la norma 27002 es una guía de buenas prácticas para mejorar la seguridad de la información de tal manera que ayuda a alcanzar los objetivos marcados en la 27001. Estas buenas prácticas se presentan en forma de controles diferenciados por dominios relativos a la seguridad de la información. Dichos controles ya aparecen nombrados en la norma 27001 en su Anexo A, pero sin ser desarrollados, y es en la 27002 donde se desarrollan.

Por tanto, se puede concluir que la norma ISO/IEC 27002 ofrece las herramientas para ayudar a alcanzar los objetivos que se establecen en la norma ISO/27001.

0.1.3 Estructura de la norma ISO/IEC 27002

INTRODUCCIÓN

La norma consta de una primera parte de introducción muy clara que expone:

- El contexto en el que se enmarca la norma
- Las fuentes para extraer los requisitos en seguridad de la información
- Una aproximación a la selección de los controles
- Como la normar puede servir para el desarrollo de directrices propias
- Reflexión sobre el ciclo de vida de la seguridad de la información y esta es un ente vivo.
- Normas relacionadas.

CAPÍTULOS DEL 1 AL 4

- Objeto y campo de aplicación: Indica que la norma establece directrices para selección, la implantación y la gestión de los controles relativos a la seguridad de la información de la organización.
- Normas de consulta: Indica que normas son de consulta indispensable en parte o en su totalidad. En este caso la ISO/IEC 27000
- Términos y Definiciones: Indica que se aplican los de la norma ISO/IEC 27000
- Estructura de la norma: Expone que los siguientes capítulos (del 5 al 18), es donde se desarrolla la norma

CAPÍTULOS DEL 5 AL 18

La norma, cuenta con 14 capítulos de controles de seguridad que contienen un total de 35 categorías principales de seguridad y 114 controles.

En la siguiente imagen se puede apreciar un esquema de los capítulos y sus apartados correspondientes.

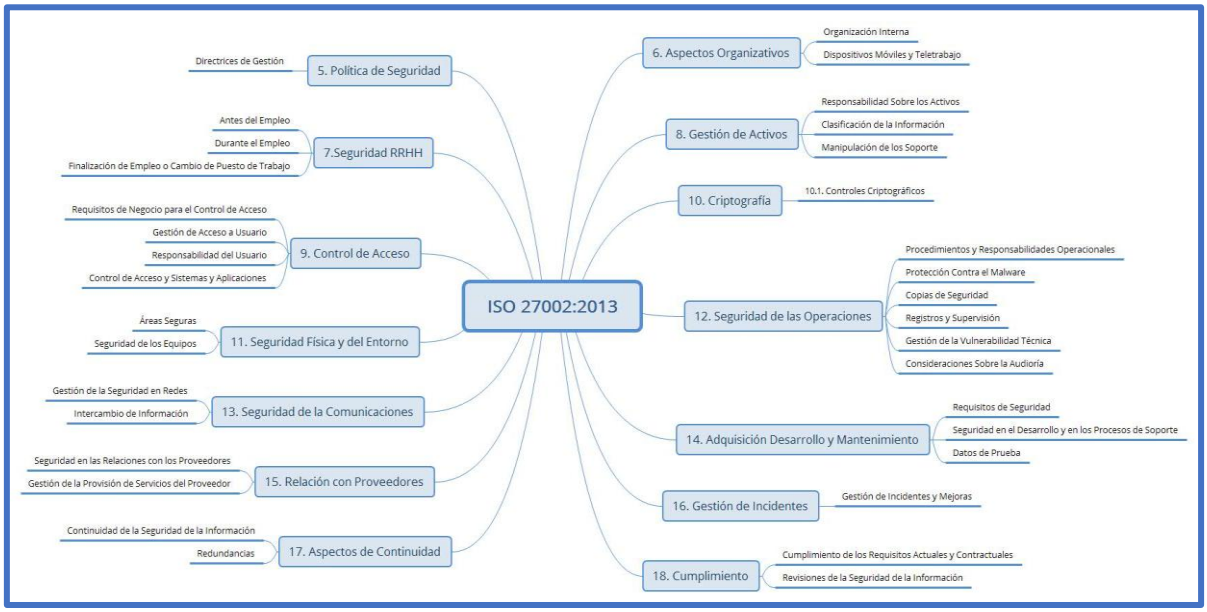

Ilustración 1. Esquema controles ISO/IEC 27002

1 Situación Actual: Contextualización, Objetivos y Análisis diferencial.

La organización objeto de este plan director es una empresa llamada Ícaro S.A.

Ícaro S.A. es una empresa española dedicada al diseño, construcción y mantenimiento de sistemas de control y gestión de plantas solares con sede en Madrid que desempeña su actividad en el territorio nacional.

1.1 Contextualización

1.1.1 Historia de la empresa

Ícaro S.A. nació en el año 2010 de la mano de cuatro compañeros de una reconocida empresa de ingeniería que deciden con sus propios recursos y el apoyo financiero de sus familias fundar su propia empresa.

Esta, se creó con el ánimo de comercializar un sistema que controle y monitorice de forma autónoma plantas solares fotovoltaicas para hacerlas más rentables. Este sistema se denomina Sirio, y es el core de negocio de la empresa.

Durante los dos primeros años se le adjudica a la empresa los primeros contratos que se desarrollan satisfactoriamente, este hecho impulsa a la empresa y le permite invertir en I+D, personal y en ofrecer un servicio de administración y monitorización remota.

En el año 2015 patentan un sistema único de movimiento de placas solares siguiendo la trayectoria del sol denominado Teseo y otro de limpieza autónoma de placas fotovoltaicas denominado Minos.

A principios de 2017, la empresa está negociando con diferentes fondos de inversión para recibir capital destinado a la expansión de la empresa en Europa y Sudamérica.

Sus principales clientes son grandes empresas eléctricas del mercado español, pero con la intención de en el año 2017 firmar contratos con empresas extranjeras.

1.1.2 Organización de la empresa

Actualmente la empresa cuenta con 120 empleado divididos en los diferentes departamentos que se observan en el siguiente organigrama.

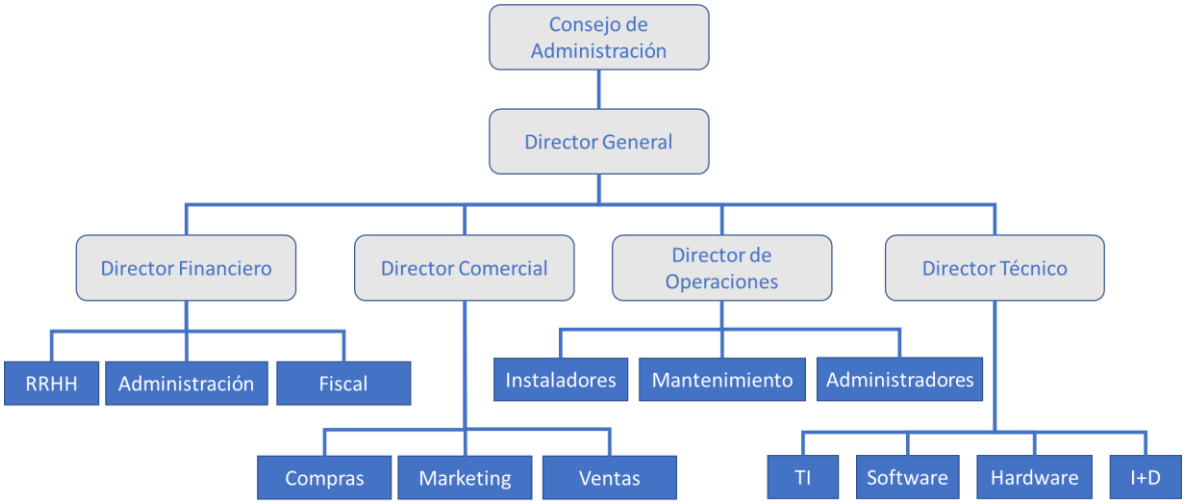

Ilustración 2. Organigrama general de la empresa

Las funciones de la dirección son:

- **Consejo de administración:** está compuesto por los socios fundadores.
- **Director general:** persona de confianza de los socios fundadores que se encarga de las relaciones de la compañía.
- **Director financiero:** se encarga de la gestión de la parte financiera/contable, fiscal y de recursos humanos de la empresa.
- **Director comercial:** se encarga de la gestión de las áreas de compras de materiales y servicios, el marketing de la compañía y la fuerza de ventas.
- **Director de operaciones:** se encarga de gestionar y coordinar con sus grupos técnicos las tareas de instalación de los sistemas de control y mantenimiento de los mismos.
- **Director técnico:** es el encargado de gestionar las áreas de desarrollo de software y hardware de los sistemas, así como los departamentos de T.I. e I+D.

A continuación, se desarrolla los organigramas de la empresa por departamentos:

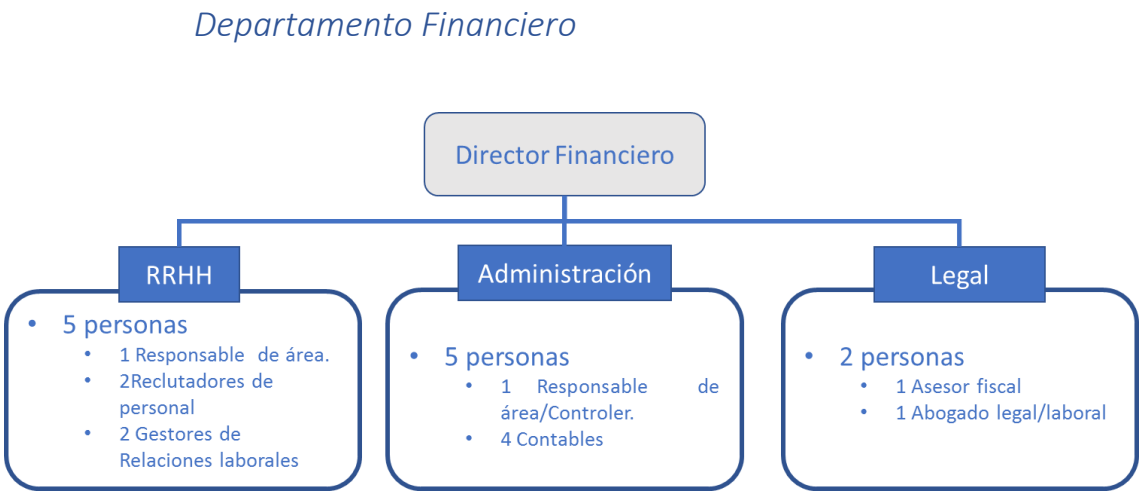

Ilustración 3. Organigrama del departamento financiero.

- El área de Recursos Humanos cuenta con cinco integrantes:
  - Un responsable de área encargado de reportar al director y coordinas el equipo de recursos humanos, además, es el encargado del diseño de los procesos de selección de los nuevos candidatos y de las modificaciones sustanciales en las nóminas de los empleados.
  - Dos reclutadores de personal dedicados a la búsqueda de candidatos y a la realización de los procesos de selección
  - Dos gestores de relaciones laborales dedicados a los trabajos administrativos de RRHH tales como la realización de nóminas, control de permisos, horas extras, etc.
- El área de Administración cuenta con cinco integrantes:
  - Un responsable de área encargado de reportar al director y controlar el estado financiero y contable de la empresa
  - Cuatro contables dedicados a las cuentas globales de la empresa tales como facturas, cobros, balance de caja, etc.
- El área Legal cuenta con dos integrantes:
  - Una persona dedicada a las obligaciones fiscales de la empresa.
  - Una persona dedicada a los contratos con clientes y proveedores, así como todos los temas legales que surgen en el día a día de la empresa.

Departamento Comercial

Ilustración 4. Organigrama del departamento comercial

- El área de Compras cuenta con cinco integrantes:
  - Un responsable de área encargado de reportar al director, coordinar al equipo de compras, y mantener las relaciones y acuerdos comerciales con los proveedores

- Cuatro personas dedicadas a realizar los pedidos a proveedor y mantener es stock de materiales en el volumen requerido en cada momento.

- El área de Marketing cuenta con tres integrantes:
  - Una persona encargada del diseño y mantenimiento de la página web corporativa, el posicionamiento en Internet de la empresa y en redes sociales
  - Dos personas encargadas de la gestión comercial de los productos de la empresa y de recoger las necesidades de los clientes para la modificación y/o diseño de nuevos productos.
- El área de Ventas cuenta con seis integrantes:
  - Un responsable de área que coordina al equipo de venta
  - Cinco comerciales repartidos por territorios a lo largo de la geografía española.

Departamento de Operaciones

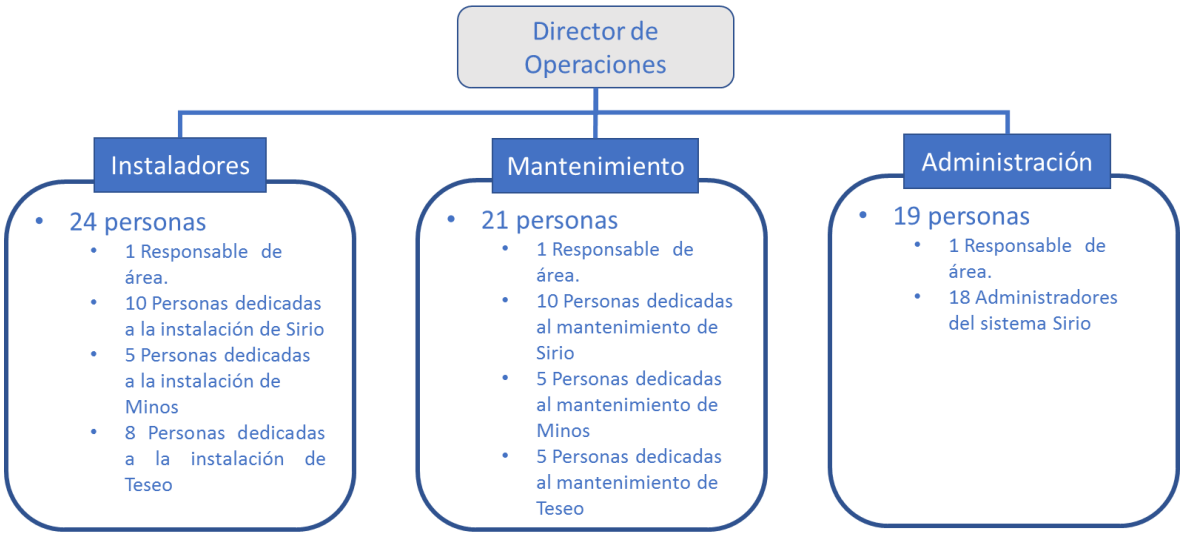

Ilustración 5. Organigrama del departamento de Operaciones

- El área de Instaladores cuenta con veinticuatro integrantes
  - Un responsable de área encargado de reportar al director, coordinar a los equipos de instaladores.
  - Diez personas dedicadas a la instalación del sistema sirio.
  - Cinco personas dedicadas a la instalación del sistema Minos.

- Ocho personas dedicadas a la instalación del sistema Teseo.

- El área de Mantenimiento cuenta con veintiún integrantes:
  - Un responsable de área encargado de reportar al director, coordinar a los equipos de mantenimiento.
  - Diez personas dedicadas al mantenimiento del sistema sirio.
  - Cinco personas dedicadas al mantenimiento del sistema Minos.
  - Cinco personas dedicadas al mantenimiento del sistema Teseo.
- El área de Administradores cuenta con siete integrantes
  - Un responsable de área encargado de coordinar el equipo de administración
  - Seis administradores del sistema software de Sirio.

Departamento Técnico

Ilustración 6. Organigrama del departamento técnico.

- El área de TI cuenta con cinco integrantes
  - Un responsable de área encargado de reportar al director, coordinar al equipo de TI, y gestionar las tareas de parcheado, actualizaciones, etc.
  - Dos personas dedicadas a realizar el mantenimiento de los equipos de puesto de trabajo (PC's, impresoras, móviles, red LAN. Etc.) y sistemas corporativos de CPD
  - Dos personas dedicadas a la administración del sistema hardware y virtualización. Además, colaboran en los sistemas de CPD con los compañeros de puesto de trabajo y sistemas corporativos.
- El área de Software cuenta con siete integrantes:
  - Un responsable de área encargado de reportar al director, coordinar al equipo de Software, y diseñar las arquitecturas software de los productos de la empresa para la personalización de cada cliente.

    - Dos desarrolladores de Frontend (BBDD de los sistemas, llamadas internas, procesamiento de datos de los sensores, etc.)
    - Dos desarrolladores aplicaciones móviles para IOS y Android para la gestión de los productos de forma remota
    - Dos desarrolladores web para para la gestión de los productos vía navegador.
- El área de Hardware cuenta con nueve integrantes:
    - Un responsable de área encargado de reportar al director, coordinar al equipo de Hardware, y diseñar las arquitecturas hardware de los productos de la empresa para la personalización de cada cliente.
    - Dos desarrolladores hardware para las placas de regulación y control de los sistemas.
    - Cuatro integradores destinados a montar los elementos hardware de los productos.
    - Dos personas destinadas a pasar los controles de calidad de los productos antes de pasarlos al departamento de operaciones.
- El área de I+D cuenta con tres integrantes:
    - Un responsable de área que coordina al equipo, reporta al director, diseña nuevos productos y modificaciones y realiza las pruebas de concepto.
    - Un desarrollador que diseña e implementa junto a los demás integrantes de I+D nuevos desarrollos para productos y optimizaciones para los existentes.
    - Un desarrollador hardware que diseña e implementa junto a los demás integrantes de I+D nuevos desarrollos para productos y optimizaciones para los existentes.

A continuación, se presenta una tabla resumen con la totalidad de los empleados a fecha de la redacción de este documento:

Tabla 1. Resumen de empleados por puesto

PUESTO	NÚMERO DE EMPLEADOS
DIRECTOR	5
RESPONSABLE DE ÁREA	12
RECLUTADOR DE PERSONAL	2
GESTOR DE RELACIONES LABORALES	2
CONTABLE	4
ASESOR FISCAL	1
ABOGADO	1
GESTOR DE COMPRAS	4
COMUNITY MANAGER	1
GESTOR DE PRODUCTO	2
COMERCIAL	5
TÉCNICO INSTALADORES	23
TÉCNICO DE MANTENIMIENTO	20
ADMINISTRADOR	18
TÉCNICO DE TI	4
DESARROLLADOR SOFTWARE	7
DESARROLLADOR HARDWARE	3
TÉCNICO DE CALIDAD	2
TÉCNICO ELECTRÓNICA	4
TOTAL	**120**

1.1.3 Instalaciones

Ícaro S.A. cuenta con una sede central en Madrid compuesta por dos plantas y un sótano en contrato de alquiler.

En estas dos plantas se distribuyen la mayoría de los empleados excluyendo una gran parte del personal de operaciones en unos 70 puestos de trabajo divididos por departamentos. Estos puestos están conectados a una red de área local 802.1X que no exige ninguna autenticación. Adicionalmente, las dos plantas cuentan con una Red Wifi con encriptación WPA2-PSK y filtrado MAC. No existe Wifi de invitados.

En el Sótano se sitúa el CPD y plazas de aparcamientos para los perfiles de responsabilidad.

Adicionalmente a las oficinas mencionadas, la empresa cuenta con una nave industrial en propiedad a las afueras de Madrid. En ella, se realizan las tareas de montaje y mantenimiento de los sistemas y es la base del personal de operaciones y mantenimiento. Cuenta con una pequeña área de oficinas con 10 puestos. Estos puestos están conectados a una red de área local 802.1X que no exige ninguna autenticación. Adicionalmente, la nave cuenta con una Red Wifi con encriptación WPA2-PSK y filtrado MAC. No existe Wifi de invitados.

Referente a los despliegues del sistema Sirio, se considera instalaciones propiedad de Ícaro S.A. los armarios que albergan el hardware del sistema de cada una de las plantas que se monitorizan. A continuación, se presenta una tabla con las ubicaciones y un mapa.

Tabla 2. Ubicaciones plantas fotovoltaicas

PLANTA	PROVINCIA
Almendralejo	Badajoz
Puertollano	Ciudad Real
Olmedilla De Alarcón	Cuenca
Arnedo	La Rioja
Las Gabias	Granada
Jumilla	Murcia
Lorca	Murcia
Olivenza	Badajoz
Calasparra	Murcia
Beneixama	Alicante
Salamanca	Salamanca
El Coronil	Sevilla
Almaraz	Cáceres
El Bonillo	Albacete
Guadarranque	Cádiz

Ilustración 7. Mapa ubicaciones plantas fotovoltaicas

1.1.4 Equipamiento Informático

Los equipos de puesto de trabajo de Ícaro, están diferenciados en tres tipos:

- Tipo A: Equipo de Sobremesa
  - DELL OptiPlex 3040 3.3GHz G4400
  - 500 Gb disco Duro
  - 8 Gb de RAM
  - Pantalla LED de 19”
  - Teclado + Ratón USB
  - Windows 7 Enterprise Edition
- Tipo B: Equipo Portátil
  - HP ProBook 640 i5-4300M
  - 500 Gb disco Duro
  - 4 Gb de RAM
  - Pantalla LED de 15,6”
  - Teclado + Ratón USB
  - Windows 7 Enterprise Edition
- Tipo C: Tableta/Laptop
  - Microsoft Surface 4 Pro Intel Core i5
  - 128 Gb disco duro SSD
  - 4 Gb de RAM
  - Pantalla LED de 12.3"
  - Microsoft Windows 10 Pro

A continuación, se presenta una tabla con el número de equipos diferenciados por Rol y Tipo:

Tabla 3. Equipamiento informático por tipo y puesto

PUESTO	TIPO	NÚMERO
DIRECTOR	C	5
RESPONSABLE DE ÁREA	C	12
RECLUTADOR DE PERSONAL	B	2
GESTOR DE RELACIONES LABORALES	A	2
CONTABLE	A	4
ASESOR FISCAL	C	1
ABOGADO	C	1
GESTOR DE COMPRAS	A	4
COMUNITY MANAGER	C	1
GESTOR DE PRODUCTO	C	2
COMERCIAL	C	5
ADMINISTRADOR	A	23
TÉCNICO DE TI	A	20
DESARROLLADOR SOFTWARE	A	18
DESARROLLADOR HARDWARE	A	4
TÉCNICO DE CALIDAD	B	7
TÉCNICO ELECTRÓNICA	A	3
DIRECTOR	C	2
RESPONSABLE DE ÁREA	C	4
TOTAL		**77**

A nivel de control de acceso, todos los equipos están bajo el mismo dominio de directorio activo y la gestión de contraseñas y permisos se realiza a través del mismo. El acceso al dominio es posible únicamente dentro de las oficinas centrales, no existiendo conexión remota.

A nivel de seguridad y parcheado todos ellos cuentan con el antivirus TrendMicro Bussiness Security y se realizan las actualizaciones de sistema operativo mensualmente orquestado por un servidor central para tal fin.

Además, la empresa cuenta con dos fotocopiadoras multifunción Kyocera TaskAlfa 3051ci en modo pago por uso ofrecidas por un Partner local.

Una se encuentra en las oficinas centrales y la otra en la nave de montaje.

1.1.5 Centro de procesamiento de datos

Cómo se ha comentado en el apartada de Instalaciones, Ícaro S.A. cuenta con un CPD en el sótano del edificio donde tiene sus oficinas centrales.

A continuación, se describen unas características generales del mismo:

- Única ubicación. (No se dispone de CPD de contingencia)

- Acceso mediante tarjeta de proximidad y código PIN.
- Equipamiento de refrigeración por aire frio forzado
- Equipos para el control de la temperatura y humedad
- Sistemas de extinción de incendios.
- Circuito cerrado de TV con grabación 24x7 y retención de las grabaciones de 72 horas.
- Dispositivos de suministro eléctrico ininterrumpido con capacidad para 15 minutos que a su vez se encuentra conectado a una línea de fuerza de emergencia facilitada por el proveedor del edificio que está alimentada por generadores eléctricos diésel.

En este CPD se alojan tanto los sistemas que ofrecen servicio de negocio (BBDD, servidores, etc.) de los sistemas que comercializa la empresa como los que ofrecen servicio a los usuarios de las oficinas (ERP, Servidor de Fichero, DA)

En la siguiente imagen se muestra el esquema lógico de los activos del CPD:

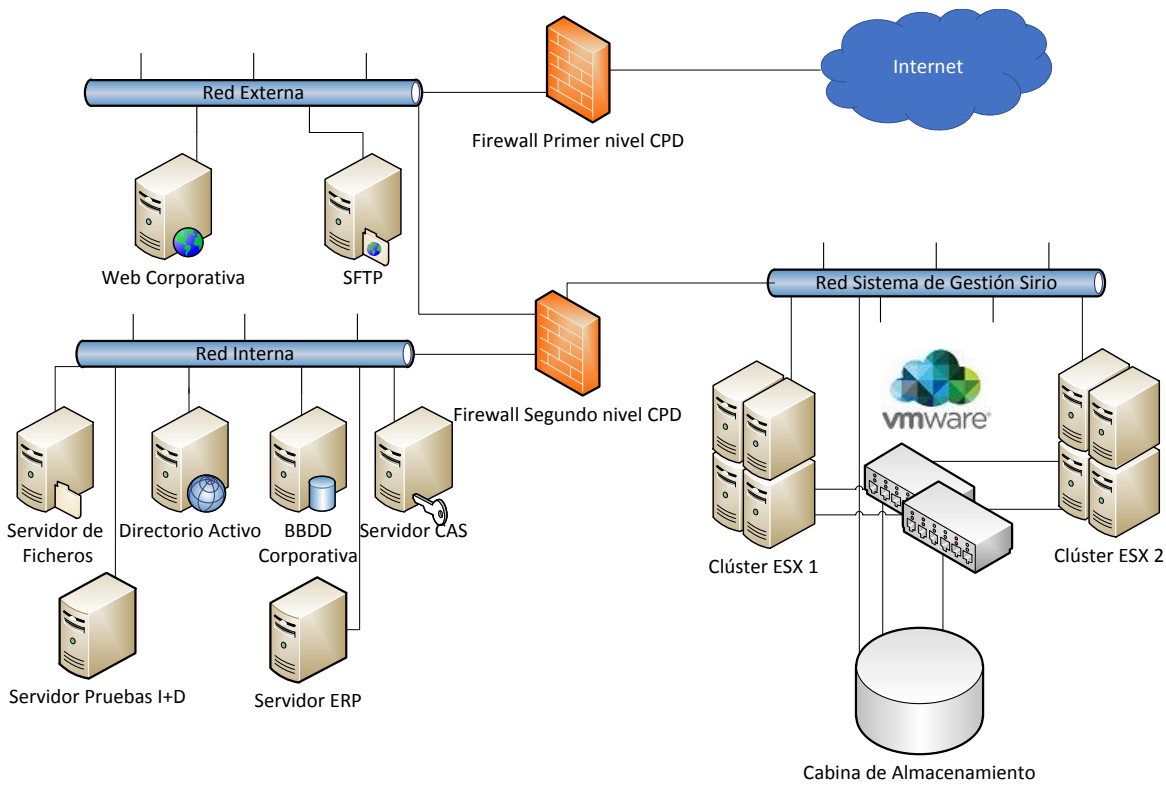

Ilustración 8. Esquema lógico del CPD

Cómo acceso de comunicaciones al CPD se encuentra un firewall de primer nivel Cisco ASA 5520 donde se conecta la red externa y el firewall de segundo nivel Cisco ASA 5505. A este último firewall se conecta la red interna de empleados y la del sistema de gestión Sirio.

En general el reparto lógico del CPD es el siguiente:

- Red Externa:
  - Servidor Web Corporativo que publica la web de la empresa
  - Servidor SFTP para acceso externo a determinados archivos.
- Red Interna:
  - Servidor de ficheros CIFS para los empleados de la oficina.
  - Directorio activo de la empresa con base LDAP.
  - BBDD corporativa. Da servicio a todos los grupos de la empresa (Financiero, Operaciones, Técnica, etc.)
  - Servidor CAS para el uso de Single Sign On
  - Servidor de pruebas del personal de I+D
  - Servidor ERP de la empresa. (Gestión de proveedores, RRHH, Clientes, Almacén, etc.)
- Red de Sistema de Gestión Sirio:
  - Clúster 1 de servidores ESX de VMware donde corren actualmente unas 60 Máquinas virtuales.
  - Clúster 2 de servidores ESX de VMware con la misma volumetría que el anterior que sirve como entorno de desarrollo e integración además de proporcional alta disponibilidad en caso de fallo del primer clúster.
  - Cabina de Almacenamiento SAN y NAS para el Sistema de Gestión Sirio. Ofrece almacenamiento de bloque y de fichero a las máquinas virtuales. La cabina cuenta con un sistema redundancia que soporta el fallo simultáneo de tres discos al mismo tiempo y el fallo de una de las dos controladoras. Además, realiza backups mediante Snapshot a proveedor externo. Una copia full semanal y una incremental diaria. La retención de la copia semanal es de un mes y la diaria de dos semanas.
  - Switches FC redundados para la conexión entre los servidores.

1.1.6 Comunicaciones

Datos

Las oficinas centrales cuentan con dos accesos FTTH de 300Mb, conectado a estos dos accesos se encuentra un servidor con el aplicativo PfSense (Firewall Software OpenSource) que hace las funciones de Firewall + Balanceador. Debajo del este equipo se encuentras dos switches (uno por planta) para el acceso a la red de los usuarios mediante cable y la conexión a los AP.

Además de lo anterior, los equipos FTTH dan acceso a Internet al CPD a través de un Firewall + Balanceador Cisco ASA 5520.

Para la nave, se cuenta con un acceso FTTH de 300 Mb que da servicio a través de un firewall de igual características al de empleados de las oficinas centrales.

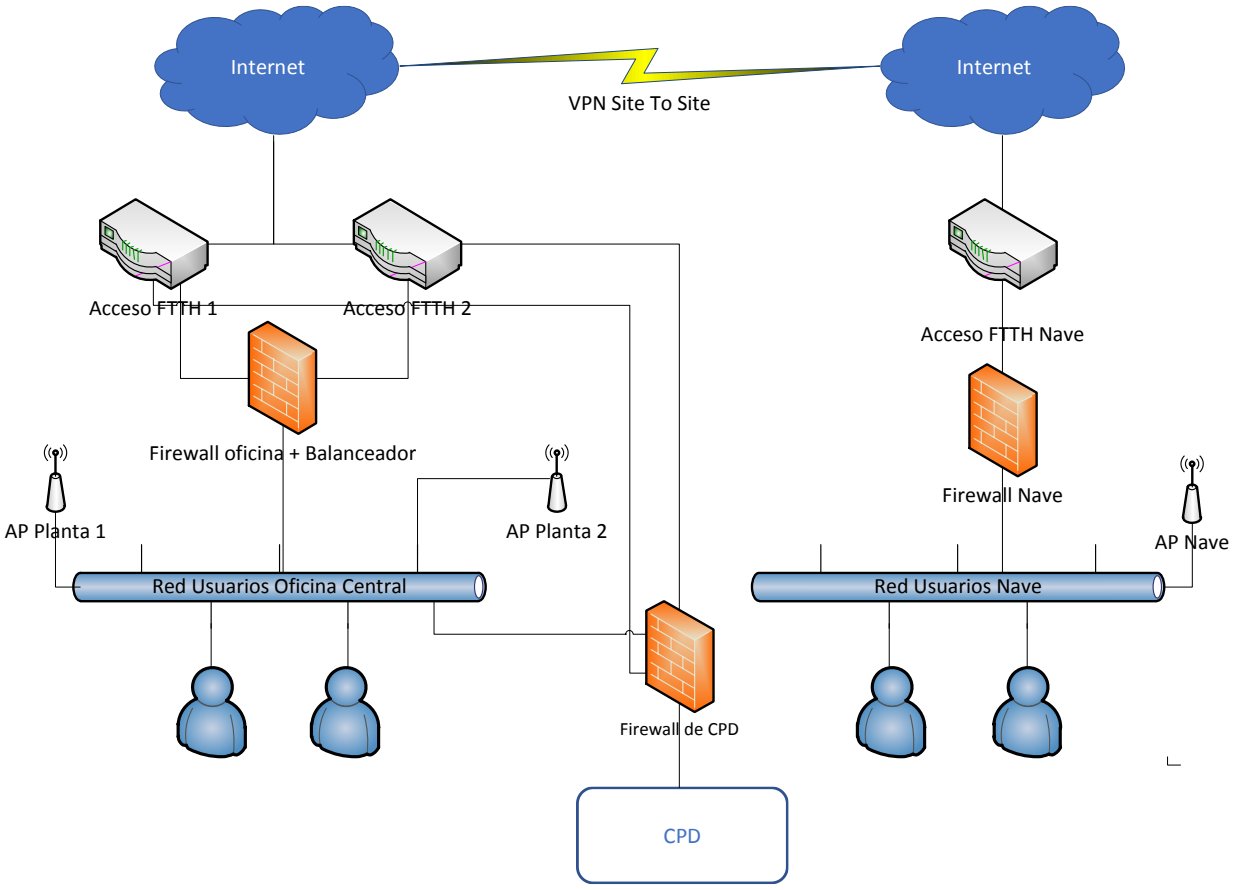

Ilustración 9. Esquema de comunicaciones

Voz Fija

Para la parte de voz fija la empresa cuenta con un servicio de centralita ofrecido por un operador de telecomunicaciones que por una parte con una numeración da servicio al personal de oficina y con otra de servicio al CAU (Centro de Atención a Usuarios) para recoger las posibles incidencias vía teléfono de las plantas solares gestionadas por la empresa.

Voz Móvil

Respecto a la planta de voz móvil está se encuentra diferenciada por tipo de usuario.

- Tipo A:
  - Contrato con 200 minutos de voz y 2 Gb de datos
  - Terminal gama media/baja Android (Ejemplo Huawei P8 Lite)
- Tipo B:
  - Contrato con minutos ilimitados de voz y 4 Gb de datos.
  - Terminal gama media/ Alta Android (Ejemplo Huawei Mate 8)
- Tipo C:
  - Contrato con minutos ilimitados de voz y 8 Gb de datos.
  - Terminal gama alta Android/Apple (Ejemplo: Samsung S7/IPhone 7)

A continuación, se presenta una tabla con el número contratos de voz móvil diferenciados por Rol y Tipo

Tabla 4. Contratos telefonía móvil

PUESTO	TIPO	NÚMERO
DIRECTOR	C	5
RESPONSABLE DE ÁREA	C	12
RECLUTADOR DE PERSONAL	B	2
GESTOR DE RELACIONES LABORALES	A	2
ASESOR FISCAL	C	1
ABOGADO	C	1
GESTOR DE COMPRAS	B	4
COMUNITY MANAGER	B	1
GESTOR DE PRODUCTO	B	2
COMERCIAL	C	5
TÉCNICO INSTALADORES	A	23
TÉCNICO DE MANTENIMIENTO	A	20
TÉCNICO DE TI	A	4
TOTAL		**82**

1.1.7 Alcance

El propósito del presente plan director es adecuar a la norma de referencia ISO/IEC 27001 y 27002, todos los activos, procesos y procedimientos organizativos y técnicos que intervienen de alguna forma en la gestión de la información de Ícaro S.A.

Por ello quedan definido dentro del alcance de este plan:

- Los activos relativos al tratamiento de la información que dan soporte a los servicios que ofrece Ícaro S.A y a los procesos internos de la empresa.
- Los propios procesos y procedimientos organizativos y técnicos relativos al tratamiento de la información.
- Los sistemas y procesos de intercambio de información que dan soporte a los servicios que ofrece Ícaro S.A. y a los procesos internos de la empresa.
- El personal interno y externo de la organización que tiene acceso a algún activo, proceso o procedimiento de Ícaro S.A., relativo al tratamiento de la información.

En definitiva, el alcance del presente son todos los sistemas de información que dan soporte a los procesos, actividades y servicios de la empresa mencionados y que son llevados a cabo y ofrecidos por la organización, de acuerdo a la declaración de aplicabilidad vigente.

1.2 Objetivos de seguridad de la información

La empresa desde su creación ha tenido una dependencia muy fuerte de los sistemas de información. Con el crecimiento que ha experimentado en los últimos años esta dependencia se ha agravado, haciendo que el futuro de la misma se pueda ver muy comprometido en el caso de que una amenaza se seguridad se produzca.

Este hecho, no ha pasado desapercibida por el consejo de administración que ha encargado el presente plan director para alcanzar los siguientes objetivos:

- Asegurar el cumplimiento de los acuerdos de niveles de servicio de gestión de plantas solares en horario 24x7 que tiene la empresa con sus clientes.
- Adecuar los sistemas de información y comunicación para soportar la expansión de la compañía a Europa y Sudamérica.
- Poner en marcha el plan de mejora continuo que establece la norma ISO/IEC 27001 para así obtener su certificación.
- Poder superar auditorías de segunda parte procedentes de clientes e inversores referente a la seguridad de la información y de las comunicaciones.

1.3 Análisis Diferencial

En esta sección se realizará el análisis diferencial con respecto la ISO/IEC 27002, este análisis nos permitirá conocer de manera global el estado actual de la empresa en relación a los requisitos que establece la norma para un Sistema de Gestión de la Seguridad de la Información.

Para elaborar este análisis se utiliza el modelo de madurez de la capacidad de los procesos de la norma ISO/IEC 15504 usado para determinar la capacidad de mejora de los sistemas de información y productos software.

A continuación, se muestra una tabla explicativa con la escala de madurez usada para la evaluación del cumplimiento de los controles establecidos en la norma ISO/IEC 27002.

Tabla 5. Modelo de Madurez

Nivel	Estado	Madurez	Descripción
Nivel 0	Incompleto	0%	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso
Nivel 1	Ejecutado	10%	El proceso está implementado y alcanza su propósito básico.
Nivel 2	Gestionado	50%	El proceso ejecutado, está implementado de forma gestionada y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
Nivel 3	Establecido	90%	El proceso gestionado, está implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (Se documenta, se comunica y se da formación).
Nivel 4	Predecible	95%	El proceso establecido descrito anteriormente, ahora se ejecuta dentro de los límites definidos para alcanzar sus resultados de proceso.
Nivel 5	Optimizado	100%	El proceso descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.

Una vez contrastados los controles de la norma ISO/IEC 27002 con los controles que se aplican actualmente en la empresa se extraen las siguientes conclusiones.

- La empresa tiene implantados 40 de los 114 controles que establece la norma, lo que se traduce en una implantación del 35%
- El porcentaje de madurez media de todos los grupos de controles según la escala de madurez de la norma ISO/IEC 15504 es del 23%.

A continuación, se muestra una tabla que indica el número de controles implantados y la media de madurez de los mismos separados por dominios.

Tabla 6. Madurez de los controles implantados

DOMINIO	MADUREZ	CONTROLES IMPLANTADOS
5. Políticas de Seguridad	10%	1 de 2
6. Organización de la Seguridad	35%	2 de 7
7. Seguridad RRHH	30%	4 de 6
8. Gestión de Activos	40%	4 de 10
9. Control de Accesos	30%	6 de 14
10. Criptografía	0%	0 de 2
11. Seguridad Física y del entorno	70%	6 de 15
12. Seguridad de las Operaciones	30%	8 de 14
13. Seguridad de las Comunicaciones	30%	2 de 7
14. Adquisición, desarrollo, y mantenimiento.	18%	5 de 14
15. Relación con los proveedores	0%	0 de 5
16. Gestión de Incidentes	0%	0 de 7
17. Gestión de la Continuidad del Negocio	0%	0 de 4
18. Cumplimiento	10%	2 de 7

En las siguientes imágenes se puede observar los valores representados en la tabla de forma gráfica.

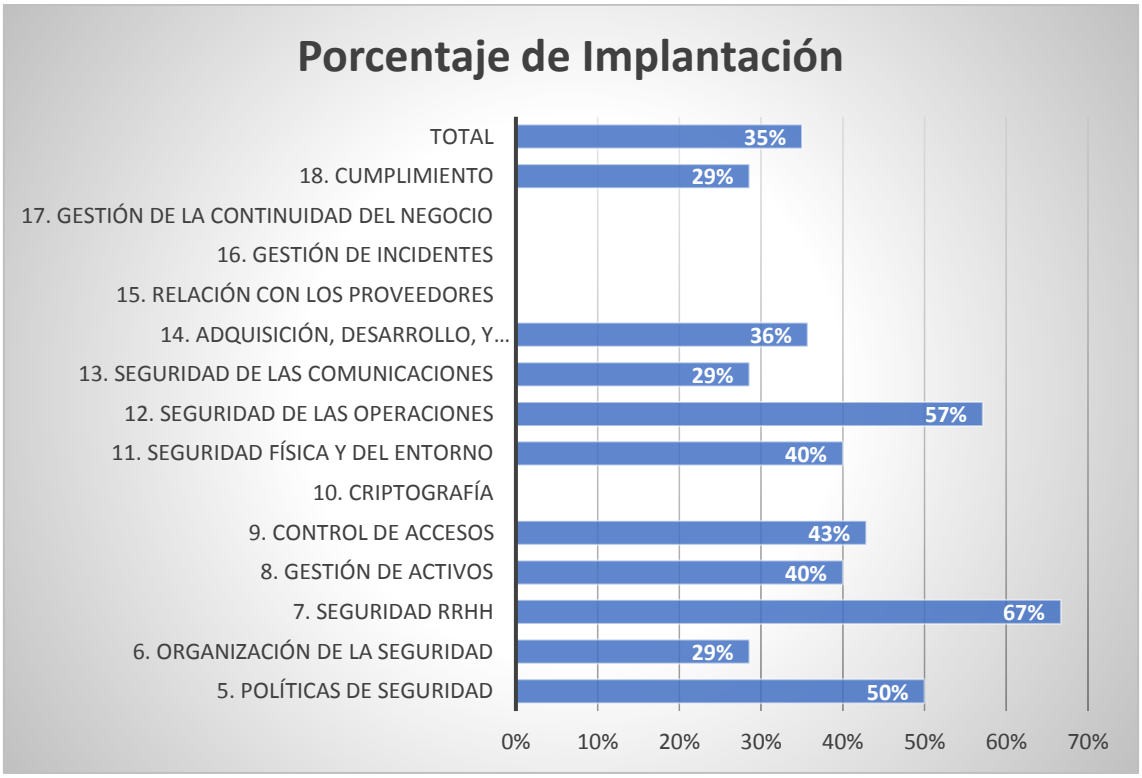

Ilustración 10. Gráfica de porcentaje de implantación

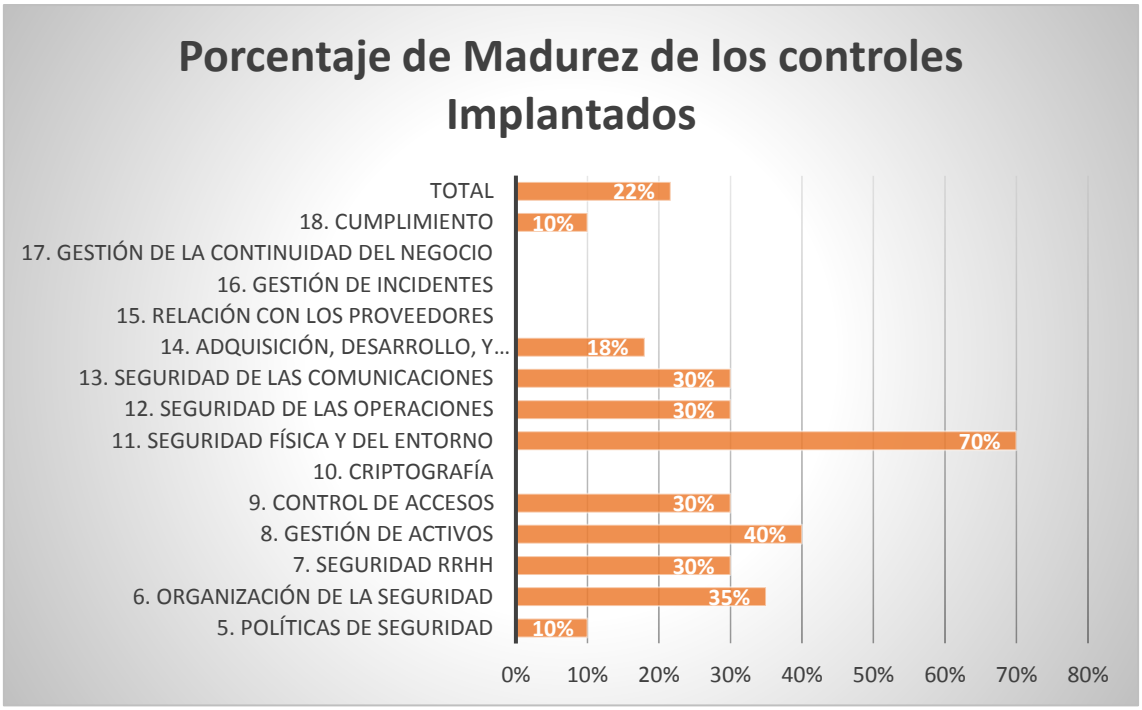

Ilustración 11. Gráfica de porcentaje de madurez de los controles implantados

Como se puede ver en la tabla y los gráficos anteriores, la empresa presenta en la actualidad una implantación baja (35% de los 114 controles) frente a la norma ISO/IEC 27002 y una madurez de los controles ya implantados aún más baja (22%).

2 Sistema de Gestión Documental

2.1 Introducción

Para alcanzar los objetivos de un SGSI es necesario que el mismo esté apoyado por un proceso sistemático, documentado y que sea difundido a toda la organización. Esto significa que en nuestro SGSI debe tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

A continuación, se listan los documentos de la norma que serán objetivo del presente pliego y que serán explicados en el siguiente apartado:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

La existencia de todos estos documentos constituye la evidencia palpable de que el Sistema de Gestión está funcionando.

2.2 Esquema documental

2.2.1 Política de Seguridad

La política de seguridad de la información es el documento donde se establecen los principios y líneas de actuación globales en cuestiones de seguridad de la información de la empresa, alineados con los objetivos del negocio de la misma, plasmando el compromiso que tiene la Dirección con la seguridad de la información.

Es un documento que debe ser conocido por todo el personal de la empresa, por lo que debe estar escrito en un modelo a alto nivel que evite los tecnicismos y las ambigüedades en su redacción, así mismo su disponibilidad debe ser total.

Al igual que el resto de documentos del SGSI, debe ser revisado periódicamente y aprobado por la Dirección de la empresa.

En el ANEXO A, se encuentra la política de seguridad de la empresa objetivo.

2.2.2 Procedimiento de auditorías internas

El propósito del documento de procedimiento de auditoría interna es incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación para verificar que todos los aspectos del SGSI funcionan como se diseñaron y para ser correctamente evolucionados llegado el caso. Además, los requisitos que se establecen a los auditores internos y los modelos de informe de auditoría.

Esto ayudará a asegurar que no sólo se apliquen políticas y procedimientos y que se puedan recopilar y aplicar las mejores prácticas.

En el ANEXO B, se encuentra la política de seguridad de la empresa objetivo.

2.2.3 Gestión de indicadores

Para que el SGSI se mantenga vivo, es necesario definir un sistema de indicadores que permita medir la eficacia y eficiencia de los controles de seguridad implantados en la empresa al igual que es importante definir el sistema para medir el nivel de implementación y madurez alcanzado respectos a los objetivos marcados. Para disponer de esta información, es imprescindible implantar indicadores que nos provean de información para poder valorar.

Para obtener esta información se plantean dos tipos de gestión de indicadores:

- Gestión de indicadores de los controles implantados referentes a la norma ISO/IEC 27002:2013 que necesiten de revisión

- Gestión de indicadores de evolución de cumplimiento de los objetivos propuestos por la dirección.

En el ANEXO C, se encuentra la gestión de indicadores de la empresa.

2.2.4 Procedimiento de revisión por dirección.

Para que la implementación de un Sistema de Gestión de la información no sea un fracaso, debe contar con el apoyo incondicional de la Dirección. Por ello, es imprescindible que la propia Dirección proporcione los medios y el apoyo para promover los cambios de gestión, tecnológicos y culturales para el éxito del SGSI.

En línea con lo expuesto en el párrafo anterior, la dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al SGSI. 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.

Es objetivos es por tanto la elaboración de un documento donde se especifique el procedimiento o acciones que debe llevar a cabo la Dirección de la empresa para la revisión del SGSI. La consecución de esta revisión, garantiza que SGSI implantado se ajuste a los cambios que afecten a la empresa y a los requisitos de negocio de la misma, además, de esta manera se demuestra su eficacia.

En el ANEXO D, se encuentra el procedimiento de revisión por parte de la Dirección.

2.2.5 Gestión de roles y responsabilidades

La seguridad de la información de la empresa sería muy poco eficaz si no tiene claro quién tiene autoridad, sobre qué aspectos y quién es responsable de qué tareas o ámbitos. Por tanto, se hace necesario crear una estructura interna con responsabilidad directa sobre la seguridad de la información.

Por las razones anteriormente expuestas se crea un Comité de Seguridad. Este comité tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema.

Debe estar compuesto al menos por una persona de Dirección, para que de esta manera la implicación, la autoridad y las decisiones que se tomen estén respaldadas por alguien de Dirección. La asignación de esta persona es una manera de avanzar ya que existe alguien para la que la seguridad de la información es una prioridad.

A parte de este comité, un rol que se hace muy necesario es el de Responsable de Seguridad.

En el ANEXO E, se encuentra descrito la gestión de roles y responsabilidades.

2.2.6 Metodología de análisis de riesgos

La 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.

Ícaro S.A. utilizará MAGERIT como metodología de análisis de riesgos. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos. Con posterioridad ha sido aplicable a cualquier organización.

Esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente.

En el ANEXO F, se encuentra descrita la metodología de análisis de riesgos.

2.2.7 Declaración de aplicabilidad

Documento que incluye todos los controles de Seguridad establecidos en la Organización basados en la norma ISO/IEC 27002:2013, con el detalle de su aplicabilidad y estado.

En el ANEXO G, se encuentra descrita la metodología de análisis de riesgos.

3 Análisis de riesgos

3.1 Introducción

El análisis de riesgos es la más importante del ciclo de vida de la gestión de la seguridad de la información, ya que nos servirá para descubrir que carencias de seguridad tiene la empresa tras detectar cuales son las vulnerabilidades, así como las amenazas a las que está expuesta.

En esta fase en primer lugar se identifican los activos de la empresa relacionados con la seguridad de la información cuyo objetivo del SGSI es protegerlos y se calcula su valor. Después, se identifican las amenazas que pueden afectar a los activos de la empresa y las vulnerabilidades que hacen que estas amenazas deriven en un incidente de seguridad.

Una vez obtenida la información anterior, se procede a estudiar la gestión del riesgo determinando el impacto potencial que tendría la materialización de las amenazas encontradas sobre los activos identificados y se calculará el nivel de riesgo aceptable y el riesgo residual.

3.2 Inventario de activos

Para MAGERIT un activo se define como:

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

En este apartado se muestran un inventario de los activos relacionados con la seguridad de la información de Ícaro S.A. clasificados acorde a la metodología MAGERIT v.3. Libro II. Se muestran en la siguiente tabla:

Tabla 7. Tipos de activos según MAGERIT

Tipo de Activo	Descripción
Instalaciones [L]	Lugares donde se hospedan los sistemas de información y comunicaciones
Hardware [HW]	Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Software [SW]	Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
Datos[D]	La información que permite a la organización prestar sus servicios

Redes de comunicaciones [COM]	Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros
Equipamiento Auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con éstos.
Personal [P]	Personas relacionadas con los sistemas de información.
Soportes de información [Media]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

En base a la clasificación de la tabla anterior se han identificado los siguientes activos en Ícaro S.A.:

Tabla 8. Inventario de activos

Ámbito	ID	Activo
Instalaciones [L]	L1	Centro de proceso de Datos
	L2	Sala de departamento de RRHH
	L3	Sala departamento de administración
	L4	Despacho de departamento de Legal
	L5	Sala de departamento comercial
	L6	Sala administradores sistema Sirio
	L7	Sala de departamento de TI
	L8	Sala de departamento de desarrollo software
	L9	Sala de departamento de desarrollo hardware
	L10	Sala de departamento de I+D
	L11	Oficina nave de operaciones
	L12	Despacho del director general
	L13	Despacho del director financiero
	L14	Despacho del director de operaciones
	L15	Despacho del director técnico
	L16	Armario técnico planta fotovoltaica de Almendralejo [BA]

	L17	Armario técnico planta fotovoltaica de Puertollano [CR]
	L18	Armario técnico planta fotovoltaica de Olmedilla de Alarcón [CU]
	L19	Armario técnico planta fotovoltaica de Arnedo [RI]
	L20	Armario técnico planta fotovoltaica de Las Gabias [GR]
	L21	Armario técnico planta fotovoltaica de Jumilla [MU]
	L22	Armario técnico planta fotovoltaica de Lorca [MU]
	L23	Armario técnico planta fotovoltaica de Olivenza [BA]
	L24	Armario técnico planta fotovoltaica de Calasparra [MU]
	L25	Armario técnico planta fotovoltaica de Beneixama [A]
	L26	Armario técnico planta fotovoltaica de Salamanca [SA]
	L27	Armario técnico planta fotovoltaica de El Coronil [SE]
	L28	Armario técnico planta fotovoltaica de Almaraz [CC]
	L29	Armario técnico planta fotovoltaica de El Bonillo [ALB]
	L30	Armario técnico planta fotovoltaica de Guadarranque [CA]
Hardware [HW]	HW1	Servidor 1 granja virtualización sistema Sirio
	HW2	Servidor 2 granja virtualización sistema Sirio
	HW3	Servidor 3 granja virtualización sistema Sirio
	HW4	Servidor 4 granja virtualización sistema Sirio
	HW5	Servidor 5 granja virtualización sistema Sirio
	HW6	Servidor 6 granja virtualización sistema Sirio
	HW7	Servidor 7 granja virtualización sistema Sirio
	HW8	Servidor 8 granja virtualización sistema Sirio
	HW9	Switch SAN 1
	HW10	Switch SAN 2
	HW11	Cabina de Almacenamiento
	HW12	Switch Ethernet Red de Gestión Sirio
	HW13	Switch Ethernet Red Externa
	HW14	Switch Ethernet Red Interna

	HW15	Switch Ethernet 1 Oficina Principal
	HW16	Switch Ethernet 2 Oficina Principal
	HW17	Switch Ethernet Nave
	HW18	AP 1 Oficina Central
	HW19	AP 2 Oficina Central
	HW20	AP Nave
	HW21	Router FTTH Oficina 1
	HW22	Router FTTH Oficina 2
	HW23	Router FTTH Nave
	HW24	Firewall Nave
	HW25	Firewall segundo nivel CPD
	HW26	Firewall primer nivel CPD
	HW27	Firewall de Oficina
	HW28	Servidor SFTP
	HW29	Servidor Web Corporativa
	HW30	Servidor de Ficheros
	HW31	Servidor de Directorio Activo
	HW32	Servidor de BBDD corporativa
	HW33	Servidor CAS
	HW34	Servidor de I+D
	HW35	Servidor ERP
	HW36	Impresora de red planta 1 Oficina central
	HW37	Impresora de red planta 2 Oficina central
	HW38	Impresora de red Nave de operaciones
	HW39	PC's tipo A (46 dispositivos)
	HW40	PC's tipo B (4 dispositivos)
	HW41	PC's tipo C (27 dispositivos)
	HW42	Móvil tipo A (49 dispositivos)
	HW43	Móvil tipo B (9 dispositivos)
	HW44	Móvil tipo C (24 dispositivos)

	HW45	Placa Base Sirio planta fotovoltaica de Almendralejo [BA]
	HW46	Placa Base Sirio planta fotovoltaica de Puertollano [CR]
	HW47	Placa Base Sirio planta fotovoltaica de Olmedilla de Alarcón [CU]
	HW48	Placa Base Sirio planta fotovoltaica de Arnedo [RI]
	HW49	Placa Base Sirio planta fotovoltaica de Las Gabias [GR]
	HW50	Placa Base Sirio planta fotovoltaica de Jumilla [MU]
	HW51	Placa Base Sirio planta fotovoltaica de Lorca [MU]
	HW52	Placa Base Sirio planta fotovoltaica de Olivenza [BA]
	HW53	Placa Base Sirio planta fotovoltaica de Calasparra [MU]
	HW54	Placa Base Sirio planta fotovoltaica de Beneixama [A]
	HW55	Placa Base Sirio planta fotovoltaica de Salamanca [SA]
	HW56	Placa Base Sirio planta fotovoltaica de El Coronil [SE]
	HW57	Placa Base Sirio planta fotovoltaica de Almaraz [CC]
	HW58	Placa Base Sirio planta fotovoltaica de El Bonillo [ALB]
	HW59	Placa Base Sirio planta fotovoltaica de Guadarranque [CA]
	HW60	Actuadores planta fotovoltaica de Almendralejo [BA] (200 sensores)
	HW61	Actuadores planta fotovoltaica de Puertollano [CR] (1333 sensores)
	HW62	Actuadores planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)
	HW63	Actuadores planta fotovoltaica de Arnedo [RI] (300 sensores)
	HW64	Actuadores planta fotovoltaica de Las Gabias [GR] (550 sensores)
	HW65	Actuadores planta fotovoltaica de Jumilla [MU] (112 sensores)
	HW66	Actuadores planta fotovoltaica de Lorca [MU] (173 sensores)

	HW67	Actuadores planta fotovoltaica de Olivenza [BA] (200 sensores)
	HW68	Actuadores planta fotovoltaica de Calasparra [MU] (226 sensores)
	HW69	Actuadores planta fotovoltaica de Beneixama [A] (80 sensores)
	HW70	Actuadores planta fotovoltaica de Salamanca [SA] (125 sensores)
	HW71	Actuadores planta fotovoltaica de El Coronil [SE] (89 sensores)
	HW72	Actuadores planta fotovoltaica de Almaraz [CC] (255 sensores)
	HW73	Actuadores planta fotovoltaica de El Bonillo [ALB] (629 sensores)
	HW74	Actuadores planta fotovoltaica de Guadarranque [CA] (136 sensores)
	HW75	Sensores Sirio planta fotovoltaica de Almendralejo [BA] (200 sensores)
	HW76	Sensores Sirio planta fotovoltaica de Puertollano [CR] (1333 sensores)
	HW77	Sensores Sirio planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)
	HW78	Sensores Sirio planta fotovoltaica de Arnedo [RI] (300 sensores)
	HW79	Sensores Sirio planta fotovoltaica de Las Gabias [GR] (550 sensores)
	HW80	Sensores Sirio planta fotovoltaica de Jumilla [MU] (112 sensores)
	HW81	Sensores Sirio planta fotovoltaica de Lorca [MU] (173 sensores)
	HW82	Sensores Sirio planta fotovoltaica de Olivenza [BA] (200 sensores)
	HW83	Sensores Sirio planta fotovoltaica de Calasparra [MU] (226 sensores)
	HW84	Sensores Sirio planta fotovoltaica de Beneixama [A] (80 sensores)
	HW85	Sensores Sirio planta fotovoltaica de Salamanca [SA] (125 sensores)

	HW86	Sensores Sirio planta fotovoltaica de El Coronil [SE] (89 sensores)
	HW87	Sensores Sirio planta fotovoltaica de Almaraz [CC] (255 sensores)
	HW88	Sensores Sirio planta fotovoltaica de El Bonillo [ALB] (629 sensores)
	HW89	Sensores Sirio planta fotovoltaica de Guadarranque [CA] (136 sensores)
Software [SW]	SW 1	Software principal sistema Sirio
	SW 2	Software sensores sistema Sirio
	SW 3	Software en desarrollo de I+D (3 unidades)
	SW 4	Sistema Operativos Windows 7 Enterprise Edition (50 unidades)
	SW 5	Sistema Operativo Windows 10 Pro (27 unidades)
	SW 6	Sistema Operativo Ubuntu Desktop (8 Unidades)
	SW 7	Sistema Operativo Debian (10 Unidades)
	SW 8	Sistema Operativo Android (70 Unidades)
	SW 9	Sistema Operativo iOS (12 Unidades)
	SW 10	Sistema Operativo CentOS (3 Unidades)
	SW 11	Sistema Operativo Ubuntu Server (3 Unidades)
	SW 12	Sistema Operativos Windows Server R2 2012 Enterprise Edition (26 Unidades)
	SW 13	Sistema Operativo DataOntap 8.3.5
	SW 14	SQL Server 2012 Enterprise Edition (6 unidades)
	SW 15	María DB (3 Unidades)
	SW 16	VMware vSphere 6.3 Enterprise Edition
	SW 17	Microsoft Navision (ERP)
	SW 18	Microsoft Active Directory
	SW 19	Open CAS
	SW 20	Apache Tomcat (3 Unidades)
	SW 21	Microsoft Information Services (6 Unidades)
	SW 22	Adobe Acrobat Pro (2 Unidades)

	SW 23	Antivirus TrendMicro Bussiness Security (80 Unidades)
	SW 24	Paquete Microsoft Office 365 (77)
	SW 25	Microsoft Project (5 Unidades)
	SW 26	Microsoft Visual Studio (7 Unidades)
	SW 27	Microsoft Visio (10 Unidades)
	SW 28	Catia V5 (4 Unidades)
	SW 29	AutoCAD 2015 (3 Unidades)
Datos [D]	D1	BBDD ERP Empleados
	D2	Datos Servidor de ficheros corporativo
	D3	BBDD Active Directory
	D4	BBDD Sistema Sirio (10 Unidades)
	D5	BBDD Corporativa (Desarrollos Sirio)
	D6	BBDD I+D
	D7	Copia de Seguridad de Sistemas Corporativos
	D8	Copia de Seguridad de Sistema Sirio
	D9	Datos corporativos en móviles de empleados
	D10	Datos corporativos en PC's y soportes de almacenamiento ext. de empleados
Red de comunicaciones [COM]	COM1	Acceso a Internet Principal Oficinas (3 Unidades)
	COM2	Acceso a Internet Secundario Oficinas (3 Unidades)
	COM3	Acceso a Internet Nave
	COM4	Líneas Móviles (77 Unidades)
	COM5	Línea voz fija principal oficinas
	COM6	Línea voz fija secundaria oficinas
	COM7	Línea voz fija nave oficinas
	COM8	Acceso de Voz Fijo (5 Unidades)
	COM9	Red de sensores planta fotovoltaica de Almendralejo [BA]
	COM10	Red de sensores planta fotovoltaica de Puertollano [CR]

	COM11	Red de sensores planta fotovoltaica de Olmedilla de Alarcón [CU]
	COM12	Red de sensores planta fotovoltaica de Arnedo [RI]
	COM13	Red de sensores planta fotovoltaica de Las Gabias [GR]
	COM14	Red de sensores planta fotovoltaica de Jumilla [MU]
	COM15	Red de sensores planta fotovoltaica de Lorca [MU]
	COM16	Red de sensores planta fotovoltaica de Olivenza [BA]
	COM17	Red de sensores planta fotovoltaica de Calasparra [MU]
	COM18	Red de sensores planta fotovoltaica de Beneixama [A]
	COM19	Red de sensores planta fotovoltaica de Salamanca [SA]
	COM20	Red de sensores planta fotovoltaica de El Coronil [SE]
	COM21	Red de sensores planta fotovoltaica de Almaraz [CC]
	COM22	Red de sensores planta fotovoltaica de El Bonillo [ALB]
	COM23	Red de sensores planta fotovoltaica de Guadarranque [CA]
	COM24	Acceso a Internet planta fotovoltaica de Almendralejo [BA]
	COM25	Acceso a Internet planta fotovoltaica de Puertollano [CR]
	COM26	Acceso a Internet planta fotovoltaica de Olmedilla de Alarcón [CU]
	COM27	Acceso a Internet planta fotovoltaica de Arnedo [RI]
	COM28	Acceso a Internet planta fotovoltaica de Las Gabias [GR]
	COM29	Acceso a Internet planta fotovoltaica de Jumilla [MU]
	COM30	Acceso a Internet planta fotovoltaica de Lorca [MU]
	COM31	Acceso a Internet planta fotovoltaica de Olivenza [BA]
	COM32	Acceso a Internet planta fotovoltaica de Calasparra [MU]
	COM33	Acceso a Internet planta fotovoltaica de Beneixama [A]

	COM34	Acceso a Internet planta fotovoltaica de Salamanca [SA]
	COM35	Acceso a Internet planta fotovoltaica de El Coronil [SE]
	COM36	Acceso a Internet planta fotovoltaica de Almaraz [CC]
	COM37	Acceso a Internet planta fotovoltaica de El Bonillo [ALB]
	COM38	Acceso a Internet planta fotovoltaica de Guadarranque [CA]
	COM39	Red LAN Oficina
	COM40	Red LAN CPD
	COM41	Red LAN Nave
	COM42	Red inalámbrica oficinas
	COM43	Red inalámbrica nave
Servicios [S]	S1	Correo electrónico corporativo [Para usuarios Internos]
	S2	Backup sistema Sirio [Para usuarios Internos]
	S3	Centralita en la nube [Para usuarios Internos]
	S4	IaaS entorno de desarrollo [Para usuarios Internos]
	S5	Servicio de Monitorización sistema Sirio [Para usuarios Externos]
	S6	Servicio de Administración sistema Sirio [Para usuarios Externos]
Equipamiento Auxiliar [AUX]	AUX1	Sistema de climatización CPD
	AUX2	Sistema de detección de incendios
	AUX3	Sistema de extinción de incendios
	AUX4	Sistema de detección de inundaciones
	AUX5	Sistema de alimentación Ininterrumpida
	AUX6	Suministro eléctrico general
	AUX7	Cableado eléctrico
	AUX8	Cableado Estructurado Oficina
	AUX9	Fibra Óptica CPD
	AUX10	Cableado Estructurado CPD
	AUX11	Cableado Estructurado Nave

	AUX12	Destructora de Papel
Personal [P]	P1	Director General
	P2	Director Financiero
	P3	Director Comercial
	P4	Director de Operaciones
	P5	Director Técnico
	P6	Responsable de área de RRHH
	P7	Reclutadores de personal (2)
	P8	Gestores de RRLL (2)
	P9	Responsable de área Administración
	P10	Contables (4)
	P11	Asesor Fiscal
	P12	Abogado
	P13	Responsable de área de compras
	P14	Gestores de compras (4)
	P15	Community Manager
	P16	Gestores de Producto (2)
	P17	Responsable de área de ventas
	P18	Comerciales (5)
	P19	Responsable del área de Instaladores
	P20	Instaladores (23)
	P21	Responsable del área de Mantenimiento
	P22	Técnicos de mantenimiento (20)
	P23	Responsable del área de administración
	P24	Administradores (6)
	P25	Responsable del área de TI
	P26	Técnicos de puesto de trabajo (2)
	P27	Técnicos de CPD (2)
	P28	Responsable del área de Software
	P29	Desarrolladores Software (7)

	P30	Responsable del área de Hardware
	P31	Desarrolladores Hardware (5)
	P32	Controladores de calidad Hardware (2)
	P33	Responsable del área de I+D
	P34	Proveedores

3.3 Valoración de los activos

Una vez que han sido identificados los activos relacionados con la seguridad de la información, se les asigna un valor. Esta valoración se basará en el análisis de tabla que propone MAGERIT en su Libro III.

Este método, aunque no se cuenta con mucha precisión, simplifica esta fase y se ha demostrado su utilidad estimando la valoración de los activos respecto a escala de clasificación de valor.

En la Tabla 7, se muestra la escala de valoración de activos para Ícaro S.A. que permitirá realizar una valoración cualitativa y cuantitativa basada en las siguientes consideraciones:

- **El valor de reposición:** es el valor que tiene para la empresa reponer ese activo en el caso de que se pierda o de que no pueda ser utilizado.
- **El valor de configuración:** es el tiempo que se necesita desde que se adquiere el nuevo activo hasta que se configura o se pone a punto para que pueda utilizarse para la función que desarrollaba el anterior activo.
- **El valor de uso del activo:** es el valor que pierde la organización durante el tiempo que no puede utilizar dicho activo para la función que desarrolla.
- **El valor de pérdida de oportunidad:** es el valor que pierde potencialmente la organización por no poder disponer de dicho activo durante un tiempo.

Tabla 9. Escala de valoración de activos

ID	Valoración	Rango	Valor estimado
MA	Muy Alta	Valor > 200K€	300K€
A	Alta	100K€ < Valor < 200K€	150K€
M	Media	50K€ < Valor < 100K€	75K€
B	Baja	10K€ < Valor < 50K€	30K€
MB	Muy baja	Valor < 10K€	10K€

En el punto 3.5. Tabla resumen de valoración, se muestra la valoración asignada a los activos identificados de Ícaro S.A.

Adicionalmente, debe tenerse en cuenta que los activos están en realidad jerarquizados. Un “activo superior” depende de otro “activo inferior”, es decir cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Deberá por tanto analizarse el árbol de dependencias o jerarquía entre los activos.

A continuación, se presentan las jerarquías de dependencia de los servicios de monitorización y administración del sistema Sirio, los cuales son el núcleo del negocio de Ícaro S.A.

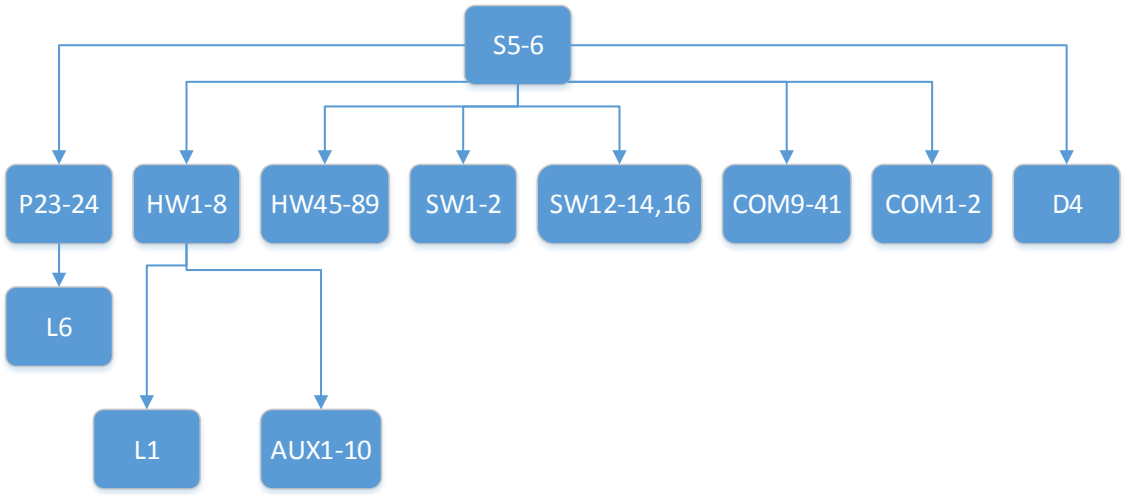

Ilustración 12. Dependencias administración y monitorización del sistema Sirio

3.4 Dimensiones de seguridad

Para la ejecución de este apartado se basa en las dimensiones de valoración que propone MAGERIT en su Libro II. En el apartado 3.

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más nos interesen y por ello se realizan un dimensionamiento de la valoración.

Las dimensiones de valoración son las características que hacen valioso a un activo y dichas dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

Para obtener el dimensionamiento se realiza una valoración del tipo ACIDT que mide la criticidad en las cinco dimensiones en seguridad de la información. Estas dimensiones se exponen a continuación:

- **Autenticidad [A]:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
- **Confidencialidad [C]:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
- **Integridad [I]:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

- **Disponibilidad [D]:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
- **Trazabilidad [T]:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Una vez que se tienen claras las cinco dimensiones de valoración, es necesario usar una escala clara y detallada. Para el dimensionamiento del valor de la seguridad de Ícaro S.A. se utiliza con base a la tabla descrita en MAGERIT en el Libro II. En el apartado 4. Se presenta a continuación:

Tabla 10. Criterios de valoración de dimensiones de seguridad

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

A la hora de realizar las ponderaciones para cada activo se ha de tener presente la importancia o participación del activo en la cadena de valor del servicio, evitando situaciones del tipo “todo es muy importante” y obligando así al o a los responsables de realizar dicha valoración a discernir entre lo que es realmente importante y lo que no lo es tanto.

La valoración respecto a las dimensiones de seguridad de los activos de Ícaro S.A. se realiza en el punto 3.5 Tabla resumen de valoración.

3.5 Tabla resumen de valoración

En este apartado se presenta una tabla resumen que integra la valoración de los activos en escala económica y en dimensiones de seguridad como se ha desarrollado en los apartados anteriores.

Tabla 11. Valoración de activos integrada

Ámbito	ID	Activo	Valor €	Aspectos Críticos				
				A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	MA	9	9	9	9	9
	L2	Sala de departamento de RRHH	M	7	1	2	2	7
	L3	Sala departamento de administración	M	6	1	2	2	7
	L4	Despacho de departamento de Legal	M	6	1	2	2	7
	L5	Sala de departamento comercial	M	3	1	2	2	6
	L6	Sala administradores sistema Sirio	A	9	7	7	8	8
	L7	Sala de departamento de TI	A	9	7	7	8	8
	L8	Sala de departamento de desarrollo software	A	9	7	7	7	8
	L9	Sala de departamento de desarrollo hardware	A	9	7	7	7	8
	L10	Sala de departamento de I+D	A	9	7	7	7	8
	L11	Oficina nave de operaciones	A	6	1	2	4	8
	L12	Despacho del director general	B	6	1	6	1	8
	L13	Despacho del director financiero	B	6	1	6	1	8
	L14	Despacho del director de operaciones	B	6	1	6	1	8
	L15	Despacho del director técnico	B	6	1	6	1	8
	L16	Armario técnico planta fotovoltaica de Almendralejo [BA]	A	8	8	8	8	8
	L17	Armario técnico planta fotovoltaica de Puertollano [CR]	A	8	8	8	8	8
	L18	Armario técnico planta fotovoltaica de Olmedilla de Alarcón [CU]	A	8	8	8	8	8
	L19	Armario técnico planta fotovoltaica de Arnedo [RI]	A	8	8	8	8	8
	L20	Armario técnico planta fotovoltaica de Las Gabias [GR]	A	8	8	8	8	8
	L21	Armario técnico planta fotovoltaica de Jumilla [MU]	A	8	8	8	8	8
	L22	Armario técnico planta fotovoltaica de Lorca [MU]	A	8	8	8	8	8
	L23	Armario técnico planta fotovoltaica de Olivenza [BA]	A	8	8	8	8	8
	L24	Armario técnico planta fotovoltaica de Calasparra [MU]	A	8	8	8	8	8
	L25	Armario técnico planta fotovoltaica de Beneixama [A]	A	8	8	8	8	8
	L26	Armario técnico planta fotovoltaica de Salamanca [SA]	A	8	8	8	8	8
	L27	Armario técnico planta fotovoltaica de El Coronil [SE]	A	8	8	8	8	8
	L28	Armario técnico planta fotovoltaica de Almaraz [CC]	A	8	8	8	8	8
	L29	Armario técnico planta fotovoltaica de El Bonillo [ALB]	A	8	8	8	8	8

	L30	Armario técnico planta fotovoltaica de Guadarranque [CA]	A	8	8	8	8	8
Hardware [HW]	HW1	Servidor 1 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW2	Servidor 2 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW3	Servidor 3 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW4	Servidor 4 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW5	Servidor 5 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW6	Servidor 6 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW7	Servidor 7 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW8	Servidor 8 granja virtualización sistema Sirio	MB	7	8	8	8	8
	HW9	Switch SAN 1	MB	7	8	8	8	7
	HW10	Switch SAN 2	MB	7	8	8	8	7
	HW11	Cabina de Almacenamiento	M	9	9	9	9	9
	HW12	Switch Ethernet Red de Gestión Sirio	MB	7	8	8	9	7
	HW13	Switch Ethernet Red Externa	MB	6	7	7	6	7
	HW14	Switch Ethernet Red Interna	MB	7	7	7	7	7
	HW15	Switch Ethernet 1 Oficina Principal	MB	4	5	5	5	7
	HW16	Switch Ethernet 2 Oficina Principal	MB	4	5	5	5	7
	HW17	Switch Ethernet Nave	MB	3	5	5	4	5
	HW18	AP 1 Oficina Central	MB	3	5	5	4	5
	HW19	AP 2 Oficina Central	MB	3	5	5	4	5
	HW20	AP Nave	MB	3	3	3	3	5
	HW21	Router FTTH Oficina 1	MB	8	8	8	9	8
	HW22	Router FTTH Oficina 2	MB	8	8	8	9	8
	HW23	Router FTTH Nave	MB	6	7	7	6	6
	HW24	Firewall Nave	B	7	7	7	9	9
	HW25	Firewall segundo nivel CPD	A	8	8	8	9	9
	HW26	Firewall primer nivel CPD	A	8	8	8	9	9
	HW27	Firewall de Oficina	A	8	8	8	8	9
	HW28	Servidor SFTP	MB	7	6	7	2	7
	HW29	Servidor Web Corporativa	MB	7	7	8	3	7
	HW30	Servidor de Ficheros	MB	7	8	8	7	7
	HW31	Servidor de Directorio Activo	MB	7	8	8	7	7
	HW32	Servidor de BBDD corporativa	MB	7	8	8	7	7
	HW33	Servidor CAS	MB	7	8	8	7	7
	HW34	Servidor de I+D	MB	9	9	8	3	7
	HW35	Servidor ERP	MB	7	8	8	4	7
	HW36	Impresora de red planta 1 Oficina central	MB	0	0	0	0	0
	HW37	Impresora de red planta 2 Oficina central	MB	0	0	0	0	0
	HW38	Impresora de red Nave de operaciones	MB	0	0	0	0	0

	HW39	PC's tipo A (46 dispositivos)	MB	7	7	7	4	8
	HW40	PC's tipo B (4 dispositivos)	MB	7	7	7	4	8
	HW41	PC's tipo C (27 dispositivos)	MB	7	7	7	4	8
	HW42	Móvil tipo A (49 dispositivos)	MB	7	7	7	4	7
	HW43	Móvil tipo B (9 dispositivos)	MB	7	7	7	4	7
	HW44	Móvil tipo C (24 dispositivos)	MB	7	7	7	4	7
	HW45	Placa Base Sirio planta fotovoltaica de Almendralejo [BA]	A	8	8	8	8	8
	HW46	Placa Base Sirio planta fotovoltaica de Puertollano [CR]	A	8	8	8	8	8
	HW47	Placa Base Sirio planta fotovoltaica de Olmedilla de Alarcón [CU]	A	8	8	8	8	8
	HW48	Placa Base Sirio planta fotovoltaica de Arnedo [RI]	A	8	8	8	8	8
	HW49	Placa Base Sirio planta fotovoltaica de Las Gabias [GR]	A	8	8	8	8	8
	HW50	Placa Base Sirio planta fotovoltaica de Jumilla [MU]	A	8	8	8	8	8
	HW51	Placa Base Sirio planta fotovoltaica de Lorca [MU]	A	8	8	8	8	8
	HW52	Placa Base Sirio planta fotovoltaica de Olivenza [BA]	A	8	8	8	8	8
	HW53	Placa Base Sirio planta fotovoltaica de Calasparra [MU]	A	8	8	8	8	8
	HW54	Placa Base Sirio planta fotovoltaica de Beneixama [A]	A	8	8	8	8	8
	HW55	Placa Base Sirio planta fotovoltaica de Salamanca [SA]	A	8	8	8	8	8
	HW56	Placa Base Sirio planta fotovoltaica de El Coronil [SE]	A	8	8	8	8	8
	HW57	Placa Base Sirio planta fotovoltaica de Almaraz [CC]	A	8	8	8	8	8
	HW58	Placa Base Sirio planta fotovoltaica de El Bonillo [ALB]	A	8	8	8	8	8
	HW59	Placa Base Sirio planta fotovoltaica de Guadarranque [CA]	A	8	8	8	8	8
	HW60	Actuadores planta fotovoltaica de Almendralejo [BA] (200 sensores)	M	6	7	7	7	8
	HW61	Actuadores planta fotovoltaica de Puertollano [CR] (1333 sensores)	M	6	7	7	7	8
	HW62	Actuadores planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	M	6	7	7	7	8
	HW63	Actuadores planta fotovoltaica de Arnedo [RI] (300 sensores)	M	6	7	7	7	8
	HW64	Actuadores planta fotovoltaica de Las Gabias [GR] (550 sensores)	M	6	7	7	7	8
	HW65	Actuadores planta fotovoltaica de Jumilla [MU] (112 sensores)	M	6	7	7	7	8
	HW66	Actuadores planta fotovoltaica de Lorca [MU] (173 sensores)	M	6	7	7	7	8
	HW67	Actuadores planta fotovoltaica de Olivenza [BA] (200 sensores)	M	6	7	7	7	8
	HW68	Actuadores planta fotovoltaica de Calasparra [MU] (226 sensores)	M	6	7	7	7	8

	HW69	Actuadores planta fotovoltaica de Beneixama [A] (80 sensores)	M	6	7	7	7	8
	HW70	Actuadores planta fotovoltaica de Salamanca [SA] (125 sensores)	M	6	7	7	7	8
	HW71	Actuadores planta fotovoltaica de El Coronil [SE] (89 sensores)	M	6	7	7	7	8
	HW72	Actuadores planta fotovoltaica de Almaraz [CC] (255 sensores)	M	6	7	7	7	8
	HW73	Actuadores planta fotovoltaica de El Bonillo [ALB] (629 sensores)	M	6	7	7	7	8
	HW74	Actuadores planta fotovoltaica de Guadarranque [CA] (136 sensores)	M	6	7	7	7	8
	HW75	Sensores Sirio planta fotovoltaica de Almendralejo [BA] (200 sensores)	M	6	7	7	7	8
	HW76	Sensores Sirio planta fotovoltaica de Puertollano [CR] (1333 sensores)	M	6	7	7	7	8
	HW77	Sensores Sirio planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	M	6	7	7	7	8
	HW78	Sensores Sirio planta fotovoltaica de Arnedo [RI] (300 sensores)	M	6	7	7	7	8
	HW79	Sensores Sirio planta fotovoltaica de Las Gabias [GR] (550 sensores)	M	6	7	7	7	8
	HW80	Sensores Sirio planta fotovoltaica de Jumilla [MU] (112 sensores)	M	6	7	7	7	8
	HW81	Sensores Sirio planta fotovoltaica de Lorca [MU] (173 sensores)	M	6	7	7	7	8
	HW82	Sensores Sirio planta fotovoltaica de Olivenza [BA] (200 sensores)	M	6	7	7	7	8
	HW83	Sensores Sirio planta fotovoltaica de Calasparra [MU] (226 sensores)	M	6	7	7	7	8
	HW84	Sensores Sirio planta fotovoltaica de Beneixama [A] (80 sensores)	M	6	7	7	7	8
	HW85	Sensores Sirio planta fotovoltaica de Salamanca [SA] (125 sensores)	M	6	7	7	7	8
	HW86	Sensores Sirio planta fotovoltaica de El Coronil [SE] (89 sensores)	M	6	7	7	7	8
	HW87	Sensores Sirio planta fotovoltaica de Almaraz [CC] (255 sensores)	M	6	7	7	7	8
	HW88	Sensores Sirio planta fotovoltaica de El Bonillo [ALB] (629 sensores)	M	6	7	7	7	8
	HW89	Sensores Sirio planta fotovoltaica de Guadarranque [CA] (136 sensores)	M	6	7	7	7	8
Software [SW]	SW 1	Software principal sistema Sirio	MA	9	9	9	9	9
	SW 2	Software sensores sistema Sirio	MA	9	9	9	9	9
	SW 3	Software en desarrollo de I+D (3 unidades)	A	9	9	9	6	9
	SW 4	Sistema Operativos Windows 7 Enterprise Edition (50 unidades)	MB	6	7	7	5	7
	SW 5	Sistema Operativo Windows 10 Pro (27 unidades)	MB	6	7	7	5	
	SW 6	Sistema Operativo Ubuntu Desktop (8 Unidades)	MB	6	7	7	5	7
	SW 7	Sistema Operativo Debian (10 Unidades)	MB	6	7	7	5	7
	SW 8	Sistema Operativo Android (70 Unidades)	MB	5	7	7	5	7

	SW 9	Sistema Operativo iOS (12 Unidades)	MB	5	7	7	5	7
	SW 10	Sistema Operativo CentOS (3 Unidades)	MB	6	7	7	5	7
	SW 11	Sistema Operativo Ubuntu Server (3 Unidades)	MB	6	7	7	5	7
	SW 12	Sistema Operativos Windows Server R2 2012 Enterprise Edition (26 Unidades)	A	8	9	9	7	9
	SW 13	Sistema Operativo DataOntap 8.3.5	A	8	9	9	9	9
	SW 14	SQL Server 2012 Enterprise Edition (6 unidades)	A	8	9	9	9	9
	SW 15	María DB (3 Unidades)	MB	7	7	7	4	7
	SW 16	VMware vSphere 6.3 Enterprise Edition	A	9	9	9	9	9
	SW 17	Microsoft Navision (ERP)	B	7	7	8	7	7
	SW 18	Microsoft Active Directory	B	7	7	8	7	7
	SW 19	Open CAS	B	7	7	8	7	7
	SW 20	Apache Tomcat (3 Unidades)	B	6	6	6	5	7
	SW 21	Microsoft Information Services (6 Unidades)	B	6	6	6	5	7
	SW 22	Adobe Acrobat Pro (2 Unidades)	B	1	1	4	2	7
	SW 23	Antivirus TrendMicro Bussiness Security (80 Unidades)	B	8	8	9	8	9
	SW 24	Paquete Microsoft Office 365 (77)	B	6	6	7	4	7
	SW 25	Microsoft Project (5 Unidades)	B	6	6	7	4	7
	SW 26	Microsoft Visual Studio (7 Unidades)	B	6	6	7	4	7
	SW 27	Microsoft Visio (10 Unidades)	B	6	6	7	4	7
	SW 28	Catia V5 (4 Unidades)	B	6	6	7	4	7
	SW 29	AutoCAD 2015 (3 Unidades)	B	6	6	7	4	7
Datos [D]	D1	BBDD ERP Empleados	B	7	7	8	6	8
	D2	Datos Servidor de ficheros corporativo	B	7	7	8	6	8
	D3	BBDD Active Directory	B	7	7	8	6	8
	D4	BBDD Sistema Sirio (10 Unidades)	MA	9	9	9	9	9
	D5	BBDD Corporativa (Desarrollos Sirio)	MA	9	9	9	9	9
	D6	BBDD I+D	M	9	9	9	9	9
	D7	Copia de Seguridad de Sistemas Corporativos	M	7	7	8	9	9
	D8	Copia de Seguridad de Sistema Sirio	MA	9	9	9	9	9
	D9	Datos corporativos en móviles de empleados	M	7	7	8	9	9
	D10	Datos corporativos en PC's y soportes de almacenamiento ext. de empleados	MA	9	9	9	9	9
Red de comunicaciones [COM]	COM1	Acceso a Internet Principal Oficinas	A	8	9	8	9	7
	COM2	Acceso a Internet Secundario Oficinas	M	6	7	6	9	7
	COM3	Acceso a Internet Nave	M	6	6	6	6	6
	COM4	Líneas Móviles (77 Unidades)	B	3	7	6	6	7
	COM5	Línea voz fija principal oficinas	A	3	7	6	7	7
	COM6	Línea voz fija secundaria oficinas	B	3	7	6	7	7
	COM7	Línea voz fija nave oficinas	MB	3	7	6	5	7
	COM8	Acceso de Voz Fijo (5 Unidades)	MB	3	7	6	7	7

	COM9	Red de sensores planta fotovoltaica de Almendralejo [BA]	M	7	7	8	8	7
	COM10	Red de sensores planta fotovoltaica de Puertollano [CR]	M	7	7	8	8	7
	COM11	Red de sensores planta fotovoltaica de Olmedilla de Alarcón [CU]	M	7	7	8	8	7
	COM12	Red de sensores planta fotovoltaica de Arnedo [RI]	M	7	7	8	8	7
	COM13	Red de sensores planta fotovoltaica de Las Gabias [GR]	M	7	7	8	8	7
	COM14	Red de sensores planta fotovoltaica de Jumilla [MU]	M	7	7	8	8	7
	COM15	Red de sensores planta fotovoltaica de Lorca [MU]	M	7	7	8	8	7
	COM16	Red de sensores planta fotovoltaica de Olivenza [BA]	M	7	7	8	8	7
	COM17	Red de sensores planta fotovoltaica de Calasparra [MU]	M	7	7	8	8	7
	COM18	Red de sensores planta fotovoltaica de Beneixama [A]	M	7	7	8	8	7
	COM19	Red de sensores planta fotovoltaica de Salamanca [SA]	M	7	7	8	8	7
	COM20	Red de sensores planta fotovoltaica de El Coronil [SE]	M	7	7	8	8	7
	COM21	Red de sensores planta fotovoltaica de Almaraz [CC]	M	7	7	8	8	7
	COM22	Red de sensores planta fotovoltaica de El Bonillo [ALB]	M	7	7	8	8	7
	COM23	Red de sensores planta fotovoltaica de Guadarranque [CA]	M	7	7	8	8	7
	COM24	Acceso a Internet planta fotovoltaica de Almendralejo [BA]	A	7	7	8	8	7
	COM25	Acceso a Internet planta fotovoltaica de Puertollano [CR]	A	7	7	8	8	7
	COM26	Acceso a Internet planta fotovoltaica de Olmedilla de Alarcón [CU]	A	7	7	8	8	7
	COM27	Acceso a Internet planta fotovoltaica de Arnedo [RI]	A	7	7	8	8	7
	COM28	Acceso a Internet planta fotovoltaica de Las Gabias [GR]	A	7	7	8	8	7
	COM29	Acceso a Internet planta fotovoltaica de Jumilla [MU]	A	7	7	8	8	7
	COM30	Acceso a Internet planta fotovoltaica de Lorca [MU]	A	7	7	8	8	7
	COM31	Acceso a Internet planta fotovoltaica de Olivenza [BA]	A	7	7	8	8	7
	COM32	Acceso a Internet planta fotovoltaica de Calasparra [MU]	A	7	7	8	8	7
	COM33	Acceso a Internet planta fotovoltaica de Beneixama [A]	A	7	7	8	8	7
	COM34	Acceso a Internet planta fotovoltaica de Salamanca [SA]	A	7	7	8	8	7
	COM35	Acceso a Internet planta fotovoltaica de El Coronil [SE]	A	7	7	8	8	7
	COM36	Acceso a Internet planta fotovoltaica de Almaraz [CC]	A	7	7	8	8	7

	COM37	Acceso a Internet planta fotovoltaica de El Bonillo [ALB]	A	7	7	8	8	7
	COM38	Acceso a Internet planta fotovoltaica de Guadarranque [CA]	A	7	7	8	8	7
	COM39	Red LAN Oficina	M	7	7	8	7	7
	COM40	Red LAN CPD	MA	7	7	8	9	7
	COM41	Red LAN Nave	B	6	6	6	6	6
	COM42	Red inalámbrica oficinas	B	5	7	6	3	7
	COM43	Red inalámbrica nave	MB	5	6	6	3	6
Servicios [S]	S1	Correo electrónico corporativo [Para usuarios Internos]	B	7	7	7	7	7
	S2	Backup sistema Sirio [Para usuarios Internos]	MA	9	9	9	9	9
	S3	Centralita en la nube [Para usuarios Internos]	A	7	6	7	7	7
	S4	IaaS entorno de desarrollo [Para usuarios Internos]	MB	7	7	7	1	7
	S5	Servicio de Monitorización sistema Sirio [Para usuarios Externos]	MA	9	9	9	9	9
	S6	Servicio de Administración sistema Sirio [Para usuarios Externos]	MA	9	9	9	9	9
Equipamiento Auxiliar [AUX]	AUX1	Sistema de climatización CPD	A	0	0	0	9	0
	AUX2	Sistema de detección de incendios	A	0	0	0	9	0
	AUX3	Sistema de extinción de incendios	A	0	0	0	9	0
	AUX4	Sistema de detección de inundaciones	A	0	0	0	9	0
	AUX5	Sistema de alimentación Ininterrumpida	MA	0	0	0	9	0
	AUX6	Suministro eléctrico general	A	0	0	0	9	0
	AUX7	Cableado eléctrico	A	0	0	0	9	0
	AUX8	Cableado Estructurado Oficina	M	7	7	7	7	0
	AUX9	Fibra Óptica CPD	A	9	8	8	9	0
	AUX10	Cableado Estructurado CPD	A	9	8	8	9	0
	AUX11	Cableado Estructurado Nave	MB	6	8	6	6	0
	AUX12	Destructora de Papel	MB	0	0	0	1	0
Personal [P]	P1	Director General	A	0	0	0	9	0
	P2	Director Financiero	A	0	0	0	9	0
	P3	Director Comercial	M	0	0	0	9	0
	P4	Director de Operaciones	MA	0	0	0	9	0
	P5	Director Técnico	MA	0	0	0	9	0
	P6	Responsable de área de RRHH	B	0	0	0	8	0
	P7	Reclutadores de personal (2)	B	0	0	0	4	0
	P8	Gestores de RRLL (2)	B	0	0	0	6	0
	P9	Responsable de área Administración	B	0	0	0	8	0
	P10	Contables (4)	B	0	0	0	6	0
	P11	Asesor Fiscal	B	0	0	0	7	0
	P12	Abogado	B	0	0	0	7	0
	P13	Responsable de área de compras	B	0	0	0	8	0
	P14	Gestores de compras (4)	B	0	0	0	6	0
	P15	Comunity Manager	B	0	0	0	4	0

	P16	Gestores de Producto (2)	B	0	0	0	6	0
	P17	Responsable de área de ventas	B	0	0	0	8	0
	P18	Comerciales (5)	B	0	0	0	5	0
	P19	Responsable del área de Instaladores	M	0	0	0	8	0
	P20	Instaladores (23)	M	0	0	0	7	0
	P21	Responsable del área de Mantenimiento	A	0	0	0	8	0
	P22	Técnicos de mantenimiento (20)	A	0	0	0	7	0
	P23	Responsable del área de administración sistema Sirio	A	0	0	0	9	0
	P24	Administradores (6)	A	0	0	0	8	0
	P25	Responsable del área de TI	A	0	0	0	9	0
	P26	Técnicos de puesto de trabajo (2)	A	0	0	0	8	0
	P27	Técnicos de CPD (2)	A	0	0	0	8	0
	P28	Responsable del área de Software	A	0	0	0	9	0
	P29	Desarrolladores Software (7)	A	0	0	0	8	0
	P30	Responsable del área de Hardware	A	0	0	0	8	0
	P31	Desarrolladores Hardware (5)	A	0	0	0	8	0
	P32	Controladores de calidad Hardware (2)	A	0	0	0	7	0
	P33	Responsable del área de I+D	A	0	0	0	7	0
	P34	Proveedores	B	0	0	0	7	0

3.6 Análisis de amenazas

Los activos de una organización siempre están expuestos a amenazas que pueden afectar a aspectos de la seguridad. Por esta razón, en este apartado se va a realizar el análisis de amenazas que pueden afectar a Ícaro S.A. Además, se estimará la vulnerabilidad de cada activo ligado a las amenazas y la posibilidad de ocurrencia de las misma.

Para realizar el análisis de amenazas se va partir de la metodología MAGERIT, en concreto el Libro 2. Apartado 5. Dicha metodología clasifica las amenazas en diferentes grupos:

- Desastres Naturales [N]
- De origen Industrial [I]
- Errores y fallos no intencionados [E]
- Ataques Intencionados [A]

En la siguiente tabla se muestra el catálogo de amenazas según MAGERIT para Ícaro S.A.

Tabla 12. Catálogo de amenazas MAGERIT

Grupo	ID	Amenaza
Desastres Naturales [N]	N1	Fuego
	N2	Daños por agua

	N3	Tormenta Eléctrica
	N4	Terremoto
Origen Industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación mecánica
	I7	Contaminación electromagnética
	I8	Avería de origen física o lógica
	I9	Corte eléctrico
	I10	Condiciones inadecuadas de temperatura y/o humedad
	I11	Fallo del servicio de comunicaciones
	I12	Interrupción de otros servicios y suministros esenciales
	I13	Degradación de los soportes de almacenamiento de la información
	I14	Emanaciones electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de usuarios
	E2	Errores de los técnicos de TI
	E3	Errores de los administradores de sirio
	E4	Errores de monitorización (log)
	E5	Errores de configuración
	E6	Deficiencias en la organización
	E7	Difusión de software dañino
	E8	Errores de [re-]encaminamiento
	E9	Errores de secuencia
	E10	Escapes de información
	E11	Alteración accidental de la información
	E12	Destrucción de información
	E13	Fugas de información
	E14	Vulnerabilidad de los programas (software)
	E15	Errores de mantenimiento / actualización de programas (software)
	E16	Errores de mantenimiento / actualización de equipos (hardware)
	E17	Caída del sistema por agotamiento de recursos
	E18	Pérdida de equipos
	E19	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad (log)
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino
	A7	[Re-]encaminamiento de mensajes
	A8	Alteración de secuencia

	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información (escucha)
	A13	Modificación deliberada de la información
	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de programas
	A17	Manipulación de los equipos
	A18	Denegación de servicio
	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social (picaresca)

Para la categorización de la frecuencia de la amenaza se medirá como se muestra en la siguiente tabla.

Tabla 13. Categorías de frecuencia de amenazas

Vulnerabilidad	ID	Rango	Valor
Frecuencia Extrema	MA	1 vez al día	1
Frecuencia Alta	A	1 vez cada 2 semanas	26/365=0.071233
Frecuencia Media	M	1 vez cada 2 meses	6/365=0.016438
Frecuencia Baja	B	1 vez cada seis meses	2/365=0.005479
Frecuencia Muy Baja	MB	1 vez al año	1/365=0.002739

Y la valoración del impacto que la ocurrencia de una amenaza producirá en las dimensiones de seguridad se basará en la siguiente tabla.

Tabla 14. Rangos de valoración de impacto

Impacto	ID	Rango
Muy Alto	MA	Valor > 95%
Alto	A	75% < Valor < 95%
Medio	M	50% < Valor < 75%
Bajo	B	30% < Valor < 50%
Muy Bajo	MB	10%< Valor < 30%

A continuación, se muestra una tabla resumen del análisis de amenazas de Ícaro S.A.

En ella se puede observar que para cada amenaza que afecta a cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo.

Para eficiencia del análisis los activos se identificarán en grupos cuando la amenaza afecte a todos los activos de ese grupo.

Tabla 15. Resumen análisis de amenazas

				% Impacto dimensiones				
Grupo	Amenaza	Grupo/Activo afectado	Frecuencia	A	C	I	D	T
Desastres naturales [N]	Fuego [N1]	Hardware [HW]	MB				100	
		Instalaciones [L]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
	Daños por agua [N2]	Hardware [HW]	MB				75	
		Instalaciones [L]	MB				75	
		Red de Comunicaciones [COM]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
	Tormenta Eléctrica [N3]	Hardware [HW]	MB				75	
		Red de Comunicaciones [COM]	MB				50	
		Equipamiento Auxiliar [AUX]	MB				50	
	Terremoto[N4]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
De origen industrial [I]	Fuego [I1]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
	Daños por agua [I2]	Hardware [HW]	MB				75	
		Instalaciones [L]	MB				75	
		Red de Comunicaciones [COM]	MB				75	
		Equipamiento Auxiliar [AUX]	B				75	

	Sobrecarga eléctrica [I3]	Hardware [HW]	B				75	
		Red de Comunicaciones [COM]	B				50	
		Equipamiento Auxiliar [AUX]	B				50	
	Explosión [I4]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
	Derrumbe [I5]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				60	
		Red de Comunicaciones [COM]	MB				60	
	Contaminación mecánica [I6]	Hardware [HW]	MB				50	
		Equipamiento Auxiliar [AUX]	MB				50	
	Contaminación electromagnética [I7]	Red de Comunicaciones [COM]	MB				75	
		Hardware [HW]	MB				75	
		Datos [D]	MB				75	
		Equipamiento Auxiliar [AUX]	MB				75	
	Avería de origen física o lógica [I8]	Instalaciones [L]	B				20	
		Hardware [HW]	M				75	
		Equipamiento Auxiliar [AUX]	M				40	
		Red de Comunicaciones [COM]	M				75	
		Software [SW]	M				75	
		Servicios [S]	M				80	
		Datos [D]	B				30	
	Corte eléctrico [I9]	Hardware [HW]	B				100	
		Equipamiento Auxiliar [AUX]	B				100	
		Red de Comunicaciones [COM]	B				100	
	Condiciones inadecuadas de [I10] temperatura y/o humedad	Hardware [HW]	B				60	
		Equipamiento Auxiliar [AUX]	B				60	
		Red de Comunicaciones [COM]	B				60	

	Fallo del servicio de comunicaciones [I11]	Acceso a Internet Principal Oficinas (3 Unidades) [COM1]	M				100	
		Acceso a Internet Secundario Oficinas (3 Unidades) [COM2]	M				100	
		Acceso a Internet Nave [COM3]	M				100	
		Líneas Móviles (77 Unidades) [COM4]	M				100	
		Línea voz fija principal oficinas [COM5]	M				100	
		Línea voz fija secundaria oficinas [COM6]	M				100	
		Línea voz fija nave oficinas [COM7]	M				100	
		Acceso de Voz Fijo (5 Unidades) [COM7]	M				100	
		Acceso a Internet Plantas [COM 24-38]	M				100	
		Servicios [S]	M				100	
	Interrupción de otros servicios y suministros esenciales [I12]	Sistema de climatización CPD	B				60	
		Sistema de alimentación Ininterrumpida	B				30	
	Degradación de los soportes de almacenamiento de la información [I13]	Servidores Sirio [HW 1-8]	MB			75	75	
		Cabina de Almacenamiento [HW 11]	MB			100	100	
		Servidores Corporativos [HW 28-35]	MB			60	60	
		PC'S [HW 39-41]	B			10	10	
	Emanaciones electromagnéticas [I14]	Instalaciones [L]	MB			20	20	
		Hardware [HW]	MB			50	50	
		Equipamiento Auxiliar [AUX]	MB			20	20	
Errores y fallos no intencionados [E]	Errores de usuarios [E1]	Instalaciones [L]	M		20	50	10	
		PC'S [HW 39-41]	M		20	20	50	
		Móviles [HW42-44]	M		20	20	50	
		Datos [D1-6]	M		75	40	75	
	Errores de los técnicos de TI [E2]	Instalaciones [L]	M		20	20	50	
		Hardware [HW]	M		20	20	75	

		Software [SW]	M		20	20	75	60
		Datos [D]	M		60	60	75	60
		Equipamiento Auxiliar [AUX]	M				75	
		Servicios [S]	M				80	
	Errores de los administradores de Sirio [E3]	Servicios Sirio [S5-6]	M				75	
	Errores de monitorización (log) [E4]	Datos [D]	B					30
	Errores de configuración [E5]	Hardware [HW]	B				50	
		Software [SW]	B				50	
		Datos [D]	B				50	
		Equipamiento Auxiliar [AUX]	B				50	
	Deficiencias en la organización [E6]	Personal [P]	M		50	30	75	
		Datos [D]	M		50	30	75	
		Instalaciones [L]	M		50	30	75	
		Servicios [S]	M		50	30	75	
	Difusión de Software dañino [E7]	Software [SW]	B		75	75	75	
		Datos [D]	B		50	50	50	
	Errores de [re-]encaminamiento [E8]	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50		75	
		Software [SW]	MB		50		75	
	Errores de secuencia [E9]	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50		75	
		Software [SW]	B		50		75	
	Escapes de información [E10]	Servicios [S]	MB		50			
		Software [SW]	B		50			
		Datos [D]	B		100			
	Alteración accidental de la información [E11]	Datos [D]	M			75		
	Destrucción de información [E12]	Datos [D]	M				100	
	Fugas de información [E13]	Servicios [S]	MB		30			
		Software [SW]	B		65			
		Datos [D]	B		100			
	Vulnerabilidad de los programas (software) [E14]	Software [SW]	M		75	20	75	
		Datos [D]	M		75	50	75	
	Errores de mantenimiento / actualización de	Software [SW]	B			50	75	

	programas (software) [E15]							
	Errores de mantenimiento / actualización de equipos (hardware) [E16]	Hardware [HW]	B				75	
	Caída del sistema por agotamiento de recursos [E17]	Servicios [S]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
	Pérdida de equipos [E18]	PC's [HW42-44]	B		50		100	
		Móviles [HW39-41]	M					
	Indisponibilidad del personal [E19]	Personal [P]	A				100	
Ataques intencionados [A	Manipulación de los registros de actividad (log) [A1]	Datos [D]	MB					75
		Servicios [S]	MB					80
	Manipulación de la configuración [A2]	Datos [D]	MB	75	75	75		
		Servicios [S]	MB	75	75	75		
	Suplantación de la identidad del usuario [A3]	Software [SW]	B	75	100	80		
		Datos [D]	B	100	100	80		
		Red de Comunicaciones [COM]	B	75	75	75		
		Servicios [S]	B	80	75	75		
	Abuso de privilegios de acceso [A4]	Instalaciones [L]	B		75	50	50	
		Software [SW]	B		75	50	50	
		Red de Comunicaciones [COM]	B		75	50	50	
		Servicios [S]	B		75	50	50	
	Uso no previsto [A5]	Instalaciones [L]	MB		25	25	25	
		Software [SW]	MB		25	25	25	
		Red de Comunicaciones [COM]	MB		25	25	25	
		Servicios [S]	MB		25	25	25	
		Hardware [HW]	MB		25	25	25	
	Difusión de software dañino [A6]	Software [SW]	B		75	20	75	
		Datos [D]	B		75	50	75	
	[Re-]encaminamiento de mensajes [A7]	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50		75	
		Software [SW]	MB		50		75	
	Alteración de secuencia [A8]	Servicios [S]	MB		50		75	
		Red de Comunicaciones [COM]	MB		50		75	

		Software [SW]	B		50		75	
	Acceso no autorizado [A9]	Servicios [S]	B		75	50	75	
		Red de Comunicaciones [COM]	B		30	30	75	
		Software [SW]	B		75	75	50	
		Hardware [HW]	MB				50	
		Datos [D]	B		100	100	100	
		Equipamiento Auxiliar [AUX]	B				50	
		Instalaciones [L]	B		20	20	20	
	Análisis de tráfico [A10]	Datos [D]	MB		50			
	Repudio [A11]	Servicios [S]	MB					80
	Interceptación de información (escucha) [A12]	Datos [D]	B		100			
	Modificación deliberada de la información [A13]	Datos [D]	B			100		
		Software [SW]	B			100		
	Destrucción de información [A14]	Datos [D]	B				100	
		Software [SW]	B				100	
	Divulgación de información [A15]	Datos [D]	B		100			
		Software [SW]			100			
	Manipulación de programas [A16]	Software [SW]	B				100	
	Manipulación de los equipos [A17]	Hardware [HW]	B				100	
	Denegación de servicio [A18]	Servicios [S]	B				100	
		Red de Comunicaciones [COM]	B				100	
	Robo [A19]	Hardware [HW]	B				75	
		Equipamiento Auxiliar [AUX]	MB				75	
		Datos [D]	MB		100		100	
		Software [SW]	MB		100		75	
	Ataque destructivo [A20]	Instalaciones [L]	MB				100	
		Hardware [HW]	MB				100	
		Software [SW]	MB				100	
		Equipamiento Auxiliar [AUX]	MB				100	
		Red de Comunicaciones [COM]	MB				100	
		Servicios [S]	MB				100	
		Datos [D]	MB				100	
	Ocupación enemiga [A21]	Instalaciones [L]	MB		20		100	
		Hardware [HW]	MB		20		100	

		Software [SW]	MB		75		100	
		Equipamiento Auxiliar [AUX]	MB		20		100	
		Red de Comunicaciones [COM]	MB		30		100	
		Servicios [S]	MB		80		100	
		Datos [D]	MB		100		100	
	Indisponibilidad del personal [A22]	Personal [P]	M				100	
	Extorsión [A23]	Personal [P]	B		25	25	25	
	Ingeniería social (picaresca) [A24]	Personal [P]	B		25	25	25	

3.7 Impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Como ya se conoce el valor de los activos en las diferentes dimensiones y la degradación que causan las amenazas en estas mismas dimensiones, es inmediato derivar el impacto que estas tendrían sobre el sistema a través de la siguiente formula.

Impacto potencial = Valor del activo x Valor del impacto de la amenaza

Se trata de un dato relevante, ya que permite priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

Ya que se ha realizado una eficiencia en el análisis de activos agrupando los activos cuando la amenazas impactaban en un grupo, a continuación, se presenta una tabla con los valores absolutos máximos de impacto de amenaza obtenidos en el análisis anterior que serán los valores que servirán para la obtención del impacto potencial.

Tabla 16. Máximos de impacto de amenazas.

	Impacto por dimensiones (Valor absoluto)				
Grupo de Activos	A	C	I	D	T
Instalaciones [L]	0	7,5	5	10	0
Hardware [HW]	0	2,5	5	10	0
Software [SW]	7,5	10	10	10	6
Datos [D]	10	10	10	10	7,5
Redes de comunicación [COM]	7,5	7,5	7,5	10	0
Servicios [S]	8	7,5	7,5	10	8
Equipamiento Auxiliar [AUX]	0	2	0	10	0
Personal [P]	0	5	3	10	0

A continuación, se presenta una tabla resumen con los resultados de aplicar la fórmula del impacto potencial a cada activo.

En el siguiente documento se pueden observar la tabla completa con los cálculos realizados.

Tabla 17. Resumen impacto potencial

Ámbito	ID	Activo	Valor €	Impacto potencial				
				A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	MA	0	6,75	4,5	9	0
	L2	Sala de departamento de RRHH	M	0	0,75	1	2	0
	L3	Sala departamento de administración	M	0	0,75	1	2	0
	L4	Despacho de departamento de Legal	M	0	0,75	1	2	0
	L5	Sala de departamento comercial	M	0	0,75	1	2	0
	L6	Sala administradores sistema Sirio	A	0	5,25	3,5	8	0
	L7	Sala de departamento de TI	A	0	5,25	3,5	8	0
	L8	Sala de departamento de desarrollo software	A	0	5,25	3,5	7	0
	L9	Sala de departamento de desarrollo hardware	A	0	5,25	3,5	7	0
	L10	Sala de departamento de I+D	A	0	5,25	3,5	7	0
	L11	Oficina nave de operaciones	A	0	0,75	1	4	0
	L12	Despacho del director general	B	0	0,75	3	1	0
	L13	Despacho del director financiero	B	0	0,75	3	1	0
	L14	Despacho del director de operaciones	B	0	0,75	3	1	0
	L15	Despacho del director técnico	B	0	0,75	3	1	0
	L16	Armario técnico planta fotovoltaica de Almendralejo [BA]	A	0	6	4	8	0
	L17	Armario técnico planta fotovoltaica de Puertollano [CR]	A	0	6	4	8	0

	L18	Armario técnico planta fotovoltaica de Olmedilla de Alarcón [CU]	A	0	6	4	8	0
	L19	Armario técnico planta fotovoltaica de Arnedo [RI]	A	0	6	4	8	0
	L20	Armario técnico planta fotovoltaica de Las Gabias [GR]	A	0	6	4	8	0
	L21	Armario técnico planta fotovoltaica de Jumilla [MU]	A	0	6	4	8	0
	L22	Armario técnico planta fotovoltaica de Lorca [MU]	A	0	6	4	8	0
	L23	Armario técnico planta fotovoltaica de Olivenza [BA]	A	0	6	4	8	0
	L24	Armario técnico planta fotovoltaica de Calasparra [MU]	A	0	6	4	8	0
	L25	Armario técnico planta fotovoltaica de Beneixama [A]	A	0	6	4	8	0
	L26	Armario técnico planta fotovoltaica de Salamanca [SA]	A	0	6	4	8	0
	L27	Armario técnico planta fotovoltaica de El Coronil [SE]	A	0	6	4	8	0
	L28	Armario técnico planta fotovoltaica de Almaraz [CC]	A	0	6	4	8	0
	L29	Armario técnico planta fotovoltaica de El Bonillo [ALB]	A	0	6	4	8	0
	L30	Armario técnico planta fotovoltaica de Guadarranque [CA]	A	0	6	4	8	0
Hardware [HW]	HW1	Servidor 1 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW2	Servidor 2 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW3	Servidor 3 granja virtualización sistema Sirio	MB	0	2	4	8	0

	HW4	Servidor 4 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW5	Servidor 5 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW6	Servidor 6 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW7	Servidor 7 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW8	Servidor 8 granja virtualización sistema Sirio	MB	0	2	4	8	0
	HW9	Switch SAN 1	MB	0	2	4	8	0
	HW10	Switch SAN 2	MB	0	2	4	8	0
	HW11	Cabina de Almacenamiento	M	0	2,25	4,5	9	0
	HW12	Switch Ethernet Red de Gestión Sirio	MB	0	2	4	9	0
	HW13	Switch Ethernet Red Externa	MB	0	1,75	3,5	6	0
	HW14	Switch Ethernet Red Interna	MB	0	1,75	3,5	7	0
	HW15	Switch Ethernet 1 Oficina Principal	MB	0	1,25	2,5	5	0
	HW16	Switch Ethernet 2 Oficina Principal	MB	0	1,25	2,5	5	0
	HW17	Switch Ethernet Nave	MB	0	1,25	2,5	4	0
	HW18	AP 1 Oficina Central	MB	0	1,25	2,5	4	0
	HW19	AP 2 Oficina Central	MB	0	1,25	2,5	4	0
	HW20	AP Nave	MB	0	0,75	1,5	3	0
	HW21	Router FTTH Oficina 1	MB	0	2	4	9	0
	HW22	Router FTTH Oficina 2	MB	0	2	4	9	0
	HW23	Router FTTH Nave	MB	0	1,75	3,5	6	0
	HW24	Firewall Nave	B	0	1,75	3,5	9	0
	HW25	Firewall segundo nivel CPD	A	0	2	4	9	0
	HW26	Firewall primer nivel CPD	A	0	2	4	9	0
	HW27	Firewall de Oficina	A	0	2	4	8	0
	HW28	Servidor SFTP	MB	0	1,5	3,5	2	0
	HW29	Servidor Web Corporativa	MB	0	1,75	4	3	0
	HW30	Servidor de Ficheros	MB	0	2	4	7	0
	HW31	Servidor de Directorio Activo	MB	0	2	4	7	0

	HW32	Servidor de BBDD corporativa	MB	0	2	4	7	0
	HW33	Servidor CAS	MB	0	2	4	7	0
	HW34	Servidor de I+D	MB	0	2,25	4	3	0
	HW35	Servidor ERP	MB	0	2	4	4	0
	HW36	Impresora de red planta 1 Oficina central	MB	0	0	0	0	0
	HW37	Impresora de red planta 2 Oficina central	MB	0	0	0	0	0
	HW38	Impresora de red Nave de operaciones	MB	0	0	0	0	0
	HW39	PC's tipo A (46 dispositivos)	MB	0	1,75	3,5	4	0
	HW40	PC's tipo B (4 dispositivos)	MB	0	1,75	3,5	4	0
	HW41	PC's tipo C (27 dispositivos)	MB	0	1,75	3,5	4	0
	HW42	Móvil tipo A (49 dispositivos)	MB	0	1,75	3,5	4	0
	HW43	Móvil tipo B (9 dispositivos)	MB	0	1,75	3,5	4	0
	HW44	Móvil tipo C (24 dispositivos)	MB	0	1,75	3,5	4	0
	HW45	Placa Base Sirio planta fotovoltaica de Almendralejo [BA]	A	0	2	4	8	0
	HW46	Placa Base Sirio planta fotovoltaica de Puertollano [CR]	A	0	2	4	8	0
	HW47	Placa Base Sirio planta fotovoltaica de Olmedilla de Alarcón [CU]	A	0	2	4	8	0
	HW48	Placa Base Sirio planta fotovoltaica de Arnedo [RI]	A	0	2	4	8	0
	HW49	Placa Base Sirio planta fotovoltaica de Las Gabias [GR]	A	0	2	4	8	0
	HW50	Placa Base Sirio planta fotovoltaica de Jumilla [MU]	A	0	2	4	8	0
	HW51	Placa Base Sirio planta fotovoltaica de Lorca [MU]	A	0	2	4	8	0
	HW52	Placa Base Sirio planta fotovoltaica de Olivenza [BA]	A	0	2	4	8	0

	HW53	Placa Base Sirio planta fotovoltaica de Calasparra [MU]	A	0	2	4	8	0
	HW54	Placa Base Sirio planta fotovoltaica de Beneixama [A]	A	0	2	4	8	0
	HW55	Placa Base Sirio planta fotovoltaica de Salamanca [SA]	A	0	2	4	8	0
	HW56	Placa Base Sirio planta fotovoltaica de El Coronil [SE]	A	0	2	4	8	0
	HW57	Placa Base Sirio planta fotovoltaica de Almaraz [CC]	A	0	2	4	8	0
	HW58	Placa Base Sirio planta fotovoltaica de El Bonillo [ALB]	A	0	2	4	8	0
	HW59	Placa Base Sirio planta fotovoltaica de Guadarranque [CA]	A	0	2	4	8	0
	HW60	Actuadores planta fotovoltaica de Almendralejo [BA] (200 sensores)	M	0	1,75	3,5	7	0
	HW61	Actuadores planta fotovoltaica de Puertollano [CR] (1333 sensores)	M	0	1,75	3,5	7	0
	HW62	Actuadores planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	M	0	1,75	3,5	7	0
	HW63	Actuadores planta fotovoltaica de Arnedo [RI] (300 sensores)	M	0	1,75	3,5	7	0
	HW64	Actuadores planta fotovoltaica de Las Gabias [GR] (550 sensores)	M	0	1,75	3,5	7	0
	HW65	Actuadores planta fotovoltaica de Jumilla [MU] (112 sensores)	M	0	1,75	3,5	7	0
	HW66	Actuadores planta fotovoltaica de Lorca [MU] (173 sensores)	M	0	1,75	3,5	7	0

	HW67	Actuadores planta fotovoltaica de Olivenza [BA] (200 sensores)	M	0	1,75	3,5	7	0
	HW68	Actuadores planta fotovoltaica de Calasparra [MU] (226 sensores)	M	0	1,75	3,5	7	0
	HW69	Actuadores planta fotovoltaica de Beneixama [A] (80 sensores)	M	0	1,75	3,5	7	0
	HW70	Actuadores planta fotovoltaica de Salamanca [SA] (125 sensores)	M	0	1,75	3,5	7	0
	HW71	Actuadores planta fotovoltaica de El Coronil [SE] (89 sensores)	M	0	1,75	3,5	7	0
	HW72	Actuadores planta fotovoltaica de Almaraz [CC] (255 sensores)	M	0	1,75	3,5	7	0
	HW73	Actuadores planta fotovoltaica de El Bonillo [ALB] (629 sensores)	M	0	1,75	3,5	7	0
	HW74	Actuadores planta fotovoltaica de Guadarranque [CA] (136 sensores)	M	0	1,75	3,5	7	0
	HW75	Sensores Sirio planta fotovoltaica de Almendralejo [BA] (200 sensores)	M	0	1,75	3,5	7	0
	HW76	Sensores Sirio planta fotovoltaica de Puertollano [CR] (1333 sensores)	M	0	1,75	3,5	7	0
	HW77	Sensores Sirio planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	M	0	1,75	3,5	7	0
	HW78	Sensores Sirio planta fotovoltaica de Arnedo [RI] (300 sensores)	M	0	1,75	3,5	7	0
	HW79	Sensores Sirio planta fotovoltaica de Las Gabias [GR] (550 sensores)	M	0	1,75	3,5	7	0

	HW80	Sensores Sirio planta fotovoltaica de Jumilla [MU] (112 sensores)	M	0	1,75	3,5	7	0
	HW81	Sensores Sirio planta fotovoltaica de Lorca [MU] (173 sensores)	M	0	1,75	3,5	7	0
	HW82	Sensores Sirio planta fotovoltaica de Olivenza [BA] (200 sensores)	M	0	1,75	3,5	7	0
	HW83	Sensores Sirio planta fotovoltaica de Calasparra [MU] (226 sensores)	M	0	1,75	3,5	7	0
	HW84	Sensores Sirio planta fotovoltaica de Beneixama [A] (80 sensores)	M	0	1,75	3,5	7	0
	HW85	Sensores Sirio planta fotovoltaica de Salamanca [SA] (125 sensores)	M	0	1,75	3,5	7	0
	HW86	Sensores Sirio planta fotovoltaica de El Coronil [SE] (89 sensores)	M	0	1,75	3,5	7	0
	HW87	Sensores Sirio planta fotovoltaica de Almaraz [CC] (255 sensores)	M	0	1,75	3,5	7	0
	HW88	Sensores Sirio planta fotovoltaica de El Bonillo [ALB] (629 sensores)	M	0	1,75	3,5	7	0
	HW89	Sensores Sirio planta fotovoltaica de Guadarranque [CA] (136 sensores)	M	0	1,75	3,5	7	0
Software [SW]	SW 1	Software principal sistema Sirio	MA	6,8	9	9	9	5,4
	SW 2	Software sensores sistema Sirio	MA	6,8	9	9	9	5,4
	SW 3	Software en desarrollo de I+D (3 unidades)	A	6,8	9	9	6	5,4
	SW 4	Sistema Operativos Windows 7 Enterprise Edition (50 unidades)	MB	4,5	7	7	5	4,2
	SW 5	Sistema Operativo Windows 10 Pro (27 unidades)	MB	4,5	7	7	5	0

	SW 6	Sistema Operativo Ubuntu Desktop (8 Unidades)	MB	4,5	7	7	5	4,2
	SW 7	Sistema Operativo Debian (10 Unidades)	MB	4,5	7	7	5	4,2
	SW 8	Sistema Operativo Android (70 Unidades)	MB	3,8	7	7	5	4,2
	SW 9	Sistema Operativo iOS (12 Unidades)	MB	3,8	7	7	5	4,2
	SW 10	Sistema Operativo CentOS (3 Unidades)	MB	4,5	7	7	5	4,2
	SW 11	Sistema Operativo Ubuntu Server (3 Unidades)	MB	4,5	7	7	5	4,2
	SW 12	Sistema Operativos Windows Server R2 2012 Enterprise Edition (26 Unidades)	A	6	9	9	7	5,4
	SW 13	Sistema Operativo DataOntap 8.3.5	A	6	9	9	9	5,4
	SW 14	SQL Server 2012 Enterprise Edition (6 unidades)	A	6	9	9	9	5,4
	SW 15	Maria DB (3 Unidades)	MB	5,3	7	7	4	4,2
	SW 16	Vmware vSphere 6.3 Enterprise Edition	A	6,8	9	9	9	5,4
	SW 17	Microsoft Navision (ERP)	B	5,3	7	8	7	4,2
	SW 18	Microsoft Active Directory	B	5,3	7	8	7	4,2
	SW 19	Open CAS	B	5,3	7	8	7	4,2
	SW 20	Apache Tomcat (3 Unidades)	B	4,5	6	6	5	4,2
	SW 21	Microsoft Information Services (6 Unidades)	B	4,5	6	6	5	4,2
	SW 22	Adobe Acrobat Pro (2 Unidades)	B	0,8	1	4	2	4,2
	SW 23	Antivirus TrendMicro Bussiness Security (80 Unidades)	B	6	8	9	8	5,4
	SW 24	Paquete Microsoft Office 365 (77)	B	4,5	6	7	4	4,2
	SW 25	Microsoft Project (5 Unidades)	B	4,5	6	7	4	4,2

	SW 26	Microsoft Visual Studio (7 Unidades)	B	4,5	6	7	4	4,2
	SW 27	Microsoft Visio (10 Unidades)	B	4,5	6	7	4	4,2
	SW 28	Catia V5 (4 Unidades)	B	4,5	6	7	4	4,2
	SW 29	AutoCAD 2015 (3 Unidades)	B	4,5	6	7	4	4,2
Datos [D]	D1	BBDD ERP Empleados	B	7	7	8	6	6
	D2	Datos Servidor de ficheros corporativo	B	7	7	8	6	6
	D3	BBDD Active Directory	B	7	7	8	6	6
	D4	BBDD Sistema Sirio (10 Unidades)	MA	9	9	9	9	6,8
	D5	BBDD Corporativa (Desarrollos Sirio)	MA	9	9	9	9	6,8
	D6	BBDD I+D	M	9	9	9	9	6,8
	D7	Copia de Seguridad de Sistemas Corporativos	M	7	7	8	9	6,8
	D8	Copia de Seguridad de Sistema Sirio	MA	9	9	9	9	6,8
	D9	Datos corporativos en móviles de empleados	M	7	7	8	9	6,8
	D10	Datos corporativos en PC's y soportes de almacenamiento ext. de empleados	MA	9	9	9	9	6,8
Red de comunicaciones [COM]	COM1	Acceso a Internet Principal Oficinas	A	6	6,75	6	9	0
	COM2	Acceso a Internet Secundario Oficinas	M	4,5	5,25	4,5	9	0
	COM3	Acceso a Internet Nave	M	4,5	4,5	4,5	6	0
	COM4	Líneas Móviles (77 Unidades)	B	2,3	5,25	4,5	6	0
	COM5	Línea voz fija principal oficinas	A	2,3	5,25	4,5	7	0
	COM6	Línea voz fija secundaria oficinas	B	2,3	5,25	4,5	7	0
	COM7	Línea voz fija nave oficinas	MB	2,3	5,25	4,5	5	0
	COM8	Acceso de Voz Fijo (5 Unidades)	MB	2,3	5,25	4,5	7	0
	COM9	Red de sensores planta fotovoltaica de Almendralejo [BA]	M	5,3	5,25	6	8	0

	COM10	Red de sensores planta fotovoltaica de Puertollano [CR]	M	5,3	5,25	6	8	0
	COM11	Red de sensores planta fotovoltaica de Olmedilla de Alarcón [CU]	M	5,3	5,25	6	8	0
	COM12	Red de sensores planta fotovoltaica de Arnedo [RI]	M	5,3	5,25	6	8	0
	COM13	Red de sensores planta fotovoltaica de Las Gabias [GR]	M	5,3	5,25	6	8	0
	COM14	Red de sensores planta fotovoltaica de Jumilla [MU]	M	5,3	5,25	6	8	0
	COM15	Red de sensores planta fotovoltaica de Lorca [MU]	M	5,3	5,25	6	8	0
	COM16	Red de sensores planta fotovoltaica de Olivenza [BA]	M	5,3	5,25	6	8	0
	COM17	Red de sensores planta fotovoltaica de Calasparra [MU]	M	5,3	5,25	6	8	0
	COM18	Red de sensores planta fotovoltaica de Beneixama [A]	M	5,3	5,25	6	8	0
	COM19	Red de sensores planta fotovoltaica de Salamanca [SA]	M	5,3	5,25	6	8	0
	COM20	Red de sensores planta fotovoltaica de El Coronil [SE]	M	5,3	5,25	6	8	0
	COM21	Red de sensores planta fotovoltaica de Almaraz [CC]	M	5,3	5,25	6	8	0
	COM22	Red de sensores planta fotovoltaica de El Bonillo [ALB]	M	5,3	5,25	6	8	0
	COM23	Red de sensores planta fotovoltaica de Guadarranque [CA]	M	5,3	5,25	6	8	0
	COM24	Acceso a Internet planta fotovoltaica de Almendralejo [BA]	A	5,3	5,25	6	8	0
	COM25	Acceso a Internet planta fotovoltaica de Puertollano [CR]	A	5,3	5,25	6	8	0

	COM26	Acceso a Internet planta fotovoltaica de Olmedilla de Alarcón [CU]	A	5,3	5,25	6	8	0
	COM27	Acceso a Internet planta fotovoltaica de Arnedo [RI]	A	5,3	5,25	6	8	0
	COM28	Acceso a Internet planta fotovoltaica de Las Gabias [GR]	A	5,3	5,25	6	8	0
	COM29	Acceso a Internet planta fotovoltaica de Jumilla [MU]	A	5,3	5,25	6	8	0
	COM30	Acceso a Internet planta fotovoltaica de Lorca [MU]	A	5,3	5,25	6	8	0
	COM31	Acceso a Internet planta fotovoltaica de Olivenza [BA]	A	5,3	5,25	6	8	0
	COM32	Acceso a Internet planta fotovoltaica de Calasparra [MU]	A	5,3	5,25	6	8	0
	COM33	Acceso a Internet planta fotovoltaica de Beneixama [A]	A	5,3	5,25	6	8	0
	COM34	Acceso a Internet planta fotovoltaica de Salamanca [SA]	A	5,3	5,25	6	8	0
	COM35	Acceso a Internet planta fotovoltaica de El Coronil [SE]	A	5,3	5,25	6	8	0
	COM36	Acceso a Internet planta fotovoltaica de Almaraz [CC]	A	5,3	5,25	6	8	0
	COM37	Acceso a Internet planta fotovoltaica de El Bonillo [ALB]	A	5,3	5,25	6	8	0
	COM38	Acceso a Internet planta fotovoltaica de Guadarranque [CA]	A	5,3	5,25	6	8	0
	COM39	Red LAN Oficina	M	5,3	5,25	6	7	0
	COM40	Red LAN CPD	MA	5,3	5,25	6	9	0
	COM41	Red LAN Nave	B	4,5	4,5	4,5	6	0
	COM42	Red inalámbrica oficinas	B	3,8	5,25	4,5	3	0
	COM43	Red inalámbrica nave	MB	3,8	4,5	4,5	3	0
Servicios [S]	S1	Correo electrónico corporativo [Para usuarios Internos]	B	5,6	5,25	5,3	70	5,6

	S2	Backup sistema Sirio [Para usuarios Internos]	MA	7,2	6,75	6,8	90	7,2
	S3	Centralita en la nube [Para usuarios Internos]	A	5,6	4,5	5,3	70	5,6
	S4	IaaS entorno de desarrollo [Para usuarios Internos]	MB	5,6	5,25	5,3	10	5,6
	S5	Servicio de Monitorización sistema Sirio [Para usuarios Externos]	MA	7,2	6,75	6,8	90	7,2
	S6	Servicio de Administración sistema Sirio [Para usuarios Externos]	MA	7,2	6,75	6,8	90	7,2
Equipamiento Auxiliar [AUX]	AUX1	Sistema de climatización CPD	A	0	0	0	9	0
	AUX2	Sistema de detección de incendios	A	0	0	0	9	0
	AUX3	Sistema de extinción de incendios	A	0	0	0	9	0
	AUX4	Sistema de detección de inundaciones	A	0	0	0	9	0
	AUX5	Sistema de alimentación Ininterrumpida	MA	0	0	0	9	0
	AUX6	Suministro eléctrico general	A	0	0	0	9	0
	AUX7	Cableado eléctrico	A	0	0	0	9	0
	AUX8	Cableado Estructurado Oficina	M	0	1,4	0	7	0
	AUX9	Fibra Óptica CPD	A	0	1,6	0	9	0
	AUX10	Cableado Estructurado CPD	A	0	1,6	0	9	0
	AUX11	Cableado Estructurado Nave	MB	0	1,6	0	6	0
	AUX12	Destructora de Papel	MB	0	0	0	1	0
Personal [P]	P1	Director General	A	0	0	0	9	0
	P2	Director Financiero	A	0	0	0	9	0
	P3	Director Comercial	M	0	0	0	9	0
	P4	Director de Operaciones	MA	0	0	0	9	0
	P5	Director Técnico	MA	0	0	0	9	0
	P6	Responsable de área de RRHH	B	0	0	0	8	0

	P7	Reclutadores de personal (2)	B	0	0	0	4	0
	P8	Gestores de RRLL (2)	B	0	0	0	6	0
	P9	Responsable de área Administración	B	0	0	0	8	0
	P10	Contables (4)	B	0	0	0	6	0
	P11	Asesor Fiscal	B	0	0	0	7	0
	P12	Abogado	B	0	0	0	7	0
	P13	Responsable de área de compras	B	0	0	0	8	0
	P14	Gestores de compras (4)	B	0	0	0	6	0
	P15	Comunity Manager	B	0	0	0	4	0
	P16	Gestores de Producto (2)	B	0	0	0	6	0
	P17	Responsable de área de ventas	B	0	0	0	8	0
	P18	Comerciales (5)	B	0	0	0	5	0
	P19	Responsable del área de Instaladores	M	0	0	0	8	0
	P20	Instaladores (23)	M	0	0	0	7	0
	P21	Responsable del área de Mantenimiento	A	0	0	0	8	0
	P22	Técnicos de mantenimiento (20)	A	0	0	0	7	0
	P23	Responsable del área de administración sistema Sirio	A	0	0	0	9	0
	P24	Administradores (6)	A	0	0	0	8	0
	P25	Responsable del área de TI	A	0	0	0	9	0
	P26	Técnicos de puesto de trabajo (2)	A	0	0	0	8	0
	P27	Técnicos de CPD (2)	A	0	0	0	8	0
	P28	Responsable del área de Software	A	0	0	0	9	0
	P29	Desarrolladores Software (7)	A	0	0	0	8	0
	P30	Responsable del área de Hardware	A	0	0	0	8	0
	P31	Desarrolladores Hardware (5)	A	0	0	0	8	0
	P32	Controladores de calidad Hardware (2)	A	0	0	0	7	0
	P33	Responsable del área de I+D	A	0	0	0	7	0
	P34	Proveedores	B	0	0	0	7	0

3.8 Nivel de Riesgo Aceptable y riesgo Residual

Sabiendo que la eliminación absoluta del riesgo es una situación casi imposible de alcanzar, es necesario definir un límite a partir del cual se pueda decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles.

Después de haber presentado el análisis de riesgos a la dirección de Ícaro S.A., esta ha decidido y aprobado que el nivel de riesgo aceptable para la empresa será de MEDIO. Todos los activos cuyo riesgo se posiciones por debajo o igual a este umbral no supondrán una amenaza importante para la seguridad de la empresa, su riesgo asociado será aceptable y no se tomarán medidas para su mitigación.

Por el contrario, los activos cuyo riesgo supere este umbral supondrán una amenaza para la seguridad de la empresa y se implantarán controles para mitigar su riesgo asociado. Una vez establecidos los controles de seguridad a los activos cuyo riesgo supere el valor este valor se reducirá, pero difícilmente podrá desaparecer, seguirá existiendo un riesgo al que se denomina residual.

Para calcular el riego de cada uno de los activos se usará la información obtenida en los anteriores análisis y se aplicará la siguiente formula:

Nivel de riesgo = Impacto potencial x frecuencia de la amenaza.

En la siguiente tabla bidimensional se muestra la relación entre el impacto y la frecuencia de la que se deduce el nivel de riesgo.

Tabla 18. Relación impacto/frecuencia

Riesgo		Frecuencia				
		MB (0,002)	B (0,005)	M (0,016)	A (0,071)	MA (1)
Impacto	MA (10)	A	MA	MA	MA	MA
	A (7-9)	M	A	A	MA	MA
	M (4-6)	B	M	M	A	A
	B (2-3)	MB	B	B	M	M
	MB (1)	MB	MB	MB	B	B

Como se ha realizado por eficiencia en el análisis de activos, se escoge el valor máximo de frecuencia de cada grupo de activos. Se muestra en la siguiente tabla.

Tabla 19. Valores máximos frecuencia

Grupo Activos	Valor	Valor Numérico
Instalaciones [L]	MEDIA	0,016438
Hardware [HW]		
Software [SW]		
Datos [D]		
Redes de comunicación [COM]		
Servicios [S]		
Equipamiento Auxiliar [AUX]		
Personal [P]	ALTA	0,071233

A continuación, se muestra la tabla resumen del análisis del nivel de riesgo por activo.

En el siguiente documento se pueden observar la tabla completa con los cálculos realizados.

Tabla 20. Resumen análisis de nivel de riesgo

Ámbito	ID	Activo	Nivel de riesgo				
			A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	0,000	0,111	0,074	0,148	0,000
	L2	Sala de departamento de RRHH	0,000	0,012	0,016	0,033	0,000
	L3	Sala departamento de administración	0,000	0,012	0,016	0,033	0,000
	L4	Despacho de departamento de Legal	0,000	0,012	0,016	0,033	0,000
	L5	Sala de departamento comercial	0,000	0,012	0,016	0,033	0,000
	L6	Sala administradores sistema Sirio	0,000	0,086	0,058	0,132	0,000
	L7	Sala de departamento de TI	0,000	0,086	0,058	0,132	0,000
	L8	Sala de departamento de desarrollo software	0,000	0,086	0,058	0,115	0,000
	L9	Sala de departamento de desarrollo hardware	0,000	0,086	0,058	0,115	0,000

	L10	Sala de departamento de I+D	0,000	0,086	0,058	0,115	0,000
	L11	Oficina nave de operaciones	0,000	0,012	0,016	0,066	0,000
	L12	Despacho del director general	0,000	0,012	0,049	0,016	0,000
	L13	Despacho del director financiero	0,000	0,012	0,049	0,016	0,000
	L14	Despacho del director de operaciones	0,000	0,012	0,049	0,016	0,000
	L15	Despacho del director técnico	0,000	0,012	0,049	0,016	0,000
	L16	Armario técnico planta fotovoltaica de Almendralejo [BA]	0,000	0,099	0,066	0,132	0,000
	L17	Armario técnico planta fotovoltaica de Puertollano [CR]	0,000	0,099	0,066	0,132	0,000
	L18	Armario técnico planta fotovoltaica de Olmedilla de Alarcón [CU]	0,000	0,099	0,066	0,132	0,000
	L19	Armario técnico planta fotovoltaica de Arnedo [RI]	0,000	0,099	0,066	0,132	0,000
	L20	Armario técnico planta fotovoltaica de Las Gabias [GR]	0,000	0,099	0,066	0,132	0,000
	L21	Armario técnico planta fotovoltaica de Jumilla [MU]	0,000	0,099	0,066	0,132	0,000
	L22	Armario técnico planta fotovoltaica de Lorca [MU]	0,000	0,099	0,066	0,132	0,000
	L23	Armario técnico planta fotovoltaica de Olivenza [BA]	0,000	0,099	0,066	0,132	0,000
	L24	Armario técnico planta fotovoltaica de Calasparra [MU]	0,000	0,099	0,066	0,132	0,000
	L25	Armario técnico planta fotovoltaica de Beneixama [A]	0,000	0,099	0,066	0,132	0,000
	L26	Armario técnico planta fotovoltaica de Salamanca [SA]	0,000	0,099	0,066	0,132	0,000
	L27	Armario técnico planta fotovoltaica de El Coronil [SE]	0,000	0,099	0,066	0,132	0,000

	L28	Armario técnico planta fotovoltaica de Almaraz [CC]	0,000	0,099	0,066	0,132	0,000
	L29	Armario técnico planta fotovoltaica de El Bonillo [ALB]	0,000	0,099	0,066	0,132	0,000
	L30	Armario técnico planta fotovoltaica de Guadarranque [CA]	0,000	0,099	0,066	0,132	0,000
Hardware [HW]	HW1	Servidor 1 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW2	Servidor 2 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW3	Servidor 3 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW4	Servidor 4 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW5	Servidor 5 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW6	Servidor 6 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW7	Servidor 7 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW8	Servidor 8 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW9	Switch SAN 1	0,000	0,033	0,066	0,132	0,000
	HW10	Switch SAN 2	0,000	0,033	0,066	0,132	0,000
	HW11	Cabina de Almacenamiento	0,000	0,037	0,074	0,148	0,000
	HW12	Switch Ethernet Red de Gestión Sirio	0,000	0,033	0,066	0,148	0,000
	HW13	Switch Ethernet Red Externa	0,000	0,029	0,058	0,099	0,000
	HW14	Switch Ethernet Red Interna	0,000	0,029	0,058	0,115	0,000
	HW15	Switch Ethernet 1 Oficina Principal	0,000	0,021	0,041	0,082	0,000
	HW16	Switch Ethernet 2 Oficina Principal	0,000	0,021	0,041	0,082	0,000
	HW17	Switch Ethernet Nave	0,000	0,021	0,041	0,066	0,000
	HW18	AP 1 Oficina Central	0,000	0,021	0,041	0,066	0,000
	HW19	AP 2 Oficina Central	0,000	0,021	0,041	0,066	0,000
	HW20	AP Nave	0,000	0,012	0,025	0,049	0,000
	HW21	Router FTTH Oficina 1	0,000	0,033	0,066	0,148	0,000
	HW22	Router FTTH Oficina 2	0,000	0,033	0,066	0,148	0,000

	HW23	Router FTTH Nave	0,000	0,029	0,058	0,099	0,000
	HW24	Firewall Nave	0,000	0,029	0,058	0,148	0,000
	HW25	Firewall segundo nivel CPD	0,000	0,033	0,066	0,148	0,000
	HW26	Firewall primer nivel CPD	0,000	0,033	0,066	0,148	0,000
	HW27	Firewall de Oficina	0,000	0,033	0,066	0,132	0,000
	HW28	Servidor SFTP	0,000	0,025	0,058	0,033	0,000
	HW29	Servidor Web Corporativa	0,000	0,029	0,066	0,049	0,000
	HW30	Servidor de Ficheros	0,000	0,033	0,066	0,115	0,000
	HW31	Servidor de Directorio Activo	0,000	0,033	0,066	0,115	0,000
	HW32	Servidor de BBDD corporativa	0,000	0,033	0,066	0,115	0,000
	HW33	Servidor CAS	0,000	0,033	0,066	0,115	0,000
	HW34	Servidor de I+D	0,000	0,037	0,066	0,049	0,000
	HW35	Servidor ERP	0,000	0,033	0,066	0,066	0,000
	HW36	Impresora de red planta 1 Oficina central	0,000	0,000	0,000	0,000	0,000
	HW37	Impresora de red planta 2 Oficina central	0,000	0,000	0,000	0,000	0,000
	HW38	Impresora de red Nave de operaciones	0,000	0,000	0,000	0,000	0,000
	HW39	PC's tipo A (46 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW40	PC's tipo B (4 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW41	PC's tipo C (27 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW42	Móvil tipo A (49 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW43	Móvil tipo B (9 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW44	Móvil tipo C (24 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW45	Placa Base Sirio planta fotovoltaica de Almendralejo [BA]	0,000	0,033	0,066	0,132	0,000
	HW46	Placa Base Sirio planta fotovoltaica de Puertollano [CR]	0,000	0,033	0,066	0,132	0,000
	HW47	Placa Base Sirio planta fotovoltaica de Olmedilla de Alarcón [CU]	0,000	0,033	0,066	0,132	0,000
	HW48	Placa Base Sirio planta fotovoltaica de Arnedo [RI]	0,000	0,033	0,066	0,132	0,000

	HW49	Placa Base Sirio planta fotovoltaica de Las Gabias [GR]	0,000	0,033	0,066	0,132	0,000
	HW50	Placa Base Sirio planta fotovoltaica de Jumilla [MU]	0,000	0,033	0,066	0,132	0,000
	HW51	Placa Base Sirio planta fotovoltaica de Lorca [MU]	0,000	0,033	0,066	0,132	0,000
	HW52	Placa Base Sirio planta fotovoltaica de Olivenza [BA]	0,000	0,033	0,066	0,132	0,000
	HW53	Placa Base Sirio planta fotovoltaica de Calasparra [MU]	0,000	0,033	0,066	0,132	0,000
	HW54	Placa Base Sirio planta fotovoltaica de Beneixama [A]	0,000	0,033	0,066	0,132	0,000
	HW55	Placa Base Sirio planta fotovoltaica de Salamanca [SA]	0,000	0,033	0,066	0,132	0,000
	HW56	Placa Base Sirio planta fotovoltaica de El Coronil [SE]	0,000	0,033	0,066	0,132	0,000
	HW57	Placa Base Sirio planta fotovoltaica de Almaraz [CC]	0,000	0,033	0,066	0,132	0,000
	HW58	Placa Base Sirio planta fotovoltaica de El Bonillo [ALB]	0,000	0,033	0,066	0,132	0,000
	HW59	Placa Base Sirio planta fotovoltaica de Guadarranque [CA]	0,000	0,033	0,066	0,132	0,000
	HW60	Actuadores planta fotovoltaica de Almendralejo [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW61	Actuadores planta fotovoltaica de Puertollano [CR] (1333 sensores)	0,000	0,029	0,058	0,115	0,000
	HW62	Actuadores planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW63	Actuadores planta fotovoltaica de Arnedo [RI] (300 sensores)	0,000	0,029	0,058	0,115	0,000

	HW64	Actuadores planta fotovoltaica de Las Gabias [GR] (550 sensores)	0,000	0,029	0,058	0,115	0,000
	HW65	Actuadores planta fotovoltaica de Jumilla [MU] (112 sensores)	0,000	0,029	0,058	0,115	0,000
	HW66	Actuadores planta fotovoltaica de Lorca [MU] (173 sensores)	0,000	0,029	0,058	0,115	0,000
	HW67	Actuadores planta fotovoltaica de Olivenza [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW68	Actuadores planta fotovoltaica de Calasparra [MU] (226 sensores)	0,000	0,029	0,058	0,115	0,000
	HW69	Actuadores planta fotovoltaica de Beneixama [A] (80 sensores)	0,000	0,029	0,058	0,115	0,000
	HW70	Actuadores planta fotovoltaica de Salamanca [SA] (125 sensores)	0,000	0,029	0,058	0,115	0,000
	HW71	Actuadores planta fotovoltaica de El Coronil [SE] (89 sensores)	0,000	0,029	0,058	0,115	0,000
	HW72	Actuadores planta fotovoltaica de Almaraz [CC] (255 sensores)	0,000	0,029	0,058	0,115	0,000
	HW73	Actuadores planta fotovoltaica de El Bonillo [ALB] (629 sensores)	0,000	0,029	0,058	0,115	0,000
	HW74	Actuadores planta fotovoltaica de Guadarranque [CA] (136 sensores)	0,000	0,029	0,058	0,115	0,000
	HW75	Sensores Sirio planta fotovoltaica de Almendralejo [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW76	Sensores Sirio planta fotovoltaica de Puertollano [CR] (1333 sensores)	0,000	0,029	0,058	0,115	0,000
	HW77	Sensores Sirio planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	0,000	0,029	0,058	0,115	0,000

	HW78	Sensores Sirio planta fotovoltaica de Arnedo [RI] (300 sensores)	0,000	0,029	0,058	0,115	0,000
	HW79	Sensores Sirio planta fotovoltaica de Las Gabias [GR] (550 sensores)	0,000	0,029	0,058	0,115	0,000
	HW80	Sensores Sirio planta fotovoltaica de Jumilla [MU] (112 sensores)	0,000	0,029	0,058	0,115	0,000
	HW81	Sensores Sirio planta fotovoltaica de Lorca [MU] (173 sensores)	0,000	0,029	0,058	0,115	0,000
	HW82	Sensores Sirio planta fotovoltaica de Olivenza [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW83	Sensores Sirio planta fotovoltaica de Calasparra [MU] (226 sensores)	0,000	0,029	0,058	0,115	0,000
	HW84	Sensores Sirio planta fotovoltaica de Beneixama [A] (80 sensores)	0,000	0,029	0,058	0,115	0,000
	HW85	Sensores Sirio planta fotovoltaica de Salamanca [SA] (125 sensores)	0,000	0,029	0,058	0,115	0,000
	HW86	Sensores Sirio planta fotovoltaica de El Coronil [SE] (89 sensores)	0,000	0,029	0,058	0,115	0,000
	HW87	Sensores Sirio planta fotovoltaica de Almaraz [CC] (255 sensores)	0,000	0,029	0,058	0,115	0,000
	HW88	Sensores Sirio planta fotovoltaica de El Bonillo [ALB] (629 sensores)	0,000	0,029	0,058	0,115	0,000
	HW89	Sensores Sirio planta fotovoltaica de Guadarranque [CA] (136 sensores)	0,000	0,029	0,058	0,115	0,000
Software [SW]	SW 1	Software principal sistema Sirio	0,111	0,148	0,148	0,148	0,089
	SW 2	Software sensores sistema Sirio	0,111	0,148	0,148	0,148	0,089
	SW 3	Software en desarrollo de I+D (3 unidades)	0,111	0,148	0,148	0,099	0,089
	SW 4	Sistema Operativos Windows 7 Enterprise Edition (50 unidades)	0,074	0,115	0,115	0,082	0,069

	SW 5	Sistema Operativo Windows 10 Pro (27 unidades)	0,074	0,115	0,115	0,082	0,000
	SW 6	Sistema Operativo Ubuntu Desktop (8 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 7	Sistema Operativo Debian (10 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 8	Sistema Operativo Android (70 Unidades)	0,062	0,115	0,115	0,082	0,069
	SW 9	Sistema Operativo iOS (12 Unidades)	0,062	0,115	0,115	0,082	0,069
	SW 10	Sistema Operativo CentOS (3 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 11	Sistema Operativo Ubuntu Server (3 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 12	Sistema Operativos Windows Server R2 2012 Enterprise Edition (26 Unidades)	0,099	0,148	0,148	0,115	0,089
	SW 13	Sistema Operativo DataOntap 8.3.5	0,099	0,148	0,148	0,148	0,089
	SW 14	SQL Server 2012 Enterprise Edition (6 unidades)	0,099	0,148	0,148	0,148	0,089
	SW 15	Maria DB (3 Unidades)	0,086	0,115	0,115	0,066	0,069
	SW 16	Vmware vSphere 6.3 Enterprise Edition	0,111	0,148	0,148	0,148	0,089
	SW 17	Microsoft Navision (ERP)	0,086	0,115	0,132	0,115	0,069
	SW 18	Microsoft Active Directory	0,086	0,115	0,132	0,115	0,069
	SW 19	Open CAS	0,086	0,115	0,132	0,115	0,069
	SW 20	Apache Tomcat (3 Unidades)	0,074	0,099	0,099	0,082	0,069
	SW 21	Microsoft Information Services (6 Unidades)	0,074	0,099	0,099	0,082	0,069
	SW 22	Adobe Acrobat Pro (2 Unidades)	0,012	0,016	0,066	0,033	0,069
	SW 23	Antivirus TrendMicro Bussiness Security (80 Unidades)	0,099	0,132	0,148	0,132	0,089
	SW 24	Paquete Microsoft Office 365 (77)	0,074	0,099	0,115	0,066	0,069
	SW 25	Microsoft Project (5 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 26	Microsoft Visual Studio (7 Unidades)	0,074	0,099	0,115	0,066	0,069

	SW 27	Microsoft Visio (10 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 28	Catia V5 (4 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 29	AutoCAD 2015 (3 Unidades)	0,074	0,099	0,115	0,066	0,069
Datos [D]	D1	BBDD ERP Empleados	0,115	0,115	0,132	0,099	0,099
	D2	Datos Servidor de ficheros corporativo	0,115	0,115	0,132	0,099	0,099
	D3	BBDD Active Directory	0,115	0,115	0,132	0,099	0,099
	D4	BBDD Sistema Sirio (10 Unidades)	0,148	0,148	0,148	0,148	0,111
	D5	BBDD Corporativa (Desarrollos Sirio)	0,148	0,148	0,148	0,148	0,111
	D6	BBDD I+D	0,148	0,148	0,148	0,148	0,111
	D7	Copia de Seguridad de Sistemas Corporativos	0,115	0,115	0,132	0,148	0,111
	D8	Copia de Seguridad de Sistema Sirio	0,148	0,148	0,148	0,148	0,111
	D9	Datos corporativos en móviles de empleados	0,115	0,115	0,132	0,148	0,111
	D10	Datos corporativos en PC's y soportes de almacenamiento ext. de empleados	0,148	0,148	0,148	0,148	0,111
Red de comunicaciones [COM]	COM1	Acceso a Internet Principal Oficinas	0,099	0,111	0,099	0,148	0,000
	COM2	Acceso a Internet Secundario Oficinas	0,074	0,086	0,074	0,148	0,000
	COM3	Acceso a Internet Nave	0,074	0,074	0,074	0,099	0,000
	COM4	Líneas Móviles (77 Unidades)	0,037	0,086	0,074	0,099	0,000
	COM5	Línea voz fija principal oficinas	0,037	0,086	0,074	0,115	0,000
	COM6	Línea voz fija secundaria oficinas	0,037	0,086	0,074	0,115	0,000
	COM7	Línea voz fija nave oficinas	0,037	0,086	0,074	0,082	0,000
	COM8	Acceso de Voz Fijo (5 Unidades)	0,037	0,086	0,074	0,115	0,000
	COM9	Red de sensores planta fotovoltaica de Almendralejo [BA]	0,086	0,086	0,099	0,132	0,000
	COM10	Red de sensores planta fotovoltaica de Puertollano [CR]	0,086	0,086	0,099	0,132	0,000

	COM11	Red de sensores planta fotovoltaica de Olmedilla de Alarcón [CU]	0,086	0,086	0,099	0,132	0,000
	COM12	Red de sensores planta fotovoltaica de Arnedo [RI]	0,086	0,086	0,099	0,132	0,000
	COM13	Red de sensores planta fotovoltaica de Las Gabias [GR]	0,086	0,086	0,099	0,132	0,000
	COM14	Red de sensores planta fotovoltaica de Jumilla [MU]	0,086	0,086	0,099	0,132	0,000
	COM15	Red de sensores planta fotovoltaica de Lorca [MU]	0,086	0,086	0,099	0,132	0,000
	COM16	Red de sensores planta fotovoltaica de Olivenza [BA]	0,086	0,086	0,099	0,132	0,000
	COM17	Red de sensores planta fotovoltaica de Calasparra [MU]	0,086	0,086	0,099	0,132	0,000
	COM18	Red de sensores planta fotovoltaica de Beneixama [A]	0,086	0,086	0,099	0,132	0,000
	COM19	Red de sensores planta fotovoltaica de Salamanca [SA]	0,086	0,086	0,099	0,132	0,000
	COM20	Red de sensores planta fotovoltaica de El Coronil [SE]	0,086	0,086	0,099	0,132	0,000
	COM21	Red de sensores planta fotovoltaica de Almaraz [CC]	0,086	0,086	0,099	0,132	0,000
	COM22	Red de sensores planta fotovoltaica de El Bonillo [ALB]	0,086	0,086	0,099	0,132	0,000
	COM23	Red de sensores planta fotovoltaica de Guadarranque [CA]	0,086	0,086	0,099	0,132	0,000
	COM24	Acceso a Internet planta fotovoltaica de Almendralejo [BA]	0,086	0,086	0,099	0,132	0,000
	COM25	Acceso a Internet planta fotovoltaica de Puertollano [CR]	0,086	0,086	0,099	0,132	0,000
	COM26	Acceso a Internet planta fotovoltaica de Olmedilla de Alarcón [CU]	0,086	0,086	0,099	0,132	0,000

	COM27	Acceso a Internet planta fotovoltaica de Arnedo [RI]	0,086	0,086	0,099	0,132	0,000
	COM28	Acceso a Internet planta fotovoltaica de Las Gabias [GR]	0,086	0,086	0,099	0,132	0,000
	COM29	Acceso a Internet planta fotovoltaica de Jumilla [MU]	0,086	0,086	0,099	0,132	0,000
	COM30	Acceso a Internet planta fotovoltaica de Lorca [MU]	0,086	0,086	0,099	0,132	0,000
	COM31	Acceso a Internet planta fotovoltaica de Olivenza [BA]	0,086	0,086	0,099	0,132	0,000
	COM32	Acceso a Internet planta fotovoltaica de Calasparra [MU]	0,086	0,086	0,099	0,132	0,000
	COM33	Acceso a Internet planta fotovoltaica de Beneixama [A]	0,086	0,086	0,099	0,132	0,000
	COM34	Acceso a Internet planta fotovoltaica de Salamanca [SA]	0,086	0,086	0,099	0,132	0,000
	COM35	Acceso a Internet planta fotovoltaica de El Coronil [SE]	0,086	0,086	0,099	0,132	0,000
	COM36	Acceso a Internet planta fotovoltaica de Almaraz [CC]	0,086	0,086	0,099	0,132	0,000
	COM37	Acceso a Internet planta fotovoltaica de El Bonillo [ALB]	0,086	0,086	0,099	0,132	0,000
	COM38	Acceso a Internet planta fotovoltaica de Guadarranque [CA]	0,086	0,086	0,099	0,132	0,000
	COM39	Red LAN Oficina	0,086	0,086	0,099	0,115	0,000
	COM40	Red LAN CPD	0,086	0,086	0,099	0,148	0,000
	COM41	Red LAN Nave	0,074	0,074	0,074	0,099	0,000
	COM42	Red inalámbrica oficinas	0,062	0,086	0,074	0,049	0,000
	COM43	Red inalámbrica nave	0,062	0,074	0,074	0,049	0,000
Servicios [S]	S1	Correo electrónico corporativo [Para usuarios Internos]	0,092	0,086	0,086	1,151	0,092
	S2	Backup sistema sirio [Para usuarios Internos]	0,118	0,111	0,111	1,479	0,118
	S3	Centralita en la nube [Para usuarios Internos]	0,092	0,074	0,086	1,151	0,092

	S4	IaaS entorno de desarrollo [Para usuarios Internos]	0,092	0,086	0,086	0,164	0,092
	S5	Servicio de Monitorización sistema Sirio [Para usuarios Externos]	0,118	0,111	0,111	1,479	0,118
	S6	Servicio de Administración sistema Sirio [Para usuarios Externos]	0,118	0,111	0,111	1,479	0,118
Equipamiento Auxiliar [AUX]	AUX1	Sistema de climatización CPD	0,000	0,000	0,000	0,148	0,000
	AUX2	Sistema de detección de incendios	0,000	0,000	0,000	0,148	0,000
	AUX3	Sistema de extinción de incendios	0,000	0,000	0,000	0,148	0,000
	AUX4	Sistema de detección de inundaciones	0,000	0,000	0,000	0,148	0,000
	AUX5	Sistema de alimentación Ininterrumpida	0,000	0,000	0,000	0,148	0,000
	AUX6	Suministro eléctrico general	0,000	0,000	0,000	0,148	0,000
	AUX7	Cableado eléctrico	0,000	0,000	0,000	0,148	0,000
	AUX8	Cableado Estructurado Oficina	0,000	0,023	0,000	0,115	0,000
	AUX9	Fibra Óptica CPD	0,000	0,026	0,000	0,148	0,000
	AUX10	Cableado Estructurado CPD	0,000	0,026	0,000	0,148	0,000
	AUX11	Cableado Estructurado Nave	0,000	0,026	0,000	0,099	0,000
	AUX12	Destructora de Papel	0,000	0,000	0,000	0,016	0,000
Personal [P]	P1	Director General	0,000	0,000	0,000	0,641	0,000
	P2	Director Financiero	0,000	0,000	0,000	0,641	0,000
	P3	Director Comercial	0,000	0,000	0,000	0,641	0,000
	P4	Director de Operaciones	0,000	0,000	0,000	0,641	0,000
	P5	Director Técnico	0,000	0,000	0,000	0,641	0,000
	P6	Responsable de área de RRHH	0,000	0,000	0,000	0,570	0,000
	P7	Reclutadores de personal (2)	0,000	0,000	0,000	0,285	0,000
	P8	Gestores de RRLL (2)	0,000	0,000	0,000	0,427	0,000
	P9	Responsable de área Administración	0,000	0,000	0,000	0,570	0,000
	P10	Contables (4)	0,000	0,000	0,000	0,427	0,000
	P11	Asesor Fiscal	0,000	0,000	0,000	0,499	0,000
	P12	Abogado	0,000	0,000	0,000	0,499	0,000

	P13	Responsable de área de compras	0,000	0,000	0,000	0,570	0,000
	P14	Gestores de compras (4)	0,000	0,000	0,000	0,427	0,000
	P15	Comunity Manager	0,000	0,000	0,000	0,285	0,000
	P16	Gestores de Producto (2)	0,000	0,000	0,000	0,427	0,000
	P17	Responsable de área de ventas	0,000	0,000	0,000	0,570	0,000
	P18	Comerciales (5)	0,000	0,000	0,000	0,356	0,000
	P19	Responsable del área de Instaladores	0,000	0,000	0,000	0,570	0,000
	P20	Instaladores (23)	0,000	0,000	0,000	0,499	0,000
	P21	Responsable del área de Mantenimiento	0,000	0,000	0,000	0,570	0,000
	P22	Técnicos de mantenimiento (20)	0,000	0,000	0,000	0,499	0,000
	P23	Responsable del área de administración sistema sirio	0,000	0,000	0,000	0,641	0,000
	P24	Administradores (6)	0,000	0,000	0,000	0,570	0,000
	P25	Responsable del área de TI	0,000	0,000	0,000	0,641	0,000
	P26	Técnicos de puesto de trabajo (2)	0,000	0,000	0,000	0,570	0,000
	P27	Técnicos de CPD (2)	0,000	0,000	0,000	0,570	0,000
	P28	Responsable del área de Software	0,000	0,000	0,000	0,641	0,000
	P29	Desarrolladores Software (7)	0,000	0,000	0,000	0,570	0,000
	P30	Responsable del área de Hardware	0,000	0,000	0,000	0,570	0,000
	P31	Desarrolladores Hardware (5)	0,000	0,000	0,000	0,570	0,000
	P32	Controladores de calidad Hardware (2)	0,000	0,000	0,000	0,499	0,000
	P33	Responsable del área de I+D	0,000	0,000	0,000	0,499	0,000
	P34	Proveedores	0,000	0,000	0,000	0,499	0,000

Una vez expuestos el nivel de riesgo de todos los activos, se muestran aquellos que superan el nivel MEDIO que serán sobre los que se implanten medidas correctivas. Se muestra una tabla a continuación.

Tabla 21. Activos que superan el nivel MEDIO

Ámbito	ID	Activo	A	C	I	D	T
Instalaciones [L]	L1	Centro de proceso de Datos	0,000	0,111	0,074	0,148	0,000
	L2	Sala de departamento de RRHH	0,000	0,012	0,016	0,033	0,000
	L3	Sala departamento de administración	0,000	0,012	0,016	0,033	0,000
	L4	Despacho de departamento de Legal	0,000	0,012	0,016	0,033	0,000
	L5	Sala de departamento comercial	0,000	0,012	0,016	0,033	0,000
	L6	Sala administradores sistema Sirio	0,000	0,086	0,058	0,132	0,000
	L7	Sala de departamento de TI	0,000	0,086	0,058	0,132	0,000
	L8	Sala de departamento de desarrollo software	0,000	0,086	0,058	0,115	0,000
	L9	Sala de departamento de desarrollo hardware	0,000	0,086	0,058	0,115	0,000
	L10	Sala de departamento de I+D	0,000	0,086	0,058	0,115	0,000
	L11	Oficina nave de operaciones	0,000	0,012	0,016	0,066	0,000
	L12	Despacho del director general	0,000	0,012	0,049	0,016	0,000
	L13	Despacho del director financiero	0,000	0,012	0,049	0,016	0,000
	L14	Despacho del director de operaciones	0,000	0,012	0,049	0,016	0,000
	L15	Despacho del director técnico	0,000	0,012	0,049	0,016	0,000
	L16	Armario técnico planta fotovoltaica de Almendralejo [BA]	0,000	0,099	0,066	0,132	0,000
	L17	Armario técnico planta fotovoltaica de Puertollano [CR]	0,000	0,099	0,066	0,132	0,000
	L18	Armario técnico planta fotovoltaica de Olmedilla de Alarcón [CU]	0,000	0,099	0,066	0,132	0,000
	L19	Armario técnico planta fotovoltaica de Arnedo [RI]	0,000	0,099	0,066	0,132	0,000
	L20	Armario técnico planta fotovoltaica de Las Gabias [GR]	0,000	0,099	0,066	0,132	0,000
	L21	Armario técnico planta fotovoltaica de Jumilla [MU]	0,000	0,099	0,066	0,132	0,000
	L22	Armario técnico planta fotovoltaica de Lorca [MU]	0,000	0,099	0,066	0,132	0,000
	L23	Armario técnico planta fotovoltaica de Olivenza [BA]	0,000	0,099	0,066	0,132	0,000
	L24	Armario técnico planta fotovoltaica de Calasparra [MU]	0,000	0,099	0,066	0,132	0,000
	L25	Armario técnico planta fotovoltaica de Beneixama [A]	0,000	0,099	0,066	0,132	0,000
	L26	Armario técnico planta fotovoltaica de Salamanca [SA]	0,000	0,099	0,066	0,132	0,000
	L27	Armario técnico planta fotovoltaica de El Coronil [SE]	0,000	0,099	0,066	0,132	0,000
	L28	Armario técnico planta fotovoltaica de Almaraz [CC]	0,000	0,099	0,066	0,132	0,000
	L29	Armario técnico planta fotovoltaica de El Bonillo [ALB]	0,000	0,099	0,066	0,132	0,000
	L30	Armario técnico planta fotovoltaica de Guadarranque [CA]	0,000	0,099	0,066	0,132	0,000

Hardware [HW]	HW1	Servidor 1 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW2	Servidor 2 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW3	Servidor 3 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW4	Servidor 4 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW5	Servidor 5 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW6	Servidor 6 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW7	Servidor 7 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW8	Servidor 8 granja virtualización sistema Sirio	0,000	0,033	0,066	0,132	0,000
	HW9	Switch SAN 1	0,000	0,033	0,066	0,132	0,000
	HW10	Switch SAN 2	0,000	0,033	0,066	0,132	0,000
	HW11	Cabina de Almacenamiento	0,000	0,037	0,074	0,148	0,000
	HW12	Switch Ethernet Red de Gestión Sirio	0,000	0,033	0,066	0,148	0,000
	HW13	Switch Ethernet Red Externa	0,000	0,029	0,058	0,099	0,000
	HW14	Switch Ethernet Red Interna	0,000	0,029	0,058	0,115	0,000
	HW15	Switch Ethernet 1 Oficina Principal	0,000	0,021	0,041	0,082	0,000
	HW16	Switch Ethernet 2 Oficina Principal	0,000	0,021	0,041	0,082	0,000
	HW17	Switch Ethernet Nave	0,000	0,021	0,041	0,066	0,000
	HW18	AP 1 Oficina Central	0,000	0,021	0,041	0,066	0,000
	HW19	AP 2 Oficina Central	0,000	0,021	0,041	0,066	0,000
	HW20	AP Nave	0,000	0,012	0,025	0,049	0,000
	HW21	Router FTTH Oficina 1	0,000	0,033	0,066	0,148	0,000
	HW22	Router FTTH Oficina 2	0,000	0,033	0,066	0,148	0,000
	HW23	Router FTTH Nave	0,000	0,029	0,058	0,099	0,000
	HW24	Firewall Nave	0,000	0,029	0,058	0,148	0,000
	HW25	Firewall segundo nivel CPD	0,000	0,033	0,066	0,148	0,000
	HW26	Firewall primer nivel CPD	0,000	0,033	0,066	0,148	0,000
	HW27	Firewall de Oficina	0,000	0,033	0,066	0,132	0,000
	HW28	Servidor SFTP	0,000	0,025	0,058	0,033	0,000
	HW29	Servidor Web Corporativa	0,000	0,029	0,066	0,049	0,000
	HW30	Servidor de Ficheros	0,000	0,033	0,066	0,115	0,000
	HW31	Servidor de Directorio Activo	0,000	0,033	0,066	0,115	0,000
	HW32	Servidor de BBDD corporativa	0,000	0,033	0,066	0,115	0,000
	HW33	Servidor CAS	0,000	0,033	0,066	0,115	0,000
	HW34	Servidor de I+D	0,000	0,037	0,066	0,049	0,000
	HW35	Servidor ERP	0,000	0,033	0,066	0,066	0,000
	HW39	PC's tipo A (46 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW40	PC's tipo B (4 dispositivos)	0,000	0,029	0,058	0,066	0,000

	HW41	PC's tipo C (27 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW42	Móvil tipo A (49 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW43	Móvil tipo B (9 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW44	Móvil tipo C (24 dispositivos)	0,000	0,029	0,058	0,066	0,000
	HW45	Placa Base Sirio planta fotovoltaica de Almendralejo [BA]	0,000	0,033	0,066	0,132	0,000
	HW46	Placa Base Sirio planta fotovoltaica de Puertollano [CR]	0,000	0,033	0,066	0,132	0,000
	HW47	Placa Base Sirio planta fotovoltaica de Olmedilla de Alarcón [CU]	0,000	0,033	0,066	0,132	0,000
	HW48	Placa Base Sirio planta fotovoltaica de Arnedo [RI]	0,000	0,033	0,066	0,132	0,000
	HW49	Placa Base Sirio planta fotovoltaica de Las Gabias [GR]	0,000	0,033	0,066	0,132	0,000
	HW50	Placa Base Sirio planta fotovoltaica de Jumilla [MU]	0,000	0,033	0,066	0,132	0,000
	HW51	Placa Base Sirio planta fotovoltaica de Lorca [MU]	0,000	0,033	0,066	0,132	0,000
	HW52	Placa Base Sirio planta fotovoltaica de Olivenza [BA]	0,000	0,033	0,066	0,132	0,000
	HW53	Placa Base Sirio planta fotovoltaica de Calasparra [MU]	0,000	0,033	0,066	0,132	0,000
	HW54	Placa Base Sirio planta fotovoltaica de Beneixama [A]	0,000	0,033	0,066	0,132	0,000
	HW55	Placa Base Sirio planta fotovoltaica de Salamanca [SA]	0,000	0,033	0,066	0,132	0,000
	HW56	Placa Base Sirio planta fotovoltaica de El Coronil [SE]	0,000	0,033	0,066	0,132	0,000
	HW57	Placa Base Sirio planta fotovoltaica de Almaraz [CC]	0,000	0,033	0,066	0,132	0,000
	HW58	Placa Base Sirio planta fotovoltaica de El Bonillo [ALB]	0,000	0,033	0,066	0,132	0,000
	HW59	Placa Base Sirio planta fotovoltaica de Guadarranque [CA]	0,000	0,033	0,066	0,132	0,000
	HW60	Actuadores planta fotovoltaica de Almendralejo [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW61	Actuadores planta fotovoltaica de Puertollano [CR] (1333 sensores)	0,000	0,029	0,058	0,115	0,000
	HW62	Actuadores planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW63	Actuadores planta fotovoltaica de Arnedo [RI] (300 sensores)	0,000	0,029	0,058	0,115	0,000
	HW64	Actuadores planta fotovoltaica de Las Gabias [GR] (550 sensores)	0,000	0,029	0,058	0,115	0,000
	HW65	Actuadores planta fotovoltaica de Jumilla [MU] (112 sensores)	0,000	0,029	0,058	0,115	0,000
	HW66	Actuadores planta fotovoltaica de Lorca [MU] (173 sensores)	0,000	0,029	0,058	0,115	0,000
	HW67	Actuadores planta fotovoltaica de Olivenza [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW68	Actuadores planta fotovoltaica de Calasparra [MU] (226 sensores)	0,000	0,029	0,058	0,115	0,000
	HW69	Actuadores planta fotovoltaica de Beneixama [A] (80 sensores)	0,000	0,029	0,058	0,115	0,000
	HW70	Actuadores planta fotovoltaica de Salamanca [SA] (125 sensores)	0,000	0,029	0,058	0,115	0,000

	HW71	Actuadores planta fotovoltaica de El Coronil [SE] (89 sensores)	0,000	0,029	0,058	0,115	0,000
	HW72	Actuadores planta fotovoltaica de Almaraz [CC] (255 sensores)	0,000	0,029	0,058	0,115	0,000
	HW73	Actuadores planta fotovoltaica de El Bonillo [ALB] (629 sensores)	0,000	0,029	0,058	0,115	0,000
	HW74	Actuadores planta fotovoltaica de Guadarranque [CA] (136 sensores)	0,000	0,029	0,058	0,115	0,000
	HW75	Sensores Sirio planta fotovoltaica de Almendralejo [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW76	Sensores Sirio planta fotovoltaica de Puertollano [CR] (1333 sensores)	0,000	0,029	0,058	0,115	0,000
	HW77	Sensores Sirio planta fotovoltaica de Olmedilla de Alarcón [CU] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW78	Sensores Sirio planta fotovoltaica de Arnedo [RI] (300 sensores)	0,000	0,029	0,058	0,115	0,000
	HW79	Sensores Sirio planta fotovoltaica de Las Gabias [GR] (550 sensores)	0,000	0,029	0,058	0,115	0,000
	HW80	Sensores Sirio planta fotovoltaica de Jumilla [MU] (112 sensores)	0,000	0,029	0,058	0,115	0,000
	HW81	Sensores Sirio planta fotovoltaica de Lorca [MU] (173 sensores)	0,000	0,029	0,058	0,115	0,000
	HW82	Sensores Sirio planta fotovoltaica de Olivenza [BA] (200 sensores)	0,000	0,029	0,058	0,115	0,000
	HW83	Sensores Sirio planta fotovoltaica de Calasparra [MU] (226 sensores)	0,000	0,029	0,058	0,115	0,000
	HW84	Sensores Sirio planta fotovoltaica de Beneixama [A] (80 sensores)	0,000	0,029	0,058	0,115	0,000
	HW85	Sensores Sirio planta fotovoltaica de Salamanca [SA] (125 sensores)	0,000	0,029	0,058	0,115	0,000
	HW86	Sensores Sirio planta fotovoltaica de El Coronil [SE] (89 sensores)	0,000	0,029	0,058	0,115	0,000
	HW87	Sensores Sirio planta fotovoltaica de Almaraz [CC] (255 sensores)	0,000	0,029	0,058	0,115	0,000
	HW88	Sensores Sirio planta fotovoltaica de El Bonillo [ALB] (629 sensores)	0,000	0,029	0,058	0,115	0,000
	HW89	Sensores Sirio planta fotovoltaica de Guadarranque [CA] (136 sensores)	0,000	0,029	0,058	0,115	0,000
Software [SW]	SW 1	Software principal sistema Sirio	0,111	0,148	0,148	0,148	0,089
	SW 2	Software sensores sistema Sirio	0,111	0,148	0,148	0,148	0,089
	SW 3	Software en desarrollo de I+D (3 unidades)	0,111	0,148	0,148	0,099	0,089
	SW 4	Sistema Operativos Windows 7 Enterprise Edition (50 unidades)	0,074	0,115	0,115	0,082	0,069
	SW 5	Sistema Operativo Windows 10 Pro (27 unidades)	0,074	0,115	0,115	0,082	0,000
	SW 6	Sistema Operativo Ubuntu Desktop (8 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 7	Sistema Operativo Debian (10 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 8	Sistema Operativo Android (70 Unidades)	0,062	0,115	0,115	0,082	0,069
	SW 9	Sistema Operativo iOS (12 Unidades)	0,062	0,115	0,115	0,082	0,069
	SW 10	Sistema Operativo CentOS (3 Unidades)	0,074	0,115	0,115	0,082	0,069
	SW 11	Sistema Operativo Ubuntu Server (3 Unidades)	0,074	0,115	0,115	0,082	0,069

	SW 12	Sistema Operativos Windows Server R2 2012 Enterprise Edition (26 Unidades)	0,099	0,148	0,148	0,115	0,089
	SW 13	Sistema Operativo DataOntap 8.3.5	0,099	0,148	0,148	0,148	0,089
	SW 14	SQL Server 2012 Enterprise Edition (6 unidades)	0,099	0,148	0,148	0,148	0,089
	SW 15	Maria DB (3 Unidades)	0,086	0,115	0,115	0,066	0,069
	SW 16	Vmware vSphere 6.3 Enterprise Edition	0,111	0,148	0,148	0,148	0,089
	SW 17	Microsoft Navision (ERP)	0,086	0,115	0,132	0,115	0,069
	SW 18	Microsoft Active Directory	0,086	0,115	0,132	0,115	0,069
	SW 19	Open CAS	0,086	0,115	0,132	0,115	0,069
	SW 20	Apache Tomcat (3 Unidades)	0,074	0,099	0,099	0,082	0,069
	SW 21	Microsoft Information Services (6 Unidades)	0,074	0,099	0,099	0,082	0,069
	SW 22	Adobe Acrobat Pro (2 Unidades)	0,012	0,016	0,066	0,033	0,069
	SW 23	Antivirus TrendMicro Bussiness Security (80 Unidades)	0,099	0,132	0,148	0,132	0,089
	SW 24	Paquete Microsoft Office 365 (77)	0,074	0,099	0,115	0,066	0,069
	SW 25	Microsoft Project (5 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 26	Microsoft Visual Studio (7 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 27	Microsoft Visio (10 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 28	Catia V5 (4 Unidades)	0,074	0,099	0,115	0,066	0,069
	SW 29	AutoCAD 2015 (3 Unidades)	0,074	0,099	0,115	0,066	0,069
Datos [D]	D1	BBDD ERP Empleados	0,115	0,115	0,132	0,099	0,099
	D2	Datos Servidor de ficheros corporativo	0,115	0,115	0,132	0,099	0,099
	D3	BBDD Active Directory	0,115	0,115	0,132	0,099	0,099
	D4	BBDD Sistema Sirio (10 Unidades)	0,148	0,148	0,148	0,148	0,111
	D5	BBDD Corporativa (Desarrollos Sirio)	0,148	0,148	0,148	0,148	0,111
	D6	BBDD I+D	0,148	0,148	0,148	0,148	0,111
	D7	Copia de Seguridad de Sistemas Corporativos	0,115	0,115	0,132	0,148	0,148
	D8	Copia de Seguridad de Sistema Sirio	0,148	0,148	0,148	0,148	0,111
	D9	Datos corporativos en móviles de empleados	0,115	0,115	0,132	0,148	0,148
	D10	Datos corporativos en PC's y soportes de almacenamiento ext. de empleados	0,148	0,148	0,148	0,148	0,111
Red de comunicaciones [COM]	COM1	Acceso a Internet Principal Oficinas	0,099	0,111	0,099	0,148	0,000
	COM2	Acceso a Internet Secundario Oficinas	0,074	0,086	0,074	0,148	0,000
	COM3	Acceso a Internet Nave	0,074	0,074	0,074	0,099	0,000
	COM4	Líneas Móviles (77 Unidades)	0,037	0,086	0,074	0,099	0,000
	COM5	Línea voz fija principal oficinas	0,037	0,086	0,074	0,115	0,000
	COM6	Línea voz fija secundaria oficinas	0,037	0,086	0,074	0,115	0,000
	COM7	Línea voz fija nave oficinas	0,037	0,086	0,074	0,082	0,000
	COM8	Acceso de Voz Fijo (5 Unidades)	0,037	0,086	0,074	0,115	0,000
	COM9	Red de sensores planta fotovoltaica de Almendralejo [BA]	0,086	0,086	0,099	0,132	0,000

	COM10	Red de sensores planta fotovoltaica de Puertollano [CR]	0,086	0,086	0,099	0,132	0,000
	COM11	Red de sensores planta fotovoltaica de Olmedilla de Alarcón [CU]	0,086	0,086	0,099	0,132	0,000
	COM12	Red de sensores planta fotovoltaica de Arnedo [RI]	0,086	0,086	0,099	0,132	0,000
	COM13	Red de sensores planta fotovoltaica de Las Gabias [GR]	0,086	0,086	0,099	0,132	0,000
	COM14	Red de sensores planta fotovoltaica de Jumilla [MU]	0,086	0,086	0,099	0,132	0,000
	COM15	Red de sensores planta fotovoltaica de Lorca [MU]	0,086	0,086	0,099	0,132	0,000
	COM16	Red de sensores planta fotovoltaica de Olivenza [BA]	0,086	0,086	0,099	0,132	0,000
	COM17	Red de sensores planta fotovoltaica de Calasparra [MU]	0,086	0,086	0,099	0,132	0,000
	COM18	Red de sensores planta fotovoltaica de Beneixama [A]	0,086	0,086	0,099	0,132	0,000
	COM19	Red de sensores planta fotovoltaica de Salamanca [SA]	0,086	0,086	0,099	0,132	0,000
	COM20	Red de sensores planta fotovoltaica de El Coronil [SE]	0,086	0,086	0,099	0,132	0,000
	COM21	Red de sensores planta fotovoltaica de Almaraz [CC]	0,086	0,086	0,099	0,132	0,000
	COM22	Red de sensores planta fotovoltaica de El Bonillo [ALB]	0,086	0,086	0,099	0,132	0,000
	COM23	Red de sensores planta fotovoltaica de Guadarranque [CA]	0,086	0,086	0,099	0,132	0,000
	COM24	Acceso a Internet planta fotovoltaica de Almendralejo [BA]	0,086	0,086	0,099	0,132	0,000
	COM25	Acceso a Internet planta fotovoltaica de Puertollano [CR]	0,086	0,086	0,099	0,132	0,000
	COM26	Acceso a Internet planta fotovoltaica de Olmedilla de Alarcón [CU]	0,086	0,086	0,099	0,132	0,000
	COM27	Acceso a Internet planta fotovoltaica de Arnedo [RI]	0,086	0,086	0,099	0,132	0,000
	COM28	Acceso a Internet planta fotovoltaica de Las Gabias [GR]	0,086	0,086	0,099	0,132	0,000
	COM29	Acceso a Internet planta fotovoltaica de Jumilla [MU]	0,086	0,086	0,099	0,132	0,000
	COM30	Acceso a Internet planta fotovoltaica de Lorca [MU]	0,086	0,086	0,099	0,132	0,000
	COM31	Acceso a Internet planta fotovoltaica de Olivenza [BA]	0,086	0,086	0,099	0,132	0,000
	COM32	Acceso a Internet planta fotovoltaica de Calasparra [MU]	0,086	0,086	0,099	0,132	0,000
	COM33	Acceso a Internet planta fotovoltaica de Beneixama [A]	0,086	0,086	0,099	0,132	0,000
	COM34	Acceso a Internet planta fotovoltaica de Salamanca [SA]	0,086	0,086	0,099	0,132	0,000
	COM35	Acceso a Internet planta fotovoltaica de El Coronil [SE]	0,086	0,086	0,099	0,132	0,000
	COM36	Acceso a Internet planta fotovoltaica de Almaraz [CC]	0,086	0,086	0,099	0,132	0,000
	COM37	Acceso a Internet planta fotovoltaica de El Bonillo [ALB]	0,086	0,086	0,099	0,132	0,000
	COM38	Acceso a Internet planta fotovoltaica de Guadarranque [CA]	0,086	0,086	0,099	0,132	0,000

	COM39	Red LAN Oficina	0,086	0,086	0,099	0,115	0,000
	COM40	Red LAN CPD	0,086	0,086	0,099	0,148	0,000
	COM41	Red LAN Nave	0,074	0,074	0,074	0,099	0,000
	COM42	Red inalámbrica oficinas	0,062	0,086	0,074	0,049	0,000
	COM43	Red inalámbrica nave	0,062	0,074	0,074	0,049	0,000
Servicios [S]	S1	Correo electrónico corporativo [Para usuarios Internos]	0,092	0,086	0,086	1,151	0,092
	S2	Backup sistema Sirio [Para usuarios Internos]	0,118	0,111	0,111	1,479	0,118
	S3	Centralita en la nube [Para usuarios Internos]	0,092	0,074	0,086	1,151	0,092
	S4	IaaS entorno de desarrollo [Para usuarios Internos]	0,092	0,086	0,086	0,164	0,092
	S5	Servicio de Monitorización sistema Sirio [Para usuarios Externos]	0,118	0,111	0,111	1,479	0,118
	S6	Servicio de Administración sistema Sirio [Para usuarios Externos]	0,118	0,111	0,111	1,479	0,118
Equipamiento Auxiliar [AUX]	AUX1	Sistema de climatización CPD	0,000	0,000	0,000	0,148	0,000
	AUX2	Sistema de detección de incendios	0,000	0,000	0,000	0,148	0,000
	AUX3	Sistema de extinción de incendios	0,000	0,000	0,000	0,148	0,000
	AUX4	Sistema de detección de inundaciones	0,000	0,000	0,000	0,148	0,000
	AUX5	Sistema de alimentación Ininterrumpida	0,000	0,000	0,000	0,148	0,000
	AUX6	Suministro eléctrico general	0,000	0,000	0,000	0,148	0,000
	AUX7	Cableado eléctrico	0,000	0,000	0,000	0,148	0,000
	AUX8	Cableado Estructurado Oficina	0,000	0,023	0,000	0,115	0,000
	AUX9	Fibra Óptica CPD	0,000	0,026	0,000	0,148	0,000
	AUX10	Cableado Estructurado CPD	0,000	0,026	0,000	0,148	0,000
	AUX11	Cableado Estructurado Nave	0,000	0,026	0,000	0,099	0,000
	AUX12	Destructora de Papel	0,000	0,000	0,000	0,016	0,000
Personal [P]	P1	Director General	0,000	0,000	0,000	0,641	0,000
	P2	Director Financiero	0,000	0,000	0,000	0,641	0,000
	P3	Director Comercial	0,000	0,000	0,000	0,641	0,000
	P4	Director de Operaciones	0,000	0,000	0,000	0,641	0,000
	P5	Director Técnico	0,000	0,000	0,000	0,641	0,000
	P6	Responsable de área de RRHH	0,000	0,000	0,000	0,570	0,000
	P7	Reclutadores de personal (2)	0,000	0,000	0,000	0,285	0,000
	P8	Gestores de RRLL (2)	0,000	0,000	0,000	0,427	0,000
	P9	Responsable de área Administración	0,000	0,000	0,000	0,570	0,000
	P10	Contables (4)	0,000	0,000	0,000	0,427	0,000
	P11	Asesor Fiscal	0,000	0,000	0,000	0,499	0,000
	P12	Abogado	0,000	0,000	0,000	0,499	0,000
	P13	Responsable de área de compras	0,000	0,000	0,000	0,570	0,000
	P14	Gestores de compras (4)	0,000	0,000	0,000	0,427	0,000
	P15	Comunity Manager	0,000	0,000	0,000	0,285	0,000

	P16	Gestores de Producto (2)	0,000	0,000	0,000	0,427	0,000
	P17	Responsable de área de ventas	0,000	0,000	0,000	0,570	0,000
	P18	Comerciales (5)	0,000	0,000	0,000	0,356	0,000
	P19	Responsable del área de Instaladores	0,000	0,000	0,000	0,570	0,000
	P20	Instaladores (23)	0,000	0,000	0,000	0,499	0,000
	P21	Responsable del área de Mantenimiento	0,000	0,000	0,000	0,570	0,000
	P22	Técnicos de mantenimiento (20)	0,000	0,000	0,000	0,499	0,000
	P23	Responsable del área de administración sistema Sirio	0,000	0,000	0,000	0,641	0,000
	P24	Administradores (6)	0,000	0,000	0,000	0,570	0,000
	P25	Responsable del área de TI	0,000	0,000	0,000	0,641	0,000
	P26	Técnicos de puesto de trabajo (2)	0,000	0,000	0,000	0,570	0,000
	P27	Técnicos de CPD (2)	0,000	0,000	0,000	0,570	0,000
	P28	Responsable del área de Software	0,000	0,000	0,000	0,641	0,000
	P29	Desarrolladores Software (7)	0,000	0,000	0,000	0,570	0,000
	P30	Responsable del área de Hardware	0,000	0,000	0,000	0,570	0,000
	P31	Desarrolladores Hardware (5)	0,000	0,000	0,000	0,570	0,000
	P32	Controladores de calidad Hardware (2)	0,000	0,000	0,000	0,499	0,000
	P33	Responsable del área de I+D	0,000	0,000	0,000	0,499	0,000
	P34	Proveedores	0,000	0,000	0,000	0,499	0,000

Como se puede observar la mayoría de los activos de Ícaro S.A. superan el umbral de riesgo impuesto por la dirección, por lo que habrá que implantar medidas que mitiguen el nivel de riesgo.

4 Propuestas de proyectos

4.1 Introducción

Llegados a este punto, tras haber realizado el análisis de riesgos de Ícaro S.A., conocemos el nivel de riesgo actual en la empresa, por lo que estamos en disposición de plantear proyectos de medidas correctivas que mitiguen estos riesgos y mejoren el estado de la seguridad de la empresa.

Como se observa en el análisis de riesgos, la mayoría de los activos superan alguna de las dimensiones de seguridad. Abarcar todo en una primera y única iteración se presenta tedioso y costoso, por esta razón la mayoría de los proyectos presentados en este apartado estarán enfocados en priorizar la mitigación de aquellos riesgos que impacten más sobre el sistema de gestión Sirio (Core de la empresa) y los sistemas corporativos.

4.2 Propuestas

Tabla 22. Proyecto propuesto 1

4.2.1 Mejora de la política de seguridad de la empresa	
Objetivo	El objetivo de este proyecto es implantar una política de seguridad de la información que cumpla las siguientes necesidades: • Defina el alcance la política de seguridad de la información • Refleje el compromiso de la dirección de la empresa • Sea conocida y aplicada por toda la organización y terceros a los que aplique el cumplimiento • Cubra los aspectos fundamentales de los procesos de negocio de la empresa.
Descripción	El ánimo de este proyecto es realizar una revisión exhaustiva de la política de seguridad actual de Ícaro S.A. para que sea acorde a con sus procesos de negocio actuales. A modo de resumen, se exponen las tareas principales que se deben reflejar en la política de seguridad: • Designación de un comité de seguridad por parte de la dirección • Asignación de roles y responsabilidades relativas a seguridad de la información. • Establecer los controles y procedimientos para asegurar la seguridad de la información. Se realizará especial hincapié en aquellas políticas que afectan a: • Desarrollos Software • Desarrollos Hardware • Confidencialidad de los datos • Recursos Humanos • Datos fuera del entorno de la empresa.
Planificación	Se estima una duración de cuatro semanas laborables a jornada completa para su realización
Coste	Estimación de 2.500€ • Jornadas del Responsable de Seguridad • Jornadas del Comité de Seguridad • Jornadas del equipo de Dirección
Indicador	[IC1] N.º de revisiones de la política de seguridad por parte de la dirección.
Beneficios	• Mejora en la concienciación de los empleados y terceras partes involucradas en la seguridad de la información de la empresa • Mitigación de los riesgos de seguridad de la información • Mejora la imagen corporativa de la empresa. • Optimización de los procesos relativos a seguridad de la información

Activos Involucrados	Todos los activos de la compañía
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable/s	• Responsable de Seguridad de la Información • Comité de Seguridad • Dirección

Tabla 23. Proyecto propuesto 2

4.2.2 Formación continua en materia de seguridad	
Objetivo	El objetivo de este proyecto es implantar un plan de formación para concienciar a los empleados de la empresa de la importancia de la seguridad de la información para el correcto funcionamiento de los procesos en los que estén involucrados.
Descripción	Con este proyecto se pretende que los empleados reciban formación y capacitación en materia de seguridad de la información para el uso de los recursos y activos a los que tienen acceso en el desempeño de sus funciones. Los empleados adquirirán: • Formación sobre amenazas y su mitigación • Formación sobre canales seguros de comunicación • Formación acerca de los protocolos de actuación en caso de incidencias relacionadas con la seguridad de la información • Información sobre el proceso disciplinario recogido en la política de seguridad • Requisitos de seguridad y responsabilidad legal
Planificación	El curso se impartirá a la totalidad de la plantilla repartida en dos sesiones al año de una semana de duración para adaptarse a la disponibilidad de los empleados. Esta formación será realizada de manera bianual.
Coste	5.000€ bianuales
Indicador	• [IC6] Satisfacción de los cursos de formación relativos a seguridad • [IC44] Cumplimiento de las políticas de seguridad
Beneficios	• Disminución de los incidentes de seguridad • Incremento de la calidad en seguridad por parte de la empresa • Mejora de imagen corporativa • Optimización en el uso de los recursos

Activos Involucrados	Todos los activos de la empresa
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable/s	• Responsable de seguridad • Formador externo

Tabla 24. Proyecto propuesto 3

4.2.3 Mejora de la seguridad física de los elementos hardware desplegados en las plantas	
Objetivo	El objetivo de este proyecto es mejorar la seguridad de los armarios que integran los sistemas hardware del sistema Sirio en las plantas fotovoltaicas.
Descripción	Con este proyecto se pretende mejorar la seguridad física de los armarios técnicos de las plantas solares para mitigar el nivel de riesgo asociado. Este proyecto será abordado desde el área de I+D que propone las siguientes medidas que se integrarán en el sistema de monitorización de la planta en cuestión: • Sistema de cámara IP para vigilancia remota • Sistema de alarma para la apertura o manipulación de los armarios. • Sistema de presencia nocturna con activación de sistema lumínico disuasorio.
Planificación	Se estima una planificación de cuarenta semanas para acometer la implantación en las plantas que actualmente monitoriza la empresa
Coste	30.000€ distribuidos entre: • Jornadas de personal I+D • Jornadas de Instaladores • Materiales • Desplazamientos
Indicador	[IC15] Eficacia de las medidas de seguridad físicas
Beneficios	• Mitigación del riesgo asociado al hardware de control implantado en las plantas
Activos Involucrados	• Instalaciones [L16-30] • Hardware [HW 45-89] • Comunicaciones [COM 9-38] • Servicios [S 5-6]
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad

	• [A] Autenticidad
Responsable/s	• Responsable de seguridad • Responsable área I+D • Responsable área instaladores

Tabla 25. Proyecto propuesto 4

4.2.4 Mejora de la seguridad física en los accesos de la empresa y a estancias sensibles	
Objetivo	El objetivo de este proyecto es mejorar la seguridad física de acceso a las oficinas de la empresa en general y en particular a las estancias de las oficinas de la empresa que sean más sensibles.
Descripción	Con este proyecto se pretende restringir el acceso físico en general a las instalaciones de la empresa y en particular a aquellas estancias de las oficinas que sean sensibles a amenazas externas. Estas instalaciones sensibles son: • Centro de datos (Ya cuenta con un sistema así, se revisa y se integra con el resto) • Sala administradores del sistema Sirio • Sala del departamento de TI • Sala de desarrollos software • Sala de desarrollos hardware • Sala de I+D Se plantea controlar el acceso a las instalaciones de la empresa mediante un acceso NFC que constará de tornos y puertas gobernadas por un receptor y tarjetas identificativas para los empleados. Los privilegios de acceso serán diferenciados según el tipo de usuario y sus necesidades de acceso a las estancias marcadas como sensibles. Todo ello centralizado con el Directorio activo.
Planificación	Se estima una planificación veintiséis semanas para acometer el diseño e instalación de esta medida de seguridad.
Coste	50.000€ distribuidos entre: • Jornadas de personal I+D (Diseño) • Jornadas empresa externa (Instalación) • Materiales
Indicador	[IC15] Eficacia de las medidas de seguridad físicas
Beneficios	• Mitigación del riesgo asociado al hardware de control implantado en las plantas
Activos Involucrados	• Instalaciones [L1-15] • Hardware [HW 1-44] • Software [SW] • Datos [D] • Servicio [S]

	• Comunicaciones [COM 1-8] • Equipamiento auxiliar [AUX] • Personal [P]
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable/s	• Responsable de seguridad • Responsable área I+D • Proveedor externo

Tabla 26. Proyecto propuesto 5

4.2.5 Mejora de la disponibilidad de la infraestructura TI del sistema Sirio.	
Objetivo	El objetivo de este proyecto es mejorar la disponibilidad de los activos TI que soporten el sistema Sirio definiendo tiempos de RTO y RPO.
Descripción	Se pretende implantar un proyecto de replicación de los datos y de la infraestructura con un proveedor externo de TI en modalidad IaaS. Este modelo se compone de infraestructura x86 (CPU, RAM, Almacenamiento) en pago por uso para poder disponer de infraestructura de respaldo en caso de incidente. La información entre el sistema principal (alojado en el CPD de la empresa) y el servicio ofrecido del proveedor externo será replicada a nivel de hipervisor del sistema y deberá cumplir unos tiempos de RPO≈10min RTO≈30min Además del servicio de alta disponibilidad se implantará un servicio de Backup externo cifrado de los datos de sistema Sirio con el mismo proveedor. Las características del backup serán: • Copia full semanal con retención de 1 mes • Copia incremental diaria con retención semanal
Planificación	Se estima una planificación de unos veintiséis semanas para el diseño e implantación del servicio ofrecido por el proveedor externo.
Coste	30.000€ anuales distribuidos entre: • Implantación del servicio

	• Comunicaciones entre CPD de la empresa y CPD proveedor • Estimación de recursos PPU (pago por uso) anuales • Una prueba anual del servicio
Indicador	• [IC38] Eficacia de sistema de respuesta a incidentes • [IC39] Operatividad de los procesos que forman parte del plan de continuidad de negocio • [IC40] Porcentaje de sistemas críticos redundados
Beneficios	• Aumento de la disponibilidad de los activos TI que soportan el sistema Sirio.
Activos Involucrados	• Hardware [HW 1-12] • Software [SW 1-3, 12, 16] • Datos [D 4,8] • Servicio [S 2-3, 5-6] • Comunicaciones [COM 1-8]
Dimensiones de riesgo mitigadas	• [D] Disponibilidad
Responsable/s	• Responsable de seguridad • Responsable de TI • Proveedor externo

Tabla 27. Proyecto propuesto 6

4.2.6 Cifrado de los datos y comunicaciones del sistema Sirio	
Objetivo	El objetivo de este proyecto es mejorar la integridad y confidencialidad de la información del sistema Sirio
Descripción	Se desea cifrar la información del sistema Sirio en base a: • Cifrado de los datos almacenados en la cabina habilitando una licencia del fabricante habilitado para ello. • Cifrado de la comunicación entres sistemas desplegados en las plantas y los servidores mediante el uso de certificados SSL.
Planificación	Se estima una planificación doce semanas para el diseño e implantación.
Coste	• 1500€ para cifrado de las comunicaciones • 3250€ anuales en licencias de cifrado de cabina • 1500€ anuales para habilitar la opción de cifrado en el proveedor del servicio de alta disponibilidad. • 2000€ en jornadas del departamento TI y desarrollo.
Indicador	• [IC13] Eficacia de la política de encriptación de datos sensibles. • [IC14] Porcentaje de claves de sistemas iguales.
Beneficios	• Mejora de la integridad y confidencialidad de la información del sistema Sirio.
Activos Involucrados	• Hardware [HW 1-12] • Software [SW 1-3, 12, 16] • Datos [D 4,8] • Servicio [S 2-3, 5-6] • Comunicaciones [COM 1-8]
Dimensiones de riesgo mitigadas	• [I] Integridad • [C]Confidencialidad
Responsable/s	• Responsable de seguridad • Responsable de TI • Responsable de desarrollo software.

Tabla 28. Proyecto propuesto 7

4.2.7 Cifrado de los datos de los PC's y móviles	
Objetivo	El objetivo de este proyecto es mejorar la integridad y confidencialidad de la información de los activos de los empleados.
Descripción	Se desea cifrar la información base a: • Cifrado de los datos alojados en los discos duros de los PC's de los empleados mediante BitLocker

	• Cifrado de la información de los datos de los móviles de los empleados según SO que corresponda (Android o IOS)
Planificación	Se estima una planificación de 10 semanas para el diseño e implantación.
Coste	• 2000€ en jornadas del personal de TI
Indicador	• [IC13] Eficacia de la política de encriptación de datos sensibles. • [IC14] Porcentaje de claves de sistemas iguales.
Beneficios	• Mejora de la integridad y confidencialidad de la información en los activos de los empleados.
Activos Involucrados	• Hardware [HW 39-44] • Software [SW 8-9] • Datos [D 9,10]
Dimensiones de riesgo mitigadas	• [I] Integridad • [C]Confidencialidad
Responsable/s	• Responsable de seguridad • Responsable de TI

Tabla 29. Proyecto propuesto 8

4.2.8 Virtualización servidores entorno corporativo

Objetivo	Virtualizar los servidores que cuelgan de la “Red Externa” y de la “Red Interna” que proporcionan los servicios corporativos (Web corporativa, SFTP, Directorio activo, etc.)

Descripción	La intención de este proyecto es de dotar de mayor disponibilidad, seguridad y capacidad de crecimiento a los servidores que albergan los servicios corporativos de la empresa gracias a la virtualización. Además, se aprovecha que el hardware actual que soporta estos servicios está próximo a su fin de vida útil.
	
	Se estima los siguientes elementos hardware y software para su implementación:
	• 4 servidores x86 con las siguientes características:
	  ○ 2 x Procesador Intel Xeon Octacore 3,2 GHz
	  ○ 128 Gb de RAM
	  ○ 2 Discos SSD 500 Gb
	  ○ 4 Discos SAS 3 Tb
	  ○ 4 Interfaces Fibra
	  ○ 4 Interface cobre
	  ○ Soporte 4 años
	• Hipervisor VMware Enterprise con las siguientes funcionalidades licenciadas:
	  ○ vMotion
	  ○ Snapshot

	○ vSAN ○ NSX • Licencia Microsoft Windows Datacenter Edition
Planificación	Se estiman una duración de 20 semanas desde la petición del hardware y las licencias.
Coste	Alrededor de 50.000€ distribuidos en: • Hardware • Software/Licenciamiento • Jornadas departamento de TI
Indicador	• [IC32] Cumplimiento del control de cambios en entornos de desarrollo. • [IC39] Operatividad de los procesos que forman parte del plan de continuidad de negocio. • [IC40] Porcentaje de sistemas críticos redundados.
Beneficios	• Aumento de la disponibilidad • Aumento de la seguridad • Aumento de la capacidad de crecimiento
Activos Involucrados	• Hardware [HW 13-14, 28-35] • Software [SW 6-7,10,16-21] • Datos [D 1-3,5-7] • Comunicaciones [COM 40] • Servicios [S 1] • Equipamiento Auxiliar [AUX 10]
Dimensiones de riesgo mitigadas	• [D] Disponibilidad • [C] Confidencialidad • [I] Integridad
Responsable/s	• Responsable del departamento de TI • Responsable de Seguridad • Responsable del departamento de desarrollo

Tabla 30. Proyecto propuesto 9

4.2.9 Comunicaciones profesionales de acceso a Internet para la sede central	
Objetivo	Dotar de mayor disponibilidad en caso de incidente a las comunicaciones de datos de la sede central.
Descripción	Actualmente se cuenta en la sede principal de la empresa con un doble acceso a Internet, pero este es de tipo doméstico (FTTH) y no proporciona la calidad de servicio, ni los Acuerdos de Nivel de Servicio (SLA) adecuados. De estos accesos depende el sistema Sirio alojado en el CPD, por lo que se estima necesaria esta mejora. Por lo tanto, este proyecto trata de contratar con un proveedor de comunicaciones que proporcione un acceso redundado y diversificado (principal y backup) de acceso a internet con un ancho de banda de 300Mbps.
Planificación	Se estima una planificación de 3 semanas desde su contratación.
Coste	6000€ al año.
Indicador	[IC38] Eficacia de sistema de respuesta a incidentes.
Beneficios	• Mayor disponibilidad en caso de incidente. • Mejor calidad de servicio. • Mejor SLA.
Activos Involucrados	• Comunicaciones [COM1-2] • Hardware [HW] • Software [SW]
Dimensiones de riesgo mitigadas	• [D] Disponibilidad.
Responsable/s	• Responsable de seguridad. • Responsable del departamento de TI. • Proveedor Externo

Tabla 31. Proyecto propuesto 10

4.2.10 Red MPLS para monitorización de plantas	
Objetivo	Dotar de una red segura y de alta disponibilidad a las conexiones entre las plantas solares y la sede central de la empresa.
Descripción	Para mejorar la disponibilidad y seguridad de las comunicaciones del sistema Sirio, se propone la contratación de una red MPLS a un proveedor de comunicaciones externo que conecte en una misma red a Nivel 2 la sede de la empresa donde se concentra los sistemas de TI del sistema Sirio y las diferentes plantas solares donde se despliega el hardware de monitorización. Los accesos a esta red MPLS estarán redundados en la sede y en las diferentes plantas solares (Principal fibra/cobre Secundario 4G) y contará con cifrado de la información extremo a extremo.
Planificación	Desde la aceptación de la oferta propuesta por el proveedor externo se estima una duración de 26 semanas.
Coste	Se estima un coste de 50.000€ al año.
Indicador	• [IC13] Eficacia de la política de encriptación de datos sensibles. • [IC14] Porcentaje de claves de sistemas iguales. • [IC38] Eficacia de sistema de respuesta a incidentes.
Beneficios	• Mayor disponibilidad de las comunicaciones del sistema Sirio. • Mayor confidencialidad e integridad en la comunicación. • Aumento de la calidad de servicio de la comunicación • Mejores SLA. • Se elimina el acceso a Internet de las plantas
Activos Involucrados	• Hardware [HW] • Comunicaciones [COM 24-38,40]
Dimensiones de riesgo mitigadas	[D] Disponibilidad [I] Integridad [C]Confidencialidad
Responsable/s	• Responsable de seguridad. • Responsable del departamento de TI. • Proveedor externo

Tabla 32. Proyecto propuesto 11

4.2.11 Mejora seguridad perimetral de red de CPD	
Objetivo	• Mejorar la seguridad perimetral ante las nuevas amenazas de (APT's DDoS, etc). • Dotar de alta disponibilidad a los elementos de seguridad.
Descripción	Este proyecto trata de sustituir los elementos de seguridad perimetrales actuales (Cercanos a su fin de vida útil) por unos equipos con mayores funcionalidades y mayor rendimiento para así poder afrontar futuros crecimientos y amenazas más sofisticadas. Se dispondrá de dos equipos que se configurarán en modo clúster (activo/pasivo) para dotar de alta disponibilidad a la seguridad perimetral de CPD. Los equipos seleccionados son los Fortigate 100E que tienen las siguientes características: • Throughput hasta 7.4Gbps • 2 millones de sesiones concurrentes • Protección a Nivel 7 • IDS/IPS • VPN/SSL • Mitigación DDoS • NGFW • Integración con NSX de VMware • Monitorización en tiempo real y análisis de histórico Al integrase con la red definida por software de VMware no se estima necesario doble nivel de firewall físico ya que se implementa gracias a la virtualización.
Planificación	Desde la adquisición de los equipos hasta su instalación y puesta en producción se estima una duración de 12 semanas.
Coste	20.000€ que incluye • Hardware • Licenciamiento • Instalación • Configuración • Soporte a 4 años • Curso de formación personal TI
Indicador	• [IC10] Porcentaje de accesos no autorizados a la red de la empresa • [IC29] Eficacia de los equipos de seguridad de red
Beneficios	• Aumento de la seguridad perimetral

	• Aumento de las funcionalidades • Aumento de la disponibilidad • Mejor integración con el resto del hardware
Activos Involucrados	• Hardware [HW 1-35]
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable/s	• Responsable de Seguridad • Responsable de entorno TI

Tabla 33. Proyecto propuesto 12

4.2.12 Revisión de la seguridad de la información

Objetivo	Comprobar el cumplimiento de las políticas de seguridad de la información y los procesos y sistemas que las soportan.
Descripción	Consiste en la realización de una auditoría de primera parte realizada por un auditor externa para obtener una imagen del estado de la seguridad de la información de la empresa para valorar posibles medidas correctivas que lleven a la mejora de la seguridad.
Planificación	Este proceso tiene una duración de dos semanas y se repetirá anualmente,
Coste	Se estima un coste de 4000€ repartido en: • Jornadas empresa externa • Jornadas Responsable de seguridad • Jornadas Dirección
Indicador	• [IC44] Revisión independiente de la seguridad de la información.
Beneficios	• Obtener una visión de la seguridad de la empresa para tomar posibles acciones correctoras para garantizar la mejora continua en materia de seguridad de la información.
Activos Involucrados	Todos los activos
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad • [A] Autenticidad • [T] Trazabilidad
Responsable/s	• Responsable de seguridad • Dirección • Auditor externo

Tabla 34. Proyecto propuesto 13

4.2.13 Modelo de relación con proveedores	
Objetivo	Crear un modelo de relación único con los proveedores de la empresa que mejore la seguridad de la información.
Descripción	Consiste en la realización de un modelo de relación con proveedores basado en las políticas de seguridad de la empresa para mitigar los riesgos en seguridad de la información.
Planificación	Este proceso tiene una duración de dos semanas y se revisará anualmente.
Coste	Se estima un coste de 1500€ repartido en: • Jornadas Responsable de seguridad • Jornadas Dirección
Indicador	• [IC34] Acceso a los sistemas del sistema Sirio por personal subcontratado • [IC35] Cumplimiento sistemas de seguridad en el entorno de desarrollo contratado a un proveedor externo • [IC36] Indisponibilidad del entorno de desarrollo contratado a un proveedor externo
Beneficios	• Mitigación de los riesgos provenientes de los proveedores de la empresa
Activos Involucrados	• Servicios [S1, 3-4] • Comunicaciones [COM]
Dimensiones de riesgo mitigadas	• [C] Confidencialidad • [I] Integridad • [D] Disponibilidad
Responsable/s	• Responsable de seguridad • Dirección

4.3 Planificación temporal de los proyectos

En este punto se muestra la planificación temporal para un año completo (52 semanas) para los proyectos definidos en el apartado anterior.

Como se puede observar ningún proyecto empieza después del primero que corresponde al de rediseño de la política de seguridad por si se identifican cambios de alcance en los mismos.

Los proyectos que depende del personal del departamento de TI se han escalonado para que no coincidan temporalmente.

El último proyecto implementado será el de revisión de seguridad para comprobar el estado después de la implantación de los anteriores proyectos.

Tabla 35. Planificación temporal de los proyectos.

Proyecto	AÑO 1																																																			
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24	S25	S26	S27	S28	S29	S30	S31	S32	S33	S34	S35	S36	S37	S38	S39	S40	S41	S42	S43	S44	S45	S46	S47	S48	S49	S50	S51	S52
4.2.1	4 semanas																																																			
4.2.2													1 S																											1 S												
4.2.3						40 Semanas																																														
4.2.4						26 Semanas																																														
4.2.5										26 Semanas																																										
4.2.6						12 Semanas																																														
4.2.7																			10 Semanas																																	
4.2.8																													15 Semanas																							
4.2.9						3 Sem.																																														
4.2.10						26 Semanas																																														
4.2.11																																						12 Semanas														
4.2.12																																																			2 S.	
4.2.13					2 S.																																															

4.4 Análisis diferencial deseable tras la implantación

Los proyectos propuestos en esta fase del Plan Director de Seguridad tienen como objetivo la reducción del nivel de riesgo detectado.

Para ello, en este apartado se va a realizar un análisis diferencial en los dominios de la ISO/IEC 27002:2013 teniendo en cuenta los proyectos presentados y será comparado con el realizado al inicio de este Plan Director donde se refleja la situación actual. Esta comparación ofrecerá un modelo predictivo de la mejora de la seguridad de la información de Ícaro S.A. y la consecuente reducción del nivel de riesgo con la implantación de los mencionados proyectos.

A continuación, se muestra una tabla con la comparación entre el análisis diferencial realizado en el apartado primero de este documento y el realizado teniendo en cuenta los proyectos de mitigación del nivel de riesgo.

DOMINIO	INICIAL		TRAS PROYECTOS	
	MADUREZ	CONTROLES IMPLANTADOS	MADUREZ	CONTROLES IMPLANTADOS
5. Políticas de Seguridad	10%	1 de 2	100%	2 de 2
6. Organización de la Seguridad	35%	2 de 7	90%	6 de 7
7. Seguridad RRHH	30%	4 de 6	95%	6 de 6
8. Gestión de Activos	40%	4 de 10	90%	9 de 10
9. Control de Accesos	30%	6 de 14	90%	14 de 14
10. Criptografía	0%	0 de 2	70%	2 de 2
11. Seguridad Física y del entorno	70%	6 de 15	80%	14 de 15
12. Seguridad de las Operaciones	30%	8 de 14	90%	14 de 14
13. Seguridad de las Comunicaciones	30%	2 de 7	90%	7 de 7
14. Adquisición, desarrollo, y mantenimiento.	18%	5 de 14	70%	13 de 14
15. Relación con los proveedores	0%	0 de 5	70%	5 de 5

16. Gestión de Incidentes	0%	0 de 7	60%	6 de 7
17. Gestión de la Continuidad del Negocio	0%	0 de 4	80%	4 de 4
18. Cumplimiento	10%	2 de 7	70%	5 de 7

A conitinuación se muestra los resultados comparativos en dos gráficas, la primera muestra el porcentaje de madurez de los controles implantados y el segundo el porcentaje de los controles implantados.

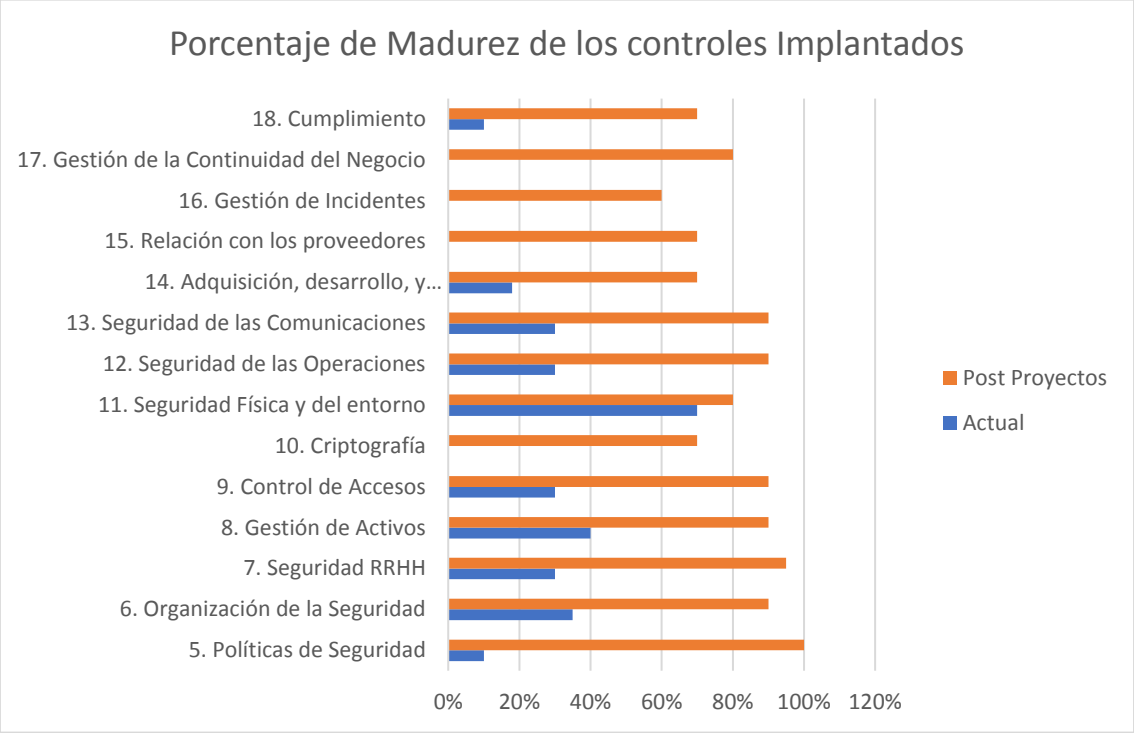

Ilustración 13. Comparativo porcentaje de madurez de los controles implantados

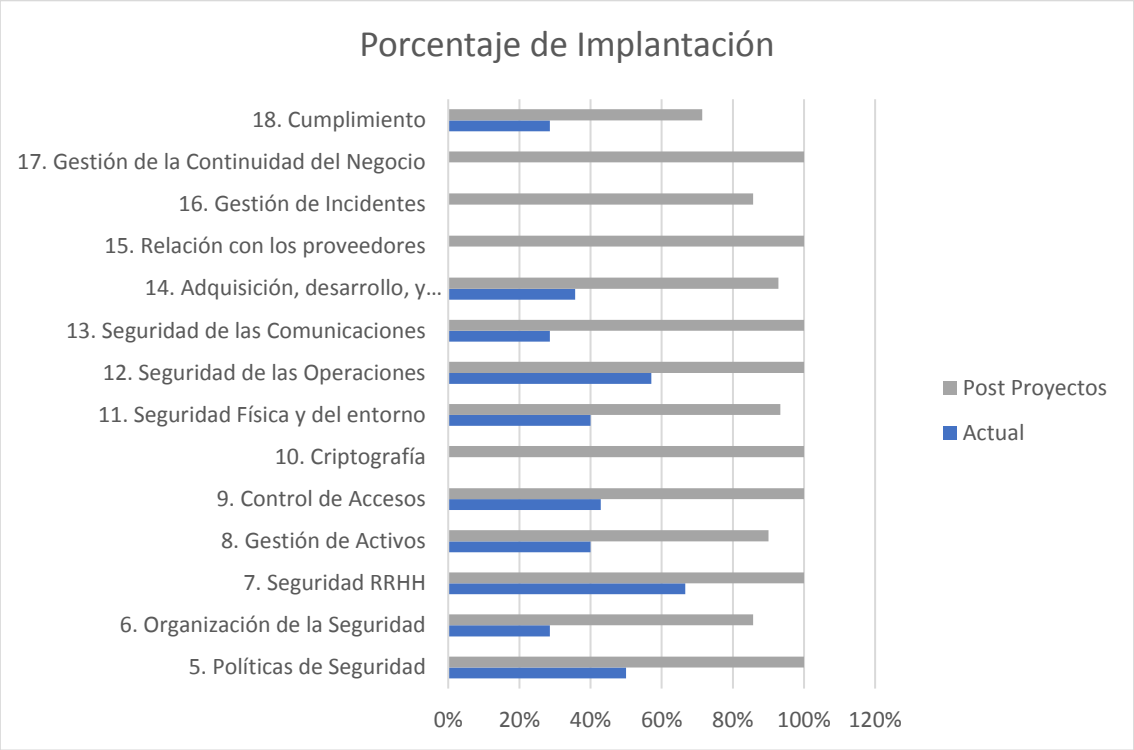

Ilustración 14. Porcentaje de implantación de los controles

5 Auditoría de cumplimiento

5.1 Introducción

Llegados a este punto, hemos realizado un inventario de activos, los hemos valorado, se ha realizado un análisis de riesgos sobre los mismos y se han propuesto una serie de proyectos para su mitigación. El siguiente paso natural es, una vez implantados dichos proyectos, realizar una auditoría de cumplimiento

Por lo tanto, el objetivo de este apartado es evaluar el cumplimiento de Ícaro S.A. en materia de seguridad. Por ello, a continuación, se van a comparar los controles de la empresa contra la norma ISO/IEC 27002:2013 que servirá de marco de control del estado de la seguridad.

5.2 Metodología

Como se ha explicado en el apartado de introducción, para evaluar correctamente la madurez de la seguridad de la información de la empresa, se va realizar una auditoría contra el estándar ISO/IEC 27002:2013.

Este estándar es internacionalmente reconocido y aplicable a cualquier organización que tenga relación con el tratamiento de información.

La 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.

En general estos controles se pueden agrupar en:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

Para comprobar el estado de la seguridad de la información de la empresa, se volverá a utilizar el Modelo de Madurez de la Capacidad (MMC) ya usado en el apartado 1.3. Análisis Diferencial de este documento contra la norma ISO/IEC 27002:2013.

A continuación, en la siguiente tabla se presentan los distintos niveles como recordatorio.

Tabla 36.Modelo de Madurez de la Capacidad

Nivel	Estado	Madurez	Descripción
Nivel 0	Inexistente	0%	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso
Nivel 1	Inicial/Ad-hoc	10%	El proceso está implementado y alcanza su propósito básico.
Nivel 2	Reproducible, pero intuitivo	50%	El proceso ejecutado, está implementado de forma gestionada y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
Nivel 3	Proceso definido	90%	El proceso gestionado, está implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (Se documenta, se comunica y se da formación).
Nivel 4	Gestionado y medible	95%	El proceso establecido descrito anteriormente, ahora se ejecuta dentro de los límites definidos para alcanzar sus resultados de proceso.
Nivel 5	Optimizado	100%	El proceso descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.

5.3 Evaluación de la madurez

En este apartado se expone la información recogido de la ejecución del proceso de evaluación de la madurez de Ícaro S.A. después de haber implantado los proyectos para la mejora de la seguridad de la información.

5.3.1 Análisis de auditoria respecto a la ISO 27002:2013

A continuación, en la siguiente tabla se exponen los resultados de la auditoría diferenciados respecto a los 114 controles de la norma ISO/IEC 27002:2014. Para mayor detalle del porcentaje de cumplimiento diríjase al siguiente documento.

Tabla 37. Análisis de auditoría

ID	Control	Justificación	% Cumplimiento	MMC
5	Políticas de seguridad de la información		100%	
5.1	Directrices de gestión de la seguridad de la información		100%	
5.1.1	Políticas para la seguridad de la información	Se comprueba que existe un conjunto de políticas de seguridad aprobado por la dirección y comunicado a las partes afectadas.	100%	L5

ID	Control	Justificación	% Cumplimiento	MMC
5.1.2	Revisión de las políticas para la seguridad de la información	Se constata la existencia de un proyecto anual de revisión y mejora del documento de Política de Seguridad de Ícaro S.A.	100%	L5
6	Organización de la seguridad de la información		71%	
6.1	Organización interna		63%	
6.1.1	Roles y responsabilidades en seguridad de la información	Existe un documento que refleja los roles y las responsabilidades de los empleados en lo que se refiere a seguridad de la información. No obstante, no se ha podido verificar que este documento se revise cada cierto tiempo.	95%	L4
6.1.2	Segregación de tareas	Existe una segregación de tareas documentada y aplicada a los procedimientos relativos a la seguridad de la información. Sin embargo, esta segregación no se monitoriza ni se comprueba su cumplimiento.	90%	L3
6.1.3	Contacto con las autoridades	Se comprueba que esta tarea está asignada a roles nominales de la empresa y que conocen el procedimiento, pero no se ha encontrado documentación del procedimiento ni indicadores de medición.	50%	L2
6.1.4	Contacto con grupos de interés especial	Se comprueba que esta tarea está asignada a roles nominales de la empresa y que conocen el procedimiento, pero no se ha encontrado documentación del procedimiento ni indicadores de medición.	50%	L2
6.1.5	Seguridad de la información en la gestión de proyectos	Se constata que existen procedimiento documentados conocidos por todos los roles implicados, de procedimiento de gestión de proyectos basados en las mejores prácticas en seguridad de la información. No obstante, no se ha podido comprobar que estos procedimientos se revisen y actualicen de manera regular.	95%	L4

ID	Control	Justificación	% Cumplimiento	MMC
6.2	Los dispositivos móviles y el teletrabajo		78%	
6.2.1	Política de dispositivos móviles	Existe un documento que refleja la política respecto a las medidas de seguridad para la protección contra los riesgos de trabajar con dispositivos móviles en entornos desprotegidos de manera genérica.	95%	L4
6.2.2	Teletrabajo	Se constata que existen normas no escritas respecto a la seguridad de la información del teletrabajo, pero no existe una política definida para tal fin.	50%	L2
7	Seguridad relativa a los RRHH		98%	
7.1	Antes del empleo		100%	
7.1.1	Investigación de antecedentes	Existe constancia de que el personal relativo a la gestión de RRHH investiga dentro de las normas y procedimientos legales a los futuros empleados. Este proceso es seguido y revisado.	100%	L5
7.1.2	Términos y condiciones del empleo	Existe constancia de que los términos laborales respecto a la seguridad de la información de empleados y contratistas están plasmados en una política que es seguida y revisada.	100%	L5
7.2	Durante el empleo		98%	
7.2.1	Responsabilidades de gestión	Se ha constatado que se comunica a los empleados la Política de Seguridad de la empresa, así como la exigencia de aplicarla. Además, este proceso es seguido y revisado para su actualización. Lo que no se ha podido comprobar es que exista un canal anónimo para el reporte de posibles violaciones de la seguridad de la información:	95%	L4
7.2.2	Concienciación, educación y capacitación en seguridad de la información	Existe un programa de formación y concienciación sobre seguridad de la información para los empleados y contratistas con una periocidad definida que es medido y actualizado.	100%	L5
7.2.3	Proceso disciplinario	Existe un proceso formal disciplinario comunicado a los empleados que recoge las acciones a tomar contra aquellos que provoquen una brecha de seguridad	100%	L5

ID	Control	Justificación	% Cumplimiento	MMC
7.3	Finalización del empleo o cambio en el puesto de trabajo		95%	
7.3.1	Responsabilidades ante la finalización o cambio.	Existe un procedimiento de actuación para cuando un empleado abandona la empresa. Se ha comprobado que se está llevando a cabo de manera adecuada. Sin embargo, no se ha podido demostrar que este proceso esté bajo constante mejora.	95%	L4
8	Gestión de activos		77%	
8.1	Responsabilidad sobre los activos		88%	
8.1.1	Inventario de activos	Se ha constatado que existe un inventario de activos y un procedimiento formal para altas, bajas y modificaciones de activos.	100%	L5
8.1.2	Propiedad de los activos	Se ha comprobado que todos los activos del inventario tienen un propietario y que se sigue un proceso formal para la modificación de este.	100%	L5
8.1.3	Uso aceptable de los activos	Existe un documento formal donde se refleja el uso aceptable de los activos inventariados, pero se ha constatado que un porcentaje alto de los empleados no conocen su existencia ni existe un procedimiento para su revisión	50%	L2
8.1.4	Devolución de activos	Se ha comprobado que existe un procedimiento y registro de devolución de activos.	100%	L5
8.2	Clasificación de la información		80%	
8.2.1	Clasificación de la información	La información está clasificada de acuerdo a una política en función de su importancia, sin embargo, este proceso no es medible.	95%	L4
8.2.2	Etiquetado de la información	Existe un procedimiento de etiquetado de la información, aunque este no sigue ningún esquema predefinido ni es medido	50%	L2
8.2.3	Manipulado de la información	Existe un procedimiento formal y documentado para la manipulación de la información de acuerdo con un esquema adoptado en la política correspondiente, aunque este procedimiento no es revisado.	95%	L4

ID	Control	Justificación	% Cumplimiento	MMC
8.3	Manipulación de los soportes		62%	
8.3.1	Gestión de soportes extraíbles	Existen procedimientos para la utilización y gestión de los soportes extraíbles. Sin embargo, no existe una métrica que permita conocer si se está aplicando correctamente.	90%	L3
8.3.2	Eliminación de soportes	Se constata que no existe procedimiento de eliminación de soportes.	0%	L0
8.3.3	Soporte físico en tránsito	Existen procedimientos para la protección contra accesos no autorizados o usos indebidos. Sin embargo, estos procedimientos no son medibles	95%	L4
9	Control de acceso		93%	
9.1	Requisitos de negocio para el control de acceso		98%	
9.1.1	Política de control de acceso	Existe una política de acceso documentada y revisada relativa al control de acceso basado en los requisitos de negocio.	100%	L5
9.1.2	Acceso a las redes y a los servicios de red	Existe un procedimiento para proporcionar acceso a las redes y servicios de red a los usuarios autorizados. Este procedimiento es medido, sin embargo, no existe revisión del mismo	9571%	L4
9.2	Gestión de acceso de usuarios		98%	
9.2.1	Registro y baja de usuario	Existe un procedimiento para el alta, baja y modificación de los usuarios que asigna los derechos de acceso. Este procedimiento es medido y revisado con una frecuencia determinada	100%	L5
9.2.2	Provisión de acceso de usuario	Existe un procedimiento formal para la asignación o revocación de los derechos de acceso de los usuarios. Este procedimiento es medido y revisado.	100%	L5
9.2.3	Gestión de privilegios de acceso	Se constata que la asignación y el uso de privilegios de acceso está restringida y controlada	100%	L5
9.2.4	Gestión de la información secreta de autenticación de los usuarios	Existe un proceso formal de gestión sobre la información secreta de autenticación de los usuarios.	100%	L5
9.2.5	Revisión de los derechos de acceso de usuario	Existe un procedimiento para la revisión de los derechos de acceso de los usuarios a intervalos regulares, sin embargo, este procedimiento no es medible.	90%	L3
9.2.6	Retirada o reasignación de los derechos de usuario	Existe un procedimiento formal para la retirada o reasignación de los derechos de usuario, sin embargo, este nos es medible.	95%	L4

ID	Control	Justificación	% Cumplimiento	MMC
9.3	Responsabilidades del usuario		95%	
9.3.1	Uso de la información secreta de autenticación	Existe una política donde se informa a los usuarios el uso correcto de la información secreta de autenticación. Esta política es comunicada y revisada, aunque no se mide.	95%	L4
9.4	Control de acceso a sistema y aplicaciones		82%	
9.4.1	Restricción del acceso a la información	Se constata que se restringe el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	100%	L5
9.4.2	Procedimientos seguros de inicio de sesión	De acuerdo con su política correspondiente se controla el acceso a los sistemas y a las aplicaciones mediante procedimientos seguros de inicio de sesión	100%	L5
9.4.3	Sistemas de gestión de contraseñas	Se constata que existe un sistema de gestión de contraseñas robusto, interactivo y seguro.	100%	L5
9.4.4	Uso de utilidades con privilegios de sistemas	Aunque en la mayoría de los sistemas se constata que no se ejecutan aplicaciones en cuentas de usuario con privilegios del sistema, se han encontrado evidencias de que en algunos sistemas esto no se cumple. La organización lo admite y lo pasa a revisión interna	10%	L1
9.4.5	Control de acceso al código fuente de los programas	Se ha constatado que acceso al código fuente está controlado, es medible y se revisa con asiduidad.	100%	L5
10	Criptografía		95%	
10.1	Controles criptográficos		95%	
10.1.1	Política de uso de los controles criptográficos	Existe una política para sobre el uso de los controles criptográficos, sin embargo, esta no es revisada	90%	L3
10.1.2	Gestión de claves	Existe una política de gestión de las claves de cifrado. Esta es medible y revisada.	100%	L5
11	Seguridad física y del entorno		70%	
11.1	Áreas seguras		68%	
11.1.1	Perímetro de seguridad física	Se ha establecido perímetros de seguridad, esto son controlados y revisados con asiduidad.	100%	L5
11.1.2	Controles físicos de entrada	Existen controles físicos de entrada con control de acceso adecuado. Este sistema es medible y revisado.	100%	L5

ID	Control	Justificación	% Cumplimiento	MMC
11.1.3	Seguridad de oficinas, despachos y recurso	Existen controles de acceso en aquellas estancias identificadas como sensibles respecto a la seguridad de la información. Estos controles son medibles, pero no se encuentra evidencias de que sean revisados	95%	L4
11.1.4	Protección contra las amenazas externas y ambientales	Existen protecciones físicas contra ataques provocados, pero estas solo alcanzan un propósito básico	10%	L1
11.1.5	El trabajo en áreas seguras	No se han encontrado indicios de procedimientos de trabajo en áreas seguras	0%	L0
11.1.6	Áreas de carga y descarga	Existen controles correctamente implementados en las áreas de carga y descarga de materiales	100%	L5
11.2	Seguridad de los equipos		72%	
11.2.1	Emplazamiento y protección de equipos	Se constata que los equipos se encuentran emplazados en lugares con control de acceso. Existen procesos de medición y de revisión	100%	L5
11.2.2	Instalaciones de suministro	Se constata que los equipos están correctamente protegidos frente a fallos por falta de suministro. Este proceso es medido y revisado.	100%	L5
11.2.3	Seguridad del cableado	Se constata que el cableado está debidamente protegido contra intercepciones, interferencias o daños	100%	L5
11.2.4	Mantenimiento de los equipos	Se sigue un procedimiento formal de mantenimiento de los equipos. Este puede ser medio, pero no se han encontrado indicios de que sea revisado	100%	L5
11.2.5	Retirada de materiales propiedad de la empresa	Aunque existe una política que dicta el procedimiento de sacar de las instalaciones, este no es controlado.	50%	L2
11.2.6	Seguridad en los equipos fuera de las instalaciones	Se constata que existen medidas para asegurar la seguridad fuera de las instalaciones de la empresa de los equipos, este proceso es medido, pero no es revisado.	90%	L3
11.2.7	Reutilización o eliminación de seguridad de equipos	Aunque existe una política que describe este procedimiento, este no puede ser comprobado ni medido	10%	L1
11.2.8	Equipo de usuario desatendido	Existe procedimiento formal comunicado a los empleados respecto a los equipos desatendidos. Este, aunque no es medible es revisado.	95%	L4

ID	Control	Justificación	% Cumplimiento	MMC
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Existe una política que describe como debe mantenerse el puesto de trabajo, pero esta no es adoptada por la mayoría de los usuarios	10%	L1
12	Seguridad de las operaciones		91%	
12.1	Procedimientos y responsabilidades operacionales		65%	
12.1.1	Documentación de procedimientos de las operaciones	Se constata que los procedimientos de las operaciones son documentados y puestos a disposición de los usuarios.	100%	L5
12.1.2	Gestión de cambios	Existen procedimientos para controlar los procesos que afectan a la seguridad, pero estos son básicos	10%	L1
12.1.3	Gestión de capacidades	Existen procedimientos de supervisión y ajuste de recursos para la gestión de la capacidad, aunque estos no son medibles ni revisados.	50%	L2
12.1.4	Separación de los recursos de desarrollo, prueba y operación	Se consta que existe separación entro los distintos entornos de la organización	100%	L5
12.2	Protección contra el malware		100%	
12.2.1	Protección contra el código malicioso	Existen sistemas y controles de detección contra el malware. Estos son medible y revisados con periocidad	100%	L5
12.3	Copias de seguridad		100%	
12.3.1	Copias de seguridad de la información	Se constata que existe política de copias de seguridad y que esta es aplicada, además el proceso es medible y revisado	100%	
12.4	Registros y supervisión		73%	
12.4.1	Registro de eventos	Se constata que existe el procedimiento y los sistemas para el registro de eventos. Este es medible y revisado con asiduidad	100%	L5
12.4.2	Protección de la información de registro	Se constata que la información de registro es protegida en base a la política afín. Este sistema es medido, pero no revisado.	95%	L4
12.4.3	Registros de administración y operación	Aunque existe procedimiento técnico para el registro de las actividades de los administradores del sistema este no es aplicado en modo alguno	0%	L0
12.4.4	Sincronización de reloj	Se constata la existencia de sistema de sincronización horaria. Este sistema es medido y revisado.	100%	L5

ID	Control	Justificación	% Cumplimiento	MMC
12.5	Control del software en explotación		100%	
12.5.1	Instalación del software en explotación	Existen procedimientos para el control de la instalación de software en explotación. Estos son documentados, medibles y revisados.	100%	L5
12.6	Gestión de la vulnerabilidad técnica		98	
12.6.1	Gestión de las vulnerabilidades técnicas	Existe procedimiento documentado para realización de auditorías de pentesting. Este procedimiento es medible y se revisa.	100%	L5
12.6.2	Restricción en instalación de software	Existen reglas basadas en roles para la restricción de instalaciones de software por parte de los usuarios, aunque no son revisadas.	95%	L4
12.7	Consideraciones sobre la auditoría de sistemas de información		100%	
12.7.1	Controles de auditoría de sistemas de información	Existen políticas que describen los requisitos, las actividades relativas a los controles de auditoría de los sistemas de información. Estas son revisadas y medidas	100%	L5
13	Seguridad de las comunicaciones		97%	
13.1	Gestión de la seguridad de redes		98%	
13.1.1	Controles de red	Existen sistemas que controlan y gestionan las redes de la organización. Estos son medidos y revisados	100%	L5
13.1.2	Seguridad de los servicios de red	Se han identificado los mecanismos de seguridad necesarios para la red y estos han sido implementados. Es posible su medición, aunque no existe procedimiento de revisión	95%	L4
13.1.3	Segregación en redes	Se constata que existe una segregación suficiente entre las redes de la organización. Esta es controlada y revisada con asiduidad	100%	L5
13.2	Intercambio de información		96%	
13.2.1	Políticas y procedimientos de intercambio de información	Existen políticas y procedimientos de intercambio de información. Estas son medidas y revisadas con asiduidad	100%	L5
13.2.2	Acuerdos de intercambio de información	Existen normas a seguir para realizar las transferencias de información de manera segura. Existe un indicador para comprobar la evolución de este control.	100%	L5
13.2.3	Mensajería electrónica	La información que se procesa a través de mensajería electrónica está debidamente protegida. Este proceso es medible.	95%	L4

ID	Control	Justificación	% Cumplimiento	MMC
13.2.4	Acuerdos de confidencialidad o no revelación	Existen acuerdos de confidencialidad con los empleados y terceros que interactúan con la organización. Aunque estos no son revisados.	90%	L3
14	Adquisición, desarrollo y mantenimiento de los sistemas de información		56%	
14.1	Requisitos de seguridad en sistemas de información		95%	
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Se constata que se realizan análisis de requisitos de los sistemas de información para los nuevos sistemas o para las mejoras de los existentes. Aunque el proceso es revisado no existe y procedimiento de medición	90%	L3
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Existen medidas implantadas para asegurar la información de aplicaciones sobre redes públicas. Estas medidas son monitorizas, pero no revisadas.	95%	L4
14.1.3	Protección de las transacciones de servicios de aplicaciones	Se constata que existen procedimientos para la protección de las transacciones entre servicios de aplicaciones. Estos son medidos y revisados.	100%	L5
14.2	Seguridad en el desarrollo y en los procesos de soporte		64%	
14.2.1	Política de desarrollo seguro	Existe política de desarrollo seguro. Esta es revisada pero no se comprueba su aplicación	50%	L3
14.2.2	Procedimiento de control de cambios en sistemas	Existe un sistema de gestión del control del cambio. Este se puede medir y es revisado.	95%	L5
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No existen políticas ni procedimiento para comprobar este punto	0%	L0
14.2.4	Restricciones al cambio en los paquetes de software	Existen controles para la restricción de cambio en el software, aunque estos controles no pueden ser medidos ni revisados.	90%	L3
14.2.5	Principios de ingeniería de sistemas seguros	No existe documentación ni se constata actividad sobre este punto	0%	L0
14.2.6	Entorno de desarrollo seguro	Se constata que existe protección sobre los sistemas de desarrollo	100%	L5
14.2.7	Externalización del desarrollo de software	No aplica	-	-
14.2.8	Pruebas funcionales de seguridad de sistemas	Existe un procedimiento documentado con las pruebas funcionales, la periocidad y la duración. Pero este no es medido ni revisado con periocidad.	90%	L3

ID	Control	Justificación	% Cumplimiento	MMC
14.2.9	Pruebas de aceptación de sistemas	Existen procedimientos documentados para la ejecución de pruebas y aceptación de los sistemas. Pero estos no son revisados.	95%	L4
14.3	Datos de prueba		10%	
14.3.1	Protección de los datos de prueba	Existe un procedimiento para su protección pero este es básico e ineficiente.	10%	L1
15	Relación con proveedores		49%	
15.1	Seguridad en las relaciones con proveedores		53%	
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Existe una política de relación con proveedores relativa a la seguridad de la información. Esta es revisada con asiduidad	100%	L5
15.1.2	Requisitos de seguridad en contrato con terceros	Existen acuerdos relativos a los requisitos de seguridad con terceros, aunque estos no son revisados	50%	L2
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Existen requisitos en los acuerdos con algunos proveedores para hacer frente a los riesgos, pero no todos. Estos no son medidos ni revisados	10%	L1
15.2	Gestión de la provisión de servicios del proveedor		50%	
15.2.1	Control y revisión de la provisión de servicios del proveedor	Existen ANS con los proveedores de suministros de tecnología de la información y comunicaciones que son medidos y revisados con asiduidad	100%	L5
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	No se realiza gestión alguna en este punto	0%	L0
16	Gestión de incidentes de seguridad de la información		45%	
16.1	Gestión de incidentes de seguridad de la información y mejoras		45%	
16.1.1	Responsabilidades y procedimientos	Existen políticas de establecimiento de responsabilidades y procedimientos para la gestión rápida y efectiva respecto a los incidentes de seguridad. Estos son comprobados y revisados.	100%	L5
16.1.2	Notificación de eventos de seguridad de la información	Existen procedimientos de notificación de eventos de seguridad, pero estos no son probados ni revisados	50%	L2
16.1.3	Notificación de puntos débiles de la seguridad	Existe una política para el cumplimiento de la notificación de vulnerabilidades por pare de los agentes de la organización. Pero este punto no es probado ni revisado	10%	L1

ID	Control	Justificación	% Cumplimiento	MMC
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Aunque existe un política que procedimental de la evaluación sobre los eventos de seguridad estos no son clasificados a posteriori.	10%	L1
16.1.5	Respuesta a incidentes de seguridad de la información	Existen procedimientos documentados y se realizan pruebas con cierta frecuencia, aunque no son revisados	90%	L3
16.1.6	Aprendizaje de los incidentes de seguridad de la información	Existe una base de datos en la que se guarda la información de los incidentes ocurridos con el objetivo de aprender de ellos y mejorar la seguridad. Sin embargo, no existe ninguna métrica para comprobar que se está utilizando esta información con el fin expuesto.	90%	L3
16.1.7	Recopilación de evidencias	Se ha constado que en algunos entornos se recopilan evidencias pero no en todos	10%	L1
17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio		98%	
17.1	Continuidad de la seguridad de la información		97%	
17.1.1	Planificación de la continuidad de la seguridad de la información	Existe una política documentada donde se desarrolla la planificación y las necesidades de la organización en caso de incidente, aunque esta no es revisada	95%	L4
17.1.2	Implementar la continuidad de la seguridad de la información	Existe un procedimiento para establecer, documentar, implementar y mantener procesos, procedimientos y controles durante una situación adversa.	100%	L5
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Existe procedimiento para la verificación, revisión y evaluación de los controles para asegurar que son válidos y eficaces. Estos se realizan con una frecuencia optima y son debidamente documentados	100%	L5
17.2	Redundancias		100%	
17.2.1	Disponibilidad de los recursos de tratamiento de la información	Existe constancia de que los recursos que así lo requieren cuentan con la redundancia necesaria en caso de indisponibilidad	100%	L5
18	Cumplimiento		99%	
18.1	Cumplimiento de los requisitos legales y contractuales		98%	
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Todos los requisitos legales pertinentes están documentados y definidos de manera explícita, esto se mantienen actualizados.	100%	L5

ID	Control	Justificación	% Cumplimiento	MMC
18.1.2	Derechos de propiedad intelectual (DPI)	Se ha comprobado que existen procedimientos que garantizan el cumplimiento de los derechos de propiedad intelectual. Además, hay implantados indicadores para comprobar su funcionamiento y evolución y así mejorar este control.	100%	L5
18.1.3	Protección de los registros de la organización	Los registros de la organización están protegidos, existiendo indicadores que así lo demuestran. No obstante, no se ha podido demostrar que se revise y/o mejore este proceso.	95%	L4
18.1.4	Protección y privacidad de la información de carácter personal	Se comprobado que se realizan los controles necesarios para la protección de la información de carácter personal. Estos son revisados	100%	L5
18.1.5	Regulación de los controles criptográficos	Se constata que la organización está adecuada respecto a la regulación de controles criptográficos. Se controla y se revisa	100%	L5
18.2	Revisiones de la seguridad de la información		100%	
18.2.1	Revisión independiente de la seguridad de la información	Se realiza una revisión externa independiente del estado de la seguridad de la información de la organización de la que existen indicadores para comprobar su evolución. Además, este proceso se revisa y se mejora de manera periódica.	100%	L5
18.2.2	Cumplimiento de la políticas y normas de seguridad	Se lleva a cabo la revisión de las políticas y normas de seguridad y se encuentran en constante mejora.	100%	L5
18.3.3	Comprobación del cumplimiento técnico	Se revisa el cumplimiento de las políticas y normas establecidas por la organización. Este proceso se revisa y mejora de manera periódica.	100%	L5
Cumplimiento medio			88%	

5.3.2 No conformidades respecto a la ISO 27002:2013

En este apartado se muestran las No Conformidades (NC) con la norma ISO 27002:2013 descubiertas durante la realización del proceso de auditoría de cumplimiento, así como las acciones correctivas recomendadas. Se considera que un control es de No Conformidad cuando este ha obtenido una evaluación de MMC inferior a L3.

Tabla 38. No conformidades (NC)

ID Control	Control	Tipo de NC	Detalle	Acción correctiva	MMC
6.1.3	Contacto con las autoridades	Menor	No existe un documento formal del procedimiento para el contacto con las autoridades. Tampoco existe un proyecto a corto plazo para llevarlo a cabo.	Llevar a cabo un proyecto para definir un documento de procedimiento de contacto con las autoridades y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L2
6.1.4	Contacto con grupos de interés especial	Menor	No existe un documento formal del procedimiento para el contacto con grupos de interés especial. Tampoco existe un proyecto a corto plazo para llevarlo a cabo.	Llevar a cabo un proyecto para definir un documento de procedimiento de contacto con las con grupos de interés especial y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L2
6.2.2	Teletrabajo	Menor	No existe un documento formal del procedimiento para asegurar la información en situación de teletrabajo. Tampoco existe un proyecto a corto plazo para llevarlo a cabo.	Llevar a cabo un proyecto para definir un documento de procedimiento en circunstancia de teletrabajo y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L2

8.1.3	Uso aceptable de los activos	Menor	Aunque existe procedimiento documentado de uso aceptable de los activos, este no ha sido comunicado de manera efectiva a los usuarios	Dar a conocer el documento de usos aceptable de los activos a los empleados.	L2
8.2.2	Etiquetado de la información	Menor	No existe un documento formal del procedimiento para para el etiquetado de la información. Tampoco existe un proyecto a corto plazo para llevarlo a cabo.	Llevar a cabo un proyecto para definir un documento de procedimiento de etiquetado de la información y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L2
8.3.2	Eliminación de soportes	Mayor	No existe ningún procedimiento de eliminación de soportes que contribuya al aseguramiento de la seguridad de la información.	Llevar a cabo un proyecto para definir un documento de procedimiento de eliminación de soportes y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L0
9.4.4	Uso de utilidades con privilegios de sistemas	Mayor	Se ha constatado que algunas aplicaciones corren sobre sistemas con privilegios de administrador.	Subsanar esta situación lo antes posible creando cuentas de usuario para estas aplicaciones con los privilegios o funcionalidades que estrictamente necesiten	L1

11.1.4	Protección contra las amenazas externas y ambientales	Mayor	Solo existe protección contra las amenazas externas y ambientales pero de un modo muy básico	Llevar a cabo un proyecto para definir protecciones contra las amenazas externas y ambientales y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L1
11.1.5	El trabajo en áreas seguras	Mayor	No se han encontrado indicios de procedimientos de trabajo en áreas seguras	Llevar a cabo un proyecto para definir un documento de procedimiento para la realización de trabajos en áreas seguras y llevarlo a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L0
11.2.5	Retirada de materiales propiedad de la empresa	Menor	Aunque existe una política para el control de retirada de materiales propiedad de la empresa este hecho no se controla	Realizar un proyecto para la implantación de controles de retirada de materiales propiedad de la empresa susceptibles a afectar a la seguridad de la información y llevarlo a cabo.	L2
11.2.7	Reutilización o eliminación de seguridad de equipos	Mayor	Aunque existe una política que describe este procedimiento, este no puede ser comprobado ni medido	Llevar a cabo un proyecto para asegurar la comprobación y/o medición acerca de la reutilización o eliminación de seguridad de los equipos y llevarlo a cabo	L1

11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Mayor	Existe una política que describe como debe mantenerse el puesto de trabajo, pero esta no es adoptada por la mayoría de los usuarios	Tomar medidas disciplinarias para asegurar el cumplimiento de la política.	L1
12.1.2	Gestión de cambios	Mayor	Existen procedimientos para controlar los procesos que afectan a la seguridad, pero estos son básicos	Llevar a cabo un proyecto de mejora de la política de gestión de cambios y aplicarlo.	L1
12.1.3	Gestión de capacidades	Menor	Existen procedimientos de supervisión y ajuste de recursos para la gestión de la capacidad, aunque estos no son medibles ni revisados	Realizar la medición por medio de indicadores y la revisión periódica de la gestión de las capacidades	L2
12.4.3	Registros de administración y operación	Mayor	Aunque existe procedimiento técnico para el registro de las actividades de los administradores del sistema este no es aplicado en modo alguno	Poner los medios necesarios para poder aplicar el procedimiento de registro de administración y operación.	L0
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Mayor	No existen políticas ni procedimiento para comprobar este punto	Llevar a cabo un proyecto para definir la política de revisión técnica de las aplicaciones tras efectuar cambios en el S.O. y llevarla a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L0

14.2.5	Principios de ingeniería de sistemas seguros	Mayor	No existen políticas ni procedimiento para comprobar este punto	Llevar a cabo un proyecto para definir la política de principios de ingeniería de sistemas seguros y llevarla a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L0
14.3.1	Protección de los datos de prueba	Mayor	Existe un procedimiento para su protección pero este es básico e ineficiente.	Llevar a cabo un proyecto para mejorar el procedimiento de la protección de los datos de prueba y llevarla a cabo. En el mismo se deberá reflejar como será medido y cada cuanto será revisado.	L1
15.1.2	Requisitos de seguridad en contrato con terceros	Menor	Existen acuerdos relativos a los requisitos de seguridad con terceros, aunque estos no son revisados	Definir y llevar a cabo una revisión periódica de los requisitos de seguridad en contratos con terceros	L2
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Mayor	Existen requisitos en los acuerdos con algunos proveedores para hacer frente a los riesgos, pero no todos. Estos no son medidos ni revisados	Revisar y realizar una nueva política respecto a los requisitos en los acuerdos con los proveedores y llevarla a cabo.	L1
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Mayor	No se realiza gestión alguna en este punto	Realizar una política que defina el procedimiento respecto a la gestión de cambios en la provisión de los servicio. Esta debe ser ejecutada, medida y revisada con frecuencia.	L0

16.1.2	Notificación de eventos de seguridad de la información	Menor	Existen procedimientos de notificación de eventos de seguridad, pero estos no son probados ni revisados	Realizar el procedimiento y poner los medios para la prueba y revisión de sobre la notificación de eventos de seguridad de la información	L2
16.1.3	Notificación de puntos débiles de la seguridad	Mayor	Existe una política para el cumplimiento de la notificación de vulnerabilidades por pare de los agentes de la organización. Pero este punto no es probado ni revisado	Realizar el procedimiento y poner los medios para la notificación de puntos débiles de la seguridad	L1
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Mayor	Aunque existe una política que procedimental de la evaluación sobre los eventos de seguridad estos no son clasificados a posteriori.	Realizar un procedimiento para la clasificación de las evaluaciones de los eventos de seguridad.	L1
16.1.7	Recopilación de evidencias	Mayor	Se ha constado que en algunos entornos se recopilan evidencias, pero no en todos	Poner los medios necesarios para poder aplicar la recopilación de evidencia en todos los entornos.	L1

5.3.3 Observaciones respecto a la ISO/IEC 27002:2013

Respecto al resto de controles que han obtenido en el análisis un nivel igual o mayor a L3, a continuación, se presenta una serie de observaciones que la empresa deberá tener en cuenta para continuar con la mejora constante en materia de seguridad de la información. Solo se incluyen aquellas que son merecedoras de alguna mención especial.

ID	Control	% Madurez	MMC	Observación	Oportunidad de Mejora
5.1.1	Políticas para la seguridad de la información	100	L5	N/A	N/A
5.1.2	Revisión de las políticas para la seguridad de la información	100	L5	N/A	Se recomienda que sea revisada la política de seguridad en caso de cambios estructurales y tecnológicos severos a parte de las revisiones programadas
6.1.1	Roles y responsabilidades en seguridad de la información	95	L4	Se deberá planificar y ejecutar la revisión de este documento para evitar incurrir en una N/C en un futuro	N/A
6.1.2	Segregación de tareas	90	L3	Se deberá comprobar la segregación de tareas periódicamente para evitar incurrir en una N/C en un futuro	N/A
6.1.5	Seguridad de la información en la gestión de proyectos	95	L4	N/A	N/A
6.2.1	Política de dispositivos móviles	95	L4		N/A
7.1.1	Investigación de antecedentes	100	L5	N/A	N/A
7.1.2	Términos y condiciones del empleo	100	L5	N/A	N/A
7.2.1	Responsabilidades de gestión	95	L4	Se insta a la empresa a habilitar un canal anónimo para el reporte de violaciones de la seguridad de la información para evitar incurrir en una NC en el futuro	N/A
7.2.2	Concienciación, educación y capacitación en seguridad de la información	100	L5	N/A	Se sugieren programas de capacitación adicionales en caso de cambios tecnológicos severos

7.2.3	Proceso disciplinario	100	L5	N/A	Se sugiere el endurecimiento de las multas para procesos disciplinarios por faltas graves
7.3.1	Responsabilidades ante la finalización o cambio.	95	L4	Se deberá planificar y ejecutar la revisión del procedimiento de abandono de la empresa por parte de un empleado para evitar incurrir en una NC en un futuro	Se sugiere a la empresa realizar un procedimiento similar con proveedores externos.
8.1.1	Inventario de activos	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
8.1.2	Propiedad de los activos	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
8.1.4	Devolución de activos	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
8.2.1	Clasificación de la información	95	L4	Se deberá implementar método de medición de la clasificación de la información para evitar incurrir en NC en el futuro.	N/A
8.2.3	Manipulado de la información	95	L4	Se deberá planificar y ejecutar la revisión del procedimiento de manipulado de la información para evitar incurrir en una NC en un futuro	N/A

8.3.1	Gestión de soportes extraíbles	90	L3	Se deben aplicar métricas para la medición del cumplimiento de la política de seguridad respecto a la gestión de soportes extraíbles para evitar incurrir en NC en el futuro	N/A
8.3.3	Soporte físicos en tránsito	95	L4	Se deben aplicar métricas para la medición del cumplimiento de la política de seguridad respecto a los soportes físicos en tránsito para evitar incurrir en NC en el futuro	N/A
9.1.1	Política de control de acceso	100	L5	N/A	N/A
9.1.2	Acceso a las redes y a los servicios de red	95	L4	Se deberá planificar y ejecutar la revisión del procedimiento de acceso a redes y servicios de red para evitar incurrir en una NC en un futuro	
9.2.1	Registro y baja de usuario	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
9.2.2	Provisión de acceso de usuario	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
9.2.3	Gestión de privilegios de acceso	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias

9.2.4	Gestión de la información secreta de autenticación de los usuarios	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
9.2.5	Revisión de los derechos de acceso de usuario	90	L3	Se deben aplicar métricas para la medición de los derechos de acceso de los usuarios para evitar incurrir en NC en el futuro	N/A
9.2.6	Retirada o reasignación de los derechos de usuario	95	L4	Se deben aplicar métricas para la medición de la retirada o reasignación de los derechos de usuario para evitar incurrir en NC en el futuro	N/A
9.3.1	Uso de la información secreta de autenticación	95	L4	Se deben aplicar métricas para la medición del uso de la información secreta de autenticación para evitar incurrir en NC en el futuro	
9.4.1	Restricción del acceso a la información	100	L5	N/A	N/A
9.4.2	Procedimientos seguros de inicio de sesión	100	L5	N/A	N/A
9.4.3	Sistemas de gestión de contraseñas	100	L5	N/A	Se sugiere a la empresa que obtenga mayor grado de automatización en este proceso para conseguir eficiencias
9.4.5	Control de acceso al código fuente de los programas	100	L5	N/A	Aunque está debidamente protegido, por su importancia se sugiere al menos doble factor de autenticación.

10.1.1	Política de uso de los controles criptográficos	90	L3	Se deberá planificar y ejecutar la revisión de la política de uso de los controles criptográficos para evitar incurrir en una NC en un futuro	N/A
10.1.2	Gestión de claves	100	L5	N/A	N/A
11.1.1	Perímetro de seguridad física	100	L5	N/A	N/A
11.1.2	Controles físicos de entrada	100	L5	N/A	N/A
11.1.3	Seguridad de oficinas, despachos y recurso	95	L4	Se deberá planificar y ejecutar la revisión de los controles de seguridad de estancias sensibles para evitar incurrir en una NC en un futuro	N/A
11.1.6	Áreas de carga y descarga	100	L5	N/A	N/A
11.2.1	Emplazamiento y protección de equipos	100	L5	N/A	El nuevo equipamiento sensible que se suministre deberá seguir las mismas premisas
11.2.2	Instalaciones de suministro	100	L5	N/A	N/A
11.2.3	Seguridad del cableado	100	L5	N/A	N/A
11.2.4	Mantenimiento de los equipos	100	L5	N/A	N/A
11.2.6	Seguridad en los equipos fuera de las instalaciones	90	L3	Se deberá planificar y ejecutar la revisión de los controles de seguridad de equipos sensibles fuera de la instalación para evitar incurrir en una NC en un futuro	N/A
11.2.8	Equipo de usuario desatendido	95	L4	Se deben aplicar métricas para la medición del cumplimiento de la política de equipos desatendidos para evitar incurrir en NC en el futuro	N/A

12.1.1	Documentación de procedimientos de las operaciones	100	L5	N/A	N/A
12.1.4	Separación de los recursos de desarrollo, prueba y operación	100	L5	N/A	N/A
12.2.1	Protección contra el código malicioso	100	L5	N/A	N/A
12.3.1	Copias de seguridad de la información	100	L5	N/A	Aunque existe una copia de seguridad de la información sensible se aconseja para aquella información marcada como esencial una segunda copia de seguridad
12.4.1	Registro de eventos	100	L5	N/A	N/A
12.4.2	Protección de la información de registro	95	L4	Se deberá planificar y ejecutar la revisión respecto a la protección de información de registro para evitar incurrir en una NC en un futuro	N/A
12.4.4	Sincronización de reloj	100	L5	N/A	N/A
12.5.1	Instalación del software en explotación	100	L5	N/A	N/A
12.6.1	Gestión de las vulnerabilidades técnicas	100	L5	N/A	N/A
12.6.2	Restricción en instalación de software	95	L4	Se deberá planificar y ejecutar la revisión de las reglas de restricción en instalación de software para evitar incurrir en una NC en un futuro	N/A
12.7.1	Controles de auditoría de sistemas de información	100	L5	N/A	N/A
13.1.1	Controles de red	100	L5	N/A	N/A
13.1.2	Seguridad de los servicios de red	95	L4	Se deberá planificar y ejecutar la revisión de los mecanismos de seguridad de los servicios de red implementados para evitar incurrir en una NC en un futuro	N/A

13.1.3	Segregación en redes	100	L5	N/A	N/A
13.2.1	Políticas y procedimientos de intercambio de información	100	L5	N/A	N/A
13.2.2	Acuerdos de intercambio de información	100	L5	N/A	N/A
13.2.3	Mensajería electrónica	95	L4		N/A
13.2.4	Acuerdos de confidencialidad o no revelación	90	L3	Se deberá planificar y ejecutar la revisión de los acuerdos de confidencialidad para evitar incurrir en una NC en un futuro	N/A
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	90	L3	Se deben aplicar métricas para la medición del cumplimiento de los análisis de requisitos para los nuevos sistemas y mejoras existentes para evitar incurrir en NC en el futuro	N/A
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	95	L4	Se deberá planificar y ejecutar la revisión de las medidas implantadas para asegurar los servicios en redes públicas para evitar incurrir en una NC en un futuro	N/A
14.1.3	Protección de las transacciones de servicios de aplicaciones	100	L5	N/A	N/A
14.2.1	Política de desarrollo seguro	90	L3	Se deben aplicar métricas para la medición del cumplimiento de la política de desarrollo seguro y planificar y ejecutar su revisión para evitar incurrir en NC en el futuro	N/A
14.2.2	Procedimiento de control de cambios en sistemas	100	L5	N/A	N/A

14.2.4	Restricciones al cambio en los paquetes de software	90	L3	Se deben aplicar métricas para la medición del cumplimiento en las restricciones a los cambios de software y planificar y ejecutar su revisión para evitar incurrir en NC en el futuro	N/A
14.2.6	Entorno de desarrollo seguro	95	L5	N/A	Se recomiendo revisar este entorno en cada nuevo proyecto que se inicie
14.2.8	Pruebas funcionales de seguridad de sistemas	90	L3	Se deben aplicar métricas para la medición para las pruebas funcionales de seguridad, además de planificar y ejecutar su revisión para evitar incurrir en NC en el futuro	N/A
14.2.9	Pruebas de aceptación de sistemas	95	L4	Se deberá planificar y ejecutar la revisión de las pruebas de aceptación de sistemas para evitar incurrir en una NC en un futuro	N/A
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	100	L5	N/A	N/A
15.2.1	Control y revisión de la provisión de servicios del proveedor	100	L5	N/A	N/A
16.1.1	Responsabilidades y procedimientos	100	L5	N/A	N/A
16.1.5	Respuesta a incidentes de seguridad de la información	90	L3	Se deberá planificar y ejecutar la revisión de los procedimientos de respuesta ante incidentes para evitar incurrir en una NC en un futuro	N/A

16.1.6	Aprendizaje de los incidentes de seguridad de la información	90	L3	Se deben aplicar métricas para la medición del uso de la información referente a los incidentes de seguridad ocurridos para evitar incurrir en NC en el futuro	N/A
17.1.1	Planificación de la continuidad de la seguridad de la información	95	L4	Se deberá planificar y ejecutar la revisión de la planificación de la continuidad de la seguridad de la información para evitar incurrir en una NC en un futuro	N/A
17.1.2	Implementar la continuidad de la seguridad de la información	100	L4		
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	100	L5	N/A	N/A
17.2.1	Disponibilidad de los recursos de tratamiento de la información	100	L5	N/A	N/A
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	100	L5	N/A	N/A
18.1.2	Derechos de propiedad intelectual (DPI)	100	L5	N/A	N/A
18.1.3	Protección de los registros de la organización	95	L4		
18.1.4	Protección y privacidad de la información de carácter personal	100	L5	N/A	N/A
18.1.5	Regulación de los controles criptográficos	100	L5	N/A	N/A
18.2.1	Revisión independiente de la seguridad de la información	100	L5	N/A	N/A
18.2.2	Cumplimiento de la políticas y normas de seguridad	100	L5	N/A	N/A
18.3.3	Comprobación del cumplimiento técnico	100	L5	N/A	N/A

5.4 Presentación de resultados

En este apartado se mostrarán los resultados obtenidos de la realización del proceso de auditoría. Para una visión más pormenorizada consultar el siguiente documento.

En primer lugar, se presenta de una manera gráfica el porcentaje de controles que caen dentro de cada uno de los niveles de madurez.

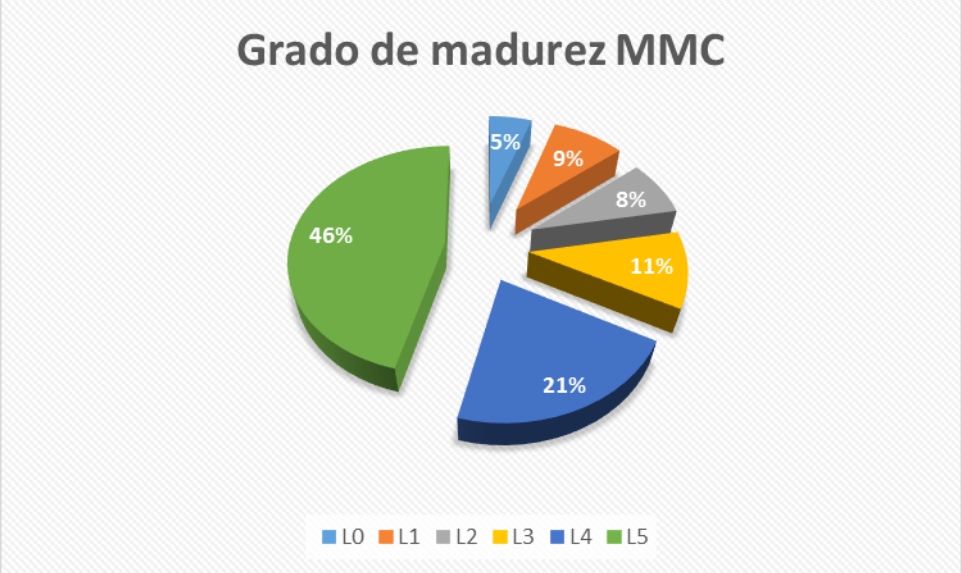

Ilustración 15. Grado de madurez MMC

Como se puede observar el nivel de madurez es en general alto, pero aún queda margen de desarrollo en algunos controles.

En la siguiente tabla se muestra el porcentaje de madurez de los dominios de la ISO/IEC 27002:2013

Tabla 39. Porcentaje de madurez de los dominios de la ISO 27002

Dominio	% Madurez
5. Políticas de Seguridad	100%
6. Organización de la seguridad de la información	75%
7. Seguridad relativa a los RRHH	98%
8. Gestión de activos	78%
9. Control de acceso	92%
10. Criptografía	95%
11. Seguridad física y del entorno	71%
12. Seguridad de las operaciones	82%
13. Seguridad de las comunicaciones	97%
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	71%
15. Relación con proveedores	52%
16. Gestión de incidentes de seguridad de la información	51%
17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	98%
18. Cumplimiento	99%

Cómo se puede observar, la mayoría de ellos tiene un porcentaje de madurez alto, pero otros como los dominios 15 y 16 tienen un margen de mejora amplio.

A continuación, se muestra un gráfico radial donde se puede observar los resultados.

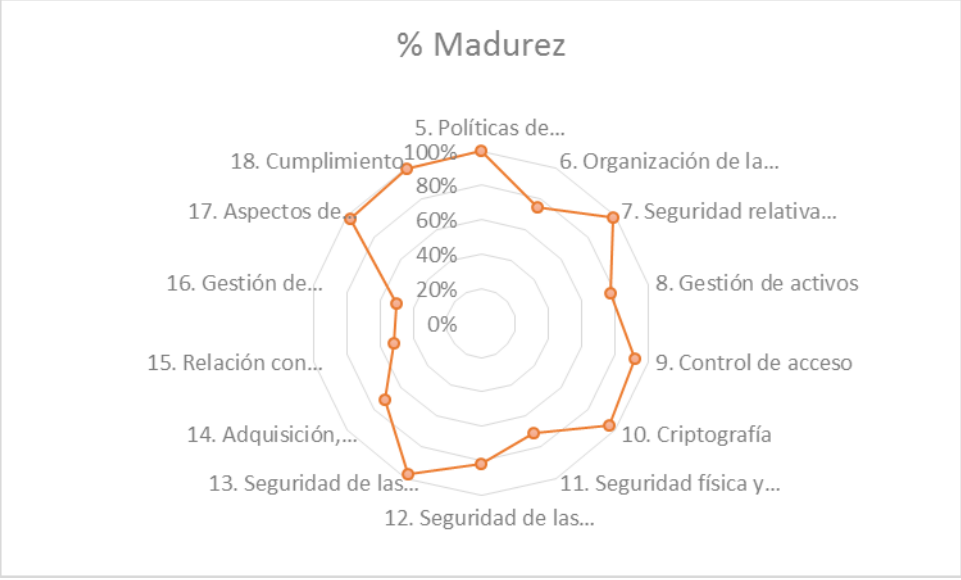

Ilustración 16. Porcentaje de madurez medido en la auditoría

En el siguiente gráfico se puede observar la comparación entre:

- Porcentaje de madurez inicial: Medido al inicio de este Plan director
- Porcentaje de madurez esperado: El valor de madurez que se esperaba tras la implantación de los proyectos.
- Porcentaje de madurez actual: El valor de madurez medido en la presenta auditoría.

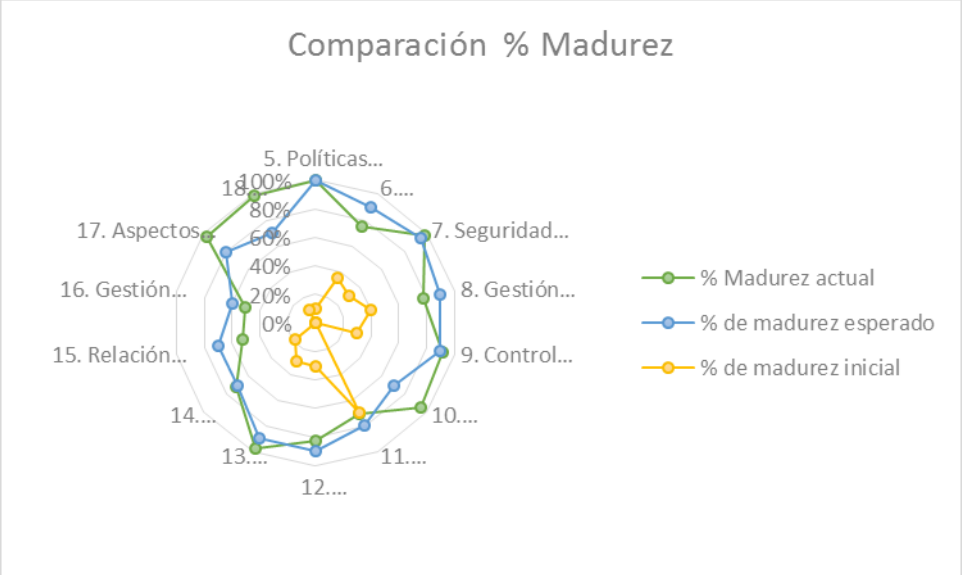

Ilustración 17. Comparación de porcentaje de madurez

Como se puede observar, los valores de madurez actuales están cercanos a los esperados en la mayoría de ellos, en otros no llega a alcanzarlo y es donde se deberá trabajar.

También cabe destacar la mejoría en seguridad de la información de la empresa desde la situación inicial a la actual.

6 Presentación de resultados y entrega de informes

6.1 Introducción

En este apartado se recopila la información relevante de este Plan Director de Seguridad para su presentación.

6.2 Objetivos

El objetivo principal de este apartado es la inclusión de la documentación dirigida, por una parte, a la Dirección de la empresa y por otra al personal involucrado en la gestión de la Seguridad de la Información para la comprensión del Plan Director de seguridad.

6.3 Entregables

La documentación que se entrega en este apartado es la que sigue:

- Resumen ejecutivo en PowerPoint con principales conclusiones del Plan Director de Seguridad.
- Presentación del proyecto en PowerPoint con resumen de las distintas fases del Plan Director de Seguridad
- Video de la defensa del Plan director de seguridad.

7 Conclusiones

7.1 Introducción

Tras haber realizado con éxito todas las fases anteriores, se puede concluir que se han cumplido los objetivos propuestos al inicio de este proyecto, es decir, mejorar la seguridad de la información de la organización gracias a la implementación de un Plan de Seguridad.

7.2 Objetivos conseguidos

- Se ha establecido el estado inicial de la seguridad de la información de la organización, así como los objetivos a alcanzar tras la implantación del SGSI.
- Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2013.
- Se ha realizado el análisis de riesgos de la organización del que se ha obtenido la lista de todos los activos de la empresa, las amenazas posibles a las que está expuesta la organización así el impacto y el riesgo de todos los activos de la empresa que ha permitido identificar los activos más prioritarios en cuanto a seguridad de la información.
- Se han definido y completado con éxito una serie de proyectos para mejorar la seguridad de la información de la organización, teniendo en cuenta al análisis de riesgos obtenido.
- Se ha evaluado el nivel de madurez de la seguridad de la información de la organización respecto a la norma ISO 27002:2013.
- Se ha conseguido reducir el riesgo de los activos de la organización.
- Tras la realización de todas las fases, se ha conseguido mejorar significativamente el estado inicial de la seguridad de la información de la organización.
- Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información.
- Existe el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

7.3 Futuribles

- Se deben implantar las mejoras propuestas en la fase de auditoría de cumplimiento.
- Una vez implantadas las mejoras propuestas se deberá intentar conseguir la certificación ISO 27001:2013 como se planteó al inicio del proyecto.
- Se debe seguir trabajando en la mejora del estado de la seguridad de la información de la organización con el objetivo de alcanzar el estado óptimo. Para ello, se deberán plantear nuevos proyectos para mejorar los controles que están menos maduros.

- Como se ha establecido en el Plan de Seguridad, se deben realizar revisiones periódicas al sistema de seguridad de la información de la organización.
- Como se ha establecido en el Plan de Seguridad, se deben realizar auditorías periódicas al sistema de seguridad de la información de la organización.

8 Glosario

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Activo: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditor: Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización y su justificación, así como la justificación de las exclusiones de controles.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evidencia: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información

Impacto: El coste para la empresa de un incidente, que puede o no ser medido en términos estrictamente financieros.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

ISO/IEC 27000: Revisión de los estándares de la serie 27000.

ISO/IEC 27001: Especificaciones para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27002: Código de buenas prácticas en la gestión de la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten ser protegidos de potenciales riesgos.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.

PDCA (plan-do-check-act): Método de mejora continua de la calidad. También conocido como ciclo Deming.

No repudio: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Plan de continuidad de negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Proceso: Conjunto de actividades que transforman unas entradas en salidas.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Mecanismo de protección frente a las amenazas. Existen diferentes tipos dependiendo si se desea prevenir o corregir un incidente.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza

9 Bibliografía

- https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad
- http://www.interior.gob.es/web/servicios-al-ciudadano/planes-de-prevencion/plan-director-para-la-convivencia-y-mejora-escolar
- https://www.secureit.es/procesos-y-gobierno-it/planes-directores/
- http://openaccess.uoc.edu/webapps/o2/handle/10609/48466
- http://noticias.juridicas.com/base_datos/CCAA/ma-l8-2001.html
- https://protejete.wordpress.com/gdr_principal/
- http://noticias.juridicas.com/base_datos/Penal/574083-directiva-2016-680-ue-de-27-abr-proteccion-personas-fisicas-respecto-al-tratamiento.html
- https://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/
- https://advisera.com/27001academy/es/knowledgebase/diferencias-y-similitudes-entre-iso-27001-e-iso-27002/
- http://www.magazcitum.com.mx/?p=2397#.WTfPyesT7ct
- http://secugest.blogspot.com.es/2007/09/diferencias-entre-iso-27001-e-iso-27002.html
- http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/
- https://es.slideshare.net/georgepereira01/ntc-isoiec-27001-jorge-h-gaviria-y-shernndra-ocampo
- http://ciudadano-mundial.blogspot.com.es/2015/04/iso-27001-2013-espanol-anexoA.html
- https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- Material de la asignatura Auditoría Técnica
- Material de la asignatura Sistema de gestión de la seguridad
- Materiales ofrecidos por el consultor de la asignatura TFM