MEMORIA DESCRIPTIVA

Plan Director de Seguridad ISO/IEC 27001:2005

Fecha entrega: 03/01/2014
Versión memoria: V6.0_03/01/2014

Consultor: Arsenio Tortajada Gallego
Alumno: Marc Serra Gordo

TRABAJO FINAL DE MÁSTER

MASTER MISTIC

Máster Interuniversitario de la Seguridad de las TIC

DEDICATORIA Y AGRADECIMIENTOS

Rebeca, como en todo, sin tu ayuda no sería posible

RESUM – RESUMEN – SUMMARY

CATALÀ

Aquest Treball Final de Màster (TFM) té com a **objectiu el desenvolupament d'un Pla Director de Seguretat (PDS) per a la implantació d'un Sistema de Gestió de Seguretat de la Informació** (SGSI) dins de la companyia MASEGO S.A.

MASEGO S.A. és una **empresa fictícia** dedicada a la distribució de pel·lícula d'estampació i els seus derivats a nivell mundial. **La seva motivació per crear un SGSI neix com un acte de diferenciació respecte als competidors.**

El SGSI ha de quedar integrat en la gestió diària de l'organització aconseguint que sigui part fonamental i necessària. Una correcta implantació del SGSI assegurarà els tres pilars bàsics de la seguretat de la informació: **Confidencialitat, Disponibilitat i Integritat** de la informació que es genera i tracta dins MASEGO S.A. Al llarg del projecte es **desenvoluparan 5 FASES ben diferenciades.**

Durant la **primera FASE** es farà un estudi de l'estat actual de MASEGO S.A. respecte al compliment d'aquesta sobre aspectes de la seguretat de la informació, prenent com a base les normes ISO 27001 (certificable) i la 27002.

A la **segona FASE** es realitzarà el desenvolupament de la documentació necessària per a l'establiment d'un SGSI. Alguns dels elements bàsics per al compliment de la norma són: política de seguretat, procediment de revisió per la direcció, etcètera. En acabar aquesta fase, obtindrem una declaració d'aplicabilitat (SOA).

La **tercera FASE**, la més crítica, ens donarà una valoració dels riscos que afecten l'organització segons els seus actius, en els seus emplaçaments i ens, així com el nivell acceptable i residual dels mateixos.

Com a conseqüència, en la **quarta FASE**, es definiran tots els projectes necessaris per mitigar els riscos detectats i que en finalitzar l'execució d'aquests, el risc no superi el valor acceptable definit per l'organització.

Finalment, la **cinquena FASE** proporciona els mecanismes necessaris per auditar el nivell de compliment de la norma i al mateix temps crear les No Conformitats (NC) que es detectin per al seu posterior tractament.

Com a **conclusió global** de tot el desenvolupament en totes i cadascuna de les fases descrites, MASEGO S.A. **estarà preparada per certificar sota la norma ISO 27001:2005 mitjançant una auditoria de certificació.** A més MASEGO S.A. s'assegura un SGSI robust, fiable i de garanties.

CASTELLANO

El presente Trabajo Final de Máster (TFM) tiene como **objetivo el desarrollo de un Plan Director de Seguridad (PDS) para la implantación de un Sistema de Gestión de Seguridad de la Información** (SGSI) dentro de la compañía MASEGO S.A.

MASEGO S.A. es una **empresa ficticia** dedicada a la distribución de película de estampación y sus derivados a nivel mundial. **Su motivación por crear un SGSI nace como un acto de diferenciación respecto a los competidores.**

El SGSI ha de quedar integrado en la gestión diaria de la organización consiguiendo que sea parte fundamental y necesaria. Una correcta implantación del SGSI asegurará los tres pilares básicos de la seguridad de la información: **Confidencialidad, Disponibilidad e Integridad** de la información que se genera y trata dentro de MASEGO S.A. A lo largo del proyecto se **desarrollarán 5 FASES bien diferenciadas**.

Durante la **primera FASE** se hará un estudio del estado actual de MASEGO S.A. respecto al cumplimiento de ésta sobre aspectos de la seguridad de la información, tomando como base las normas ISO 27001 (certificable) y la 27002.

En la **segunda FASE** se realizará el desarrollo de la documentación necesaria para el establecimiento de un SGSI. Algunos de los elementos básicos para el cumplimiento de la norma son: política de seguridad, procedimiento de revisión por la dirección, etcétera. Al finalizar esta fase, obtendremos una declaración de aplicabilidad (SOA).

La **tercera FASE**, la más crítica, nos dará una valoración de los riesgos que afectan a la organización según sus activos, en sus emplazamientos y entes, y el nivel aceptable y residual de los mismos.

Como consecuencia, en la **cuarta FASE**, se definirán todos los proyectos necesarios para mitigar los riesgos detectados y que al finalizar la ejecución de estos proyectos, el riesgo no supere el valor aceptable definido por la organización.

Finalmente, la **quinta FASE** proporciona los mecanismos necesarios para auditar el nivel de cumplimiento de la norma y al mismo tiempo crear las No Conformidades (NC) que se detecten para su posterior tratamiento.

Como **conclusión global** de todo el desarrollo en todas y cada una de las fases descritas, MASEGO S.A. **estará preparada para certificarse bajo la norma ISO 27001:2005 mediante una auditoría de certificación.** Además MASEGO S.A. se asegura un SGSI robusto, fiable y de garantías.

ENGLISH

This Master's degree final project aims to develop a Safety Director Plan (SDP) for the implementation of an Information Security Management System (ISMS) within the company MASEGO S.A.

MASEGO S.A. is an invented company dedicated to the distribution of film printing and its derivatives worldwide. The motivation for creating the ISMS is born as an act of differentiation from competitors.

The integration of the ISMS into the daily management of the organization is critical and necessary. Proper implementation of the ISMS will ensure the three foundations of information security: **Confidentiality**, **Availability** and **Integrity** of information generated and treated within MASEGO S.A. To achieve this goal, 5 different stages have been developed throughout the Project:

During the **first stage**, a study of the current state of MASEGO S.A. regarding compliance with aspects regarding information security has been done. This analysis is based on the ISO 27001 (certifiable) and 27002 standards.

In the **second stage**, development of the necessary documentation for the establishment of an MSIS is performed. Some of the basic elements for the compliance of the standard are: security policy, procedure management review, etc. At the end of this stage, we will get a statement of applicability (SOA).

The **third stage**, the most critical one, will give us an assessment of the risks to the organization as their assets, their locations and entities, and acceptable residual level.

As a consequence, in the **fourth stage**, the projects needed to overcome detected risks are defined. Therefore, at the end of this stage, the risk levels mustn't reach the minimum level previously defined by the company.

Finally, the **fifth stage** provides mechanisms to audit the level of compliance with the standard while creating the non-conformities (NC) that are detected for further treatment.

In **conclusion**, after development of all described stages, MASEGO S.A. **will be ready to be certified** under the ISO 27001:2005 certification through an audit. Moreover, MASEGO S.A. ensures a robust, reliable and with guarantees ISMS.

ÍNDICE

ÍNDICE DE TABLAS Y FIGURAS

FASE 1

1. INTRODUCCIÓN

La seguridad de la información es un término relativamente nuevo, el cual nace por la necesidad de las empresas, de cualquier magnitud, de salvaguardar la información que éstos tratan y generan.

Se entiende por información, todos los activos de la empresa que crean o almacenan dicha información; es decir, tanto sistemas informáticos, como los lugares donde éstos se encuentran, o los soportes de los mismos, así como el tratamiento que las personas pueden hacer sobre los datos y las relaciones con terceras partes.

La norma **ISO 27001** es la base para la gestión de la seguridad de la información de una empresa, y el **plan director de seguridad**, el camino, hoja de ruta, a seguir para:

1. conocer el estado actual, situación de la empresa antes de comenzar
2. y realizar las actuaciones necesarias para mitigar todo riesgo sobre dicha información.

Este plan director de seguridad se aplicará a la empresa **MASEGO S.A.** la cual se dedica a la distribución de película de estampación de calor y frío y sus derivados. Cuenta con un sistema de calidad certificado bajo la norma **ISO 9001:2008**. Es una empresa con más de 30 años de experiencia en el sector. **MASEGO S.A.** es una empresa fuertemente establecida.

A nivel nacional, la empresa no puede crecer más. Internacionalmente el mercado está muy definido, con lo cual, la apuesta de esta empresa es la **diferenciación sobre los competidores**.

Des del año 2001, la empresa está **certificada en la gestión de la calidad** (ISO 9001). Ahora se está pensando en la certi**ficación de la seguridad de la información bajo la norma ISO 27001:2005**, como un nuevo acto de diferenciación y mejora sobre todos los procesos de la empresa, mejorando su imagen, y también con la idea de mejorar la seguridad de la información, a petición e insistencia, desde hace un par de años, del responsable del departamento de informática y calidad.

1.1. PLANIFICACION DEL PROYECTO

Las entregas del presente plan director de seguridad se dividen en **6 fases**. Cada una de las fases aborda una de las partes de las que está compuesto el plan director de seguridad de la información.

El desarrollo de cada una de las fases es secuencial. Es decir, no se comenzará una fase sin que haya acabado la anterior. Eso sí, en caso de que se tenga que revisar una de las fases anteriores a la que se esté tratando en un momento dado, se entregará la actual y la fase revisada.

La siguiente **tabla I**, muestra dicha planificación en las fechas acordadas, y el contenido de cada una de ellas:

FASE	INICIO / ENTREGA	DESCRIPCIÓN
FASE 1	18/09/2013 – **04/10/2013**	**Introducción al Proyecto.** Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa respecto a la ISO/IEC 27001+ISO/IEC 27002
FASE 2	05/10/2013 – **18/10/2013**	**Sistema de Gestión Documental**: Elaboración de la Política de Seguridad. Declaración de la aplicabilidad y documentación del SGSI
FASE 3	19/10/2013 – **15/11/2013**	**Análisis de riesgos:** Elaboración de una metodología de análisis de riesgos: Identificación y valoración de los activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.
FASE 4	16/11/2013 – **29/11/2013**	**Evaluación de proyectos** que ha de llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.
FASE 5	30/11/2013 – **13/12/2013**	**Auditoría de Cumplimiento:** Evaluación de controles, madurez y nivel de cumplimiento.
FASE 6	14/12/2013 – **03/01/2014**	**Presentación de resultados y entrega de informes:** Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a Dirección. Entrega del proyecto final.

Tabla I – Planificación por Fases del proyecto Plan Director de Seguridad

2. CONTEXTUALIZACIÓN

2.1. DESCRIPCIÓN DEL NEGOCIO

MASEGO S.A. es una empresa fuertemente establecida y reconocida en el sector de la distribución (no son fabricantes) de películas de estampación por calor y frio, y sus derivados, tanto a nivel nacional como internacional, con una cartera de más de 200 clientes, de los cuales, el **85%** se encuentran en la península ibérica (España y Portugal). Su estrategia se basa en la diferenciación de sus competidores y mantener el alto grado de servicio para y por el cliente.

Las **acciones comerciales internacionales** se basan en un **85% en la compra** de material para la posterior venta, y un **15% en la venta** de éstos mismos materiales. Las compras a proveedores internacionales se gestionan en su totalidad desde la sede central de Barcelona, basadas en **contratos de representación** de duración determinada y en lo referente a las **ventas**, con la definición de un % de comisión.

2.2. LA INFRAESTRUCTURA ORGANIZATIVA

La principal zona de actuación y negocio de la empresa se lleva a cabo en España. Dicha infraestructura se compone de:

- La sede central y CPD en BCN – **Edificio de Oficinas de 700 m^2** (una sola planta)
- Subsede en Madrid – **Edificio de Oficinas de 300 m^2** (una sola planta)
- Almacen 1 en BDN – **nave industrial 1000 m2** (diáfana 1 sola planta)
- Almacen 2 en Madrid – **nave industrial 1000 m2** (diáfana 1 sola planta)

Así como de comerciales repartidos por las zonas de:

- **Zona 1**: Aragón y Catalunya.
- **Zona 2:** Madrid, Castilla León y Castilla la Mancha.
- **Zona 3:** Valencia, Murcia y Baleares.
- **Zona 4:** Galicia y Portugal.
- **Zona 5:** País Vasco, Asturias, Pamplona, La Rioja, Cantabria.
- **Zona 6:** Andalucía, Extremadura, Canarias, Ceuta y Melilla.

Estos comerciales son independientes, y se basan en un % de comisión de las ventas que consigan en sus respectivas zonas.

En lo referente a las **conexiones y redes,** tanto los almacenes como el CDP (y sede principal) y la subsede de Madrid están interconectados físicamente (mediante VPN) como se muestra en la **figura 1** con la unión de éstas mediante líneas rojas, (como veremos más adelante en el punto 2.3).

Los **comerciales usan conexiones remotas (VPN)** para el acceso remoto a todo aquello que necesiten. No existen conexiones, a nivel de sistemas, con ningún representante internacional. Las **ventas internacionales** se realizan desde la sede central o subsede de Madrid a través de los respectivos directores comerciales.

La siguiente **figura 1**, muestra este escenario:

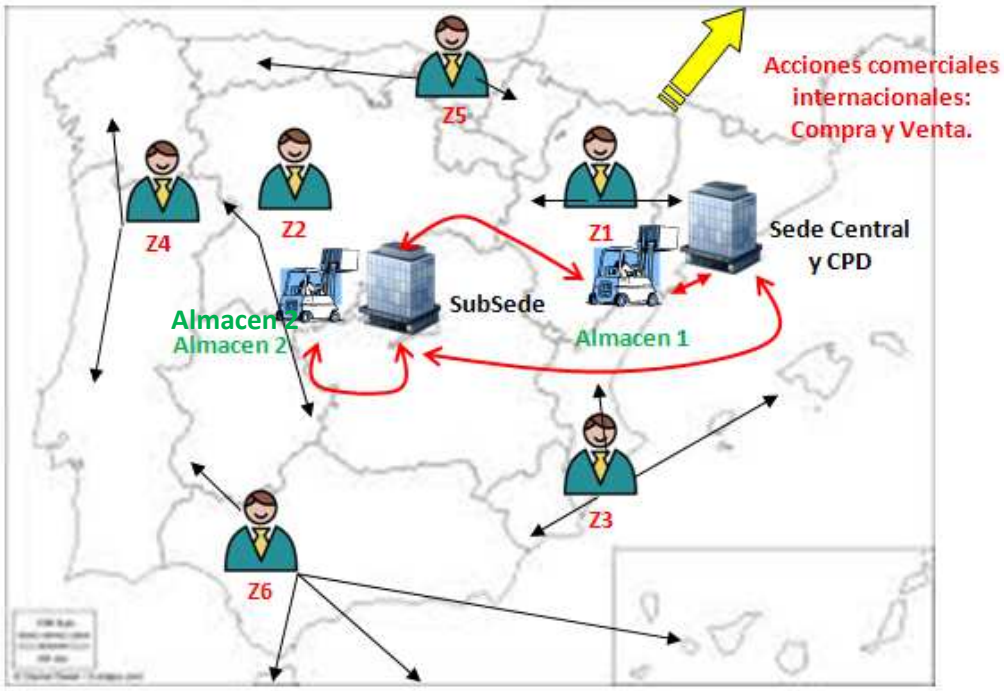


Figura 1 – Infraestructura actual de la Organización

2.3. LA INFRAESTRUCTURA DE SISTEMAS

La siguiente **figura 2**, muestra los tipos y elementos existentes para las conexiones entre sedes y almacenes, y finalmente, con los comerciales:

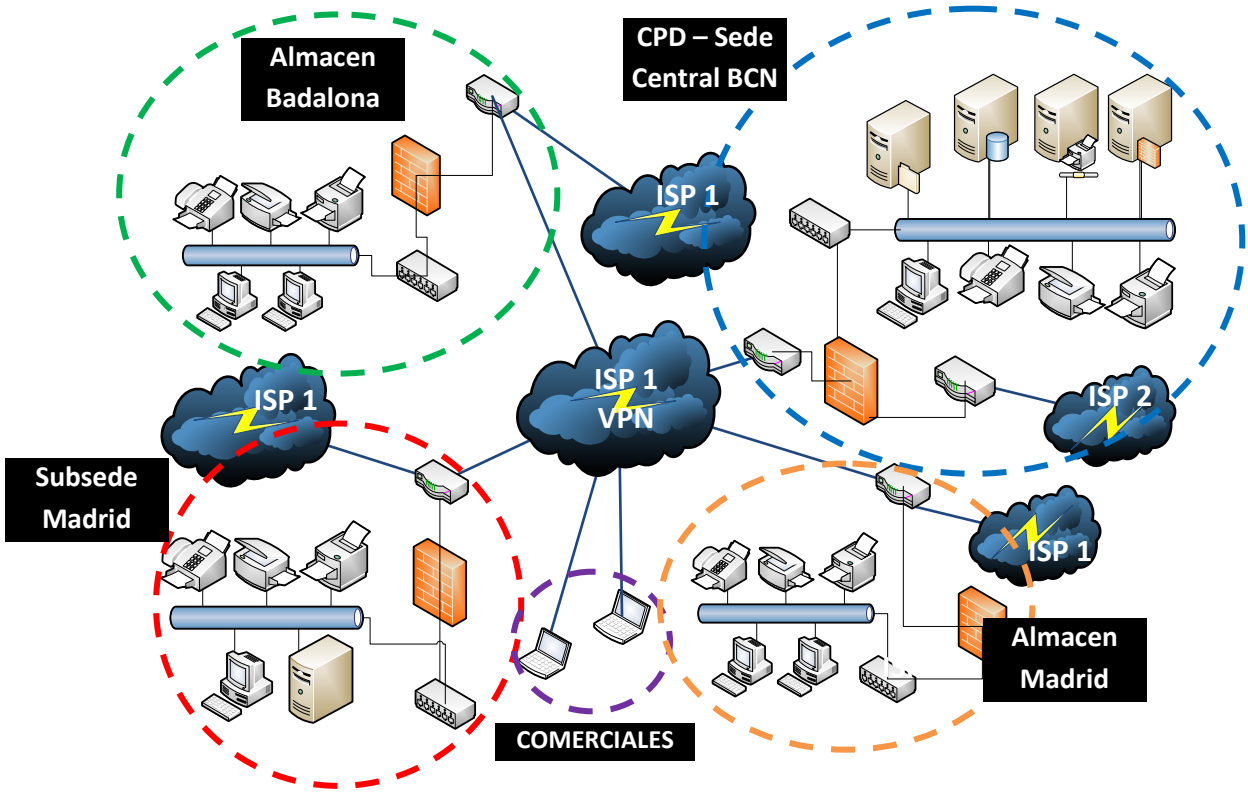


Figura 2 – Estructura de la red

De la anterior **figura 2**, **no se muestran todos los dispositivos.** A continuación podemos ver la correlación de colores para cada una de las sedes, almacenes o comerciales:

Sede Central y CPD – Conexión VPN (ISP 1) + ISP 2

Subsede Madrid – Conexión VPN (ISP 1)

Almacen Madrid – Conexión VPN (ISP 1)

Almacen Badalona – Conexión VPN (ISP 1)

Comerciales – Conexión VPN (ISP 1)

Sobre las Conexiones (Internet & VPN), aclarar que la conexión proporcionada por el **ISP1** corresponde tanto a salida a Internet para todas las sedes como para la conexión **VPN** de todos los centros que forman parte de la organización y comerciales. El **ISP2** proporciona salida a Internet exclusivamente en la sede central y CPD de Barcelona, además de todo lo necesario para gestión el servidor de correo: IP Fija, gestión del dominio, Hosting Web, etcétera.

2.4. ACTIVOS DE LA EMPRESA

Sede central y CPD

- 1 Servidor de ficheros **(HW1)**
- 1 Servidor de impresión **(HW2)**
- 1 Servidor de correo **(HW3)**
- 1 Servidor SQL de datos **(HW4)**
- 1 Servidor General **(HW5)**
- 100 ordenadores personales **(HW6)**
- 5 impresoras multifunción (copiadora / impresora / fax) **(HW7)**
- 1 concentrador **(HW8)**
- 2 enrutadores para ISP 1 e ISP 2 respectivamente **(HW9)**
- 1 cortafuegos **(HW10)**
- 2 SAI para CPD **(HW11)**

Subsede Madrid

- 1 Servidor **(HW12)**
- 50 ordenadores personales **(HW13)**
- 2 impresoras multifunción (copiadora / impresora / fax) **(HW14)**
- 1 concentrador **(HW15)**
- 1 enrutador para ISP 1 **(HW16)**
- 1 cortafuegos **(HW17)**
- 1 SAI **(HW18)**

Almacen de Badalona

- 5 ordenadores **(HW19)**
- 1 impresora multifunción (copiadora / impresora / fax) **(HW20)**
- 1 concentrador **(HW21)**
- 1 enrutador para ISP 1 **(HW22)**
- 1 cortafuegos **(HW23)**
- 1 SAI **(HW24)**

Almacen de Madrid

- 5 ordenadores **(HW25)**
- 1 impresora multifunción (copiadora / impresora / fax) **(HW26)**
- 1 concentrador **(HW27)**
- 1 enrutador para ISP 1 **(HW28)**
- 1 cortafuegos **(HW29)**
- 1 SAI **(HW30)**

Comerciales

- 6 ordenadores portátiles **(HW31)**
- 6 enrutadores portátiles 3G para ISP 1 **(HW32)**
- 6 cortafuegos (uno en cada portátil) **(HW33)**

HARDWARE

Sede central y CPD

- Windows Server 2012 **(SW1)**
- Windows Exchange Server 2012 **(SW2)**
- Windows ISA Server 2012 **(SW3)**
- Windows SQL Server 2012 **(SW4)**
- Server FAX de Windows **(SW5)**
- McAfee Total Defense 11 para Servidor **(SW6)**
- McAfee Groupshield integrado en Exchange Server **(SW7)**
- Windows 7/8 Professional 32/64 bits **(SW8)**
- Office 2010 Professional **(SW9)**
- McAfee antivirus para equipos de usuarios **(SW10)**
- ERP – A3ERP (ventas, compras, CRM integrado, contabilidad) **(SW11)**

Subsede Madrid

- Windows Server 2012 **(SW12)**
- Windows ISA Server 2012 **(SW13)**
- Server FAX de Windows **(SW14)**
- McAfee Total Defense 11 para Servidor **(SW15)**
- McAfee Groupshield integrado en Exchange Server **(SW16)**
- Windows 7/8 Professional 32/64 bits **(SW17)**
- Office 2010 Professional **(SW18)**
- McAfee antivirus para equipos de usuarios **(SW19)**
- Acceso VPN al ERP – A3ERP (ventas, compras, CRM integrado, contabilidad) **(SW20)**

Almacen de Badalona

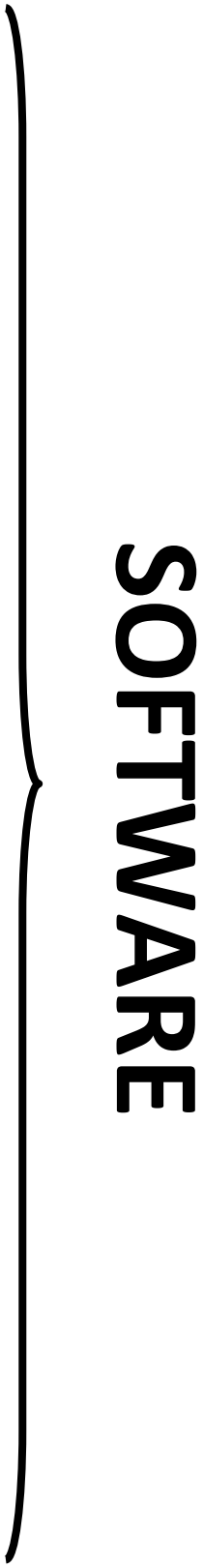
- Windows 7/8 Professional 32/64 bits **(SW21)**
- Office 2010 Professional **(SW22)**
- McAfee antivirus para equipos de usuarios **(SW23)**
- Acceso VPN al ERP – A3ERP (ventas, compras, CRM integrado, contabilidad) **(SW24)**

Almacen de Madrid

- Windows 7/8 Professional 32/64 bits **(SW25)**
- Office 2010 Professional **(SW26)**
- McAfee antivirus para equipos de usuarios **(SW27)**
- Acceso VPN al ERP – A3ERP (ventas, compras, CRM integrado, contabilidad) **(SW28)**

Comerciales

- Windows 7/8 Professional 32/64 bits **(SW29)**
- Office 2010 Professional **(SW30)**
- McAfee antivirus para equipos de usuarios **(SW31)**
- Acceso VPN al ERP – A3ERP (ventas, compras, CRM integrado, contabilidad) **(SW32)**



Sede central y CPD

- El CPD
  - Caja fuerte ignífuga para guardar copias de seguridad **(INST1)**
  - Despacho del Responsable de las TIC **(INST2)**
- Despacho del presidente
  - Caja fuerte ignífuga **(INST3)**
- Despacho director de la sede
  - Caja fuerte ignífuga para contratos y documentos financieros y contables **(INST4)**
- Despacho director comercial de Barcelona **(INST5)**
- Despacho responsable de contabilidad **(INST6)**
- Despacho responsable de RRHH **(INST7)**
- Sala de trabajo para personal auxiliar **(INST8)**
- Cuadro red eléctrica **(INST9)**
- Cuadro entrada telefonía **(INST10)**
- Cuadro de red informática **(INST11)**
- 20 Extintores **(INST12)**
- Cámaras de Seguridad (Video vigilancia) **(INST13)**
- 3 Coches de gerencia **(INST14)**

Subsede Madrid

- Despacho director de la sede **(INST15)**
- Despacho director comercial de Madrid **(INST16)**
- Cuadro red eléctrica **(INST16)**
- Cuadro entrada telefonía **(INST17)**
- Cuadro de red informática **(INST18)**
- 10 Extintores **(INST19)**
- Cámaras de Seguridad (Video vigilancia) **(INST20)**
- 2 coches de Gerencia **(INST21)**

Almacen de Badalona

- Despacho responsable del almacén **(INST21)**
- Cuadro de red eléctrica **(INST22)**
- Cuadro entrada telefonía **(INST23)**
- Cuadro de red informática **(INST24)**
- 2 BIEs y 10 extintores **(INST25)**
- 12 Máquinas de corte y rebobinado **(INST26)**
- 2 Furgonetas de reparto **(INST27)**

Almacen de Madrid

- Despacho responsable del almacén **(INST28)**
- Cuadro red eléctrica **(INST29)**
- Cuadro entrada telefonía **(INST30)**
- Cuadro de red informática **(INST31)**
- 2 BIEs y 10 extintores **(INST32)**
- 10 Máquinas de corte y rebobinado **(INST33)**
- 2 Furgonetas de reparto **(INST34)**

Comerciales

- Sin instalaciones. Uso de coche propio – se les paga por quilómetro.

INSTALACIONES, SERVICIOS Y MAQUINARIA

Sede central y CPD

- Contratos IT **(L1)**
- Contratos Proveedores del negocio **(L2)**
- Contratos Transportistas **(L3)**
- Contratos Telefonía Fija / móvil / ADSL **(L4)**
- BBDD del ERP y CRM **(L5)**
- BBDD correo electrónico **(L6)**
- BBDD usuarios del sistema **(L7)**
- Contratos Clientes **(L8)**
- Contratos Servicios **(L9)**
- Ofertas por clientes **(L10)**
- Documentación contable y financiera **(L11)**
- Discos Duros PCs / Servidores **(L12)**
- Documentación Sistema de Gestión de la Calidad ISO 9001 **(L13)**
- Documentación PRL **(L14)**
- Contratos trabajadores **(L15)**
- Cintas de Copia se Seguridad **(L16)**

Subsede Madrid

- Contratos Servicios **(L17)**
- Ofertas por clientes **(L18)**
- Documentación contable y financiera **(L19)**
- Discos Duros PCs y Servidor **(L20)**
- Documentación Sistema de Gestión de la Calidad ISO 9001 **(L20)**
- Documentación PRL **(L21)**
- BBDD usuarios del sistema **(L22)**
- Cintas de Copia se Seguridad **(L23)**
- Acceso remoto por VPN de la BBDD del ERP y CRM **(L24)**

Almacen de Badalona

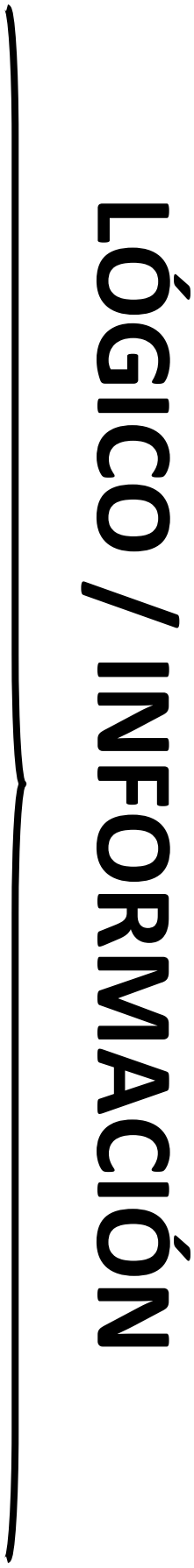
- Contratos Servicios **(L25)**
- Ofertas por clientes **(L26)**
- Discos Duros PCs y Servidor **(L27)**
- Documentación Sistema de Gestión de la Calidad ISO 9001 **(L28)**
- Documentación PRL **(L29)**
- Acceso remoto por VPN de la BBDD del ERP y CRM **(L30)**

Almacen de Madrid

- Contratos Servicios **(L31)**
- Ofertas por clientes **(L32)**
- Discos Duros PCs y Servidor **(L33)**
- Documentación Sistema de Gestión de la Calidad ISO 9001 **(L34)**
- Documentación PRL **(L35)**
- Acceso remoto por VPN de la BBDD del ERP y CRM **(L36)**

Comerciales

- Contratos Servicios **(L37)**
- Ofertas por clientes **(L38)**
- Discos Duros Portátiles **(L39)**
- Documentación Sistema de Gestión de la Calidad ISO 9001 **(L40)**
- Documentación PRL **(L41)**
- Acceso remoto por VPN de la BBDD del ERP y CRM **(L42)**



Todas las localizaciones:

- 1 presidente **(PP)**
- 1 director General **(PDG)**
- 2 directores de Sede **(PDS)**
- 2 directores comerciales **(PDC)**
- 8 responsables de área:
  - Responsable TIC **(PTIC)**
  - Responsable de Calidad **(PQ)**
  - Responsable RRHH & PRL **(PRHPRL)**
  - Responsable Contabilidad y Finanzas **(PCF)**
  - Responsable Transporte Nacional **(PTN)**
  - Responsable Transporte Internacional **(PTI)**
  - **Responsable SGSI (PSGSI)**

Nuevo ROL para el SGSI

- 191 auxiliares repartidos por todos los centros para las áreas **(PAUX)**:
  - Administración
  - RRHH & PRL
  - TIC
  - Mozos de almacén (y 4 con rol de conductor & mozo)
  - Contabilidad
- 6 comerciales repartidos por toda la península (ver zonas en el punto 2.2 del presente documento) **(PC)**

PERSONAL

En lo referente a **números absolutos** de **personal de cada sede, almacén y comerciales**, se componen por:

- Sede Principal – CPD Barcelona con **125 personas**
- Subsede Madrid con **50 personas**
- Almacen de Badalona con **20 personas**
- Almacen de Madrid con **10 personas**
- Comerciales **6 personas**

En los siguientes puntos (2.5 y 2.6) se profundiza en lo referente al personal.

Finalmente, se ha de tener en cuenta la **información intangible** que se genera a través del negocio, la cual afecta a todos (sede principal / CPD; subsede Madrid, Almacén de Badalona, Almacén de Madrid y Comerciales):

- Imagen de la empresa
- Know How por departamentos

INFORMACIÓN INTANGIBLE

NOTA**: toda la clasificación de activos hecha en este apartado nos servirá para realizar el análisis de riesgos, en próximas fases, en especial la fase III. En todo caso, **la lista anterior podrá verse modificada a lo largo de las diferentes fases del proyecto para incluir, modificar o eliminar alguno de los activos de la empresa.

2.5. ORGANIGRAMA

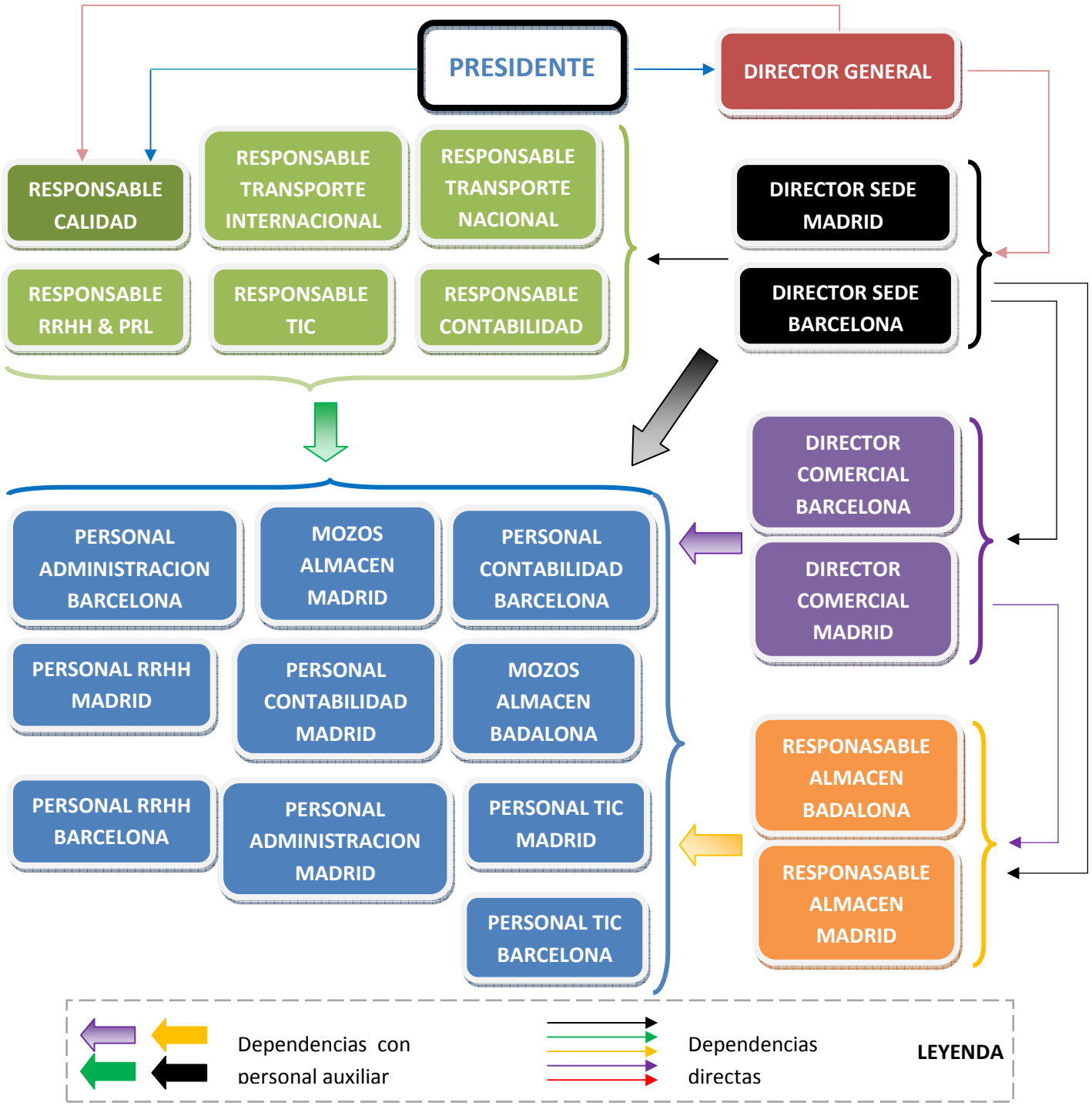


Figura 3 – Organigrama

2.6. FUNCIONES Y RESPONSABILIDADES DEL PERSONAL

- **Presidente:** fundador de la empresa. Posee acceso total y sin restricciones a toda la información de la empresa. Delega directamente sobre el director general, realizando reuniones semanales con éste. Localizado en la sede central y CPD de Barcelona. No suele pasar, pero tiene comunicación, cuando así lo requiera, con cualquier empleado del

personal auxiliar (ver mapa organizativo) y en mayor frecuencia con los mandos intermedios. Finalmente, suele tener contacto con el responsable de Calidad, tanto para definición de objetivos, como revisiones anuales por la dirección entre otros.

- **Director General:** mano derecha del presidente. Reuniones semanales con éste. Acceso total y sin restricciones a toda la información de la empresa, excepto a la del presidente de la compañía. Éste le da la información a la cual no tiene acceso, cuando así lo cree, en la cantidad que cree, y atendiendo a las peticiones del director general. Controla los dos directores de sedes, con reuniones diarias con el director de la sede de Barcelona y de Madrid (en este caso vía teleconferencia y presencial 1 vez cada 15 días como normal general). Según sea el proyecto o situación en un momento dado, se implicará con los diferentes responsables de la empresa, en persona. Localizado en la sede central y CPD de Barcelona. Tiene comunicación, cuando así lo requiera, con cualquier empleado del personal auxiliar y reuniones del comité de calidad del cual forma parte.

- **Director sede de Barcelona:** Control total de la información generada en el CPD y sede central de Barcelona. Comunicación exhaustiva con el Director General y cuando así lo requiera, con cualquier empleado del personal auxiliar y en mayor grado con el Presidente de la organización. Comunicación con el responsable de calidad para seguimiento del cumplimiento de la norma, definición de objetivos, revisión por la dirección, etcétera. Por último, comunicación directa con el resto de responsables de departamentos (RRHH, contabilidad, etcétera.)

- **Director sede de Madrid:** Control total de la información generada en la sede de Madrid. Comunicación exhaustiva con el Director General (vía teleconferencia y 1 vez cada 15 días en personas en la sede central de Barcelona) y cuando así lo requiera, con cualquier empleado del personal auxiliar y en mayor grado con el Presidente de la organización, siempre presencialmente. Comunicación con el responsable de calidad para seguimiento del cumplimiento de la norma, definición de objetivos, revisión por la dirección, etcétera. Por último, comunicación directa con el resto de responsables de departamentos (RRHH, contabilidad, etcétera.)

- **Director Comercial Barcelona:** Control total de la información de clientes y proveedores (acciones comerciales en general) generada en la sede de Barcelona y los diferentes comerciales in itinere en todo momento. Depende y reporta directamente al director de la sede de Barcelona y tiene comunicación abierta con el director comercial de Madrid, director de sede de Madrid, y responde cuando se le requiere al director general (es raro que el Presidente se reúna con él). La comunicación con el personal auxiliar y responsables de otras áreas es alta, sobre todo con el responsable de calidad para el cumplimiento de los procedimientos, indicadores que le afectan entre otros.

- **Director Comercial Madrid:** Control total de la información de clientes y proveedores (acciones comerciales en general) generada en la sede de Madrid y los diferentes comerciales in itinere en todo momento. Depende y reporta directamente al director de la sede de Madrid y tiene comunicación abierta con el director comercial de Barcelona,

director de sede de Barcelona, y responde cuando se le requiere al director general (es raro que el Presidente se reúna con él). La comunicación con el personal auxiliar y responsables de otras áreas es alta, sobre todo con el responsable de calidad para el cumplimiento de los procedimientos, indicadores que le afectan entre otros.

- **Responsable de Calidad ISO 9001:2008:** Control total de la información generada en ambas sedes con el fin de cumplir con la norma de calidad. Se sitúa nominativamente al lado de los directores de sedes, con una fluida comunicación con ambos y también con el director general a la hora de definición de objetivos y revisiones por la dirección. El Presidente suele aparecer en dichas revisiones y definición de objetivos, así como para la evaluación de resultados, satisfacción de clientes, etcétera. Finalmente fluye la información con los diferentes responsables de áreas, para el seguimiento de los procedimientos de cada uno, los registros que generan, seguimiento de indicadores y resultados de éstos entre otra documentación.

- **Responsable de Contabilidad y finanzas:** Control total sobre los datos contables y financieros de la organización, generados en ambas sedes. Comunicación directa con ambos directores de sedes y cuando así se requiera, con el director general y/o presidente. Finalmente, a parte de la comunicación con otros responsables y personal auxiliar, para el desarrollo de sus funciones diarias, se reúne con el responsable de Calidad, para el control de los procedimientos, indicadores, etcétera, que le afectan.

- **Responsable de RRHH & PRL:** Control de información de riesgo sobre las personas que forman parte de la organización reportando directamente sobre los directores de sedes, y director general y presidente cuando éstos se lo soliciten. Como **Responsable PRL:** Control de información de riesgo sobre las personas que forman parte de la organización, sobretodo en la parte de Vigilancia de la Salud, reportando directamente sobre los directores de sedes, y director general y presidente cuando éstos se lo soliciten. Su función es la de prevención de accidentes, con especial atención en los dos almacenes. Todas las revisiones y documentación se llevan a cabo a través de un centro ajeno a la compañía, en este caso, **FREMAP**.

- **Responsable TIC:** Controla y asegura toda la información que se genera en la empresa mediante dispositivos informáticos. Depende directamente de los directores de sedes, y atiende para el cumplimiento de la norma de calidad, al responsable de calidad. Así mismo, puede (aunque no es lo normal) reunirse tanto con el director general como con el Presidente (en situaciones como renovación de los sistemas centrales). Existe comunicación con los directores comerciales, para reportar sobre los comerciales in itinere, sobre sus necesidades, problemas de conexiones, necesidades sobre las Tics para el desempeño de sus funciones, y atiende al resto de personal auxiliar y responsables de otras áreas.

- **Responsable Transporte Nacional:** Dependencia directa de los directores de sedes, y comunicación efectiva con el resto de responsables de áreas y personal auxiliar, en especial con los responsables de los almacenes, comerciales, y directores comerciales.

Trabaja información sensible con terceras partes, los transportistas, y los contratos que se generan con éstos. Comunicación especialmente intensa y al minuto con los almacenes tanto de Badalona como el de Madrid así como con los clientes y proveedores de ámbito nacional.

- **Responsable Transporte Internacional:** Dependencia directa de los directores de sedes, y comunicación efectiva con el resto de responsables de áreas y personal auxiliar, en especial con los responsables de los almacenes, comerciales, y directores comerciales. Trabaja información sensible con terceras partes, los transportistas, y los contratos que se generan con éstos. Comunicación especialmente intensa y al minuto con los almacenes tanto de Badalona como el de Madrid así como con los clientes y proveedores de ámbito internacional.

- **Responsable Almacen de Badalona:** Dependencia directa con el director de la sede de Barcelona. Comunicación efectiva y diaria con el resto de responsables de áreas y personal auxiliar, en especial con los responsables de transportes, comerciales y directores comerciales.

- **Responsable Almacen de Madrid:** Dependencia directa con el director de la sede de Madrid. Comunicación efectiva y diaria con el resto de responsables de áreas y personal auxiliar, en especial con los responsables de transportes, comerciales y directores comerciales.

- **Personal auxiliar:** En dependencia directa sobre sus superiores en cada uno de los ámbitos a los que corresponden, realizando tareas de apoyo y del desarrollo diario de la compañía, en cualquiera de las sedes y almacenes. Este personal auxiliar se compone de:

    - Personal de Administración Barcelona
    - Personal de Administración Madrid
    - Mozos de almacén Badalona
    - Mozos de almacén Madrid
    - Personal TIC Barcelona
    - Personal TIC Madrid
    - Personal Contabilidad Barcelona
    - Personal Contabilidad Madrid
    - Personal RRHH & PRL Madrid
    - Personal RRHH & PRL Barcelona

Finalmente, existe el **comité de dirección con el rol añadido de comité de calidad**, dado que el tamaño de la organización no es demasiado grande, en su día, se acordó que ambos comités formaran uno solo.

***NOTA**: en la próxima **FASE II** veremos los roles y responsabilidades de los diferentes comités y nuevos roles, todo ello, enfocado a la seguridad de la información. Veremos el Comité de Dirección, el Comité de Seguridad y la figura del Responsable de Seguridad de la Información.*

3. OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

En el **ANEXO I** podemos ver los **objetivos del presente plan director de seguridad** para **MASEGO S.A.** En este **ANEXO I** encontraremos los siguientes contenidos:

1. INTRODUCCION Y PUNTO DE PARTIDA
2. OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD
3. ALCANCE DEL PLAN DIRECTOR DE SEGURIDAD
4. BENEFICIOS DEL PLAN DIRECTOR DE SEGURIDAD
5. TÉCNICAS PARA RECOLECCION DE DATOS
6. NORMATIVAS APLICABLES AL PLAN DIRECTOR DE SEGURIDAD

4. ANÁLISIS DIFERENCIAL

El **modelo de Capacidad y Madurez o CMM** (Capability Maturity Model), es un modelo de evaluación de procesos de una organización; desarrollado inicialmente para los procesos relativos al Software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).Con este modelo, podremos **averiguar el nivel de implantación actual**. Podemos ver esta configuración en la siguiente **tabla II:**

VALOR	EFECTIVIDAD	Significado	DESCRIPCIÓN
L0	**0%**	**Inexistente**	Carencia completa de cualquier proceso conocido.
L1	**10%**	**Inicial / Ad-hoc**	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	**50%**	**Reproducible, pero intuitivo**	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	**90%**	**Proceso definido**	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	**95%**	**Gestionado y medible**	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	**100%**	**Optimizado**	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	**N/A**	**No aplica**	

Tabla II – Valoración del nivel de implantación

El **nivel 3** es el nivel de implantación requerido para certificarse, y el **nivel 4** para los controles de más alto riesgo. Usaremos este modelo CMM para comprobar el nivel de aplicación y madurez de la empresa bajo las normas ISO 27001 y 27002 respectivamente.

4.1. ANÁLISI DIFERENCIAL BAJO LA NORMA ISO 27001:2005

La norma ISO 27001:2005 se compone de 5 puntos esenciales (del 4 al 8 ambos inclusive). Con el siguiente análisis veremos que puntos de esta norma son aplicables a la empresa objeto de este estudio, y, veremos a qué nivel de implantación se encuentra. **En el ANEXO II podemos ver el resultado del análisis diferencial bajo la norma ISO 27001:2005**

4.2. ANÁLISIS DIFERENCIAL BAJO LA NORMA ISO 27002 (ANEXO A ISO 27001:2005)

En la ANEXO III podemos ver el resultado del análisis diferencial, viendo el tipo de control (si es de tipo jurídico, de gestión o técnico), si aplica (si cada uno de los controles se ha de tener en cuenta en el escenario de la organización) y el valor (o nivel de madurez en el que se encuentra).

4.3. CONCLUSIONES DEL ANÁLISIS DIFERENCIAL

Hacer un análisis diferencial no es un análisis exhaustivo, proporciona una idea aproximada de la distancia que le separa de la conformidad con la norma y el camino que habrá que recorrer.

A. **Del apartado 4.1 y su ANEXO II**, como era de esperar, vemos que la implantación es inexistente salvo uno de los puntos **(5.2.2 d) de la norma),** el cual se controla y está totalmente establecido a través del sistema de gestión de calidad.

   Aunque el nivel de implantación sea pobre y casi nulo, el Responsable de las TIC ha realizado un fuerte aprendizaje y formación para no partir de cero, demostrando ciertos conocimientos de seguridad de la información por su parte. Así mismo, algunos de los puntos tratados en la ISO 27001, son similares a los establecidos en el actual sistema de gestión de la calidad bajo la norma ISO 9001:2008, y por lo tanto, este conocimiento de las normativas y en general todo lo que ello conlleva (generar procedimientos, políticas, indicadores, revisiones por la dirección, auditorias internas), son una base más que sólida para la consecución y puesta en marcha, con bastantes puntos a favor para conseguir el objetivo con garantías. Por lo tanto, las iniciativas personales como procedimientos y cumplimientos de otras áreas de la empresa (RRHH, PRL y Gestión de la Calidad) facilitarán sin lugar a dudas una adaptación y puesta en marcha del SGSI fácilmente y sin grandes problemas.

B. **Respecto al apartado 4.2 y su ANEXO III**, y ampliando un poco la anterior, vemos que **algunos de los 133 controles** ya están en marcha (por iniciativa propia del responsable de turno), o por obligado cumplimiento de otros requisitos legales a los cuales queda expuesta la organización (por ejemplo temas de seguridad física y legales de la PRL como hemos comentado o temas legales de RRHH). En general, **el escenario es bueno**. Hay voluntad y compromiso, como se desprende de los resultados de ambos análisis, en realizar una implantación del SGSI (en especial por la iniciativa propia del responsable TIC). Algunos de los elementos de la norma ISO 27001:2005 coinciden o se asemejan mucho al sistema de PRL, el cual, está totalmente implantado en la organización (con ayuda de FREMAP y el sistema de Calidad con procedimientos e indicadores para los almacenes) y

cumpliendo con todos los requisitos legales y de seguridad en el trabajo, así como la vigilancia de la salud de los empleados.

Los **resultados globales** son los siguientes:

Podemos clasificar los controles tal y como muestra la **figura 4**:

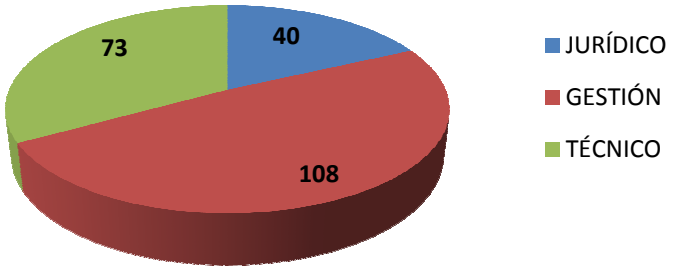


Figura 4 – Clasificación de controles

1. **De los 133** controles **APLICAN** la gran mayoría (127) sobre la organización, es decir, el **95 % aproximadamente,** tal y como puede verse en la siguiente **figura 5:**

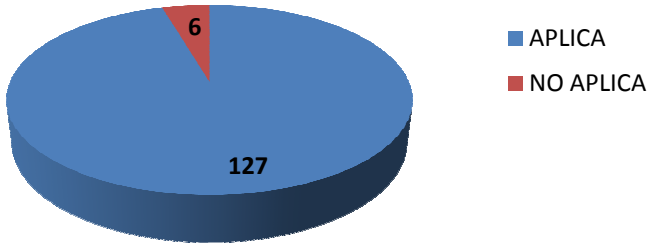


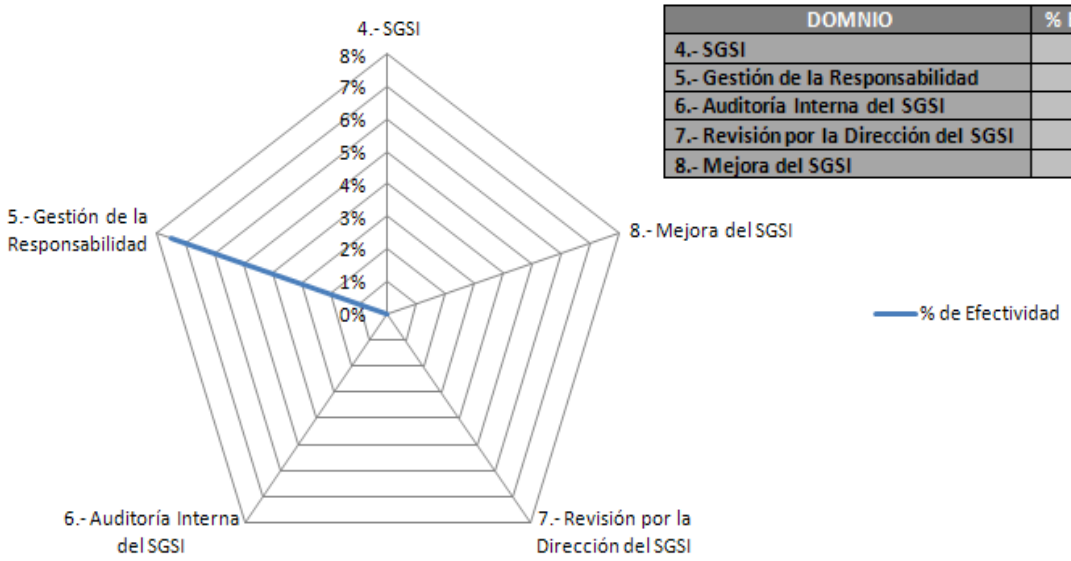
Figura 5 – Aplicabilidad de los controles en la organización

Mirando el **ANEXO III**, vemos que **existen 6 controles que no aplican** a la organización. Estos tratan conceptos de comercio electrónico, y de seguridad de ficheros de los sistemas. En lo referente al primer caso (controles del dominio 10.9), la empresa no utiliza la plataforma de comercio electrónico ni todo lo que ello conlleva.

Y, en el segundo caso (controles del dominio 12.4), la organización no tiene control sobre el software que ha implantado.

El ERP y CRM lo proporciona un tercero en base a un producto estándar, al cual mediante programación a medida se adapta a la empresa. **La empresa no posee software propio.**

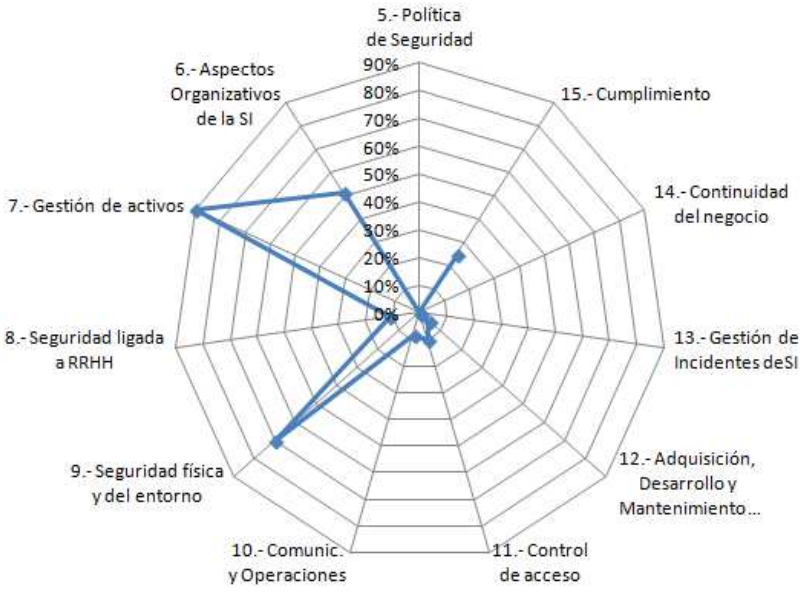
2. En porcentaje, los **niveles de madurez** para la norma ISO 27001 (**ANEXO II**) los vemos en la siguiente **figura 6**:



DOMNIO	% EFECTIVIDAD
4.- SGSI	0%
5.- Gestión de la Responsabilidad	8%
6.- Auditoría Interna del SGSI	0%
7.- Revisión por la Dirección del SGSI	0%
8.- Mejora del SGSI	0%

Figura 6 – Resultados GAP ISO 27001

3. En porcentaje, los **niveles de madurez** para la norma ISO 27002 (**ANEXO III**) los vemos en la siguiente **figura 7**:



DOMINIO	% EFECTIVIDAD
5.- Política de Seguridad	0%
6.- Aspectos organizativos de la SI	51%
7.- Gestión de activos	90%
8.- Seguridad ligada a RRHH	11%
9.- Seguridad física y del entorno	70%
10.- Comunicaciones y Operaciones	9%
11.- Control de acceso	10%
12.- Adquisición, Desarrollo y Mantenimiento de los SI	4%
13.- Gestión de Incidentes de SI	0%
14.- Continuidad del negocio	0%
15.- Cumplimiento	25%

Figura 7 – Resultados GAP ISO 27002

NOTA: *Estos resultados nos servirán para comparar los resultados obtenidos en la* ***Fase III*** *(gestión del riesgo), comprobando los niveles de madurez antes (análisis diferencial) y después (gestión del riesgo).*

FASE 2

1. INTRODUCCIÓN AL ESQUEMA DOCUMENTAL

Todos los sistemas de gestión tienen como base un sistema de gestión documental según indica el cumplimiento normativo. **MASEGO S.A.** cumple con la normativa establecida dentro del sistema de gestión de calidad con una madurez media (valorada por AENOR en su última auditoría de renovación). En el caso que nos ocupa y dentro del marco de los SGSI, **MASEGO S.A.** no cumple con la normativa por no tener ningún tipo de documentación específica para el sistema de gestión de seguridad de la información que se desea implantar, salvo iniciativas personales gran parte de las cuales las ha realizado el Responsable de las TIC.

A lo largo de esta **FASE II** se desarrollará la documentación básica y necesaria según lo establecido en la norma ISO/IEC 27001. La siguiente **figura 8**, representa esquemáticamente la documentación de obligado cumplimiento y necesaria para poder certificar el presente SGSI (optativo) y garantizar su correcto funcionamiento:

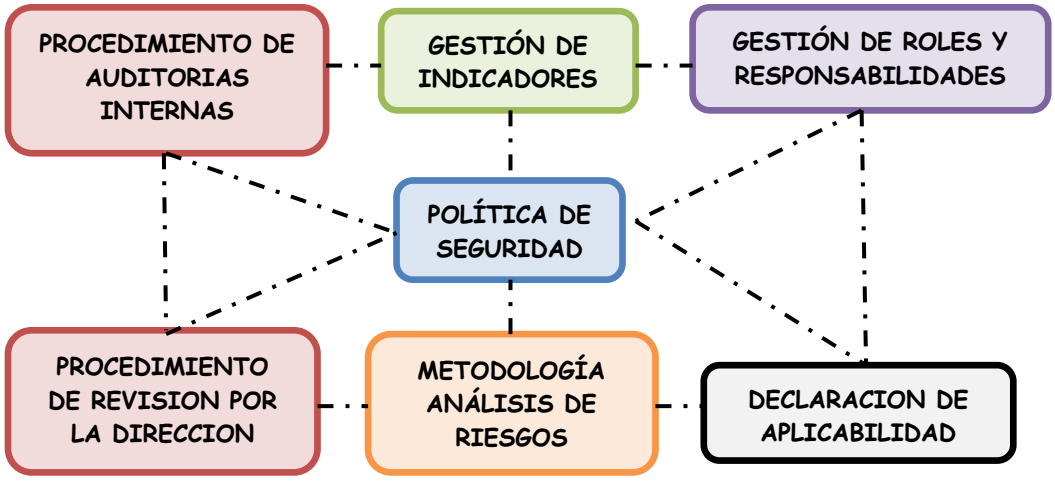


Figura 8 – Esquema básico documental SGSI

Como ya se ha comentado, este esquema representa un conjunto de documentación básica y mínima para poder implantar el sistema de gestión de seguridad de la información, es decir, la documentación puede ser mayor, tanto de inicio, como a lo largo de los años, según se identifiquen nuevas necesidades.

2. POLÍTICA DE SEGURIDAD

Podemos ver en el **ANEXO IV** la política de Seguridad para **MASEGO S.A.**

3. PROCEDIMIENTO DE AUDITORÍAS INTERNAS

Podemos ver en el **ANEXO V** la descripción del procedimiento para auditorías internas para **MASEGO S.A.**

4. GESTIÓN DE INDICADORES

Podemos ver en el **ANEXO VI, la ficha para la gestión de indicadores de la organización MASEGO S.A.**

Todos los indicadores **extraen la información** de:

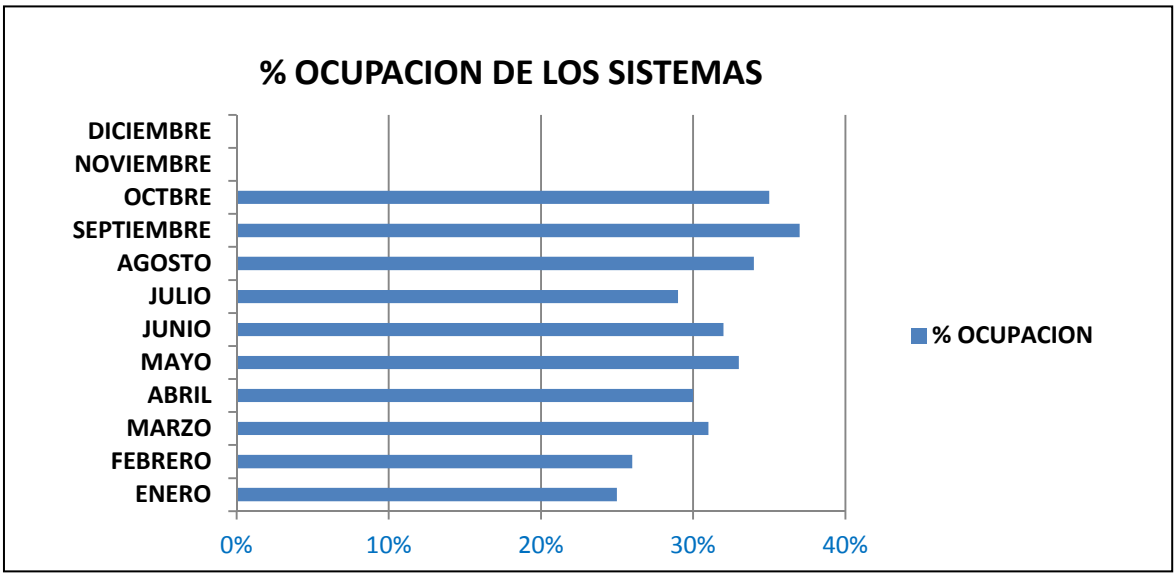
- Normas
- Procedimientos
- Registro de No Conformidades (PGNC): este registro a su vez se nutre de información diversa:
  - Logs y registros de servidores
  - Logs y registros de equipos
  - Logs y registros de aplicaciones
  - Contratos de terceras partes, clientes y proveedores
  - Reuniones, informes, etcétera.

Veamos a continuación un **EJEMPLO** de ficha de indicador (tamaño real: 1 página A4):

MASEGO S.A.	**CUADRO DE MANDO DE INDICADORES**		
	AÑO: 2013	**REVISION:** 0	**Página:** 1 de 1

INDICADOR	Capacidad de los sistemas	**IDENTIFICADOR**	IND_13
PROCESO	General del SGSI		
PROPIETARIO	Responsable de Seguridad		
OBJETIVO	Comprobar la capacidad de los sistemas		

FÓRMULA CÁLCULO	OBTENCION DE DATOS	FRECUENCIA	ARCHIVO
<= 70% de capacidad de los sistemas	Sistema Informático	MENSUAL	IND_13.docx



OBSERVACIONES: Hasta Octubre, último mes analizado, la tendencia es al alza. No obstante, el porcentaje de ocupación está a la mitad del 70% permitido. Se recomienda realizar un seguimiento.

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	18/10/2013	

5. PROCEDIMIENTO DE REVISION POR LA DIRECCIÓN

Podemos ver en el **ANEXO VII el procedimiento de revisión por la Dirección** para **MASEGO S.A.**

6. GESTION DE ROLES Y RESPONSABILIDADES

Podemos ver en el **ANEXO VIII l**os **roles y responsabilidades** definidos para **MASEGO S.A.**

7. METODOLOGÍA DE ANÁLISIS DE RIESGOS

Podemos ver en el **ANEXO IX** la **metodología para el análisis de riesgos** que se desarrollará dentro de la organización de **MASEGO S.A.**

8. DECLARACION DE APLICABILIDAD (SOA)

Podemos ver en el **ANEXO X** la declaración de aplicabilidad (SOA).

Tal y como se pudo ver en la **FASE I** del presente Plan Director de Seguridad de la Información, existen **6 controles de los 133** que define la norma, que **no aplican** dado que:

A. Los controles definidos dentro del punto **10.9 SERVICIOS DE COMERCIO ELECTRONICO (10.9.1 | 10.9.2 | 10.9.3)** hacen referencia a los procesos sobre comercio electrónico. Este caso no aplica dado que MASEGO S.A. no realizan ni implementan ningún proceso ni plataforma, respectivamente, para el comercio electrónico, por el momento.

B. Los controles definidos dentro del punto **12.4 SEGURIDAD DE LOS FICHEROS DE LOS SISTEMAS (12.4.1 | 12.4.2 | 12.4.3)** hacen referencia a la creación propia de código. Este caso no aplica dado que MASEGO S.A. tiene contratado un proveedor para los sistemas de información ERP & CRM bajo el mismo proveedor. MASEGO S.A. no es propietario del código de dichas aplicaciones ni tiene acceso al mismo.

El resto de controles **SI APLICAN** tal y como se muestra en el **ANEXO X.**

FASE 3

1. INTRODUCCIÓN

En la anterior **FASE 2,** pudimos estudiar a fondo la metodología **MAGERIT (V3),** entre muchos otros aspectos del plan director de seguridad. En esta **FASE 3,** se desarrollará esta metodología.

Es un punto crítico dentro del plan director, de vital importancia. Una mal clasificación de activos, valoración de los mismos, de las amenazas, de las vulnerabilidades, etcétera pueden resultar fatales en los valores obtenidos y por lo tanto, obtener un plan director ineficiente e inútil, dando lugar a una mala gestión del riesgo, pérdida de tiempo en reparar los errores y volver a empezar.

2. INVENTARIO DE LOS ACTIVOS

A lo largo del desarrollo de la **FASE 1 (punto 2.4)** se realizó un inventario de los activos más importantes y a tener en cuenta de la organización MASEGO S.A. Veremos en los siguientes puntos alguna variación en la **cantidad de activos definidos en esa FASE 1 respecto los que nos encontraremos en esta FASE 3.**

Tal y como vimos en la **FASE 2,** la gestión de riesgos en el presente plan director se basa en la metodología **MAGERIT (V3)** y por lo tanto la clasificación de los activos se realiza de una manera determinada. En concreto, la **clasificación correcta de los activos** bajo esta metodología se distribuye de la siguiente manera:

Hardware	→	**[HW]**
Software	→	**[SW]**
Instalaciones	→	**[L]**
Datos / Información	→	**[D]**
Redes / Comunicaciones	→	**[COM]**
Servicios	→	**[S]**
Soportes de Información	→	**[SI]**
Equipamiento auxiliar	→	**[AUX]**
Personal	→	**[P]**

A modo resumen podemos ver en la siguiente t**abla III** la distribución de los activos para **MASEGO S.A** bajo la clasificación **MAGERIT V3**:

	SEDE CENTRAL	SUBSEDE MADRID	ALMACEN BADALONA	ALMACEN MADRID	COMERCIALES	
[SW]	6	6	5	5	2	
[HW]	11	8	4	4	4	
[L]	4	3	3	3	0	
[D]	6	6	6	6	6	
[COM]	4	4	4	4	1	
[S]	3	3	3	3	3	
[SI]	5	5	4	4	3	
[AUX]	7	6	7	7	1	
[P]	7	4	2	2	1	TOTAL 195 ACTIVOS
	53	45	38	38	21	

Tabla III – Resumen de activos por sede / entidad

Con el fin de diferenciar claramente todos los emplazamientos que forman parte de MASEGO S.A, se definirá una tabla por cada una de las instalaciones o entes representativos. En el **punto 5** de la presente **FASE 3** podremos ver las **tablas (VI, VII, VIII, IX y X)** con el resultado de la valoración de todos los activos y su criticidad según las dimensiones de seguridad.

Como iremos viendo **los activos de cada emplazamiento se identificarán por un color**. De esta manera el **negro se le asigna a la sede central & CPD de Barcelona**, el **rojo a la subsede de Madrid,** el **verde al almacén de Badalona,** el **azul al almacén de Madrid** y el **lila a los Comerciales.** De esta manera sabremos a quién afecta los activos que estamos tratando en todo momento, sobre todo de cara al análisis de amenazas según **MAGERIT (V3).**

3. VALORACIÓN DE LOS ACTIVOS

Tal y como se vio en la metodología **MAGERIT (V3)** desarrollada en las **FASE 2** del presente Plan Director de Seguridad, la valoración de cada uno de los activos, se basa en la clasificación siguiente:

VALORACION	RANGO	VALOR
Muy Alta (MA)	Valor > 200 mil €	300 mil €
Alta (A)	100 mil € < valor > 200 mil €	150 mil €
Media (M)	50 mil € < valor > 100 mil €	75 mil €
Baja (B)	10 mil € < valor > 50 mil €	30 mil €
Muy Baja (MB)	Valor < 10 mil €	10 mil €

Tabla IV – Valoración de los activos

4. DIMENSIONES DE SEGURIDAD

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos.

A. **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.

B. **Integridad (I):** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
C. **Disponibilidad (D):** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
D. **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.
E. **Trazabilidad (T):** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Estas dimensiones nos ayudarán a valorar la criticidad de cada uno de los activos. Las dimensiones se utilizan para **valorar las consecuencias de la materialización de una amenaza.** La valoración que recibe un activo en una cierta dimensión es la **medida del perjuicio** para la organización si el activo se ve dañado en dicha dimensión. Para valorar **los activos en referencia a estas dimensiones** se opta por el definido dentro de la metodología **MAGERIT (V3)** en su punto 4 (Criterios de Valoración) y que podemos ver en la siguiente **tabla V**:

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

Tabla V – Criterios de Valoración

5. RESULTADOS DE LA VALORACIÓN DE LOS ACTIVOS

En este punto, realizaremos un análisis más exhaustivo de los activos en base a su valoración (cualitativa y cuantitativa) y criticidad según las dimensiones vistas en el apartado anterior. Esta valoración de los activos, que podemos ver en las siguientes tablas, será la base del análisis de la gestión del riesgo.

Se ha optado por diferenciar los activos según su ubicación. Por lo tanto, y dado que la empresa MASEGO S.A está formada por una sede principal, una subsede, dos almacenes y comerciales in itinere, crearemos **5 tablas** que veremos a continuación.

5.1. DEPENDENCIAS ENTRE ACTIVOS

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente **este valor se acumula en los inferiores**, lo que **no quita** para que también puedan asignarse, adicionalmente, **su valoración propia**.

Las **dependencias entre los activos** son:

A. Instalaciones [L] no tiene dependencias

B. Hardware [HW] depende de las instalaciones [L], algunos elementos de las comunicaciones [COM] y de la corriente eléctrica [AUX]
C. Software [SW] depende del Hardware [HW]
D. Datos [D] depende de del Hardware [HW] + Software [SW]
E. Comunicaciones [COM] depende del Hardware [HW] + Instalaciones [L] y de la corriente eléctrica [AUX]
F. Servicios [S] depende del Hardware [HW] + Software [SW] + Comunicaciones [COM] + Instalaciones [L]
G. Soportes de información [SI] dependen de instalaciones [L] + según cual sea el activo a tratar [AUX]
H. Auxiliares [AUX] depende de las Instalaciones [L] + Hardware [HW] y otros [AUX]
I. Personal [P] no tiene dependencias

No se ha querido profundizar más en las dependencias con el fin de **no complicar** más las tablas, dejando solo las más directas. Cabe destacar que las dependencias indican que las valoraciones de las dimensiones de seguridad pesarán las de mayor valoración, en los activos dependientes de los activos "padre", pero no siempre (dependerá del tipo de activo).

5.2. VALORACIÓN DE ACTIVOS DE LA SEDE PRINCIPAL & CPD EN BARCELONA

En esta **tabla VI**, podemos ver el resultado de la valoración de los activos en la sede principal:

TIPO	ACTIVO	ID_ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
					C	I	D	A	T
HW	5 Servidores	**[HW1]**	A	[L1] [COM1] [COM2] [AUX3] [AUX4]	9	9	10	9	9
	100 Ordenadores Personales	**[HW2]**	A	[L2] [L4] [AUX3] [AUX4] [COM1]	4	5	6	5	6
	5 impresoras multifunción	**[HW3]**	B	[L2] [L4] [AUX3] [AUX4] [COM1]	3	2	3	5	5
	10 concentrador	**[HW4]**	B	[L1] [AUX3] [AUX4]	3	2	3	5	5
	2 enrutadores	**[HW5]**	B	[L1] [AUX3] [AUX4] [COM1] [COM2]	9	7	7	5	8
	2 Firewall	**[HW6]**	B	[L1] [AUX3] [AUX4] [COM1] [COM2]	7	7	7	5	7
SW	1 Windows Server 2012	**[SW1]**	B	[HW1]	9	9	10	9	9
	1 Windows Exchange Server 2012	**[SW2]**	MB	[HW1]	9	9	10	9	9
	1 Windows ISA Server 2012	**[SW3]**	MB	[HW1]	9	9	10	9	9
	1 Windows SQL Server 2012	**[SW4]**	MB	[HW1]	9	9	10	9	9
	1 Server FAX de Windows	**[SW5]**	MB	[HW1]	9	9	10	9	9
	1 McAfee Total Defense 11	**[SW6]**	MB	[HW1]	9	9	10	9	9
	1 McAfee GroupShield para Exchange	**[SW7]**	MB	[HW1]	9	9	10	9	9
	100 McAfee antivirus para usuarios	**[SW8]**	MB	[HW2]	4	5	6	5	6
	100 Windows 7 Professional	**[SW9]**	B	[HW2]	4	5	6	5	6
	100 Office 2010 Professional	**[SW10]**	B	[HW2]	4	5	6	5	6
	1 ERP + CRM – Software A3ERP	**[SW11]**	B	[HW1]	4	5	6	5	6
L	1 CPD	**[L1]**	MA	-	9	9	10	9	9
	5 Despachos Responsables	**[L2]**	A	-	9	8	8	9	8
	5 Puertas blindadas	**[L3]**	MB	-	6	6	6	7	5
	1 Sala personal auxiliar	**[L4]**	B	-	6	6	7	5	6
D	Generados por el ERP & CRM	**[D1]**	MA	[HW1] [SW4] [SW11]	9	9	10	9	9
	Datos confidenciales	**[D2]**	MA	[HW1] [HW2] [SW4] [AUX1]	9	9	10	9	9
	Datos de carácter personal	**[D3]**	MA	[HW1] [HW2] [SW4] [AUX1]	9	9	10	9	9
	Contratos	**[D4]**	A	[HW1] [HW2] [SW4] [AUX1]	9	9	10	9	9
	Imagen de la empresa	**[D5]**	M	-	-	-	-	-	-
	Know How	**[D6]**	M	-	-	-	-	-	-
COM	1 LAN con salida a Internet por ISP2	**[COM1]**	MB	[L1] [HW4] [HW5] [AUX3] [AUX4]	7	9	5	5	7
	1 VPN con ISP1	**[COM2]**	MB	[L1] [HW5] [AUX3] [AUX4]	7	9	5	5	7

	1 Centralita Telefónica	**[COM3]**	MB	[L1] [AUX4]	3	1	6	5	2
	1 Circuito TV seguridad	**[COM4]**	MB	[L1] [L2] [L4] [AUX4]	6	5	7	5	7
S	Servicios Internos	**[S1]**	M	[L1] [L2] [L4] [HW1] [HW5] [COM1]	7	8	7	5	7
	CISCO VPN (sede principal)	**[S2]**	MB	[L1] [HW1] [HW5] [COM2]	7	8	7	5	7
	Servicios Terceras partes	**[S3]**	B	-	8	8	7	5	7
SI	15 Discos Duros Externos	**[SI1]**	MB	[AUX4]	8	8	8	7	7
	100 Grabadoras DVD	**[SI2]**	MB	[HW1] [HW2]	3	2	1	2	2
	15 Pen Drive	**[SI3]**	MB	[HW1] [HW2]	8	8	5	5	7
	10 cintas DAT (magnéticas)	**[SI4]**	MB	[HW1] [AUX1]	8	8	8	7	7
	Documentación impresa en papel	**[SI5]**	MB	[L1] [L2] [L4] [AUX1]	8	8	8	8	8
AUX	3 Cajas Fuertes	**[AUX1]**	M	[L1] [L2] [L4]	9	9	10	9	9
	1 Circuito Climatización	**[AUX2]**	B	[L1] [L2] [L4] [AUX4]	-	-	10	-	-
	1 Cableado de Red LAN	**[AUX3]**	MB	[L1] [L2] [L4] [AUX4]	-	-	10	-	-
	1 Cableado suministro eléctrico	**[AUX4]**	MB	[L1] [L2] [L4]	-	-	10	-	-
	3 Coches de Gerencia	**[AUX5]**	MA	-	-	-	1	-	-
	20 Extintores	**[AUX6]**	MB	[L1] [L2] [L4]	-	-	10	-	-
	2 SAI para CPD	**[AUX7]**	A	[L1] [AUX4]	-	-	10	-	-
P	1 Presidente	**[P1]**	MA	-	-	-	5	-	-
	1 Director General	**[P2]**	MA	-	-	-	4	-	-
	1 Director Sede Barcelona	**[P3]**	MA	-	-	-	3	-	-
	1 Director comercial Sede Barcelona	**[P4]**	MA	-	-	-	3	-	-
	6 Responsables Áreas	**[P5]**	MA	-	-	-	2	-	-
	15 Mandos intermedios	**[P6]**	MA	-	-	-	2	-	-
	100 Personal Auxiliar	**[P7]**	MA	-	-	-	1	-	-

Tabla VI – Valoración de Activos Sede Barcelona

5.3. VALORACIÓN DE ACTIVOS DE LA SUBSEDE DE MADRID

Veamos a continuación en esta **tabla VII**, la valoración de los activos en la sede de Madrid:

TIPO	ACTIVO	ID_ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
					C	I	D	A	T
HW	1 Servidor	**[HW7]**	B	[L5] [COM5] [COM6] [AUX9] [AUX10]	8	8	10	8	8
	50 Ordenadores Personales	**[HW8]**	M	[L5] [L7] [COM5] [COM6] [AUX9] [AUX10]	3	4	5	5	5
	2 impresoras multifunción	**[HW9]**	MB	[L5] [L7] [COM5] [AUX9] [AUX10]	2	2	2	5	3
	5 concentrador	**[HW10]**	B	[L5] [COM5] [AUX9] [AUX10]	2	2	2	5	5
	1 enrutador	**[HW11]**	B	[L5] [COM5] [COM6] [AUX9] [AUX10]	9	7	7	5	7
	1 Firewall	**[HW12]**	B	[L5] [COM5] [COM6] [AUX9] [AUX10]	6	6	7	5	7
SW	1 Windows Server 2012	**[SW12]**	B	[HW7]	8	8	10	8	8
	1 Windows ISA Server 2012	**[SW13]**	MB	[HW7]	8	8	10	8	8
	1 Server FAX de Windows	**[SW14]**	MB	[HW7]	8	8	10	8	8
	1 McAfee Total Defense 11 Server	**[SW15]**	MB	[HW7]	8	8	10	8	8
	1 McAfee GroupShield para Exchange	**[SW16]**	MB	[HW7]	8	8	10	8	8
	50 Windows 7 Professional	**[SW17]**	MB	[HW8]	3	4	5	5	5
	50 Office 2010 Professional	**[SW18]**	MB	[HW8]	3	4	5	5	5
	50 McAfee antivirus para usuarios	**[SW19]**	MB	[HW8]	3	4	5	5	5
L	2 Despachos Responsables	**[L5]**	B	-	9	8	8	9	8
	2 Puertas blindadas	**[L6]**	MB	-	6	-	6	-	-
	1 Sala personal auxiliar	**[L7]**	B	-	6	6	7	5	6
D	Generados por el ERP & CRM	**[D7]**	A	[HW7]	8	8	10	8	8
	Datos confidenciales	**[D8]**	A	[HW7] [HW8]	8	8	10	8	8
	Datos de carácter personal	**[D9]**	A	[HW7] [HW8]	8	8	10	8	8
	Contratos	**[D10]**	M	[HW8] [HW7]	8	8	10	8	8
	Imagen de la empresa	**[D11]**	M	-	-	-	-	-	-
	Know How	**[D12]**	M	-	-	-	-	-	-
COM	1 LAN con salida a Internet por ISP1	**[COM5]**	MB	[L7] [HW10] [HW11] [AUX9] [AUX10]	6	5	5	5	6

	1 VPN con ISP1	[COM6]	MB	[L1] [HW11] [AUX9] [AUX10]	7	9	7	7	7
	1 Centralita Telefónica	[COM7]	MB	[L7] [AUX10]	3	1	6	5	2
	1 Circuito TV seguridad	[COM8]	MB	[L5] [L7] [AUX10]	6	5	7	5	7
S	Servicios Internos	[S4]	B	[L5] [L7] [HW7] [HW11] [COM5]	7	8	7	5	7
	CISCO VPN (sede secundaria 1)	[S5]	MB	[L5] [HW7] [HW11] [COM6]	7	8	7	5	7
	Servicios Terceras partes	[S6]	B	-	8	8	7	5	7
SI	5 Discos Duros Externos	[SI6]	MB	[AUX10]	8	8	8	7	7
	50 Grabadoras DVD	[SI7]	MB	[HW8]	3	2	1	2	2
	5 Pen Drive	[SI8]	MB	[HW7] [HW8]	8	8	5	5	7
	10 cintas DAT (magnéticas)	[SI9]	MB	[HW7]	8	8	8	7	7
	Documentación impresa en papel	[SI10]	MB	[L5] [L7]	8	8	8	8	8
AUX	1 Circuito Climatización	[AUX8]	MB	[L5] [L7] [AUX10]	-	-	10	-	-
	1 Cableado de Red LAN	[AUX9]	MB	[L5] [L7] [AUX10]	-	-	10	-	-
	1 Cableado suministro eléctrico	[AUX10]	MB	[L5] [L7]	-	-	10	-	-
	2 Coches de Gerencia	[AUX11]	A	-	-	-	1	-	-
	10 Extintores	[AUX12]	MB	[L5] [L7]	-	-	10	-	-
	1 SAI	[AUX13]	M	[L5] [AUX10]	-	-	10	-	-
P	1 Director Sede Madrid	[P8]	MA	-	-	-	3	-	-
	1 Director comercial Sede Madrid	[P9]	MA	-	-	-	3	-	-
	8 Mandos intermedios	[P10]	MA	-	-	-	2	-	-
	40 Personal Auxiliar	[P11]	MA	-	-	-	1	-	-

Tabla VII – Valoración de activos sede Madrid

5.4. VALORACIÓN DE ACTIVOS DEL ALMACÉN DE BADALONA

Veamos en esta **tabla VIII**, la valoración de los activos en la sede del almacén de Badalona:

TIPO	ACTIVO	ID_ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
					C	I	D	A	T
HW	5 Ordenadores Personales	[HW13]	MB	[L8] [L10] [COM9] [COM10] [AUX15] [AUX16]	3	4	5	5	5
	1 impresoras multifunción	[HW14]	MB	[L8] [L10] [COM9] [AUX15] [AUX16]	2	2	2	5	3
	1 concentrador	[HW15]	MB	[L8] [COM9] [AUX15] [AUX16]	2	2	2	5	5
	1 enrutador	[HW16]	B	[L8] [COM9] [COM10] [AUX15] [AUX16]	9	7	7	5	7
	1 Firewall	[HW17]	B	[L8] [COM9] [COM10] [AUX15] [AUX16]	6	6	7	5	7
SW	5 Windows 7 Professional	[SW20]	MB	[HW13]	3	4	5	5	5
	5 Office 2010 Professional	[SW21]	MB	[HW13]	3	4	5	5	5
	5 McAfee antivirus para usuarios	[SW22]	MB	[HW13]	3	4	5	5	5
	Acceso VPN al ERP + CRM – A3ERP	[SW23]	MB	[HW16]	7	7	8	8	8
L	1 Despacho Responsable Almacén	[L8]	B	-	7	6	6	7	6
	2 Puertas blindadas	[L9]	MB	-	4	-	4	-	-
	1 Sala diáfana personal auxiliar	[L10]	B	-	5	5	8	5	5
D	Generados por el ERP & CRM	[D13]	B	[HW13]	8	8	10	8	8
	Datos confidenciales	[D14]	B	[HW13]	8	8	10	8	8
	Datos de carácter personal	[D15]	B	[HW13]	8	8	10	8	8
	Contratos	[D16]	MB	[HW13]	8	8	10	8	8
	Imagen de la empresa	[D17]	MB	-	-	-	-	-	-
	Know How	[D18]	MB	-	-	-	-	-	-
COM	1 LAN con salida a Internet por ISP1	[COM9]	MB	[L8] [HW15] [HW16] [AUX15] [AUX16]	4	5	5	5	7
	1 VPN con ISP1	[COM10]	MB	[L8] [HW16] [AUX15] [AUX16]	7	9	7	7	7
	1 Centralita Telefónica	[COM11]	MB	[L8] [AUX16]	3	1	6	5	2
	1 Circuito TV seguridad	[COM12]	MB	[L8] [L10] [AUX16]	6	5	7	5	7
S	Servicios Internos	[S7]	MB	[L8] [L10] [COM9]	7	8	7	5	7
	CISCO VPN (sede secundaria 2)	[S8]	MB	[L8] [SW23] [COM10]	7	8	7	5	7
	Servicios Terceras partes	[S9]	MB	-	8	8	7	5	7
SI	1 Discos Duro Externo	[SI11]	MB	[AUX16]	8	8	8	7	7
	5 Grabadoras DVD	[SI12]	MB	[HW13]	3	2	1	2	2

	1 Pen Drive	[SI13]	MB	[HW13]	8	8	5	5	7
	Documentación impresa en papel	[SI14]	MB	[HW13]	8	8	8	8	8
AUX	1 Circuito Climatización	[AUX14]	B	[L8] [L10] [AUX16]	-	-	10	-	-
	1 Cableado de Red LAN	[AUX15]	MB	[L8] [L10] [AUX16]	-	-	10	-	-
	1 Cableado suministro eléctrico	[AUX16]	MB	[L8] [L10]	-	-	10	-	-
	2 Furgonetas de reparto	[AUX17]	M	-	-	-	7	-	-
	12 Máquinas de corte y rebobinado	[AUX18]	MA	[L10] [AUX16]	-	-	10	-	-
	10 Extintores + 2 BIEs	[AUX19]	MB	[L8] [L10]	-	-	10	-	-
	1 SAI	[AUX20]	M	[L8] [AUX16]	-	-	10	-	-
P	2 Mandos intermedios	[P12]	MA	-	-	-	2	-	-
	18 Personal Auxiliar	[P13]	MA	-	-	-	1	-	-

Tabla VIII – Valoración de activos Almacén de Badalona

5.5. VALORACIÓN DE ACTIVOS DEL ALMACÉN DE MADRID

Veamos la valoración de los activos en la sede del almacén de Madrid **(tabla IX)**:

TIPO	ACTIVO	ID_ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
					C	I	D	A	T
HW	5 Ordenadores Personales	[HW18]	MB	[L11] [L13] [COM13] [COM14] [AUX22] [AUX23]	3	4	5	5	5
	1 impresoras multifunción	[HW19]	MB	[L11] [L13] [COM13] [AUX22] [AUX23]	2	2	2	5	3
	1 concentrador	[HW20]	MB	[L11] [COM13] [AUX22] [AUX23]	2	2	2	5	5
	1 enrutador	[HW21]	B	[L11] [COM13] [COM14] [AUX22] [AUX23]	9	7	7	5	7
	1 Firewall	[HW22]	B	[L11] [COM13] [COM14] [AUX22] [AUX23]	6	6	7	5	7
SW	5 Windows 7 Professional	[SW24]	MB	[HW18]	3	4	5	5	5
	5 Office 2010 Professional	[SW25]	MB	[HW18]	3	4	5	5	5
	5 McAfee antivirus para usuarios	[SW26]	MB	[HW18]	3	4	5	5	5
	Acceso VPN al ERP + CRM – A3ERP	[SW27]	MB	[HW21]	7	7	8	8	8
L	1 Despacho Responsable Almacén	[L11]	B	-	7	6	6	7	6
	2 Puertas blindadas	[L12]	MB	-	4	-	4	-	-
	1 Sala diáfana personal auxiliar	[L13]	B	-	5	5	8	5	5
D	Generados por el ERP & CRM	[D19]	MB	[HW18]	8	8	10	8	8
	Datos confidenciales	[D20]	MB	[HW18]	8	8	10	8	8
	Datos de carácter personal	[D21]	MB	[HW18]	8	8	10	8	8
	Contratos	[D22]	MB	[HW18]	8	8	10	8	8
	Imagen de la empresa	[D23]	MB	-	-	-	-	-	-
	Know How	[D24]	MB	-	-	-	-	-	-
COM	1 LAN con salida a Internet por ISP1	[COM13]	MB	[L11] [HW20] [HW21] [AUX22] [AUX23]	4	5	5	5	7
	1 VPN con ISP1	[COM14]	MB	[L11] [HW21] [AUX22] [AUX23]	7	9	7	7	7
	1 Centralita Telefónica	[COM15]	MB	[L11] [AUX23]	3	1	6	5	2
	1 Circuito TV seguridad	[COM16]	MB	[L11] [L13] [AUX23]	6	5	7	5	7
S	Servicios Internos	[S10]	MB	[L11] [L13] [COM13]	7	8	7	5	7
	CISCO VPN (sede secundaria 3)	[S11]	MB	[L11] [SW27] [COM14]	7	8	7	5	7
	Servicios Terceras partes	[S12]	MB	-	8	8	7	5	7
SI	1 Discos Duro Externo	[SI15]	MB	[AUX23]	8	8	8	7	7
	5 Grabadoras DVD	[SI16]	MB	[HW18]	3	2	1	2	2
	1 Pen Drive	[SI17]	MB	[HW18]	8	8	5	5	7
	Documentación impresa en papel	[SI18]	MB	[HW18]	8	8	8	8	8
AUX	1 Circuito Climatización	[AUX21]	B	[L11] [L13] [AUX23]	-	-	10	-	-
	1 Cableado de Red LAN	[AUX22]	MB	[L11] [L13] [AUX23]	-	-	10	-	-
	1 Cableado suministro eléctrico	[AUX23]	MB	[L11] [L13]	-	-	10	-	-
	2 Furgonetas de reparto	[AUX24]	M	-	-	-	7	-	-
	10 Máquinas de corte y rebobinado	[AUX25]	MA	[L13] [AUX23]	-	-	10	-	-
	10 Extintores + 2 BIEs	[AUX26]	MB	[L11] [L13]	-	-	10	-	-
	1 SAI	[AUX27]	M	[L11] [AUX23]	-	-	10	-	-
P	1 Mandos intermedios	[P14]	MA	-	-	-	2	-	-

	9 Personal Auxiliar	[P15]	MA	-	-	-	1	-	-

Tabla IX – Valoración de activos Almacén Madrid

5.6. VALORACIÓN DE ACTIVOS DE LOS COMERCIALES

Veamos a continuación **(tabla X)**, la valoración de los activos para los Comerciales:

TIPO	ACTIVO	ID_ACTIVO	VALOR	DEPENDENCIAS	CRITICIDAD				
					C	I	D	A	T
HW	6 Ordenadores Portátiles	[HW23]	B	[COM17]	8	8	7	8	8
	1 PEN 3G de Movistar	[HW24]	MB	[S14]	7	4	7	8	8
SW	6 Windows 7 Professional	[SW28]	MB	[HW23]	3	4	5	5	5
	6 Office 2010 Professional	[SW29]	MB	[HW23]	3	4	5	5	5
	6 McAfee antivirus para usuarios	[SW30]	MB	[HW23]	3	4	5	5	5
	Acceso VPN al ERP + CRM – A3ERP	[SW31]	MB	[HW23] [COM17]	7	7	8	8	8
D	Generados por el ERP & CRM	[D25]	MB	[HW23]	8	8	10	8	8
	Datos confidenciales	[D26]	MB	[HW23]	8	8	10	8	8
	Datos de carácter personal	[D27]	MB	[HW23]	8	8	10	8	8
	Contratos	[D28]	MB	[HW23]	8	8	10	8	8
	Imagen de la empresa	[D29]	B	-	-	-	-	-	-
	Know How	[D30]	B	-	-	-	-	-	-
COM	1 VPN con ISP1	[COM17]	MB	[HW23] [HW24]	7	9	7	7	7
S	Servicios Internos	[S13]	MB	[HW23]	7	8	7	5	7
	CISCO VPN (accesos remotos)	[S14]	MB	[HW23] [HW24] [COM17]	7	8	7	5	7
	Servicios Terceras partes	[S15]	MB	-	8	8	7	5	7
SI	1 Grabadoras DVD	[SI19]	MB	[HW23]	3	2	1	2	2
	1 Pen Drive	[SI20]	MB	[HW23]	8	8	5	5	7
	Documentación impresa en papel	[SI21]	MB	-	8	8	8	8	8
AUX	6 coches para comercial	[AUX28]	A	-	-	-	7	-	-
P	6 Comerciales	[P16]	MA	-	-	-	5	-	-

Tabla X – Valoración de activos de los Comerciales

5.7. NOTAS Y ACLARACIONES

Seguidamente se presenta una lista con **justificaciones y aclaraciones** sobre las valoraciones de los activos y la clasificación de los mismos.

1. La clasificación de activos vista en este **Punto 5**, representa una **evolución y clasificación** sobre la metodología **MAGERIT (V3)** respecto a la lista de activos definidos previamente en la **FASE 1** del plan director de seguridad.

2. Se han diferenciado los **activos por sedes** (5 tablas, una por cada emplazamiento). Entendemos que la entidad "Comerciales" será un tipo de sede dado que son personal sin instalaciones propias que trabajan sobre el terreno, cada día en un lugar diferente.

3. No obstante se ha seguido una **numeración correlativa**, independientemente del lugar de donde procedan.

4. El **alcance del SGSI** y por lo tanto del alcance del análisis de riesgo, abarca todos los procesos relacionados con la seguridad de la información, y no solo con los sistemas informáticos. Por ello, **se ha realizado el análisis sobre todos los activos detectados**.

5. Los activos clasificados como **SERVICIOS [S] se han agrupado** con el fin de simplificar la tabla:
    I. **Servicios internos:** Son todos aquellos servicios que interactúan con los usuarios de la empresa, según su ubicación (la sede donde se encuentren). Algunos ejemplos serían:
        a) Servicio de correo electrónico
        b) Servicio de formación
        c) Servicio de red LAN
        d) Servicio de acceso a Internet
        e) Servicio de acceso a la Intranet
        f) Servicio de monitorización de los sistemas
        g) Servicio de actualización de los sistemas de equipos y servidores
        h) Etcétera.

    II. **Servicios a terceras partes:** Son todos aquellos servicios que interactúan con el personal de terceros contratado por **MASEGO S.A.** según su ubicación (la sede donde se encuentren). Algunos ejemplos serían:
        a) Servicio de mantenimiento de las TIC
        b) Servicio de mantenimiento de las instalaciones
        c) Servicio de revisión de extintores y BIE
        d) Servicio de limpieza
        e) Etcétera.

    III. **Servicio CISCO VPN:** dada la importancia y relevancia de este servicio, se ha optado por identificarlo claramente y sin agrupar (de lo contrario estaría en servicios internos).

6. La clasificación del activo **Contratos** aglutina en un solo activo, todo tipo de contratos como los de los empleados, los de clientes y proveedores, de terceras partes, etcétera.

7. En lo referente a los **Comerciales**, al ser estos itinerantes, no tienen Instalaciones fijas ni habilitadas para ellos. Por consiguiente, no tienen ningún activo de este tipo.

8. Los **activos intangibles** como **imagen de la empresa y Know How** se agrupan dentro de la categoría **DATOS [D]** según la metodología **MAGERIT (V3)**.

9. Se puede observar la similitud entre activos en cada una de las tablas definidas anteriormente. **La duplicidad nos indica que el tratamiento de esos activos** será diferente, dependiendo donde se encuentran. Es decir, el KNOW HOW de la sede principal respecto a las otras agrupaciones será diferente, tendrá su propia razón de ser y contenido: cada emplazamiento o entidad **genera un conocimiento de los procesos de MASEGO S.A.** y así se quiere contemplar.

10. En siguientes tablas de análisis de riesgos (valoración de las amenazas) utilizaremos el **ID_ACTIVO** visto en las tablas anteriores para identificar un activo, en lugar de todo su nombre.

6. ANÁLISIS DE LAS AMENAZAS

Las amenazas se clasificaran dentro de las siguientes agrupaciones (MAGERIT (V3)):

A. **Desastres Naturales: [N.'x']:** Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
B. **De origen industrial: [I.'x']:** Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
C. **Errores y fallos no intencionados: [E.'x']:** Fallos no intencionales causados por las personas.
D. **Ataques intencionados: [A.'x']:** Fallos deliberados causados por las personas.

La siguiente **tabla XI** nos muestra la clasificación de amenazas definidas en la metodología **MAGERIT V3, en su capítulo 5 "Amenazas"** y en la cual nos basaremos para realizar este análisis de amenazas:

AGRUPACIONES	AMENAZA	ID
DESASTRES NATURALES	Fuego	**N.1**
	Daños por agua	**N.2**
	Desastres naturales	**N.***
DE ORIGEN INDUSTRIAL	Fuego	**I.1**
	Daños por agua	**I.2**
	Desastres industriales	**I.***
	Contaminación electromagnética	**I.4**
	Avería de origen físico o lógico	**I.5**
	Corte de suministro eléctrico	**I.6**
	Condiciones inadecuadas de temperatura o humedad	**I.7**
	Fallo de servicios de comunicaciones	**I.8**
	Interrupción de otros servicios y suministros esenciales	**I.9**
	Degradación de los soportes de almacenamiento de la información	**I.10**
	Emanaciones electromagnéticas	**I.11**
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios	**E.1**
	Errores del administrador	**E.2**
	Errores de monitorización	**E.3**
	Errores de configuración	**E.4**
	Difusión de SW dañino	**E.8**
	Errores de [re]-encaminamiento	**E.9**
	Errores de secuencia	**E.10**
	Alteración accidental de la información	**E.15**
	Destrucción de la información	**E.18**
	Fugas de información	**E.19**
	Vulnerabilidades de los programas (SW)	**E.20**
	Errores de mantenimiento / actualización de programas (SW)	**E.21**
	Errores de mantenimiento / actualización de equipos (HW)	**E.23**
	Caída del sistema por agotamiento de recursos	**E.24**
	Pérdida de equipos	**E.25**
	Indisponibilidad del personal	**E.28**

ATAQUES INTENCIONADOS	Manipulación de los registros de actividad (log)	**A.3**
	Manipulación de la configuración	**A.4**
	Suplantación de la identidad del usuario	**A.5**
	Abuso de privilegios de acceso	**A.6**
	Uso no previsto	**A.7**
	Difusión de software dañino	**A.8**
	[Re-]encaminamiento de mensajes	**A.9**
	Alteración de secuencia	**A.10**
	Acceso no autorizado	**A.11**
	Análisis de tráfico	**A.12**
	Repudio	**A.13**
	Interceptación de información (escucha)	**A.14**
	Modificación deliberada de la información	**A.15**
	Destrucción de información	**A.18**
	Divulgación de información	**A.19**
	Manipulación de programas	**A.22**
	Manipulación de los equipos	**A.23**
	Denegación de servicio	**A.24**
	Robo	**A.25**
	Ataque destructivo	**A.26**
	Ocupación enemiga	**A.27**
	Indisponibilidad del personal	**A.28**
	Extorsión	**A.29**
	Ingeniería social (picaresca)	**A.30**

Tabla XI – Clasificación de las amenazas según MAGERIT (V3)

Para la frecuencia con la que una amenaza puede materializarse, vemos la **tabla XII,** donde podemos ver la clasificación de la frecuencia de ocurrencia de una amenaza, suponiendo que el año tiene 52 semanas y que la frecuencia de ocurrencia es la correcta para este tipo de empresa:

FRECUENCIA	ID_FRECUENCIA	RANGO	VALOR
Frecuencia Extrema	**FE**	1 vez al día	**100**
Frecuencia Alta	**FA**	1 vez cada 2 semanas	**10**
Frecuencia Media	**FM**	1 vez cada 2 meses	**1**
Frecuencia Baja	**FB**	1 vez cada 6 meses	**0,1**
Frecuencia Muy Baja	**FMB**	1 vez al año o menos	**0,01**

***NOTA**: La presente tabla ha cambiado respecto a la FASE 2. Para facilitar cálculos he fijado los valores de cada frecuencia a valores absolutos.*

Tabla XII – Clasificación de la frecuencia de las amenazas

A continuación, en primer lugar agruparemos los activos según el tipo al que pertenecen. Habrán tantas agrupaciones como tipos de activos hayan. Es por lo tanto uno de los puntos más largos y extensos de todo el proceso de análisis de riesgo, y pieza fundamental para el posterior análisis de impacto potencial, riesgo aceptable y residual.

Las agrupaciones que veremos, son una de las muchas opciones posibles, pudiendo ir aun más al detalle. No obstante, como **primera aproximación** de éstas creemos que será más que suficiente para MASEGO S.A. No obstante, entendemos que en los **siguientes ciclos del PDCA** estas clasificaciones podrán mejorarse en todos los sentidos.

6.1. RESUMEN AMENAZAS POR AGRUPACIONES DE ACTIVOS SEGÚN TIPO

Como podremos ver a continuación, se ha decidido agrupar todos los activos, según su tipo y consideración, independientemente del lugar o sede donde éstos se encuentren.

Esto es así, dado que por ejemplo, en lo referente al Hardware de Servidores, tanto en la sede Central como en Madrid, se tratará y valorará igual, pero no serán iguales al Hardware de los equipos personales. Se respeta y sigue la numeración descrita en anteriores puntos para los activos. Las agrupaciones que podremos ver a continuación las veremos aplicadas en su tabla correspondiente (del **ANEXO XI**). De manera resumida, las agrupaciones que veremos son las siguientes:

2. Hardware Servidores – **Tabla I**
3. Hardware Equipos Fijos– **Tabla II**
4. Hardware Equipos portátiles – **Tabla III**
5. Hardware de Red – **Tabla IV**
6. Software de Servidores – **Tabla V**
7. Software de Equipos – **Tabla VI**
8. Instalaciones CPD – **Tabla VII**
9. Instalaciones Oficinas – **Tabla VIII**
10. Datos – **Tabla IX**
11. Comunicaciones ISP2 – **Tabla X**
12. Comunicaciones VPN – **Tabla XI**
13. Comunicaciones varias – **Tabla XII**
14. Servicios VPN – **Tabla XIII**
15. Servicios Internos – **Tabla XIV**
16. Servicios terceras partes – **Tabla XV**
17. Soportes de información HW – **Tabla XVI**
18. Soportes de información Papel – **Tabla XVII**
19. Auxiliar General – **Tabla XVIII**
20. Auxiliar: parque móvil – **Tabla XIX**
21. Auxiliar: maquinaria del negocio – **Tabla XX**
22. Personal Directivo – **Tabla XXI**
23. Personal Responsable – **Tabla XXII**
24. Personal Auxiliar – **Tabla XXIII**
25. Personal Comerciales – **Tabla XXIV**

LOCALIZACIONES / ENTIDADES

Sede Central & CPD Barcelona

Subsede de Madrid

Almacén de Badalona

Almacén de Madrid

Comerciales

En el ANEXO XI podemos ver todas las tablas (**de la I a la XXIV** ambas inclusive**),** con la **valoración de las amenazas según las agrupaciones que acabamos de definir** (cada activo tendrá el color definido según su ubicación en anteriores apartados, como ya se ha comentado anteriormente; así sabremos el origen de cada activo para cada amenaza).Estas agrupaciones son una de las muchas opciones, interpretaciones posibles que en el caso que nos ocupa creemos suficiente y correcta. No obstante, cabe la posibilidad de ampliar estas agrupaciones a un detalle mucho mayor hasta el punto de tratar cada uno de los activos por separado. Una vez se han valorado todas las amenazas según las agrupaciones definidas, podemos proceder al cálculo del riesgo potencial y finalmente, el cálculo del riesgo aceptable y residual.

7. IMPACTO POTENCIAL

7.1. CÁLCULO DEL IMPACTO POTENCIAL

En este punto, y en base a todo el análisis de riesgo anterior, estamos en posición de calcular el impacto potencial de las amenazas sobre los activos. Al igual que en el punto 5 (de la presente FASE 3) vamos a diferenciar dicha valoración según la ubicación (sede, subsede y almacenes) o entidad (comerciales).

La estructura de las tablas que veremos a continuación, se basa en la columna **CRITICIDAD** (extraída de las tablas del punto 5), la columna **% CRITICIDAD** (extraída de las tablas del punto 6) y la columna **% IMPACTO POTENCIAL**, que será el resultado del cálculo de las dos anteriores. Para realizar este cálculo, se usará la siguiente fórmula:

IMPACTO POTENCIAL = VALOR DEL ACTIVO X VALOR DEL IMPACTO

7.2. VALORACIÓN DEL IMPACTO POTENCIAL DE LA SEDE PRINCIPAL & CPD EN BARCELONA

Veamos la valoración del impacto potencial en la sede principal **(tabla XIII)**:

TIPO	ID_ACTIVO	VALOR	CRITICIDAD					% IMPACTO					% IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[HW]	[HW1]	A	9	9	10	9	9	100%	50%	100%			9	4,5	10	0	0
	[HW2]	A	4	5	6	5	6	100%	20%	100%			4	1	6	0	0
	[HW3]	B	3	2	3	5	5	100%	20%	100%			3	0,4	3	0	0
	[HW4]	B	3	2	3	5	5	100%	50%	100%			3	1	3	0	0
	[HW5]	B	9	7	7	5	8	100%	50%	100%			9	3,5	7	0	0
	[HW6]	B	7	7	7	5	7	100%	50%	100%			7	3	7	0	0
[SW]	[SW1]	B	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW2]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW3]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW4]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW5]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW6]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW7]	MB	9	9	10	9	9	100%	100%	100%	100%		9	9	10	9	0
	[SW8]	MB	4	5	6	5	6	100%	100%	100%	100%		4	5	6	5	0
	[SW9]	B	4	5	6	5	6	100%	100%	100%	100%		4	5	6	5	0
	[SW10]	B	4	5	6	5	6	100%	100%	100%	100%		4	5	6	5	0
	[SW11]	B	4	5	6	5	6	100%	100%	100%	100%		4	5	6	5	0
[L]	[L1]	MA	9	9	10	9	9	50%	50%	100%			4,5	4,5	10	0	0
	[L2]	A	9	8	8	9	8	50%	50%	100%			4,5	4	8	0	0
	[L3]	MB	6	6	6	7	5	50%	50%	100%			3	3	6	0	0
	[L4]	B	6	6	7	5	6	50%	50%	100%			3	3	7	0	0
[D]	[D1]	MA	9	9	10	9	9	100%	50%	75%	100%	100%	9	4,5	7,5	9	9
	[D2]	MA	9	9	10	9	9	100%	50%	75%	100%	100%	9	4,5	7,5	9	9
	[D3]	MA	9	9	10	9	9	100%	50%	75%	100%	100%	9	4,5	7,5	9	9
	[D4]	A	9	9	10	9	9	100%	50%	75%	100%	100%	9	4,5	7,5	9	9
	[D5]	M	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
	[D6]	M	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
[COM]	[COM1]	MB	7	9	5	5	7	50%	20%	100%	100%		3,5	1,8	5	5	0
	[COM2]	MB	7	9	5	5	7	50%	20%	100%	100%		3,5	1,8	5	5	0

	[COM3]	MB	3	1	6	5	2	50%	20%	100%	100%		1,5	0,2	6	5	0
	[COM4]	MB	6	5	7	5	7	50%	20%	100%	100%		3	1	7	5	0
[S]	[S1]	M	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S2]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S3]	B	8	8	7	5	7	100%	50%	100%	100%	100%	8	4	7	5	7
[SI]	[SI1]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI2]	MB	3	2	1	2	2	100%	50%	100%			3	1	1	0	0
	[SI3]	MB	8	8	5	5	7	100%	50%	100%			8	4	5	0	0
	[SI4]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI5]	MB	8	8	8	8	8	50%	50%	100%			4	4	8	0	0
[AUX]	[AUX1]	M	9	9	10	9	9	50%	50%	100%			4,5	4,5	10	0	0
	[AUX2]	B	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX3]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX4]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX5]	MA	-	-	1	-	-	10%		100%			0	0	1	0	0
	[AUX6]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX7]	A	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
[P]	[P1]	MA	-	-	5	-	-	20%	20%	100%			0	0	5	0	0
	[P2]	MA	-	-	4	-	-	20%	20%	100%			0	0	4	0	0
	[P3]	MA	-	-	3	-	-	20%	20%	100%			0	0	3	0	0
	[P4]	MA	-	-	3	-	-	20%	20%	100%			0	0	3	0	0
	[P5]	MA	-	-	2	-	-	20%	20%	100%			0	0	2	0	0
	[P6]	MA	-	-	2	-	-	20%	20%	100%			0	0	2	0	0
	[P7]	MA	-	-	1	-	-	50%	10%	100%			0	0	1	0	0

Tabla XIII – Valoración del impacto potencial en la Sede Barcelona

7.3. VALORACIÓN DEL IMPACTO POTENCIAL EN LA SUBSEDE DE MADRID

Veamos la valoración del impacto potencial en la sede de Madrid **(tabla XIV)**:

TIPO	ID_ACTIVO	VALOR	CRITICIDAD					% IMPACTO					% IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[HW]	[HW7]	B	8	8	10	8	8	100%	50%	100%			8	4	10	0	0
	[HW8]	M	3	4	5	5	5	100%	20%	100%			3	0,8	5	0	0
	[HW9]	MB	2	2	2	5	3	100%	20%	100%			2	0,4	2	0	0
	[HW10]	B	2	2	2	5	5	100%	50%	100%			2	1	2	0	0
	[HW11]	B	9	7	7	5	7	100%	50%	100%			9	3,5	7	0	0
	[HW12]	B	6	6	7	5	7	100%	50%	100%			6	3	7	0	0
[SW]	[SW12]	B	8	8	10	8	8	100%	100%	100%	100%		8	8	10	8	0
	[SW13]	MB	8	8	10	8	8	100%	100%	100%	100%		8	8	10	8	0
	[SW14]	MB	8	8	10	8	8	100%	100%	100%	100%		8	8	10	8	0
	[SW15]	MB	8	8	10	8	8	100%	100%	100%	100%		8	8	10	8	0
	[SW16]	MB	8	8	10	8	8	100%	100%	100%	100%		8	8	10	8	0
	[SW17]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW18]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW19]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
[L]	[L5]	B	9	8	8	9	8	50%	50%	100%			4,5	4	8	0	0
	[L6]	MB	6	-	6	-	-	50%	50%	100%			3	0	6	0	0
	[L7]	B	6	6	7	5	6	50%	50%	100%			3	3	7	0	0
[D]	[D7]	A	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D8]	A	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D9]	A	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D10]	M	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D11]	M	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
	[D12]	M	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0

[COM]	[COM5]	MB	7	9	5	5	7	50%	20%	100%	100%		3,5	1,8	5	5	0
	[COM6]	MB	7	9	5	5	7	50%	20%	100%	100%		3,5	1,8	5	5	0
	[COM7]	MB	3	1	6	5	2	50%	20%	100%	100%		1,5	0,2	6	5	0
	[COM8]	MB	6	5	7	5	7	50%	20%	100%	100%		3	1	7	5	0
[S]	[S4]	B	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S5]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S6]	B	8	8	7	5	7	100%	50%	100%	100%	100%	8	4	7	5	7
[SI]	[SI6]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI7]	MB	3	2	1	2	2	100%	50%	100%			3	1	1	0	0
	[SI8]	MB	8	8	5	5	7	100%	50%	100%			8	4	5	0	0
	[SI9]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI10]	MB	8	8	8	8	8	50%	50%	100%			4	4	8	0	0
[AUX]	[AUX8]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX9]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX10]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX11]	A	-	-	1	-	-	10%		100%			0	0	1	0	0
	[AUX12]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX13]	M	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
[P]	[P8]	MA	-	-	3	-	-	20%	20%	100%			0	0	3	0	0
	[P9]	MA	-	-	3	-	-	20%	20%	100%			0	0	3	0	0
	[P10]	MA	-	-	2	-	-	20%	20%	100%			0	0	2	0	0
	[P11]	MA	-	-	1	-	-	50%	10%	100%			0	0	1	0	0

Tabla XIV – Valoración del impacto potencial en la subsede de Madrid

7.4. VALORACIÓN DE IMPACTO POTENCIAL EN EL ALMACÉN DE BADALONA

Veamos la valoración del impacto potencial en el almacén de Badalona (**tabla XV)**:

TIPO	ID_ACTIVO	VALOR	CRITICIDAD					% IMPACTO					% IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[HW]	[HW13]	MB	3	4	5	5	5	100%	20%	100%			3	0,8	5	0	0
	[HW14]	MB	2	2	2	5	3	100%	20%	100%			2	0,4	2	0	0
	[HW15]	MB	2	2	2	5	5	100%	50%	100%			2	1	2	0	0
	[HW16]	B	9	7	7	5	7	100%	50%	100%			9	3,5	7	0	0
	[HW17]	B	6	6	7	5	7	100%	50%	100%			6	3	7	0	0
[SW]	[SW20]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW21]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW22]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW23]	MB	7	7	8	8	8	100%	100%	100%	100%		7	7	8	8	0
[L]	[L8]	B	7	6	6	7	6	50%	50%	100%			3,5	3	6	0	0
	[L9]	MB	4	-	4	-	-	50%	50%	100%			2	0	4	0	0
	[L10]	B	5	5	8	5	5	50%	50%	100%			2,5	2,5	8	0	0
[D]	[D13]	B	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D14]	B	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D15]	B	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D16]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D17]	MB	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
	[D18]	MB	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
[COM]	[COM9]	MB	4	5	5	5	7	50%	20%	100%	100%		2	1	5	5	0
	[COM10]	MB	7	9	7	7	7	50%	20%	100%	100%		3,5	1,8	7	7	0
	[COM11]	MB	3	1	6	5	2	50%	20%	100%	100%		1,5	0,2	6	5	0
	[COM12]	MB	6	5	7	5	7	50%	20%	100%	100%		3	1	7	5	0
[S]	[S7]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S8]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S9]	MB	8	8	7	5	7	100%	50%	100%	100%	100%	8	4	7	5	7

[SI]	[SI11]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI12]	MB	3	2	1	2	2	100%	50%	100%			3	1	1	0	0
	[SI13]	MB	8	8	5	5	7	100%	50%	100%			8	4	5	0	0
	[SI14]	MB	8	8	8	8	8	50%	50%	100%			4	4	8	0	0
[AUX]	[AUX14]	B	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX15]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX16]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX17]	M	-	-	7	-	-	10%		100%			0	0	7	0	0
	[AUX18]	MA	-	-	10	-	-	10%		100%			0	0	10	0	0
	[AUX19]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX20]	M	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
[P]	[P12]	MA	-	-	2	-	-	20%	20%	100%			0	0	2	0	0
	[P13]	MA	-	-	1	-	-	50%	10%	100%			0	0	1	0	0

Tabla XV – Valoración del impacto potencial en el Almacén de Badalona

7.5. VALORACIÓN DE IMPACTO POTENCIAL EN EL ALMACÉN DE MADRID

Veamos la valoración del impacto potencial en el almacén de Madrid (**tabla XVI**):

TIPO	ID_ACTIVO	VALOR	CRITICIDAD					% IMPACTO					% IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[HW]	[HW18]	MB	3	4	5	5	5	100%	20%	100%			3	0,8	5	0	0
	[HW19]	MB	2	2	2	5	3	100%	20%	100%			2	0,4	2	0	0
	[HW20]	MB	2	2	2	5	5	100%	50%	100%			2	1	2	0	0
	[HW21]	B	9	7	7	5	7	100%	50%	100%			9	3,5	7	0	0
	[HW22]	B	6	6	7	5	7	100%	50%	100%			6	3	7	0	0
[SW]	[SW24]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW25]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW26]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW27]	MB	7	7	8	8	8	100%	100%	100%	100%		7	7	8	8	0
[L]	[L11]	B	7	6	6	7	6	50%	50%	100%			3,5	3	6	0	0
	[L12]	MB	4	-	4	-	-	50%	50%	100%			2	0	4	0	0
	[L13]	B	5	5	8	5	5	50%	50%	100%			2,5	2,5	8	0	0
[D]	[D19]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D20]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D21]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D22]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D23]	MB	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
	[D24]	MB	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
[COM]	[COM13]	MB	4	5	5	5	7	50%	20%	100%	100%		2	1	5	5	0
	[COM14]	MB	7	9	7	7	7	50%	20%	100%	100%		3,5	1,8	7	7	0
	[COM15]	MB	3	1	6	5	2	50%	20%	100%	100%		1,5	0,2	6	5	0
	[COM16]	MB	6	5	7	5	7	50%	20%	100%	100%		3	1	7	5	0
[S]	[S10]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S11]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S12]	MB	8	8	7	5	7	100%	50%	100%	100%	100%	8	4	7	5	7
[SI]	[SI15]	MB	8	8	8	7	7	100%	50%	100%			8	4	8	0	0
	[SI16]	MB	3	2	1	2	2	100%	50%	100%			3	1	1	0	0
	[SI17]	MB	8	8	5	5	7	100%	50%	100%			8	4	5	0	0
	[SI18]	MB	8	8	8	8	8	50%	50%	100%			4	4	8	0	0
[AUX]	[AUX21]	B	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX22]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX23]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX24]	M	-	-	7	-	-	10%		100%			0	0	7	0	0
	[AUX25]	MA	-	-	10	-	-	10%		100%			0	0	10	0	0

	[AUX26]	MB	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
	[AUX27]	M	-	-	10	-	-	50%	50%	100%			0	0	10	0	0
[P]	[P14]	MA	-	-	2	-	-	20%	20%	100%			0	0	2	0	0
	[P15]	MA	-	-	1	-	-	50%	10%	100%			0	0	1	0	0

Tabla XVI – Valoración del impacto potencial en el Almacén Madrid

7.6. VALORACIÓN DEL IMPACTO POTENCIAL EN LOS COMERCIALES

Veamos la valoración del impacto potencial para los Comerciales **(tabla XVII)**:

TIPO	ID_ACTIVO	VALOR	CRITICIDAD					% IMPACTO					% IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[HW]	[HW23]	B	8	8	7	8	8	100%	30%	100%			8	2,4	7	0	0
	[HW24]	MB	7	4	7	8	8	100%	30%	100%			7	1,2	7	0	0
[SW]	[SW28]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW29]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW30]	MB	3	4	5	5	5	100%	100%	100%	100%		3	4	5	5	0
	[SW31]	MB	7	7	8	8	8	100%	100%	100%	100%		7	7	8	8	0
[D]	[D25]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D26]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D27]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D28]	MB	8	8	10	8	8	100%	50%	75%	100%	100%	8	4	7,5	8	8
	[D29]	B	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
	[D30]	B	-	-	-	-	-	100%	50%	75%	100%	100%	0	0	0	0	0
[COM]	[COM17]	MB	7	9	7	7	7	50%	20%	100%	100%		3,5	1,8	7	7	0
[S]	[S13]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S14]	MB	7	8	7	5	7	100%	50%	100%	100%	100%	7	4	7	5	7
	[S15]	MB	8	8	7	5	7	100%	50%	100%	100%	100%	8	4	7	5	7
[SI]	[SI19]	MB	3	2	1	2	2	100%	50%	100%			3	1	1	0	0
	[SI20]	MB	8	8	5	5	7	100%	50%	100%			8	4	5	0	0
	[SI21]	MB	8	8	8	8	8	50%	50%	100%			4	4	8	0	0
[AUX]	[AUX28]	A	-	-	7	-	-	10%		100%			0	0	7	0	0
[P]	[P16]	MA	-	-	5	-	-	50%	10%	100%			0	0	5	0	0

Tabla XVII – Valoración del impacto potencial en los Comerciales

Las tablas que acabamos de ver nos sirven y son de gran importancia para conocer los valores de referencia para cada activo, y por lo tanto poder decidir que acciones, sobre qué activos priorizar en su ejecución.

Con estos resultados, podemos **proceder a calcular el riesgo aceptable y residual**. Lo podemos ver en el siguiente **punto 8.**

8. NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

8.1. CÁLCULO DEL RIESGO ACEPTABLE Y RESIDUAL

Veremos, para finalizar como calcular el riesgo aceptable y por lo tanto conocer el riesgo residual en la valoración de los activos, como última fase dentro del proceso de análisis de riesgo tratado a lo largo de toda esta **FASE 3.** Al igual que en el punto anterior vamos a diferenciar dicha valoración según la ubicación (sede, subsede y almacenes) o entidad (comerciales). La estructura de las tablas que veremos a continuación, se basa en la columna **IMPACTO POTENCIAL** (extraída de las tablas del **punto 7**), la **FRECUENCIA** (definida en las tablas del **punto 6**) y la columna **RIESGO**, que será el resultado del cálculo de las dos anteriores. Para realizar este cálculo, se usará la siguiente fórmula:

RIESGO = FRECUENCIA X IMPACTO POTENCIAL

8.2. VALORACIÓN DEL RIESGO ACEPTABLE Y RESIDUAL DE LA SEDE PRINCIPAL & CPD EN BARCELONA

Veamos la valoración del riesgo aceptable y residual para la sede principal **(tabla XVIII)**:

TIPO	ID_ACTIVO	VALOR	FRECUENCIA	% IMPACTO POTENCIAL					RIESGO				
				C	I	D	A	T	C	I	D	A	T
[HW]	[HW1]	A	0,1 (FB)	9	4,5	10	0	0	0,9	0,45	1	0	0
	[HW2]	A	1 (FM)	4	1	6	0	0	4	1	6	0	0
	[HW3]	B	1 (FM)	3	0,4	3	0	0	3	0,4	3	0	0
	[HW4]	B	0,1 (FB)	3	1	3	0	0	0,3	0,1	0,3	0	0
	[HW5]	B	0,1 (FB)	9	3,5	7	0	0	0,9	0,35	0,7	0	0
	[HW6]	B	0,1 (FB)	7	3	7	0	0	0,7	0,3	0,7	0	0
[SW]	[SW1]	B	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW2]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW3]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW4]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW5]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW6]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW7]	MB	0,1 (FB)	9	9	10	9	0	0,9	0,9	1	0,9	0
	[SW8]	MB	1 (FA)	4	5	6	5	0	40	**50**	**60**	**50**	0
	[SW9]	B	1 (FA)	4	5	6	5	0	40	**50**	**60**	**50**	0
	[SW10]	B	1 (FA)	4	5	6	5	0	40	**50**	**60**	**50**	0
	[SW11]	B	0,1 (FB)	4	5	6	5	0	0,4	0,5	0,6	0,5	0
[L]	[L1]	MA	0,1 (FB)	4,5	4,5	10	0	0	0,45	0,45	1	0	0
	[L2]	A	1 (FM)	4,5	4	8	0	0	4,5	4	8	0	0
	[L3]	MB	1 (FM)	3	3	6	0	0	3	3	6	0	0
	[L4]	B	1 (FM)	3	3	7	0	0	3	3	7	0	0
[D]	[D1]	MA	10 (FA)	9	4,5	7,5	9	9	**90**	45	**75**	**90**	**90**
	[D2]	MA	10 (FA)	9	4,5	7,5	9	9	**90**	45	**75**	**90**	**90**
	[D3]	MA	10 (FA)	9	4,5	7,5	9	9	**90**	45	**75**	**90**	**90**
	[D4]	A	10 (FA)	9	4,5	7,5	9	9	**90**	45	**75**	**90**	**90**
	[D5]	M	10 (FA)	0	0	0	0	0	0	0	0	0	0
	[D6]	M	10 (FA)	0	0	0	0	0	0	0	0	0	0
[COM]	[COM1]	MB	1 (FM)	3,5	1,8	5	5	0	3,5	1,8	5	5	0

	[COM2]	MB	1 (FM)	3,5	1,8	5	5	0	3,5	1,8	5	5	0
	[COM3]	MB	1 (FM)	1,5	0,2	6	5	0	1,5	0,2	6	5	0
	[COM4]	MB	1 (FM)	3	1	7	5	0	3	1	7	5	0
[S]	[S1]	M	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S2]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S3]	B	0,1 (FB)	8	4	7	5	7	0,8	0,4	0,7	0,5	0,7
[SI]	[SI1]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI2]	MB	1 (FM)	3	1	1	0	0	3	1	1	0	0
	[SI3]	MB	1 (FM)	8	4	5	0	0	8	4	5	0	0
	[SI4]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI5]	MB	0,1 (FB)	4	4	8	0	0	0,4	0,4	0,8	0	0
[AUX]	[AUX1]	M	1 (FM)	4,5	4,5	10	0	0	4,5	4,5	10	0	0
	[AUX2]	B	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX3]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX4]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX5]	MA	0,01 (FMB)	0	0	1	0	0	0	0	0,01	0	0
	[AUX6]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX7]	A	1 (FM)	0	0	10	0	0	0	0	10	0	0
[P]	[P1]	MA	0,01 (FMB)	0	0	5	0	0	0	0	0,05	0	0
	[P2]	MA	0,01 (FMB)	0	0	4	0	0	0	0	0,04	0	0
	[P3]	MA	0,01 (FMB)	0	0	3	0	0	0	0	0,03	0	0
	[P4]	MA	0,01 (FMB)	0	0	3	0	0	0	0	0,03	0	0
	[P5]	MA	0,01 (FMB)	0	0	2	0	0	0	0	0,02	0	0
	[P6]	MA	0,01 (FMB)	0	0	2	0	0	0	0	0,02	0	0
	[P7]	MA	10 (FA)	0	0	1	0	0	0	0	10	0	0

Tabla XVIII – Valoración del riesgo aceptable y residual en la Sede Barcelona

8.3. VALORACIÓN DEL RIESGO ACEPTABLE Y RESIDUAL EN LA SUBSEDE DE MADRID

Veamos la valoración del riesgo aceptable y residual para la sede de Madrid **(tabla XIX)**:

TIPO	ID_ACTIVO	VALOR	FRECUENCIA	% IMPACTO POTENCIAL					RIESGO				
				C	I	D	A	T	C	I	D	A	T
[HW]	[HW7]	B	0,1 (FB)	8	4	10	0	0	0,8	0,4	1	0	0
	[HW8]	M	1 (FM)	3	0,8	5	0	0	3	0,8	5	0	0
	[HW9]	MB	1 (FM)	2	0,4	2	0	0	2	0,4	2	0	0
	[HW10]	B	0,1(FB)	2	1	2	0	0	0,2	0,1	0,2	0	0
	[HW11]	B	0,1(FB)	9	3,5	7	0	0	0,9	0,35	0,7	0	0
	[HW12]	B	0,1(FB)	6	3	7	0	0	0,6	0,3	0,7	0	0
[SW]	[SW12]	B	0,1 (FB)	8	8	10	8	0	0,8	0,8	1	0,8	0
	[SW13]	MB	0,1 (FB)	8	8	10	8	0	0,8	0,8	1	0,8	0
	[SW14]	MB	0,1 (FB)	8	8	10	8	0	0,8	0,8	1	0,8	0
	[SW15]	MB	0,1 (FB)	8	8	10	8	0	0,8	0,8	1	0,8	0
	[SW16]	MB	0,1 (FB)	8	8	10	8	0	0,8	0,8	1	0,8	0
	[SW17]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW18]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW19]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
[L]	[L5]	B	1 (FM)	4,5	4	8	0	0	4,5	4	8	0	0
	[L6]	MB	1 (FM)	3	0	6	0	0	3	0	6	0	0
	[L7]	B	1 (FM)	3	3	7	0	0	3	3	7	0	0
[D]	[D7]	A	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D8]	A	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D9]	A	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D10]	M	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D11]	M	10 (FA)	0	0	0	0	0	0	0	0	0	0

	[D12]	M	10 (FA)	0	0	0	0	0	0	0	0	0	0
[COM]	[COM5]	MB	1 (FM)	3,5	1,8	5	5	0	3,5	1,8	5	5	0
	[COM6]	MB	1 (FM)	3,5	1,8	5	5	0	3,5	1,8	5	5	0
	[COM7]	MB	1 (FM)	1,5	0,2	6	5	0	1,5	0,2	6	5	0
	[COM8]	MB	1 (FM)	3	1	7	5	0	3	1	7	5	0
[S]	[S4]	B	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S5]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S6]	B	0,1 (FB)	8	4	7	5	7	0,8	0,4	0,7	0,5	0,7
[SI]	[SI6]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI7]	MB	1 (FM)	3	1	1	0	0	3	1	1	0	0
	[SI8]	MB	1 (FM)	8	4	5	0	0	8	4	5	0	0
	[SI9]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI10]	MB	0,1 (FB)	4	4	8	0	0	0,4	0,4	0,8	0	0
[AUX]	[AUX8]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX9]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX10]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX11]	A	0,01(FMB)	0	0	1	0	0	0	0	0,01	0	0
	[AUX12]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX13]	M	1 (FM)	0	0	10	0	0	0	0	10	0	0
[P]	[P8]	MA	0,01(FMB)	0	0	3	0	0	0	0	0,03	0	0
	[P9]	MA	0,01(FMB)	0	0	3	0	0	0	0	0,03	0	0
	[P10]	MA	0,01(FMB)	0	0	2	0	0	0	0	0,02	0	0
	[P11]	MA	10 (FA)	0	0	1	0	0	0	0	10	0	0

Tabla XIX – Valoración del riesgo aceptable y residual en la Sede de Madrid

8.4. VALORACIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA EL ALMACÉN DE BADALONA

Veamos la valoración del riesgo aceptable y residual para el almacén de Badalona (**tabla XX)**:

TIPO	ID_ACTIVO	VALOR	FRECUENCIA	% IMPACTO POTENCIAL					RIESGO				
				C	I	D	A	T	C	I	D	A	T
[HW]	[HW13]	MB	1 (FM)	3	0,8	5	0	0	3	0,8	5	0	0
	[HW14]	MB	1 (FM)	2	0,4	2	0	0	2	0,4	2	0	0
	[HW15]	MB	0,1 (FB)	2	1	2	0	0	0,2	0,1	0,2	0	0
	[HW16]	B	0,1 (FB)	9	3,5	7	0	0	0,9	0,35	0,7	0	0
	[HW17]	B	0,1 (FB)	6	3	7	0	0	0,6	0,3	0,7	0	0
[SW]	[SW20]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW21]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW22]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW23]	MB	10 (FA)	7	7	8	8	0	**70**	**70**	**80**	**80**	0
[L]	[L8]	B	1 (FM)	3,5	3	6	0	0	3,5	3	6	0	0
	[L9]	MB	1 (FM)	2	0	4	0	0	2	0	4	0	0
	[L10]	B	1 (FM)	2,5	2,5	8	0	0	2,5	2,5	8	0	0
[D]	[D13]	B	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D14]	B	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D15]	B	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D16]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D17]	MB	10 (FA)	0	0	0	0	0	0	0	0	0	0
	[D18]	MB	10 (FA)	0	0	0	0	0	0	0	0	0	0
[COM]	[COM9]	MB	1 (FM)	2	1	5	5	0	2	1	5	5	0
	[COM10]	MB	1 (FM)	3,5	1,8	7	7	0	3,5	1,8	7	7	0
	[COM11]	MB	1 (FM)	1,5	0,2	6	5	0	1,5	0,2	6	5	0
	[COM12]	MB	1 (FM)	3	1	7	5	0	3	1	7	5	0
[S]	[S7]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S8]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**

	[S9]	MB	0,1 (FB)	8	4	7	5	7	0,8	0,4	0,7	0,5	0,7
[SI]	[SI11]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI12]	MB	1 (FM)	3	1	1	0	0	3	1	1	0	0
	[SI13]	MB	1 (FM)	8	4	5	0	0	8	4	5	0	0
	[SI14]	MB	0,1 (FB)	4	4	8	0	0	0,4	0,4	0,8	0	0
[AUX]	[AUX14]	B	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX15]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX16]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX17]	M	0,01 (FMB)	0	0	7	0	0	0	0	0,07	0	0
	[AUX18]	MA	0,01 (FMB)	0	0	10	0	0	0	0	0,1	0	0
	[AUX19]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX20]	M	1 (FM)	0	0	10	0	0	0	0	10	0	0
[P]	[P12]	MA	0,01 (FMB)	0	0	2	0	0	0	0	0,02	0	0
	[P13]	MA	10 (FA)	0	0	1	0	0	0	0	10	0	0

Tabla XX – Valoración del riesgo aceptable y residual para el Almacén de Badalona

8.5. VALORACIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA EL ALMACÉN DE MADRID

Veamos la valoración del riesgo aceptable y residual para el almacén de Madrid (**tabla XXI**):

TIPO	ID_ACTIVO	VALOR	FRECUENCIA	% IMPACTO POTENCIAL					RIESGO				
				C	I	D	A	T	C	I	D	A	T
[HW]	[HW18]	MB	1 (FM)	3	0,8	5	0	0	3	0,8	5	0	0
	[HW19]	MB	1 (FM)	2	0,4	2	0	0	2	0,4	2	0	0
	[HW20]	MB	0,1 (FB)	2	1	2	0	0	0,2	0,1	0,2	0	0
	[HW21]	B	0,1 (FB)	9	3,5	7	0	0	0,9	0,35	0,7	0	0
	[HW22]	B	0,1 (FB)	6	3	7	0	0	0,6	0,3	0,7	0	0
[SW]	[SW24]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW25]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW26]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW27]	MB	10 (FA)	7	7	8	8	0	**70**	**70**	**80**	**80**	0
[L]	[L11]	B	1 (FM)	3,5	3	6	0	0	3,5	3	6	0	0
	[L12]	MB	1 (FM)	2	0	4	0	0	2	0	4	0	0
	[L13]	B	1 (FM)	2,5	2,5	8	0	0	2,5	2,5	8	0	0
[D]	[D19]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D20]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D21]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D22]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D23]	MB	10 (FA)	0	0	0	0	0	0	0	0	0	0
	[D24]	MB	10 (FA)	0	0	0	0	0	0	0	0	0	0
[COM]	[COM13]	MB	1 (FM)	2	1	5	5	0	2	1	5	5	0
	[COM14]	MB	1 (FM)	3,5	1,8	7	7	0	3,5	1,8	7	7	0
	[COM15]	MB	1 (FM)	1,5	0,2	6	5	0	1,5	0,2	6	5	0
	[COM16]	MB	1 (FM)	3	1	7	5	0	3	1	7	5	0
[S]	[S10]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S11]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S12]	MB	0,1 (FB)	8	4	7	5	7	0,8	0,4	0,7	0,5	0,7
[SI]	[SI15]	MB	1 (FM)	8	4	8	0	0	8	4	8	0	0
	[SI16]	MB	1 (FM)	3	1	1	0	0	3	1	1	0	0
	[SI17]	MB	1 (FM)	8	4	5	0	0	8	4	5	0	0
	[SI18]	MB	0,1 (FB)	4	4	8	0	0	0,4	0,4	0,8	4	8
[AUX]	[AUX21]	B	1 (FM)	0	0	10	0	0	0	0	3	1	1
	[AUX22]	MB	1 (FM)	0	0	10	0	0	0	0	8	4	5
	[AUX23]	MB	1 (FM)	0	0	10	0	0	0	0	4	4	8
	[AUX24]	M	0,01 (FMB)	0	0	7	0	0	0	0	0,07	0	0

	[AUX25]	MA	0,01 (FMB)	0	0	10	0	0	0	0	0,1	0	0
	[AUX26]	MB	1 (FM)	0	0	10	0	0	0	0	10	0	0
	[AUX27]	M	1 (FM)	0	0	10	0	0	0	0	10	0	0
[P]	[P14]	MA	0,01 (FMB)	0	0	2	0	0	0	0	0,02	0	0
	[P15]	MA	10 (FA)	0	0	1	0	0	0	0	10	0	0

Tabla XXI – Valoración del riesgo aceptable y residual para el Almacén Madrid

8.6. VALORACIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA COMERCIALES

Veamos la valoración del riesgo aceptable y residual para los Comerciales **(tabla XXII)**:

TIPO	ID_ACTIVO	VALOR	FRECUENCIA	% IMPACTO POTENCIAL					RIESGO				
				C	I	D	A	T	C	I	D	A	T
[HW]	[HW23]	B	1 (FM)	8	2,4	7	0	0	8	2,4	7	0	0
	[HW24]	MB	1 (FM)	7	1,2	7	0	0	7	1,2	7	0	0
[SW]	[SW28]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW29]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW30]	MB	10 (FA)	3	4	5	5	0	30	40	**50**	**50**	0
	[SW31]	MB	10 (FA)	7	7	8	8	0	**70**	**70**	**80**	**80**	0
[D]	[D25]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D26]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D27]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D28]	MB	10 (FA)	8	4	7,5	8	8	**80**	40	**75**	**80**	**80**
	[D29]	B	10 (FA)	0	0	0	0	0	0	0	0	0	0
	[D30]	B	10 (FA)	0	0	0	0	0	0	0	0	0	0
[COM]	[COM17]	MB	1 (FM)	3,5	1,8	7	7	0	3,5	1,8	7	7	0
[S]	[S13]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S14]	MB	10 (FA)	7	4	7	5	7	**70**	40	**70**	**50**	**70**
	[S15]	MB	0,1 (FB)	8	4	7	5	7	0,8	0,4	0,7	0,5	0,7
[SI]	[SI19]	MB	1 (FM)	3	1	1	0	0	3	1	1	0	0
	[SI20]	MB	1 (FM)	8	4	5	0	0	8	4	5	0	0
	[SI21]	MB	0,1 (FB)	4	4	8	0	0	0,4	0,4	0,8	0	0
[AUX]	[AUX28]	A	0,01 (FMB)	0	0	7	0	0	0	0	0,07	0	0
[P]	[P16]	MA	0,1 (FB)	0	0	5	0	0	0	0	0,5	0	0

Tabla XXII – Valoración del riesgo aceptable y residual para los Comerciales

8.7. NOTAS Y ACLARACIONES

1. **El nivel aceptable definido por el comité de Seguridad de la información** y por lo tanto aceptado por éstos se fija en 50 **(el 50 no es asumido, sino los que son más pequeños de 50)**. Toda valoración de activos que **supere o iguale** en cualesquiera de sus dimensiones de seguridad **ese 50,** deberá ser tomado en consideración y tendrá que mitigar el riesgo dejando su valoración **por debajo de 50** lo antes posible. Se han marcado valores altos pero que no superan el nivel aceptable (entre 30 y 40 de valoración) para que se tengan en cuenta.

2. Vemos que el **SW, Datos y Servicios** son los dominios más críticos en cuanto a la puntuación obtenida, y por lo tanto, sobre los que se tendrá que trabajar más para mitigarlos.

9. CONCLUSIONES

9.1. CONCLUSIONES SOBRE LOS ACTIVOS

En lo referente a los activos, la siguiente **figura 9** muestra el **máximo valor dado y el valor medio en cada una de las dimensiones de la seguridad,** teniendo en cuenta todos los activos. Es un resumen de lo visto en el anterior **punto 5** del presente documento.

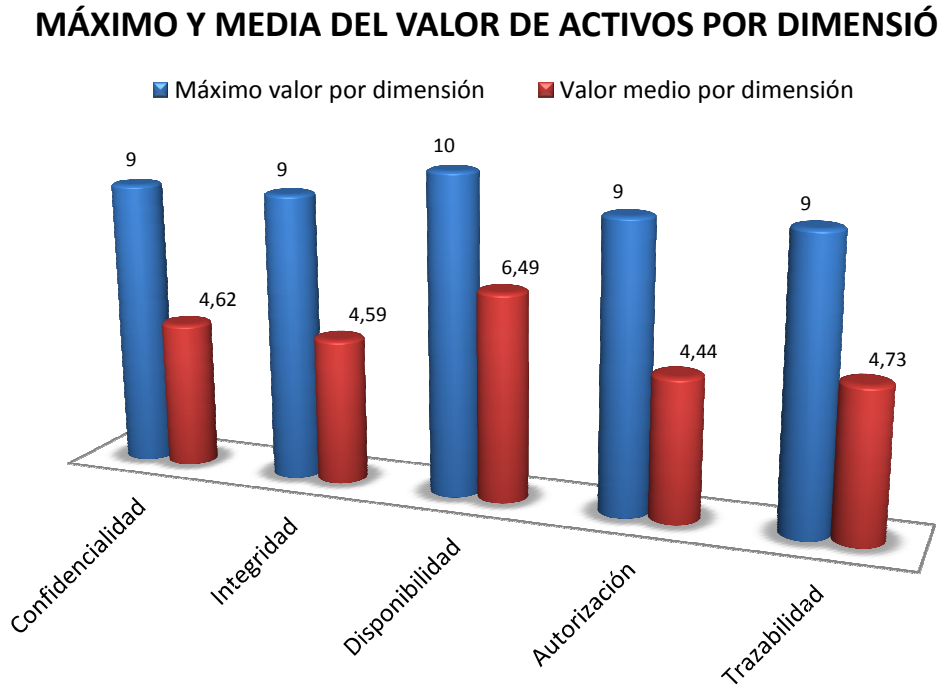


Figura 9 – Máximos y media de valoración de activos por dimensión

En lo referente a **valores máximos**, todos son muy parecidos. Destaca la dimensión de la Disponibilidad, que alcanza la valoración máxima (10). En segundo lugar destaca la dimensión de **Trazabilidad**, la cual implica el poder realizar un seguimiento de lo ocurrido (pérdida o robo de información).

En lo referente a los **valores medios**, vemos que la **Disponibilidad** es la dimensión más valorada. La **Integridad** es el punto fuerte (aunque la Autorización tenga una media menor, ésta no está presente en tantos activos como lo está la Integridad), y globalmente, el valor con peor previsión (Disponibilidad) no llega a una puntuación de 6,5 (en su media) con lo cual, en términos generales, se puede asegurar que el estado del riesgo **no es para nada crítico**.

9.2. CONCLUSIONES SOBRE LAS AMENAZAS

En la siguiente **figura 10** podemos ver la valoración máxima de las vulnerabilidades tratadas en el punto 6 de la presente FASE 3, según las dimensiones de seguridad y tipo de activo.

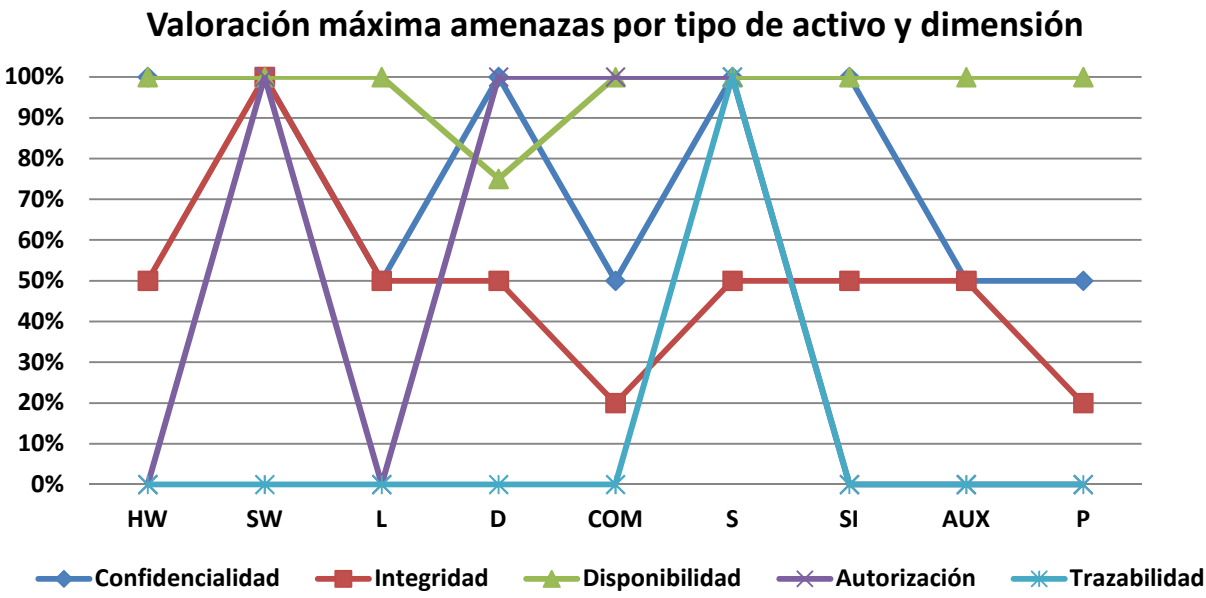


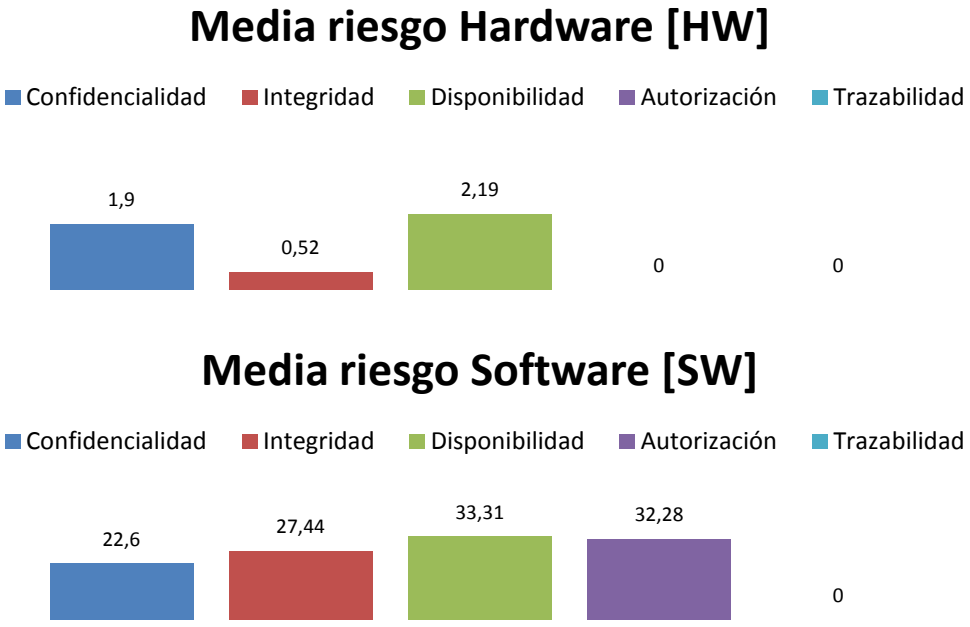
Figura 10 – Máximos valores de amenazas por activo y dimensión

De la figura anterior podemos sacar las siguientes **conclusiones**:

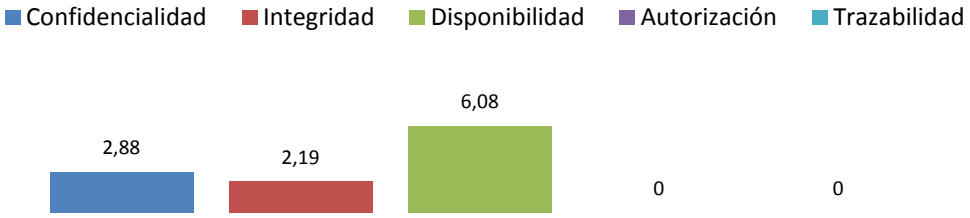
1. Respecto al tipo de activos, las amenazas están más presentes en el **SW, D y S**
2. La **disponibilidad**, en casi todos los activos se valora con un **100%**
3. La **trazabilidad** hace acto de presencia en los Servicios [S] y en ningún otro tipo de activo.

9.3. CONCLUSIONES SOBRE EL RIESGO ACEPTABLE Y RESIDUAL

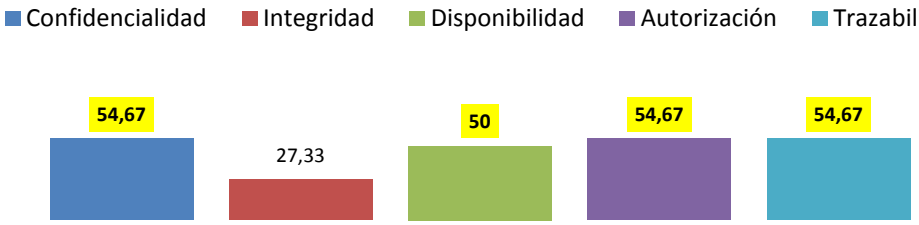
En la siguiente **figura 11** podemos ver la valoración **MEDIA** de los riesgos aceptados y residuales.



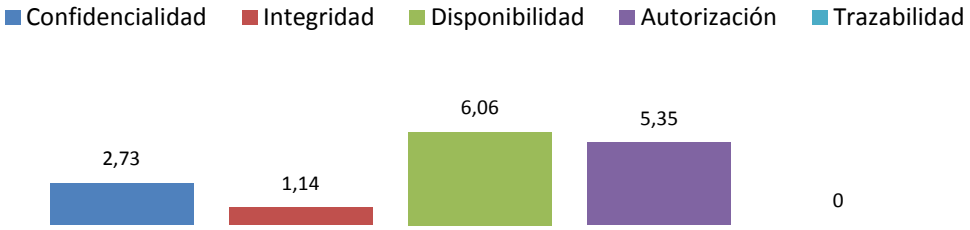
Media riesgo Instalaciones [L]



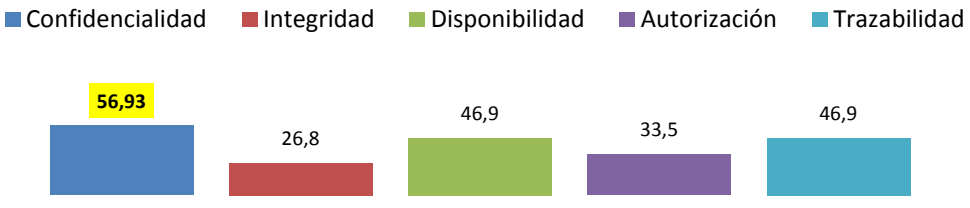
Media riesgo Datos [D]



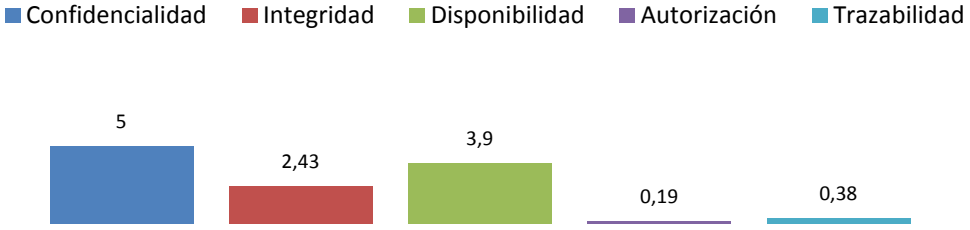
Media riesgo Comunicaciones [COM]



Media riesgo Servicios [S]



Media riesgo Soportes de Información [SI]



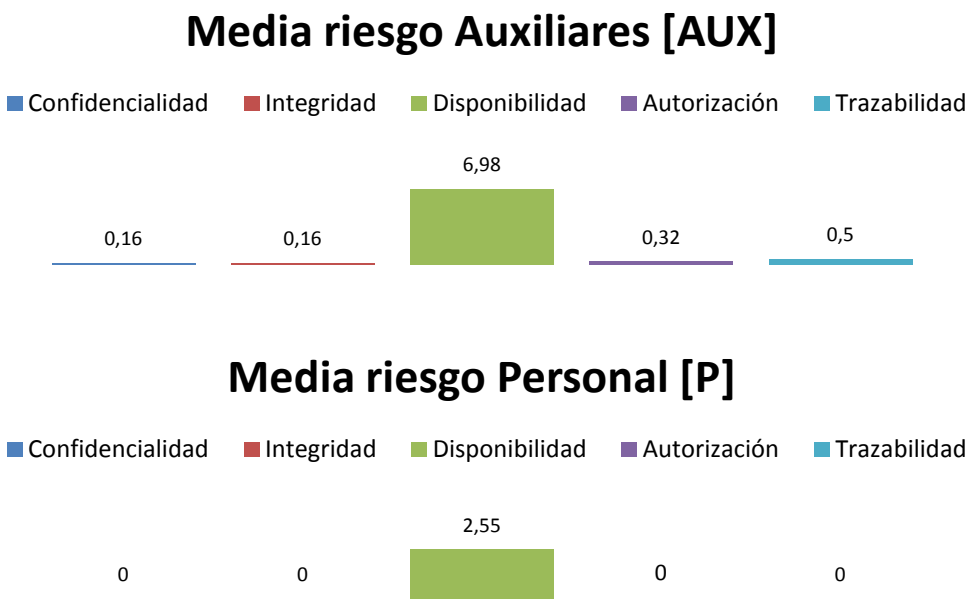


Figura 3 – Valor medio del riesgo aceptable y residual por activo y dimensión

De la anterior gráfica podemos **sacar diversas conclusiones**:

1. Los activos de tipo **SW** están por debajo del límite definido en su media, pero por valoraciones unitarias, hemos podido ver que algunos activos están por encima.
2. Los activos de tipo **D**, están en todas las dimensiones excepto la de Integridad, por encima del límite definido en su media. Es sin duda la agrupación de activos con mayor riesgo.
3. Los activos de tipo **S**, están por debajo del límite definido en su media (excepto para la dimensión de Confidencialidad que queda por encima).
4. El resto de activos (**HW, L, COM, SI, AUX y P**) están por debajo del límite definido, en la media de cada uno de éstos y en todas las valoraciones unitarias de los mismos.
5. Los activos de tipo **SW, D y S** son las agrupaciones de activos más expuestas al riesgo, donde algunos de sus activos correspondientes superan el nivel definido y por lo tanto la media de sus valoraciones suben respecto al resto.

A **modo resumen** citaremos los activos según tipo y ubicación que **superan el límite definido**:

1. **Para la agrupación de activos [SW]**
   a. [SW8]
   b. [SW9]
   c. [SW10]
   d. [SW17]
   e. [SW18]
   f. [SW19]
   g. [SW20]
   h. [SW21]
   i. [SW22]
   j. [SW23]

   Lo activos de tipo Software que superan el límite o quedan muy cerca del mismo, hacen referencia a las aplicaciones para los usuarios como el Sistema Operativo, el paquete Office o antivirus local entre otras. Estas aplicaciones de uso diario y para muchos usuarios están expuestas en mayor medida a vulnerabilidades por errores del uso de los mismos por parte de los usuarios entre otros factores. Cabe destacar que los sistemas de servidores están por debajo del límite definido.

k. [SW24]
l. [SW25]
m. [SW26]
n. [SW27]
o. [SW28]
p. [SW29]
q. [SW30]
r. [SW31]

2. **Para la agrupación de activos [D]**

a. [D1]
b. [D2]
c. [D3]
d. [D4]
e. [D7]
f. [D8]
g. [D9]
h. [D10]
i. [D13]
j. [D14]
k. [D15]
l. [D16]
m. [D10]
n. [D20]
o. [D21]
p. [D22]
q. [D25]
r. [D26]
s. [D27]
t. [D28]

Lo activos de tipo Datos, en concreto los generados por el ERP & CRM, los de carácter personal y los confidenciales quedan por encima del límite definido. Son activos críticos y por lo tanto se han de mitigar lo antes posible.

3. **Para la agrupación de activos [S]**

a. [S1]
b. [S2]
c. [S4]
d. [S5]
e. [S7]
f. [S8]
g. [S10]
h. [S11]
i. [S13]
j. [S14]

Lo activos de tipo Servicios, en concreto el de servicios internos implica muchos servicios que en su momento integramos en uno solo. Correo electrónico etcétera son ejemplos de este tipo de servicio. Son servicios de uso diario por la mayoría de usuarios de la empresa, y por lo tanto más condicionados a vulnerabilidades, tanto por errores de usuario como externas, por ello su riesgo supera el límite definido. El otro activo, la VPN se trata de manera similar al anterior.

Los esfuerzos en **mitigar el riesgo recaen en estos activos y dimensiones en concreto**. Se ha comentado en puntos anteriores la necesidad de prestar atención a otros activos con un riesgo cercano al límite, o alto (30 a 49). Siempre que sea posible, por tiempo y recursos será una buena práctica mejorar esos resultados aún estando aceptados sus respectivos riesgos.

FASE 4

1. INTRODUCCIÓN

En la anterior **FASE 3** se realizó el análisis de riesgos completo para **MASEGO S.A.** En este **FASE 4,** y conociendo los activos más vulnerables y con mayor riesgo dentro de la organización, se realizará un estudio y desarrollo de propuestas de proyectos, con el objetivo de mitigar dichos riesgos.

2. PROPUESTAS DE MEJORAS

Durante el análisis de riesgo desarrollado a lo largo de **la FASE 3**, se pudo ver los activos y agrupaciones de los mismos más críticos y por lo tanto susceptibles a una o muchas vulnerabilidades. En esta **FASE 4** se pretende mitigar los riesgos que están por encima del umbral tolerable definido y también de otros que aun estando por debajo de dicho umbral, se ha querido mejorar su gestión. Estos proyectos tendrán, a parte del propio contenido, **dos aspectos fundamentales**: la **temporalidad** (punto 4) y el **costo económico** (punto 5).

En el **ANEXO XII** podemos ver los **proyectos definidos en formato ficha**. Cada ficha tiene tamaño A4.

3. PLANIFICACION TEMPORAL PARA LA EJECUCIÓN DE LOS PROYECTOS

En la siguiente **tabla XXIII** se presenta la planificación temporal de los proyectos definidos en el anterior **punto 2 de la presente FASE 4.** Cada uno de los cuadrados dentro de las columnas correspondientes a los años equivale a un mes. El proyecto es bien sabido **comenzó en octubre del 2013**. Se pretende tener lista la **FASE CHECK** del primer **ciclo de Damming (PDCA)** a **finales del 2015**, incluyendo la **auditoría interna**.

PROYECTO	DURACIÓN	2013			2014											2015											
PRO-01	3 meses																										
PRO-02	1 mes																										
PRO-03	1 mes																										
PRO-04	1 mes																										
PRO-05	2 meses																										
PRO-06	2 meses																										
PRO-07	1 mes																										
PRO-08	1 mes																										
PRO-09	1 mes																										
PRO-10	2 meses																										
PRO-11	2 meses																										
PRO-12	3 meses																										
PR0-13	2 meses																										
PRO-14	2 meses																										
PRO-15	1 mes																										

Tabla XXIII – Planificación temporal de la ejecución de los proyectos

NOTA: *En ningún caso se solapan los proyectos dado que* ***todos han sido asignados a la misma persona*** *(Responsable de Seguridad que a su vez es el Responsable de las TIC).*

De la figura anterior vemos que cada casilla representa un mes del año en curso; el cuadrado amarillo representa el mes de **Octubre y Noviembre del 2013**, momento en el que se prepararon (en Octubre del 2013 en reunión del Comité de Seguridad) y aprobaron todos los proyectos (en Noviembre del 2013 por el Responsable de Seguridad) desde **PRO-01 a PRO-15** con presupuesto definido + **PRO_X** para ampliación de proyectos nuevos o modificación de los existentes con presupuesto igualmente definido (como veremos).

Una vez finalizada la **FASE CHECK** del primer ciclo del **PDCA**, restarán unos **6 meses** para solucionar todas las incidencias detectadas dentro del Sistema de Gestión de la Seguridad de la Información **(FASE ACT)** una vez finalizada la auditoría interna. **Al finalizar la auditoría interna se conocerán los resultados para el cumplimiento de la norma ISO 27001.**

En la siguiente **tabla XXIV** podemos ver la **planificación para la revisión de incidencias detectadas en la auditoría interna**, lo cual tendrá un doble servicio:

A. Solucionar proyectos existentes
B. Empezar nuevos proyectos necesarios

En este punto la organización podrá disponer de suficiente tiempo como para subsanar las no conformidades detectadas de cualquier grado, empezando por las más severas y así, preparar todo el SGSI para la auditoria reglamentaria la cual **se llevará a cabo el 1 de Septiembre del 2016.**

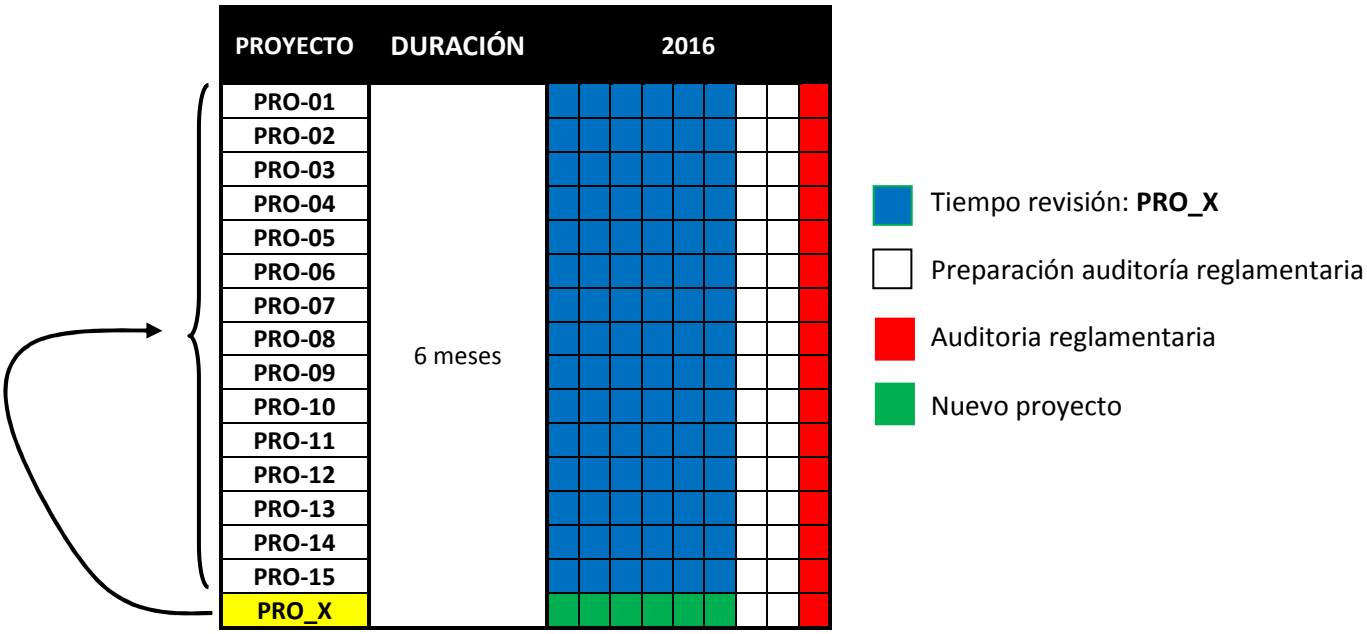


Tabla XXIV – Planificación temporal para revisión resultados auditoría interna

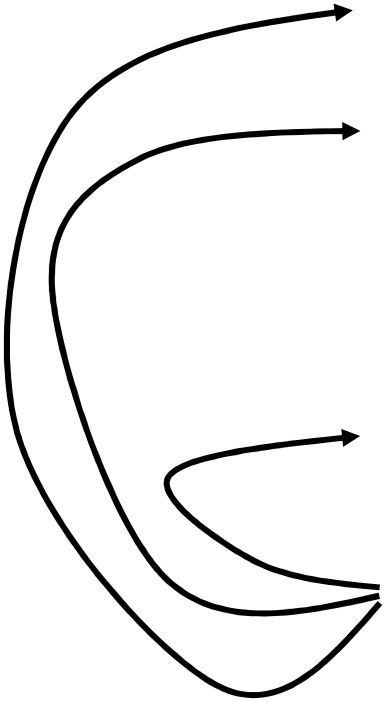
NOTA: *PRO_X representa un* ***nuevo proyecto, o modificación de uno existente****, que sea necesario para mitigar, solucionar cualquier no conformidad detectada o incluso mejorar un proyecto existente (todo ello en base a los 6 meses de margen definido)*

Algunos de los proyectos que según el tiempo que se tenga disponible según el calendario anterior, **referente a PRO_X** podrían ser los siguientes (de Enero a Septiembre del 2016):

1. Renovación HW Servidores
2. Renovación SW Servidores: virtualización
3. Renovación de material auxiliar para seguridad de acceso físico a sedes y almacenes mediante códigos de entrada en paneles
4. Renegociar contrato con ERP: solución de Backup en la nube (Cloud)
5. Negociar con proveedor de TIC soluciones de continuidad en servidores frente a desastres (sustitución de equipos en menos de 2 días)

4. PLANIFICACIÓN ECONÓMICA PARA LA EJECUCIÓN DE LOS PROYECTOS

En la **siguiente tabla XXV** podemos ver la planificación económica para la ejecución de los proyectos definidos en el **punto 2** de la presente **FASE 4.**



PROYECTO	COSTE	AÑO	COSTE / AÑO
PRO-01	42.000 €	**2013**	42.000€
PRO-02	12.000 €	**2014**	34.200 €
PRO-03	10.000 €		
PRO-04	2.000 €		
PRO-05	1.700 €		
PRO-06	2.000 €		
PRO-07	3.000 €		
PRO-08	1.000 €		
PRO-09	2.500 €		
PRO-10	3.300 €	**2015**	44.700 €
PRO-11	6.500 €		
PRO-12	25.500 €		
PRO-13	3.700 €		
PRO-14	2.200 €		
PRO-15	3.500 €		
PRO_X	100.000 €	**2016**	100.000 €
TOTAL PRESUPUESTADO 227.900 €			

Tabla XXV – Planificación económica de los proyectos

En total, todos los proyectos están presupuestados **en un total de 227.900 €.** De este importe total se reserva **un poco menos de la mitad** (100 mil euros) para proyectos nuevos o modificación como resultado de la necesidad de completar o mejorar los existentes o modificación y ampliación de los ya creados (del PRO-01 al PRO-15 ambos inclusive) a **ejecutar en el 2016**.

5. EVOLUCIÓN DEL RIESGO TRAS LA IMPLANTACIÓN DE LOS PROYECTOS

5.1. CÁLCULO DE LA EVOLUCIÓN DEL RIESGO

Veremos, para finalizar, cómo ha evolucionado el riesgo en la valoración de los activos respecto al análisis realizado en la anterior **FASE 3**, **gracias a la consecución de todos los proyectos definidos.** De los anteriores proyectos comentar que se han focalizado los esfuerzos en aquellos activos en los que superaban el riesgo aceptable (<50) pero también sobre otros activos que estaban cerca de ese límite o incluso activos sin riesgos como simple mejora.

5.2. EVOLUCIÓN DEL RIESGO ACEPTABLE Y RESIDUAL DE LA SEDE PRINCIPAL & CPD EN BARCELONA

Veamos la evolución del riesgo aceptable y residual para la sede principal **(tabla XXVI)**:

TIPO	ID_ACTIVO	% IMPACTO POTENCIAL					RIESGO				
		C	I	D	A	T	C	I	D	A	T
[HW]	[HW1]	0,9	0,45	1	0	0	0,8	0,4	0,9	0	0
	[HW2]	4	1	6	0	0	3	1	5	0	0
	[HW3]	3	0,4	3	0	0	2	0,35	2	0	0
	[HW4]	0,3	0,1	0,3	0	0	0,3	0,8	0,2	0	0
	[HW5]	0,9	0,35	0,7	0	0	0,7	0,3	0,6	0	0
	[HW6]	0,7	0,3	0,7	0	0	0,6	0,2	0,6	0	0
[SW]	[SW1]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW2]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW3]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW4]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW5]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW6]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW7]	0,9	0,9	1	0,9	0	0,7	0,7	0,8	0,7	0
	[SW8]	40	**50**	**60**	**50**	0	4	**5**	6	5	0
	[SW9]	40	**50**	**60**	**50**	0	4	**5**	6	5	0
	[SW10]	40	**50**	**60**	**50**	0	4	**5**	6	5	0
	[SW11]	0,4	0,5	0,6	0,5	0	0,35	0,4	0,5	0,45	0
[L]	[L1]	0,45	0,45	1	0	0	0,4	0,4	0,9	0	0
	[L2]	4,5	4	8	0	0	4,25	3,5	6	0	0
	[L3]	3	3	6	0	0	2	2,25	5	0	0
	[L4]	3	3	7	0	0	2	2,25	5	0	0
[D]	[D1]	**90**	45	**75**	**90**	**90**	9	4	7,5	9	9
	[D2]	**90**	45	**75**	**90**	**90**	9	4	7,5	9	9
	[D3]	**90**	45	**75**	**90**	**90**	9	4	7,5	9	9
	[D4]	**90**	45	**75**	**90**	**90**	9	4	7,5	9	9
	[D5]	0	0	0	0	0	0	0	0	0	0
	[D6]	0	0	0	0	0	0	0	0	0	0
[COM]	[COM1]	3,5	1,8	5	5	0	3	1,6	4	4	0
	[COM2]	3,5	1,8	5	5	0	3	1,6	4	4	0
	[COM3]	1,5	0,2	6	5	0	1	0,1	5	4	0
	[COM4]	3	1	7	5	0	2	1	6	4	0
[S]	[S1]	**70**	40	**70**	**50**	**70**	7	4	7	5	7
	[S2]	**70**	40	**70**	**50**	**70**	7	4	7	5	7
	[S3]	0,8	0,4	0,7	0,5	0,7	0,6	0,3	0,6	0,4	0,6
[SI]	[SI1]	8	4	8	0	0	7	3	6	0	0
	[SI2]	3	1	1	0	0	2	0,8	0,8	0	0

	[SI3]	8	4	5	0	0	7	3	4	0	0
	[SI4]	8	4	8	0	0	7	3	7	0	0
	[SI5]	0,4	0,4	0,8	0	0	0,3	0,3	0,7	0	0
[AUX]	[AUX1]	4,5	4,5	10	0	0	4	4	9	0	0
	[AUX2]	0	0	10	0	0	0	0	9	0	0
	[AUX3]	0	0	10	0	0	0	0	9	0	0
	[AUX4]	0	0	10	0	0	0	0	9	0	0
	[AUX5]	0	0	0,01	0	0	0	0	0	0	0
	[AUX6]	0	0	10	0	0	0	0	9	0	0
	[AUX7]	0	0	10	0	0	0	0	9	0	0
[P]	[P1]	0	0	0,05	0	0	0	0	0,03	0	0
	[P2]	0	0	0,04	0	0	0	0	0,03	0	0
	[P3]	0	0	0,03	0	0	0	0	0,02	0	0
	[P4]	0	0	0,03	0	0	0	0	0,02	0	0
	[P5]	0	0	0,02	0	0	0	0	0,01	0	0
	[P6]	0	0	0,02	0	0	0	0	0,01	0	0
	[P7]	0	0	10	0	0	0	0	8	0	0

Tabla XXVI – Evolución del riesgo aceptable y residual en la Sede Barcelona

5.3. EVOLUCIÓN DEL RIESGO ACEPTABLE Y RESIDUAL EN LA SUBSEDE DE MADRID

Veamos la evolución del riesgo aceptable y residual para la sede de Madrid **(tabla XXVII)**:

TIPO	ID_ACTIVO	% IMPACTO POTENCIAL					RIESGO				
		C	I	D	A	T	C	I	D	A	T
[HW]	[HW7]	0,8	0,4	1	0	0	0,6	0,3	0,9	0	0
	[HW8]	3	0,8	5	0	0	2	0,6	4	0	0
	[HW9]	2	0,4	2	0	0	1	0,3	1	0	0
	[HW10]	0,2	0,1	0,2	0	0	0,1	0,07	0,1	0	0
	[HW11]	0,9	0,35	0,7	0	0	0,7	0,3	0,5	0	0
	[HW12]	0,6	0,3	0,7	0	0	0,4	0,2	0,5	0	0
[SW]	[SW12]	0,8	0,8	1	0,8	0	0,6	0,6	0,7	0,6	0
	[SW13]	0,8	0,8	1	0,8	0	0,6	0,6	0,7	0,6	0
	[SW14]	0,8	0,8	1	0,8	0	0,6	0,6	0,7	0,6	0
	[SW15]	0,8	0,8	1	0,8	0	0,6	0,6	0,7	0,6	0
	[SW16]	0,8	0,8	1	0,8	0	0,6	0,6	0,7	0,6	0
	[SW17]	30	40	**50**	**50**	0	3	4	5	5	0
	[SW18]	30	40	**50**	**50**	0	3	4	5	5	0
	[SW19]	30	40	**50**	**50**	0	3	4	5	5	0
[L]	[L5]	4,5	4	8	0	0	4,2	3,8	7	0	0
	[L6]	3	0	6	0	0	2,8	0	5,5	0	0
	[L7]	3	3	7	0	0	2,8	2,9	6,7	0	0
[D]	[D7]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D8]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D9]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D10]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D11]	0	0	0	0	0	0	0	0	0	0
	[D12]	0	0	0	0	0	0	0	0	0	0
[COM]	[COM5]	3,5	1,8	5	5	0	3	1,4	4	4	0
	[COM6]	3,5	1,8	5	5	0	3	1,4	4	4	0
	[COM7]	1,5	0,2	6	5	0	1	0,1	5	4	0
	[COM8]	3	1	7	5	0	2,2	0,8	6	4	0
[S]	[S4]	**70**	40	**70**	**50**	**70**	7	4	7	5	7
	[S5]	**70**	40	**70**	**50**	**70**	7	4	7	5	7

	[S6]	0,8	0,4	0,7	0,5	0,7	0,6	0,2	0,5	0,4	0,5
[SI]	[SI6]	8	4	8	0	0	7,6	3,6	7,7	0	0
	[SI7]	3	1	1	0	0	2,6	0,8	0,7	0	0
	[SI8]	8	4	5	0	0	7,6	3,8	3	0	0
	[SI9]	8	4	8	0	0	7,6	3,8	7	0	0
	[SI10]	0,4	0,4	0,8	0	0	0,2	0,2	0,4	0	0
[AUX]	[AUX8]	0	0	10	0	0	0	0	9	0	0
	[AUX9]	0	0	10	0	0	0	0	9	0	0
	[AUX10]	0	0	10	0	0	0	0	9	0	0
	[AUX11]	0	0	0,01	0	0	0	0	0	0	0
	[AUX12]	0	0	10	0	0	0	0	9	0	0
	[AUX13]	0	0	10	0	0	0	0	9	0	0
[P]	[P8]	0	0	0,03	0	0	0	0	0,02	0	0
	[P9]	0	0	0,03	0	0	0	0	0,02	0	0
	[P10]	0	0	0,02	0	0	0	0	0,01	0	0
	[P11]	0	0	10	0	0	0	0	8	0	0

Tabla XXVII – Evolución del riesgo aceptable y residual en la Sede de Madrid

5.4. EVOLUCIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA EL ALMACÉN DE BADALONA

Veamos la evolución del riesgo aceptable y residual para el almacén de Badalona (**tabla XXVIII)**:

TIPO	ID_ACTIVO	% IMPACTO POTENCIAL					RIESGO				
		C	I	D	A	T	C	I	D	A	T
[HW]	[HW13]	3	0,8	5	0	0	2	0,78	4,7	0	0
	[HW14]	2	0,4	2	0	0	1	0,38	1,8	0	0
	[HW15]	0,2	0,1	0,2	0	0	0,1	0,08	0,1	0	0
	[HW16]	0,9	0,35	0,7	0	0	0,7	0,25	0,5	0	0
	[HW17]	0,6	0,3	0,7	0	0	0,5	0,2	0,5	0	0
[SW]	[SW20]	30	40	50	50	0	3	4	5	5	0
	[SW21]	30	40	50	50	0	3	4	5	5	0
	[SW22]	30	40	50	50	0	3	4	5	5	0
	[SW23]	70	70	80	80	0	7	7	8	8	0
[L]	[L8]	3,5	3	6	0	0	3,1	2	5	0	0
	[L9]	2	0	4	0	0	1	0	3	0	0
	[L10]	2,5	2,5	8	0	0	2,1	2,2	7	0	0
[D]	[D13]	80	40	75	80	80	8	4	7,5	8	8
	[D14]	80	40	75	80	80	8	4	7,5	8	8
	[D15]	80	40	75	80	80	8	4	7,5	8	8
	[D16]	80	40	75	80	80	8	4	7,5	8	8
	[D17]	0	0	0	0	0	0	0	0	0	0
	[D18]	0	0	0	0	0	0	0	0	0	0
[COM]	[COM9]	2	1	5	5	0	1,9	0,8	4	4	0
	[COM10]	3,5	1,8	7	7	0	3,1	1,6	6	6	0
	[COM11]	1,5	0,2	6	5	0	1,2	0,1	5	4	0
	[COM12]	3	1	7	5	0	2,9	0,9	6	4	0
[S]	[S7]	70	40	70	50	70	7	4	7	5	7
	[S8]	70	40	70	50	70	7	4	7	5	7
	[S9]	0,8	0,4	0,7	0,5	0,7	0,3	0,1	0,5	0,2	0,2
[SI]	[SI11]	8	4	8	0	0	7,9	3,8	7,7	0	0
	[SI12]	3	1	1	0	0	2,9	1	0,8	0	0
	[SI13]	8	4	5	0	0	7,8	3,8	4,6	0	0
	[SI14]	0,4	0,4	0,8	0	0	0,3	0,15	0,7	3,7	7
[AUX]	[AUX14]	0	0	10	0	0	0	0	2	0,9	1

	[AUX15]	0	0	10	0	0	0	0	7	3	4
	[AUX16]	0	0	10	0	0	0	0	3	3	7
	[AUX17]	0	0	0,07	0	0	0	0	0,05	0	0
	[AUX18]	0	0	0,1	0	0	0	0	0,09	0	0
	[AUX19]	0	0	10	0	0	0	0	9	0	0
	[AUX20]	0	0	10	0	0	0	0	9	0	0
[P]	[P12]	0	0	0,02	0	0	0	0	0,01	0	0
	[P13]	0	0	10	0	0	0	0	9	0	0

Tabla XXVIII – Evolución del riesgo aceptable y residual para el Almacén de Badalona

5.5. EVOLUCIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA EL ALMACÉN DE MADRID

Veamos la evolución del riesgo aceptable y residual para el almacén de Madrid (**tabla XXIX**):

TIPO	ID_ACTIVO	% IMPACTO POTENCIAL					RIESGO				
		C	I	D	A	T	C	I	D	A	T
[HW]	[HW18]	3	0,8	5	0	0	2	0,78	4,7	0	0
	[HW19]	2	0,4	2	0	0	1	0,38	1,8	0	0
	[HW20]	0,2	0,1	0,2	0	0	0,1	0,08	0,1	0	0
	[HW21]	0,9	0,35	0,7	0	0	0,7	0,25	0,5	0	0
	[HW22]	0,6	0,3	0,7	0	0	0,5	0,2	0,5	0	0
[SW]	[SW24]	30	40	**50**	**50**	0	3	4	5	5	0
	[SW25]	30	40	**50**	**50**	0	3	4	5	5	0
	[SW26]	30	40	**50**	**50**	0	3	4	5	5	0
	[SW27]	**70**	**70**	**80**	**80**	0	7	7	8	8	0
[L]	[L11]	3,5	3	6	0	0	3,1	2	5	0	0
	[L12]	2	0	4	0	0	1	0	3	0	0
	[L13]	2,5	2,5	8	0	0	2,1	2,2	7	0	0
[D]	[D19]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D20]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D21]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D22]	**80**	40	**75**	**80**	**80**	8	4	7,5	8	8
	[D23]	0	0	0	0	0	0	0	0	0	0
	[D24]	0	0	0	0	0	0	0	0	0	0
[COM]	[COM13]	2	1	5	5	0	1,9	0,8	4	4	0
	[COM14]	3,5	1,8	7	7	0	3,1	1,6	6	6	0
	[COM15]	1,5	0,2	6	5	0	1,2	0,1	5	4	0
	[COM16]	3	1	7	5	0	2,9	0,9	6	4	0
[S]	[S10]	**70**	40	**70**	**50**	**70**	7	4	7	5	7
	[S11]	**70**	40	**70**	**50**	**70**	7	4	7	5	7
	[S12]	0,8	0,4	0,7	0,5	0,7	0,3	0,1	0,5	0,2	0,2
[SI]	[SI15]	8	4	8	0	0	7,9	3,8	7,7	0	0
	[SI16]	3	1	1	0	0	2,9	1	0,8	0	0
	[SI17]	8	4	5	0	0	7,8	3,8	4,6	0	0
	[SI18]	0,4	0,4	0,8	4	8	0,3	0,15	0,7	3,7	7
[AUX]	[AUX21]	0	0	3	1	1	0	0	2	0,9	1
	[AUX22]	0	0	8	4	5	0	0	7	3	4
	[AUX23]	0	0	4	4	8	0	0	3	3	7
	[AUX24]	0	0	0,07	0	0	0	0	0,05	0	0
	[AUX25]	0	0	0,1	0	0	0	0	0,09	0	0
	[AUX26]	0	0	10	0	0	0	0	9	0	0
	[AUX27]	0	0	10	0	0	0	0	9	0	0
[P]	[P14]	0	0	0,02	0	0	0	0	0,01	0	0
	[P15]	0	0	10	0	0	0	0	9	0	0

Tabla XXIX – Evolución del riesgo aceptable y residual para el Almacén Madrid

5.6. EVOLUCIÓN DEL RIESGO ACEPTABLE Y RESIDUAL PARA COMERCIALES

Veamos la evolución del riesgo aceptable y residual para los Comerciales **(tabla XXX)**:

TIPO	ID_ACTIVO	% IMPACTO POTENCIAL					RIESGO				
		C	I	D	A	T	C	I	D	A	T
[HW]	[HW23]	8	2,4	7	0	0	7	2,2	6	0	0
	[HW24]	7	1,2	7	0	0	6	1,1	6	0	0
[SW]	[SW28]	30	40	50	50	0	3	4	5	5	0
	[SW29]	30	40	50	50	0	3	4	5	5	0
	[SW30]	30	40	50	50	0	3	4	5	5	0
	[SW31]	70	70	80	80	0	7	7	8	8	0
[D]	[D25]	80	40	75	80	80	8	4	7,5	8	8
	[D26]	80	40	75	80	80	8	4	7,5	8	8
	[D27]	80	40	75	80	80	8	4	7,5	8	8
	[D28]	80	40	75	80	80	8	4	7,5	8	8
	[D29]	0	0	0	0	0	0	0	0	0	0
	[D30]	0	0	0	0	0	0	0	0	0	0
[COM]	[COM17]	3,5	1,8	7	7	0	3,3	1,6	6	6	0
[S]	[S13]	70	40	70	50	70	7	4	7	5	7
	[S14]	70	40	70	50	70	7	4	7	5	7
	[S15]	0,8	0,4	0,7	0,5	0,7	0,6	0,4	0,7	0,4	0,6
[SI]	[SI19]	3	1	1	0	0	2	0,8	0,9	0	0
	[SI20]	8	4	5	0	0	7	3	4	0	0
	[SI21]	0,4	0,4	0,8	0	0	0,2	0,3	0,6	0	0
[AUX]	[AUX28]	0	0	0,07	0	0	0	0	0,05	0	0
[P]	[P16]	0	0	0,5	0	0	0	0	0,45	0	0

Tabla XXX – Evolución del riesgo aceptable y residual para los Comerciales

6. EVOLUCIÓN DEL CUMPLIMIENTO DE LA NORMA ISO 27002:2005

Tal y como se ha comentado en puntos anteriores, se ha contemplado una ejecución de proyectos que influyera de la siguiente manera y en este orden:

1. Mitigar los riesgos identificados en la anterior **FASE 3** con un riesgo superior o igual a 50 (valor definido) así como aquellos riesgos cercanos a ese valor. De ese análisis de riesgos, el **SW, los DATOS y los SERVICIOS** han sido el objetivo primordial en el desarrollo de esta **FASE 4.**

2. **Mejorar**, dentro del **presupuesto y temporalidad de 3 años** definida por la organización como plazo y recursos objetivos antes de realizar el proceso de certificación bajo la norma ISO 27001, se ha querido evolucionar todos los puntos de la norma (del 5 al 15 ambos inclusive), definiendo y ejecutando proyectos para todos los dominios, consiguiendo así una mejora en todo los puntos de la norma.

La siguiente **tabla XXXI** muestra los proyectos definidos para evolucionar cada uno de los puntos, dominios de la norma ISO 27002:

DOMINIO NORMA ISO 27002:2005	CONTROLES	PROYECTO
1. Política de Seguridad	5.1	PRO-04
2. Aspectos organizativos de la SI	6.1, 6.2	PRO-09
3. Gestión de activos	7.1, 7.2	PRO-05, PRO-08
4. Seguridad ligada a los RRHH	8.1, 8.2, 8.3	PRO-02, PRO-03
5. Seguridad física y del entorno	9.2	PRO-14
6. Gestión de comunicaciones y operaciones	10.1, 10.3, 10.4, 10.5, 10.6, 10.8, 10.10	PRO-12, PRO-13, PRO-15
7. Control de acceso	11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7	PRO-10
8. Adquisición, desarrollo y mantenimiento de los SI	12.1, 12.2, 12.3, 12.5, 12.6	PRO-11
9. Gestión de incidentes de SI	13.1, 13.2	PRO-06
10. Gestión de la continuidad del negocio	14.1	PRO-01
11. Cumplimiento	15.1, 15.2, 15.3	PRO-07

Tabla XXXI – Evolución en el cumplimiento de la norma ISO 27002:2005

La anterior **tabla XXXI** queda abierta a cambios durante los **6 primeros meses del 2016**, tiempo que se ha fijado para posibles cambios en proyectos ya definidos o inclusión de nuevos como requisito o mejora de los existentes. De hecho **se espera** que todos aquellos controles, los cuales no han sido implementados, durante esos **6 primeros meses del 2016** sean **creados, tratados y ejecutados** para la consecución de una evolución total de toda la norma ISO 27001, **al 100% en todos los dominios de la ISO 27002.**

7. GRÁFICO DE LA EVOLUCIÓN CUMPLIMIENTO DE LA ISO 27002:05

Todos los proyectos definidos y comentados anteriormente tienen una finalidad clara: **mejorar todo el sistema de gestión de la seguridad de la información, mitigando riesgos no aceptables o simplemente mejorando lo existente.**

En modo **cronología** veremos a continuación la **evolución** desde el inicio del plan director de la seguridad de la información. **En primer lugar**, rescatamos y vemos en la **figura 12**, el grado de efectividad visto en la **FASE 1** del presente plan director de seguridad.

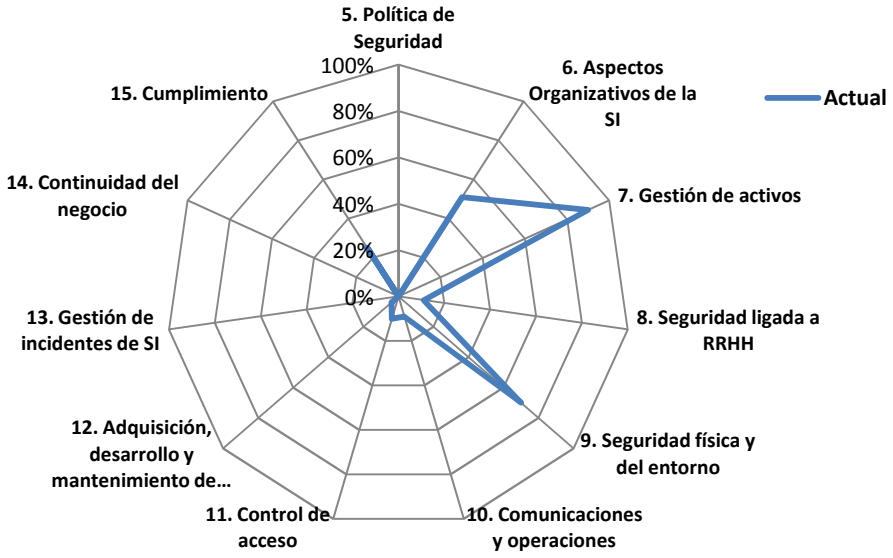


Figura 12 – Resultados GAP de la **FASE 1** ISO 27002

En segundo lugar, vemos en la **figura 13,** el resultado esperado tras la ejecución de los proyectos definidos para lo que queda de **año 2013, comparado a la valoración actual**:

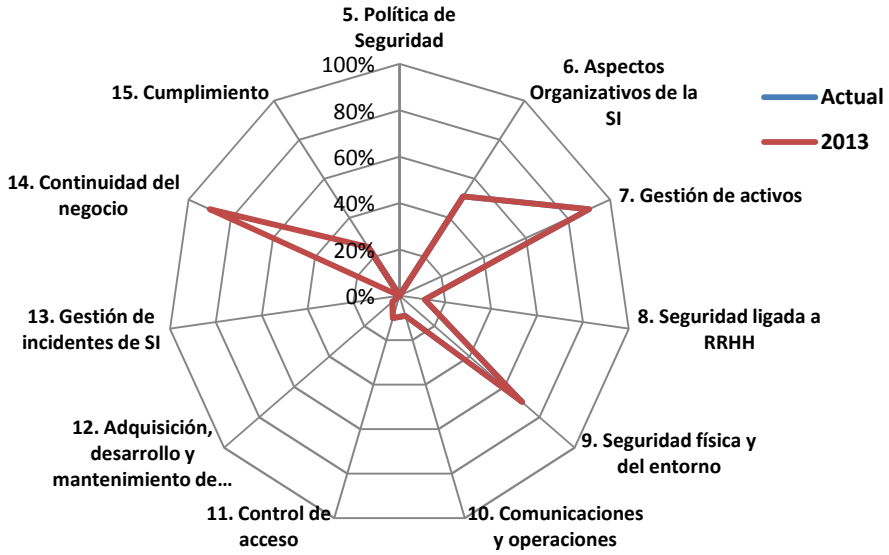


Figura 13 – Resultados GAP ISO 27002 para el 2013

El cambio no es significativo, dado que en el corto espacio de tiempo para la ejecución en este 2013, solo se ha podido empezar un solo proyecto (de todas formas en el gráfico se contempla como si se hubiera finalizado el proyecto).

En tercer lugar, vemos en la **figura 14,** el resultado esperado tras la ejecución de los proyectos definidos para el **año 2014, comparado a la valoración actual y la del 2013**:

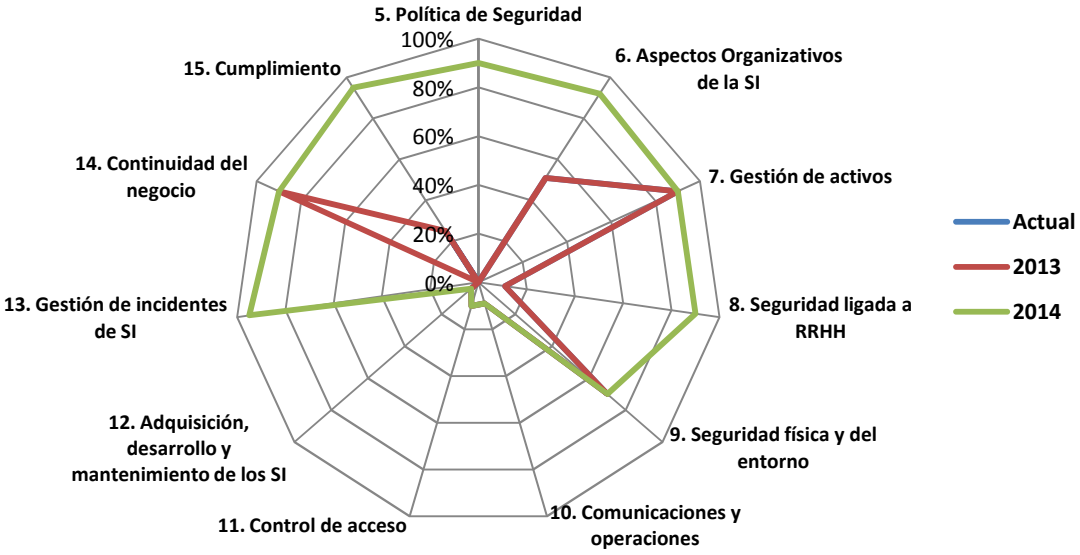


Figura 14 – Resultados GAP ISO 27002 para el 2014

En cuarto lugar, vemos en la **figura 15,** el resultado esperado tras la ejecución de los proyectos definidos para el **año 2015, comparado a la valoración actual, la del 2013 y 2014**:

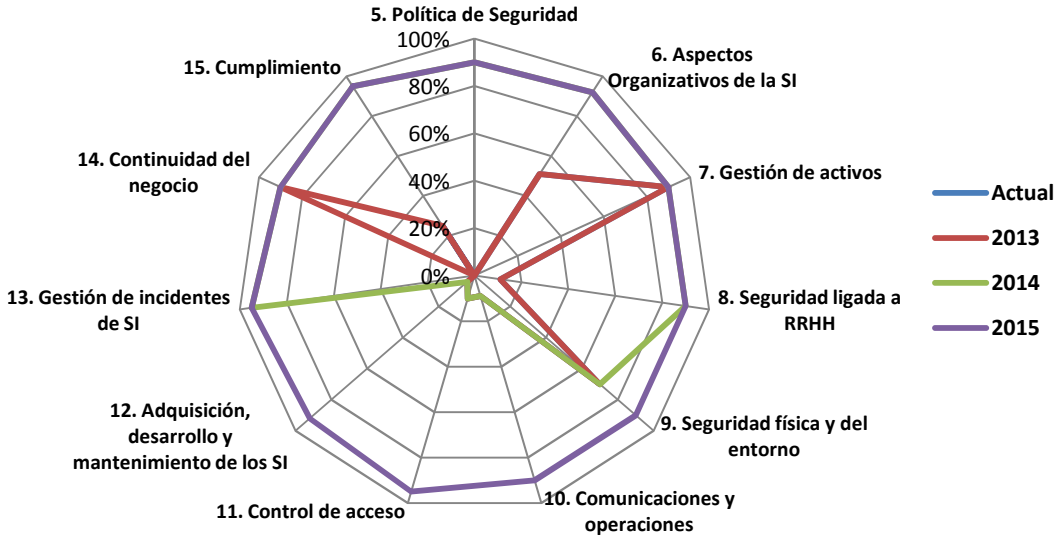


Figura 15 – Resultados GAP ISO 27002 para el 2015

Durante el 2015 se ejecutan los proyectos que cubrirán las necesidades de los controles restantes que aun no han sido tratados (controles del dominio 9, 10, 11 y 12 respectivamente). En esta figura 15 se ha podido ver una evolución hacia el cumplimiento de la norma. Todos los dominios de la norma ISO 27002 quedan **por encima o igual al 90%** del cumplimiento.

Finalmente, en quinto lugar, vemos en la **figura 16,** el resultado esperado tras la ejecución de los proyectos a determinar **PRO_X** para la definición de nuevos proyectos y/o de mejora de los proyectos existentes para el **año 2016, comparado a la valoración actual, la del 2013, 2014 y 2015**:

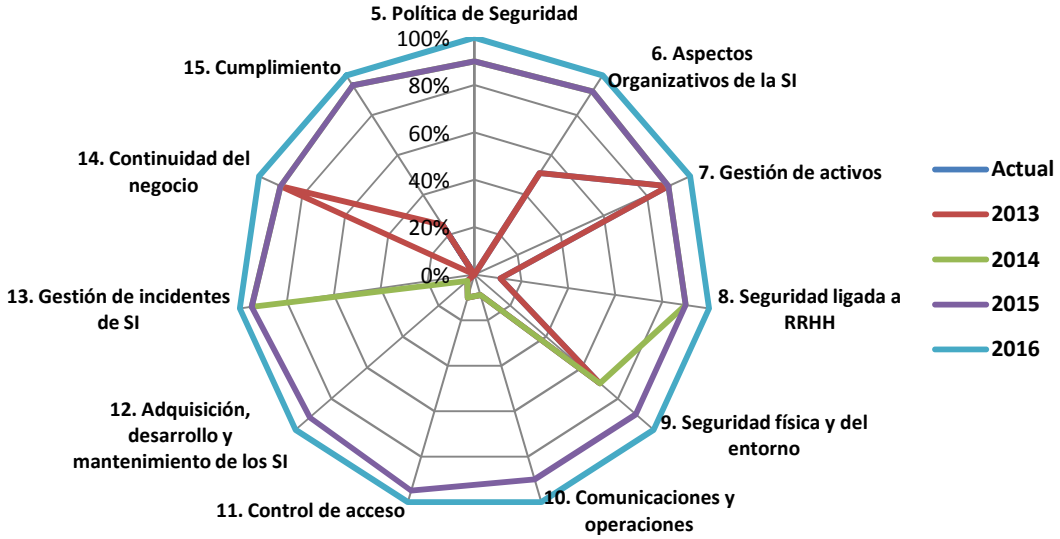


Figura 16 – Resultados esperados para la evolución ISO 27002 en el 2016

Se espera que en el 2016 el cumplimiento y evolución de la norma ISO 27002 sea completa, al 100% en sus dominios y controles (del 5 al 15 ambos inclusive)

Finalmente la siguiente **tabla XXXII** muestra los resultados desde antes hasta después de la ejecución de los proyectos:

	ACTUAL	2013	2014	2015	2016
5. Política de Seguridad	0%	0%	**90%**	90%	**100%**
6. Aspectos Organizativos de la SI	51%	51%	**92%**	92%	**100%**
7. Gestión de activos	90%	90%	**90%**	90%	**100%**
8. Seguridad ligada a RRHH	11%	11%	**90%**	90%	**100%**
9. Seguridad física y del entorno	70%	70%	70%	**90%**	**100%**
10. Comunicaciones y operaciones	9%	9%	9%	**90%**	**100%**
11. Control de acceso	10%	10%	10%	**95%**	**100%**
12. Adquisición, desarrollo y mantenimiento de los SI	4%	4%	4%	**92%**	**100%**
13. Gestión de incidentes de SI	0%	0%	**95%**	95%	**100%**
14. Continuidad del negocio	0%	**90%**	90%	90%	**100%**
15. Cumplimiento	25%	25%	**95%**	95%	**100%**

Tabla XXXII – Resumen final de la evolución para el cumplimiento de la norma ISO 27002

NOTA: *Se han resaltado (fondo amarillo) aquellos dominios que han **mostrado una mejora** respecto al estado inicial o año anterior al tratado (según que año estemos tratando).*

8. CONCLUSIONES

Como se ha podido ver en los puntos anteriores y en especial en el **punto 2** de la presente **FASE 4,** con esta definición de proyectos en concreto, se ha querido cubrir todos los puntos y dominios de la norma **ISO 27002** con el fin de mejorar la totalidad del **Sistema de Gestión de la Seguridad de la Información,** con especial atención a los riesgos que no eran aceptables, detectados en la anterior **FASE 3,** en la gestión del riesgo (SW, DATOS, SERVICIOS).

De esta manera, **se ha asegurado**, tal y como se ha podido apreciar, la mitigación del riesgo actual e incluso una mejora en puntos que antes de la realización de los diferentes proyectos, ya estaban dentro del riesgo aceptable.

Cabe destacar en la **planificación temporal el espacio de tiempo dedicado al proyecto PRO_X** (6 meses; de Enero a Septiembre del 2016). Este proyecto, aunque ya se haya comentado en varias ocasiones, es vital para por una parte, modificar proyectos existentes (con el fin de solucionar cualquier problemática surgida en éstos en el momento de su ejecución), creación de nuevos proyectos dependientes de los ya creados (para mejorar sus resultados si cabe) y para la creación de nuevos proyectos independientes (con el único fin de mejorar todo el sistema).

La implicación de todo el personal será clave, vital y esencial para la consecución de todos los proyectos. Sin este compromiso por parte de todos, el esfuerzo y dedicación que se ha invertido no habrá servido de nada.

FASE 5

1. INTRODUCCIÓN

En esta **FASE 5** se tratará de realizar una auditoría interna para evaluar el nivel de cumplimiento de **MASEGO S.A.** según la norma ISO 27002:2005 en todos sus dominios y controles establecidos y documentados en ésta.

Cabe destacar y dejar bien claro que esta auditoría **se ejecuta después de la consecución de todos los proyectos definidos en la anterior FASE 4,** y no antes.

Recordemos que la **auditoría interna** se fijo para **Enero del 2016**, y que **la de certificación** realizada por una entidad certificada se realizará en **Septiembre del 2016**.

Desde finales de **Enero del 2016**, al finalizar la auditoría interna de cumplimiento, se ha establecido un período de **6 meses para ejecutar el proyecto que se denominó PRO_X** en la anterior FASE 4, el cual recordemos, cubriría las necesidades de mitigar las **No Conformidades detectadas en esta FASE 5** y en caso de tener tiempo disponible y recursos, mejorar todo el Sistema de Gestión de la Seguridad de la Información.

2. AUDITORÍA DE CUMPLIMIENTO DE LA NORMA ISO 27002:2005

2.1. METODOLOGÍA PARA LA AUDITORÍA DE CUMPLIMIENTO

El **objetivo principal** de la presente auditoría de cumplimiento es dar una valoración del nivel de madurez respecto a la **norma ISO 27002:2005**, y detectar las no conformidades menores, o graves para la posterior gestión de éstas con el único fin de subsanarlas y conseguir un nivel de implantación adecuado, o incluso mejorarlo. Para ello sabemos que esta norma se compone de 133 controles creados para el desarrollo de las buenas prácticas necesarias para una correcta gestión de la seguridad de la información. Estos **133 controles se agrupan en 11 dominios y 39 objetivos de control.**

Las especificaciones del proceso de **auditoría interna** para un SGSI está descrito en el **Apartado 6 de la norma ISO27001**. La organización debe realizar auditorías internas del SGSI a intervalo planificados para determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI:

- **A.** Cumplen los requisitos de esta norma internacional y la legislación y reglamentación correspondientes
- **B.** Cumplen a los requisitos de seguridad de la información identificados
- **C.** Se implementen y se mantienen de forma efectiva
- **D.** Dan el resultado esperado

Se debe **planificar un programa de auditoría** teniendo en cuenta el estado e importancia de los procesos y las áreas que serán auditados, así como los resultados de las auditorías previas (que no es el caso, dado que estamos frente a la primera que MASEGO S.A. realizará).

Los **criterios, el alcance, la frecuencia y los métodos de auditoría deben ser definidos**. La **selección de auditores** y la dirección de las auditorías deben garantizar la **objetividad e imparcialidad** del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las **responsabilidades y los requisitos** para planificar y realizar las auditorías, y para informar de los resultados y mantener los registros deben estar definidos en un **procedimiento documentado.**

La **dirección responsable del área auditada debe velar que se realicen**, sin retrasos injustificados, acciones para **eliminar las disconformidades detectadas**. Las actividades de seguimiento deben incluir la **verificación de las acciones tomadas y el informe de los resultados de verificación.**

La organización deberá interpretar la norma, y elaborar sus **propios métodos y criterios de auditoría**, así como producir y acometer un **plan de auditoría**.

La organización tiene bastante libertad para elegir los controles a auditar y la forma de auditarlo, mientras asegure la objetividad, calidad y imparcialidad del proceso.

Los **objetivos concretos para la auditoria de cumplimiento** (ISO27006 9.2.3.2 Stage 2 audit) son los siguientes:

- Confirmar que la organización cumple con sus políticas, objetivos y procedimientos
- Confirmar que el SGSI cumple con los requisitos documentados. responsables y usuarios
- Comprobar la eficacia de los controles de seguridad

El contenido de la **auditoria de cumplimiento** implica la realización de **2 actividades**.

1. Realización del Plan de auditoría:
    - **a.** Entrevistar los responsables y usuarios del SGSI
    - **b.** Revisar los controles técnicos en las áreas de bajo-medio-alto riesgo
    - **c.** Inspeccionar visualmente las oficinas y especialmente el CPD
2. Preparación de los informes de las no conformidades

2.2. PLANIFICACIÓN DE LA AUDITORÍA Y PROCESOS POSTERIORES

Antes de la ejecución de la auditoría de cumplimiento, se han llevado a cabo procesos de mejora mediante los **proyectos definidos en la FASE 4.** Es el momento de verificar el correcto funcionamiento y madurez del Sistema de Gestión de la Seguridad de la Información.

El resultado de la presente auditoría de cumplimiento generará un informe de conclusiones (informe de auditoría) del análisis para el posterior tratamiento.

La siguiente **tabla XXXIII representa el detalle de la Tabla III definida en la anterior FASE 4**.

PROYECTO	DURACIÓN	2016
AUDITORÍA CUMPLIMIENTO	1 mes	
PRO-01	5 meses	
PRO-02		
PRO-03		
PRO-04		
PRO-05		
PRO-06		
PRO-07		
PRO-08		
PRO-09		
PRO-10		
PRO-11		
PRO-12		
PRO-13		
PRO-14		
PRO-15		
PRO_X		
PREPARACION AUDITORIA	2 meses	
AUDITORIA REGLAMENTARIA	1 mes	

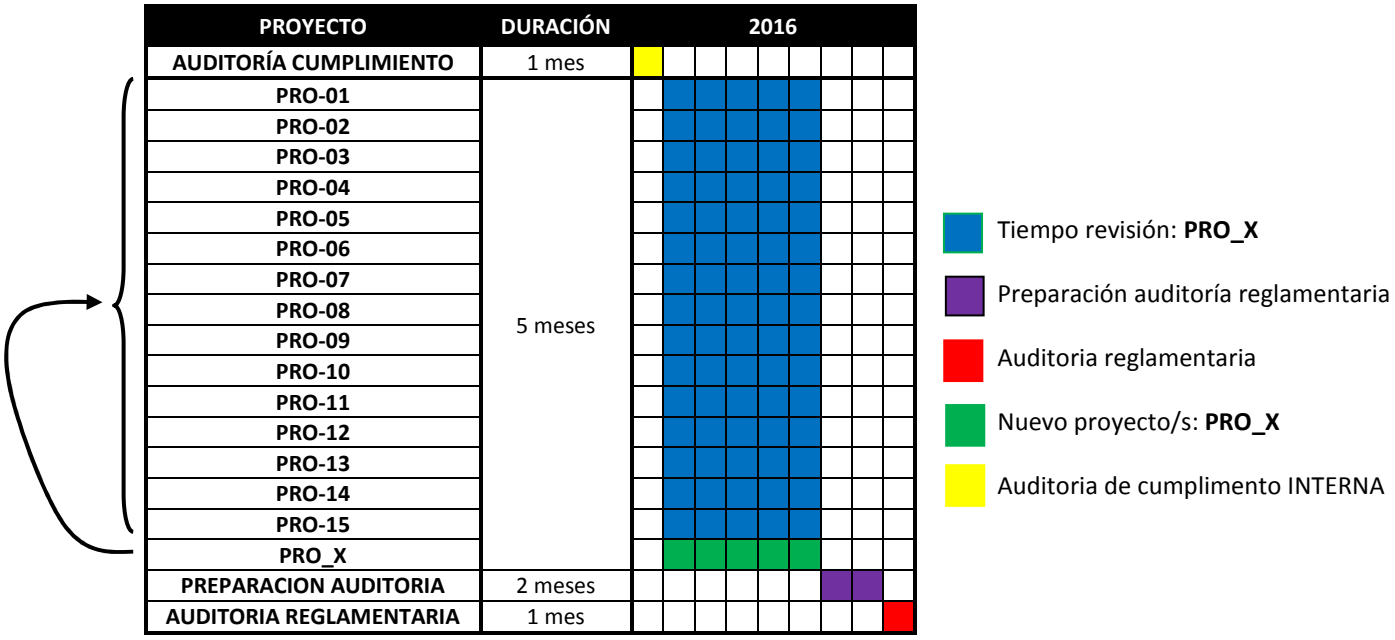


Tabla XXXIII – Planificación auditoría de cumplimiento y pasos posteriores

Esta planificación ya establecida en el **anterior FASE 4**, asegura poder tratar con suficiente tiempo y antelación, así como los recursos económicos necesarios, todas las no conformidades detectadas en la presente auditoría de cumplimiento. Tras ejecutar todos los proyectos vistos en la anterior **FASE 4**, se producirá la **auditoría de cumplimiento (presente FASE 5)**, detectando todas las incidencias posibles dentro del **SGSI** según la norma **ISO 27002:2005**.

Esta auditoría se llevará a cabo en **Enero del 2016**. Al finalizar el proceso de auditoría, a partir del **1 de Febrero del 2016** se procederá a tratar todas las **no conformidades** registradas, y **creación de los proyectos** que sean necesarios para su tratamiento y mitigación (modificación / mejora de los proyectos definidos en la FASE 4 del presente plan director de seguridad).

Éstos se ejecutarán **desde Febrero a Junio del 2016**, en base a esta temporalidad y el **presupuesto definido** (100.000 €). Una vez completado el proceso de **mitigación de las no conformidades** detectadas, se especifica un tiempo de **2 meses** (Julio y Agosto del 2016) para preparar todo el SGSI para la **auditoría reglamentaria** para certificar **MASEGO S.A.** bajo la norma ISO 27001.

Esta preparación culmina con la **ejecución por parte de una entidad certificada de la auditoría reglamentaria, en Septiembre del 2016.**

3. EVALUACIÓN DE LA MADUREZ

La presente valoración de madurez se basa en el **modelo de Capacidad y Madurez o CMM** (Capability Maturity Model) de igual forma que se hizo en la FASE 1 del presente Plan Director de Seguridad.

Con este modelo, podremos **averiguar el nivel de implantación actual en esta FASE 5**. Recordemos esta configuración definida anteriormente en la **Tabla II** (Valoración del nivel de implantación) de la FASE 1.

Para dar por bueno un SGSI, éste debe alcanzar en todos y cada uno de los 11 dominios de la norma ISO 27002:2005 un nivel de madurez L3 ó del 90%, y en algunos casos, según la importancia del control analizado, dentro de cada uno de esos 11 dominios, un nivel L4 ó del 95%. Niveles inferiores no son aceptables para poder certificar la organización.

L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia

Para poder apreciar los cambios, mejoras conseguidas durante el desarrollo del plan director de seguridad se quiere **realizar una comparativa entre los valores obtenidos a lo largo de la FASE 1 y los obtenidos en la presente FASE** 5.

Este proceso es **bastante significativo e importante** dentro del global del proyecto. Si el desarrollo de todas las fases que se han estado llevando a cabo a lo largo de todo este tiempo por la organización **ha sido el correcto**, los resultados obtenidos nos mostrarán esta mejora.

Si por el contrario no obtenemos resultados obtenidos podremos asegurar todo lo contrario, y desde luego asumir pérdidas tanto económicas como temporales destinadas a la creación del SGSI.

En el próximo **punto 4 de la presente FASE 5,** podremos ver para todos los dominios y controles de la norma, su valoración antes y después de aplicar los proyectos para la mejora y cumplimiento de la norma, así como en el resumen de sus resultados.

4. RESULTADOS DE LA AUDITORÍA DE CUMPLIMIENTO

En este punto podemos ver los **resultados obtenidos según los dominios de la norma**. Para poder analizar mejor los resultados de la presente **FASE 5,** y por lo tanto, la evolución desde el principio del plan director de seguridad que se está tratando, **se ha incluido la columna VALOR FASE 1,** para poder ver dicha evolución.

Recordemos que el valor de la columna **VALOR FASE 5** es el valor una vez los proyectos definidos en la anterior **FASE 4** se han ejecutado de manera correcta y efectiva. De las tablas que veremos en el ANEXO XIII (Tabla I a la XI) veremos en el dominio un color para el valor calculado en la **FASE 1** y otro color para la valoración de la presente **FASE 5** que se basa en la distribución vista en el punto anterior. De esta forma, la valoración que veamos será:

- Color rojo – Valoración **L0** (del 0% a 9%)
- Color naranja – Valoración **L1** (del 10% al 49%)
- Color amarillo – Valoración **L2** (del 50% al 89%)
- Color verde – Valoración **L3** (del 90% al 94%)
- Color azul – Valoración **L4** (del 95% al 99%)
- Color gris – Valoración **L5** (100%)
- Color blanco – Valoración **L6** (no aplica)

4.1. ANÁLISIS DE CUMPLIMIENTO SEGÚN DOMINIO DE LA NORMA 27002:2005

En el **ANEXO XIII** podemos ver el resultado de las **valoraciones según dominio de la norma**.

4.2. RESUMEN DE LOS RESULTADOS DEL ANÁLISIS DE MADUREZ POR DOMINIO

A modo resumen, podemos ver en la siguiente **tabla XXXIV** las valoraciones obtenidas en la presente **FASE 5** y las anteriores de la **FASE 1**:

DOMINIO DE LA NORMA ISO 27002:05	VALORACIÓN CMM	
	FASE 1	FASE 5
5. Política de Seguridad	0%	90%
6. Aspectos organizativos de la SI	51,25%	93,12%
7. Gestión de activos	90%	95%
8. Seguridad ligada a los RRHH	16,66%	95%
9. Seguridad física y del entorno	70,83%	93,33%
10.Gestión de comunicaciones y operaciones	9,11%	75,64%
11.Adquisición, desarrollo y mantenimiento de los SI	10%	95%
12.Control de acceso	3,2%	91,6%
13.Gestión de incidentes de SI	0%	95%
14.Gestión de la continuidad del negocio	0%	95%
15.Cumplimiento	25%	95%

L0	0%
L1	10%
L2	50%
L3	90%
L4	95%
L5	100%
L6	N/A

Valores CMM

Tabla XXXIV – Resumen de la valoración madurez dominio de la norma 27002

4.3. RESULTADOS DE LA MADUREZ SEGÚN EL MODELO CMM

A continuación podemos ver en la **figura 17** el porcentaje de nivel de madurez para los 133 controles de la norma. Se puede apreciar el nivel de cumplimiento obtenido, donde EL 70% de todos los controles están situados en un nivel de L4, es decir, con una madurez del 95%. Por el contrario cabe destacar que EL 5% de todos los controles están situados en un nivel de L1, es decir, con una madurez del 10%, y por lo tanto lejos del nivel de madurez deseado y mínimo para poder certificar la empresa.

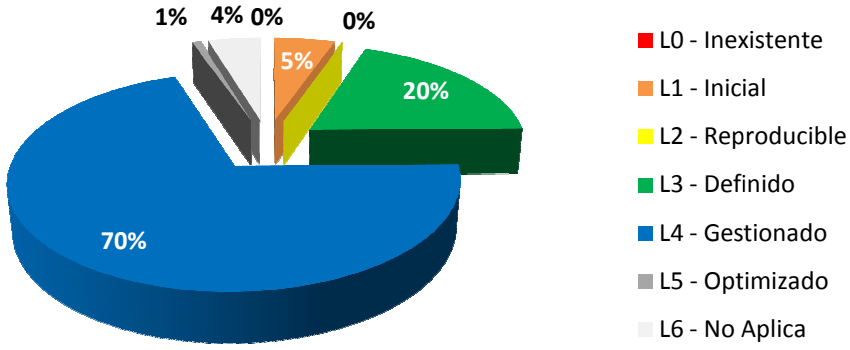


Figura 17 – Porcentaje del nivel de madurez para los 133 controles

La siguiente **figura 18** muestra la comparativa entre el nivel de madurez en la FASE 5 respecto a la inicial definida en la FASE 2. Como se podrá observar, la mejora es evidente. No obstante, como ya se ha comentado, el 10º dominio de la norma es el punto débil dado que este queda por debajo del nivel tolerable para poder **certificar MASEGO S.A. bajo la norma ISO 27001**. Por ello será necesario mejorar esta valoración y llegar un nivel igual o superior a L3 según el modelo CMM (90%). Existen recursos suficientes (tiempo y presupuesto económico) para ello, y por lo tanto no será problema, y también se llegará al nivel **OBJETIVO**, es decir, el 100%.

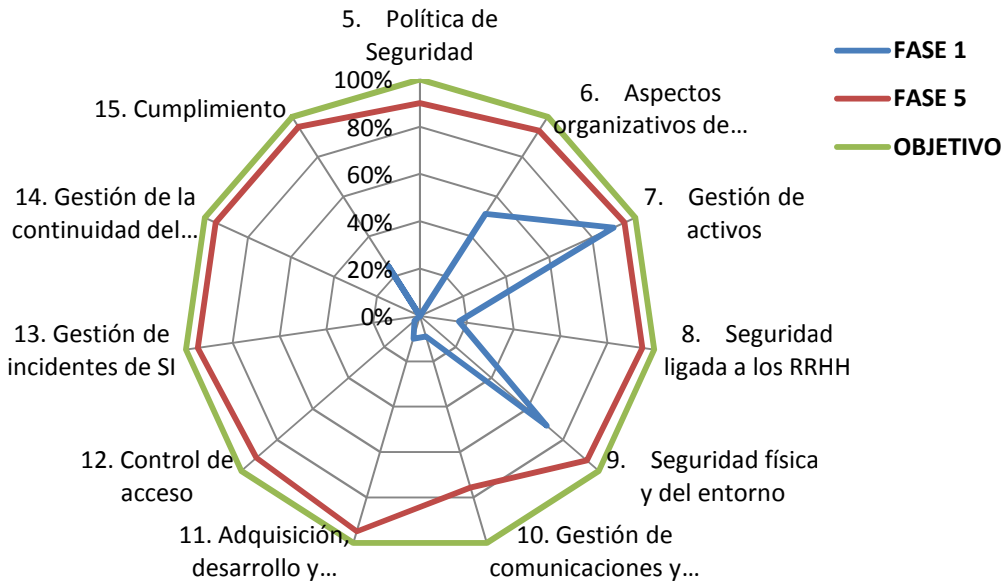


Figura 18 – Nivel de madurez de la FASE 5 vs FASE 1 & Objetivo

4.4. CONCLUSIONES DEL ANÁLISIS DE MADUREZ

En resumen, el análisis realizado nos indica que existe uno de los dominios valorado por debajo de lo necesario (el mínimo necesario sería un **90% - L3**), que corresponde al 10º dominio de la norma. Para éste, no se crearon proyectos para su mejora en algunos de sus puntos **(en concreto en los puntos 10.2 y 10.7)** y por ello no se ha conseguido una valoración mínima en su madurez.

Será necesario por lo tanto, **en primer lugar** crear un **nuevo proyecto a Fecha 1 de Febrero del 2016 para mitigar este problema y alcanzar un nivel de madurez en todo el 10º dominio de un 90% (L3) como mínimo.** Dado el espacio de tiempo antes de la auditoria reglamentaria, se asume que **no habrá problema para subsanar esta incidencia**.

A continuación, analizando los dominios 5, 6, 9 y 12, han sido puntuados con una madurez de **tipo L3**. Se asume que con los recursos y tiempo que reste después de solucionar el problema anterior (dominio 10), se intentará mejorar estas valoraciones, para que como mínimo se llegue a una valoración del 95% - L4.

Finalmente, el resto de dominios con **valoración L4** son más que correctos. No obstante y en caso de que queden recursos y tiempo una vez subsanados los problemas en el 10º dominio y mejorado los dominios 5, 6, 9 y 12, el resto de dominios (7, 8, 11, 13, 14 y 15) se intentarán mejorar para conseguir una valoración de nivel L5 o 100% de madurez tal y como se ha marcado como objetivo la organización.

5. INFORME DE AUDITORIA

5.1. INTRODUCCION

La siguiente **tabla XXXV**, representa la primera página del informe. Contiene información vital de la empresa a auditar, el alcance como marco del SGSI así como sus límites, los emplazamientos a los que afecta, el tipo de auditoría y las normas y legislación que serán de aplicación.

EMPRESA Y RAZÓN SOCIAL	**MASEGO S.A.**
FECHA DE LA AUDITORÍA	Del 7 de Enero al 29 de Enero del 2016
LUGAR DE LA AUDITORÍA	1. Sede Central & CPD Barcelona 2. Subsede Madrid 3. Almacén de Badalona 4. Almacén de Madrid 5. Comerciales
ALCANCE DE LA CERTIFICACIÓN	El mismo que el del Plan Director
TIPO DE AUDITORÍA	Inicial e interna de cumplimiento
NORMAS Y REFERENCIAS LEGALES APLICABLES EN EL PROCESO DE AUDITORÍA	ISO 27001 ISO 27002 ISO 27006

Tabla XXXV – Datos iniciales del informe de auditoría

La anterior **tabla XXXVI**, representa la primera hoja en **tamaño A4** del informe de auditoría (después de la portada e índice). La **planificación de la presente auditoria para MASEGO S.A**. la podemos ver en la siguiente **figura 19**:

Figura 19 – Planificación de la auditoría de cumplimiento

A continuación veremos las **fichas de no conformidad** resultantes del proceso de auditoría.

5.2. FICHAS DE NO CONFORMIDAD

Podemos ver en el **ANEXO XIV** todas las **fichas de no conformidad generadas** a lo largo del proceso de auditoría de cumplimiento.

5.3. RESUMEN DE RESULTADOS DE LA AUDITORÍA DE CUMPLIMIENTO

La siguiente **tabla XXXVI**, muestra el resumen de los resultados de la auditoría de forma esquemática:

DOMINIO DE LA NORMA ISO 27002:05	NO CONFORMIDADES	
	MENOR	MAYOR
5. Política de Seguridad	**1**	-
6. Aspectos organizativos de la SI	-	-
7. Gestión de activos	-	**1**
8. Seguridad ligada a los RRHH	-	-
9. Seguridad física y del entorno	-	**1**
10.Gestión de comunicaciones y operaciones	**10**	-
11.Control de acceso	-	-
12.Adquisición, desarrollo y mantenimiento de los SI	-	-
13.Gestión de incidentes de SI	-	-
14.Gestión de la continuidad del negocio	-	**1**
15.Cumplimiento	-	-
TOTAL NO CONFORMIDADES	**11**	**3**

Tabla XXXVI – Resultados NC por dominio ISO 27002

En La siguiente **figura 20** podemos ver de manera gráfica el **tipo de no conformidades detectadas** según dominio de la norma ISO 27002:2005:

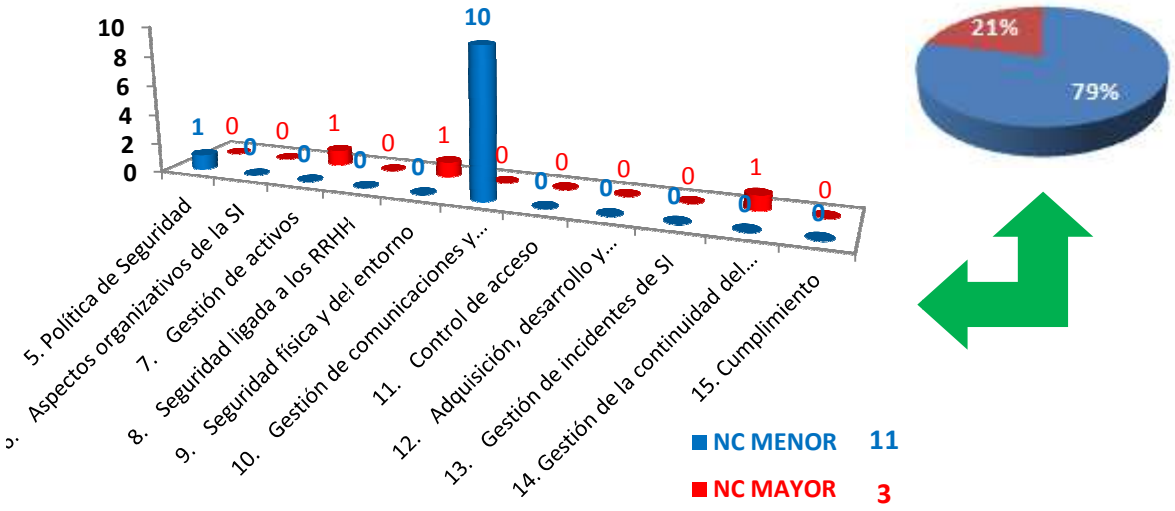


Figura 20 – Resumen gráfico NC según tipo y dominio

6. CONCLUSIONES

La primera conclusión es que el Sistema de Gestión de Seguridad de la Información ha sido implantado con un alto grado de éxito a excepción del cumplimiento del 10º dominio. Esto se debe a que **en la FASE 4 no se definieron proyectos específicos para los controles 10.2 y 10.7, lo cual en el global del 10º dominio hace que no se llegue a una madurez del 90% o L3 según el modelo CMM.** Por ello, estos dos controles **acaparan un 75%** del total de no conformidades detectadas (aunque sean de tipo menor). **Este escenario era previsible**, pero gracias a los **5 meses** que quedan para la auditoría de certificación, **la situación se resolverá**, en principio sin problema, creando los proyectos necesarios para este fin.

Cabe destacar las **3 no conformidades mayores para los dominios 7, 9 y 14.** Estas NC serán fácilmente mitigadas y se deben principalmente a descoordinación y olvidos. Se crearán los proyectos necesarios para paliar esta situación en el tiempo estimado para este fin (5 meses antes de la auditoría de renovación), como en el caso anterior.

El **resto de dominios están sobradamente establecidos** y en principio no será necesario realizar ninguna actuación. Sólo se mejorarán en caso que quede tiempo y recursos para ello, una vez hayan sido cerradas las No Conformidades (primero las mayores y luego las menores).

Recordemos, que ya en las **FASE 4 se destinaron recursos (tiempo y presupuesto monetario) para solucionar todas las NC detectadas en esta FASE 5.** Recordar como ya se ha dicho que **MASEGO S.A. dispone de 5 meses** para mitigar dichas NC y mejorar en segundo lugar el resto de dominios de la norma. **Y 100.000 €** para implantar y desarrollar los proyectos que sean necesarios. Por lo tanto, **se puede ser optimista y asegurar el nivel de cumplimiento objetivo definido en la anterior FASE 4, que era del 100% en todos sus dominios.**

CONCLUSIONES

1. Se ha conseguido obtener una **visión clara y objetiva del estado de la empresa en lo referente a la seguridad de la información**, punto clave para el inicio del plan director de seguridad y englobado en la **FASE 1** del mismo.

2. Se ha obtenido un **esquema documental eficiente, gestionado y bien desarrollado** a lo largo de la **FASE 2**. En esta línea, MASEGO S.A. ha adaptado la documentación existente proveniente de iniciativas propias y muy focalizadas a este esquema documental.

3. **Se ha conseguido pleno conocimiento de los riesgos y amenazas** presentes para la organización, vistos en la **FASE 3**.

4. **Se ha mitigado el riesgo no aceptable mediante los proyectos necesarios** definidos en la **FASE 4**.

5. Se ha comprobado **el nivel de cumplimiento mediante auditoría interna** en la última **FASE 5**, obteniendo resultados muy positivos para la gran mayoría de los dominios analizados y con tiempo y recursos económicos para mejorar cualquier incidencia o simplemente mejorar, si cabe.

6. Se ha alcanzado un **alto nivel de compromiso de la dirección**, tanto a nivel de implicación en el proyecto como a nivel de proporcionar los recursos necesarios para la implantación de los proyectos.

7. Se ha conseguido un **alto grado de concienciación por parte del personal** de MASEGO S.A, en lo referente a la seguridad de la información.

8. El **SGSI ha quedado integrado** dentro de MASEGO S.A. respetando las máximas de **Disponibilidad, Confidencialidad e Integridad de la información que se gestiona.**

9. MASEGO S.A. **está preparada para certificarse bajo la norma ISO 27001:2005** con plenas garantías de éxito en el mes de Septiembre del 2016.

BIBLIOGRAFÍA

- **Material curso AENOR S0-A –** Auditor Sistemas de Gestión de la seguridad de la Información

- **Material curso AENOR S0-B –** Especialista implantador de Sistemas de Gestión de la Seguridad de la Información

- **Material asignatura UOC – MISTIC** "Sistemas de Gestión de la Seguridad de la Información"

- **WIKIPEDIA:**
  - **SGSI:** http://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Seguridad_de_la_Informaci%C3%B3n
  - **Modelo CMM:** http://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez
  - **MAGERIT:** http://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa)

- **INTECO:** http://www.inteco.es/

- **PORTAL DE ISO 27001 (EN CASTELLANO):** http://www.iso27000.es/sgsi.html

- **ISACA:** http://www.isaca.org/

- **MAGERIT:** https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

- **NORMATIVAS ISO FAMILIA 27000:**
  1. ISO/IEC 27000:2012 – proporciona una introducción y visión de conjunto de toda la familia ISO 27000 y facilita un glosario común.
  2. ISO/IEC 27001:2005 recopilación de los requisitos para la implantación de un SGSI, y es certificable.
  3. ISO/IEC 27002:2005 código de buenas prácticas para la gestión de la seguridad de la información, y recopilación de un amplio catálogo de controles y buenas prácticas en la materia. Es el conjunto de controles que toman como referencia la norma ISO 27001 a la hora de seleccionar controles de seguridad.
  4. ISO/IEC 27003:2010 ofrece una guía para implementar un SGSI según la norma ISO 27001**.**
  5. ISO/IEC 27004:2009 guiará y sugerirá mecanismos para mesurar la eficiencia de un SGSI.
  6. ISO/IEC 27005:2011 facilita una guía para la gestión de los riesgos de seguridad de la información, y proporciona un marco para hacer un análisis de riesgos.
  7. ISO/IEC 27006:2011 recopilación de los requisitos de las entidades de certificación acreditadas para certificar SGSI según la norma ISO 27001.
  8. ISO/IEC 27007:2011 es una guía para auditar SGSI**.**
  9. ISO/IEC TR 27008:2011 guía para auditar los controles del SGSI**.**
  10. ISO/IEC 27010:2012 ofrece las guías per a la gestión de la seguridad en les comunicaciones entre diferentes sectores, con especial énfasis en infraestructuras criticas o sistemas industriales.

11. ISO/IEC 27011:2008 ofrece las directrices para la gestión de la seguridad y la información en el sector de les telecomunicaciones.
12. ISO/IEC 27013:2012 proporciona orientación sobre la aplicación integrada / articulaciones de las normes ISO / IEC 27001 (SGSI) i la ISO / IEC 20000-1
13. ISO/IEC 27014 pronto cubrirá la gobernabilidad de la seguridad informática
14. ISO/IEC TR 27015 proporciona directrices para la gestión de la información de seguridad para los servicios financieros
15. ISO/IEC TR 27016 cubrirá los aspectos económicos de la gestión de la seguridad de la información
16. ISO/IEC 27017 cubrirá los aspectos sobre la seguridad de la información de la computación en la nube
17. ISO/IEC 27018 cubrirá aspectos de privacidad de la computación en la nube.
18. ISO/IEC TR 27019 cubrirá la seguridad de la información para el control de procesos en la industria de la energía
19. ISO/IEC 27031:2011 es un estándar en les TIC centrado en la continuidad del negocio
20. ISO/IEC 27032:2012 cubre aspectos de la ciberseguridad
21. ISO/IEC 27033 substituye la norma ISO 18028 en seguridad de redes IT
22. ISO/IEC 27034 está proporcionando directrices para la seguridad de aplicaciones
23. ISO/IEC 27035:2011 reemplazará un informe técnico ya existente con modificaciones menores y relacionadas con la gestión de incidentes de seguridad
24. ISO/IEC 27036 será una guía de seguridad para las relaciones con proveedores, incluyendo la computación en la nube
25. ISO/IEC 27037:2012 alcanza la identificación, recolección y preservación de evidencias digitales
26. ISO/IEC 27038 guía sobre las especificaciones de la redacción digital
27. ISO/IEC 27039 guía sobre la detección de intrusiones y sistemas de prevención
28. ISO/IEC 27040 guía sobre la seguridad en el almacenaje de datos
29. ISO/IEC 27041 guía sobre la garantía de los métodos de investigación de evidencias digitales
30. ISO/IEC 27042 guía sobre el análisis y interpretación de evidencias digitales
31. ISO/IEC 27043 guía sobre los principios y procesos en la investigación de evidencias digitales
32. ISO/IEC 27044 guía sobre la gestión de sucesos y de la seguridad de la información
33. ISO 27799:2008 ofrece orientación en el sector salud para implementación específica de un SGSI basado en la norma ISO / IEC 27002.

ANEXO I – OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

1. INTRODUCCION Y PUNTO DE PARTIDA

La necesidad de la creación de un plan director, por parte de la empresa, **nace a raíz de**:

- la alternativa a un crecimiento al cual no se puede optar, y por ello, se opta por la **diferenciación y obtención de un valor añadido** superior al que, los pocos competidores que existen no puedan competir.
- al mismo tiempo se atiende a la **petición al responsable del departamento informático,** el cual contemplaba todo el plan, como una ordenación y seguro de vida no solo de los sistemas informáticos sino de la seguridad de la información en todos los ámbitos.

El **motivo** de la elaboración del Plan Director es el de **definir un plan de acciones con el fin de cumplir con los objetivos que se establecerán en el SGSI.** El **ámbito** del plan director **abarca la totalidad de la empresa**, con lo que las medidas que se establezcan se orientarán a aspectos funcionales, técnicos y organizativos.

2. OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

Los **objetivos** deseados desde la Dirección de **MASEGO S.A.** son los siguientes:

1. Preservar la confidencialidad, integridad i disponibilidad de la información.
2. Establecer la seguridad de la información como un proceso más en la empresa; igual que se ha hecho anteriormente con el sistema de gestión de Calidad.
3. Convertir la seguridad de la información en una de las prioridades en el día a día de los sistemas e información en general.
4. Proteger de forma adecuada la información para asegurar la continuidad del negocio,
5. Minimizar los posibles daños a la organización y maximizar el ROI (Return of Investement) y las oportunidades del negocio.
6. Garantizar el compromiso de la dirección con la seguridad de la información.
7. Crear y desarrollar los controles (técnicos, jurídicos y de gestión) necesarios para garantizar el cumplimiento de los niveles de riesgo aprobados por la Organización.
8. Cumplir en todo momento la legislación vigente en materia de protección de datos, así como cualquier otra que afecte a la seguridad de los activos de la Organización.
9. Implantar una “cultura de seguridad” compartida por todo el personal de la Organización.
10. Tratar la seguridad de la información como un proceso de mejora continua con el fin optimizar los controles de seguridad.
11. Por último, certificar la empresa en la ISO 27001:2005.

3. ALCANCE DEL PLAN DIRECTOR DE SEGURIDAD

El alcance de todo el proyecto abarca a todas y cada una de las instalaciones de la empresa, sin tener en cuenta la disponibilidad geográfica de todos esos centros. Es decir, **el proyecto afectará a todos y a toda la información que está o se mueve dentro de la organización**. Más en detalle podemos definir el alcance de la siguiente manera:

Asegurar, en todos los centros de los que se compone la empresa, los servicios y procesos de gestión de la información, tanto internos (personal de la empresa) como externos (clientes, proveedores y terceras partes), gestionados a través de las Tecnologías de la Información y de todos los soportes tanto físicos (papel y emplazamientos) como lógicos (servidores, ordenadores, etc.).

4. BENEFICIOS DEL PLAN DIRECTOR DE SEGURIDAD

Los **beneficios que reportará el plan director de seguridad a la empresa serán grandes**. Veamos algunos ejemplos:

1. Facilita la planificación.
2. Facilita el conocimiento de las líneas de actuación que se han de llevar en materia de seguridad.
3. Facilita conocer el estado actual de la empresa.
4. Facilita una definición clara del alcance.
5. Facilita un conocimiento exhaustivo de las medidas de seguridad a implantar.
6. Asegura una gestión de la información más eficiente.
7. Asegura un correcto funcionamiento del sistema de control de seguridad.
8. Asegura una minimización de pérdidas de la información.
9. Aumenta el prestigio y reputación de la empresa.

5. TÉCNICAS PARA RECOLECCION DE DATOS

Uno de tantos puntos críticos, es tener un conocimiento lo más real y exacto de la empresa. Para ello, existen **varios métodos**:

A. **Selección de interlocutores** → principalmente los elegidos serán el personal con medio o alto grado de responsabilidades y en todo caso, con alto grado de experiencia en sus respectivos campos, de todos y cada uno de los departamentos y centros que entran dentro del alcance del proyecto. Según el tamaño de estos centros y departamentos, se escogerán 1 o más de 1 persona.
B. **Entrevistas personales** → Del paso anterior, a cada uno de los elegidos, siempre que sea posible, se realizarán entrevistas personales para conocer todos los riesgos de cada uno de los departamentos.
C. **Cuestionarios** → De menor impacto, y sabiendo que los resultados pueden no ser del todo objetivos, tiene el mismo objetivo que el anterior, conocer todos los riesgos de cada uno de los departamentos.

D. **Revisión de la documentación actual** → Tener al alcance toda la información que se pueda de la empresa. Con ello, se conseguirá un alto grado de conocimiento sobre la organización con el fin de facilitar todo el proceso posterior.

6. NORMATIVAS APLICABLES AL PLAN DIRECTOR DE SEGURIDAD

Los planes directores de seguridad de la información se basan en la familia de la norma ISO 27000, en especial en su norma auditable **ISO 27001 y su Anexo A**, desarrollado en la 27002. Además, se usará **MARGERIT** como herramienta para la gestión del riesgo (que veremos en fases posteriores).

En primer lugar, el sistema de gestión de la seguridad de la información que se está confeccionando se base en procedimiento cíclico repetitivo en el tiempo conocido como **PDCA** (Plan – Do – Check – Act → Planificar – Hacer – Comprobar – Actuar) que **consta de 4 etapas** bien definidas y diferenciadas. Gráficamente, la siguiente **figura 1** nos muestra esta idea:

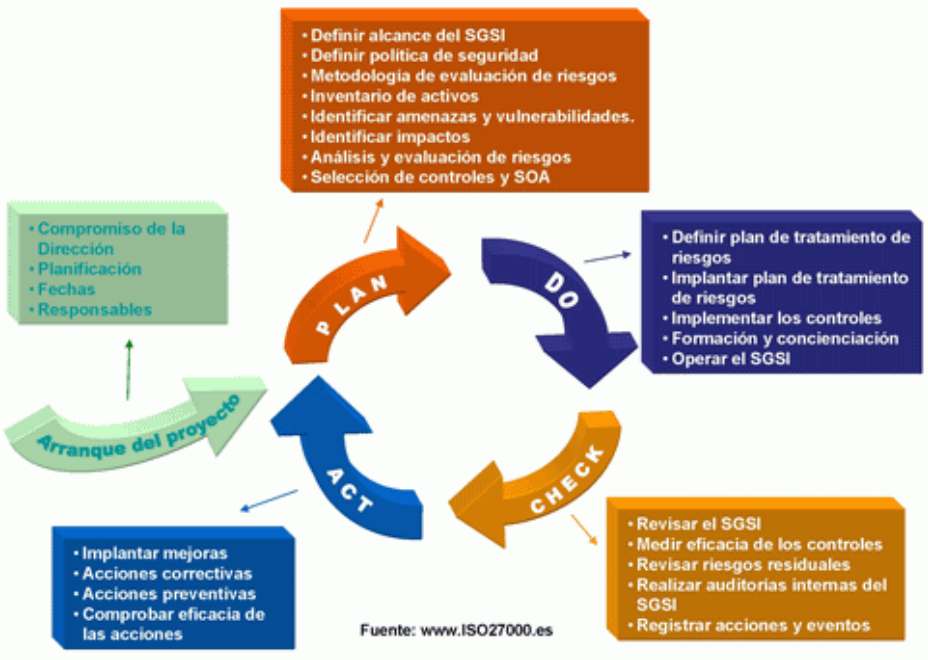


Figura 1 – Modelo PDCA

Veremos a continuación una breve introducción a éstas normas y guías base para el desarrollo del presente plan director de seguridad, así como los beneficios, ventajas que supone su implementación.

A. Norma ISO 27001

Esta norma se divide en varias partes:

2. **La primera parte** sirve para definir los fundamentos y principios de la norma, el modelo de gestión PDCA y especialmente en cuanto a su aplicabilidad y límites. Se compone de los apartados:

   a. **Introducción** (apartado 0 de la norma)
   b. **Alcance** (apartado 1 de la norma)
   c. **Norma para la consulta** (apartado 2 de la norma)
   d. **Términos y definiciones** (apartado 3 de la norma)

3. **La segunda parte** especifica los controles de gestión del sistema, asociados al modelo PDCA y no puede excluir ninguno para justificar conformidad. Se compone de los apartados:
   a. **Marco general del SGSI** (apartado 4 de la norma)
   b. **Responsabilidad de la dirección** (apartado 5 de la norma)
   c. **Auditoría interna** (apartado 6 de la norma)
   d. **Revisión del SGSI** (apartado 7 de la norma)
   e. **Proceso de mejora** (apartado 8 de la norma)

4. **La tercera parte** está compuesta por lo anexos siguientes:
   a. **De carácter NORMATIVO**
      i. **ANEXO A:** Especificaciones de los objetivos y controles de seguridad cuya aplicación o exclusión se debe justificar
   b. **De carácter INFORMATIVO**
      i. **ANEXO B:** Para explicar los principios de la cultura de la seguridad definidos por el OECD.
      ii. **ANEXO C: Correspondencia** con otros sistemas de gestión para ayudar a integrarse.

El objetivo de implementar esta norma y en definitiva de un **SGSI** no es solo que se implanten medidas de una lista básica de 133 controles del Anexo A, sino también de comprobar que se consiga el objetivo por los cuales aplican, en función de los requerimientos de la organización. **Los beneficios** que aporta un SGSI son:

- Mejorar la confianza con Clientes, Proveedores y Partners
- Asegurar la conformidad con la legislación y los contratos firmados
- Garantía interna de una adecuación independiente de la seguridad a sus objetivos
- Mejorar R.O.I. (Retorno de la inversión) de las Tecnologías y de la Seguridad
- Reducir el impacto de los incidentes
- Consistencia de las acciones de seguridad
- Alineamiento con los estándares de las TI (ITIL, COBIT).

B. Norma ISO 27002

En esta norma encontramos desarrollados los 133 controles del Anexo A de la norma 27001, de manera más extendida y detallada. Estos controles servirán para **asegurar la integridad, confidencialidad y disponibilidad de la información**. Esta norma se divide en 3 bloques (en la **Figura 5** podremos ver cada uno de ellos):

1. **BLOQUE 1:**
   - Política de seguridad (punto 5)
   - Estructura organizativa para la seguridad (interna y externa) – (punto 6)

- Clasificación y control de activos (punto 7)

2. **BLOQUE 2:**
   - Seguridad en el personal (punto 8)
   - Seguridad física y de entorno (punto 9)
   - Gestión de comunicaciones y operaciones (punto 10)
   - Control de accesos (punto 11)
   - Desarrollo y mantenimiento de sistemas (punto 12)
3. **BLOQUE 3:**
   - Gestión de incidencias (punto 13)
   - Gestión de continuidad del negocio (punto 14)
   - Cumplimiento (punto 15)

La siguiente **figura 2** muestra los diferentes dominios (bloques) de los que consta (del 5 al 15):

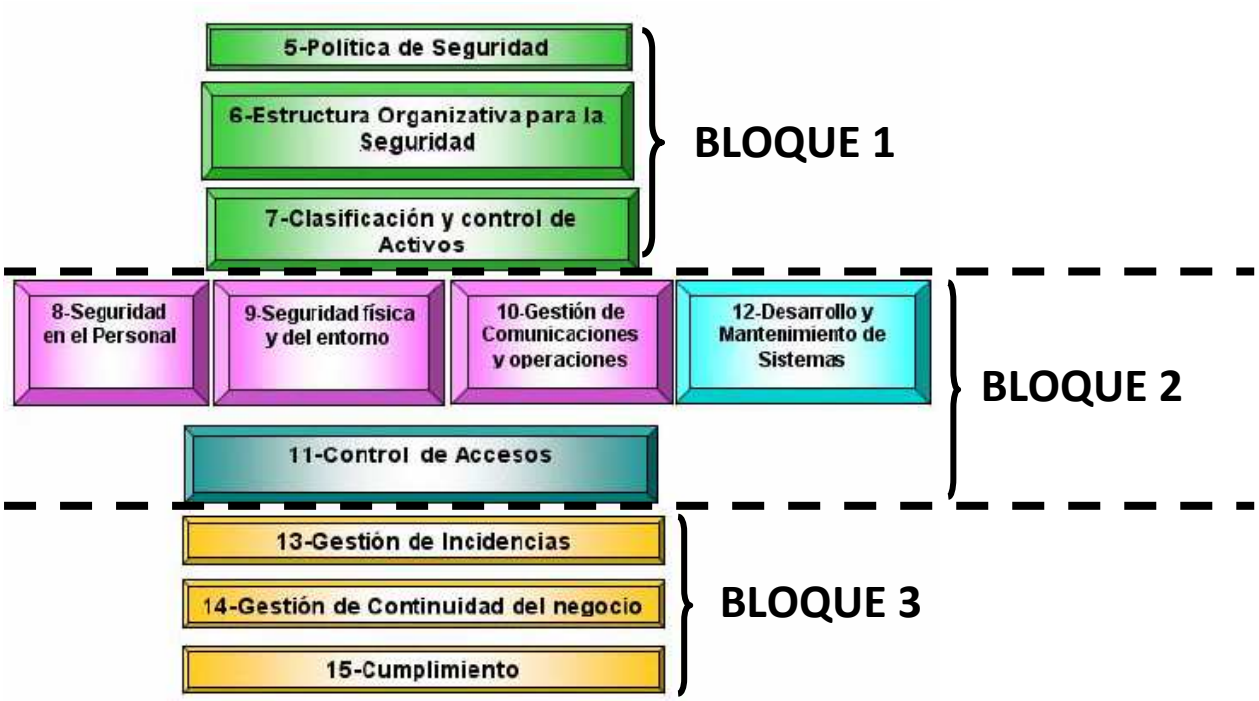


Figura 2 – Código de buenas prácticas en la Gestión de la Seguridad de la Información

Las **ventajas más importantes** que nos ofrece este estándar son:

- Cobertura consistente de todos los aspectos de la seguridad
- Enfoque a la prevención y a la rapidez de respuesta
- Marco de referencia para estimar el grado de seguridad
- Catálogo mínimo y guía de implantación de los controles de seguridad para los sistemas de gestión de seguridad certificables
- Consistencia con otras normas ISO, y también entre controles de seguridad

ANEXO II – ANÁLISIS DIFERENCIAL BAJO LA NORMA 27001:05

SECCION	TITULO	APLICA	VALOR
4	**SGSI**		
4.1	**Requerimientos Generales**		
4.1	Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado	**SI**	**L0**
4.2	**Establecer y Gestionar el SGSI**		
4.2.1	**Establecer el SGSI**		
4.2.1 (a)	Definir el alcance y los límites del SGSI	**SI**	**L0**
4.2.1 (b)	Definir una política de SGSI		
4.2.1 (c)	Definir el enfoque de la evaluación de Riesgos		
4.2.1 (d)	Identificar los riesgos		
4.2.1 (e)	Analizar y evaluar los riesgos		
4.2.1 (f)	Identificar y evaluar opciones para el tratamiento de riesgos		
4.2.1 (g)	Seleccionar objetivos de control y controles para el tratamientos de riesgos		
4.2.1 (h)	Obtener la aprobación por parte de la dirección de los riesgos residuales propuestos		
4.2.1 (i)	Obtener la autorización de la Dirección para implementar y operar el SGSI		
4.2.1 (j)	Preparar una Declaración de aplicabilidad		
4.2.2	**Implementar el SGSI**		
4.2.2 (a)	Elaborar un plan de tratamiento de riesgos	**SI**	**L0**
4.2.2 (b)	Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados		
4.2.2 (c)	Implementar los controles seleccionados en 4.2.1g para llegar a los objetivos de control		
4.2.2 (d)	Medir la efectividad de los controles para evaluar la efectividad y producir resultados comparables y reproducibles		
4.2.2 (e)	Implementar programas de formación y concienciación		
4.2.2 (f)	Gestionar la operación del SGSI		
4.2.2 (g)	Gestionar los recursos para el SGSI		
4.2.2 (h)	Procedimientos/controles para rápida detección de eventos seg. Y respuesta a incidentes de seguridad		
4.2.3	**Monitorizar y Revisar el SGSI**		
4.2.3 (a)	Ejecutar procedimientos de monitorización y revisión y otros controles	**SI**	**L0**
4.2.3 (b)	Llevar a cabo revisiones periódicas de la efectividad del SGSI		
4.2.3 (c)	Medir la efectividad de los controles para verificar que se cumplen los requerimientos de seguridad		
4.2.3 (d)	Revisar las evaluaciones de riesgos; los riesgos residuales; niveles aceptables de riesgos identificados.		
4.2.3 (e)	Llevar a cabo auditorías internas del SGSI de manera regular (ver 6)		
4.2.3 (f)	Llevar a cabo una revisión por la dirección del SGSI de manera regular		
4.2.3 (g)	Actualizar los planes de seguridad por hallazgos en las actividades de monitorización y revisión		
4.2.3 (h)	Registrar acciones/eventos con posible impacto en la efectividad/rendimiento del SGSI		
4.2.4	**Mantener y mejorar el SGSI**		
4.2.4 (a)	Implementar las mejoras identificadas en el SGSI	**SI**	**L0**
4.2.4 (b)	Llevar a cabo las AC y AP de acuerdo con 8.2 y 8.3		
4.2.4 (c)	Comunicar las acciones y mejoras a todas las partes interesadas		
4.2.4 (d)	Asegurar que las mejoras consiguen sus objetivos propuestos		
4.3	**Requerimientos de Documentación**		
4.3.1	**Documentación General del SGSI**		
4.3.1 (a)	Documentar los procedimientos y objetivos de la política del SGSI	**SI**	**L0**
4.3.1 (b)	Alcance del SGSI		
4.3.1 (c)	Procedimientos y controles de apoyo al SGSI		
4.3.1 (d)	Descripción de la metodología de evaluación de Riesgos		
4.3.1 (e)	Informe de evaluación de Riesgos		
4.3.1 (f)	Plan de Tratamiento de Riesgos		
4.3.1 (g)	Proced. para la planificación efectiva, operación y control de sus procesos de SI. Medir la efectividad de los controles		
4.3.1 (h)	Registros requeridos por este Estándar Internacional		
4.3.1 (i)	Declaración de Aplicabilidad		
4.3.2	**Control de Documentos**		

4.3.2 (a) 4.3.2 (b) 4.3.2 (c) 4.3.2 (d) 4.3.2 (e) 4.3.2 (f) 4.3.2 (g) 4.3.2 (h) 4.3.2 (i) 4.3.2 (j)	Aprobar documentos para su adecuación antes de su emisión Revisar y actualizar documentos cuando sea necesario y re-aprobar documentos. Asegurar que los cambios y que los estados de revisión actual de los documentos están identificados Asegurar que las versiones pertinentes de documentos aplicables están disponible Asegurar que los documentos permanecen legibles y fácilmente identificables Asegurar que los documentos están disponibles para aquellos que lo necesiten y son transferidos, almacenados y en última instancia, eliminados de acuerdo a los procedimientos aplicables en base a su clasificación Asegurar que los documentos de procedencia externa están identificados. Asegurar que la distribución de los documentos está controlada. Prevenir el uso no intencionado de documentos obsoletos. Aplicar una identificación adecuada a los documentos si éstos son retenidos para cualquier propósito.	**SI**	**L0**
4.3.3	**Control de los Registros**		
4.3.3 (a) 4.3.3 (b) 4.3.3 (c) 4.3.3 (d) 4.3.3 (e) 4.3.3 (f)	Establecer/Mantener registros para obtener evidencias de conform. de requerim. & eficacia del SGSI Los registros serán protegidos y controlados El SGSI debe tener en cuenta los requisitos legales o reglamentarios y las obligaciones contractuales. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Controles para: identificación, almacén, protección, recuperación, tiempo de retención y desecho de los registros. Se mantendrán registros de los resultados del proceso de todas las ocurrencias de incidentes de seguridad en SGSI	**SI**	**L0**
5	**Gestión de la Responsabilidad**		
5.1	**Compromiso de la dirección**		
5.1 (a) 5.1 (b) 5.1 (c) 5.1 (d) 5.1 (e) 5.1 (f) 5.1 (g) 5.1 (h)	Establecer una política de SGSI Asegurar de que se establecen los objetivos y los planes del ISMS Establecer roles y responsabilidades para la seguridad de la información Satisfacer los objetivos del SI, definir responsabilidades (por ley) y la necesidad de la mejora continua Recursos para establecer,implementar,operar,monitorizar,revisar,mantener,mejorar el SGSI Decidir los criterios de aceptación de riesgos y los niveles de riesgo aceptables Asegurarse de que las auditorías internas del SGSI se llevan a cabo La realización de revisiones por la dirección del SGSI	**SI**	**L0**
5.2	**Gestión de los recursos**		
5.2.1	**Provisión de Recursos**		
5.2.1 (a) 5.2.1 (b) 5.2.1 (c) 5.2.1 (d) 5.2.1 (e) 5.2.1 (f)	Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI Asegurar procedimientos de seguridad de la info son compatibles con los requerim. del negocio Identificar y abordar los requisitos legales/reglamentarios y obligaciones contractuales de seguridad Mantener la seguridad con la aplicación correcta de todos los controles implementados Llevar a cabo revisiones cuando sea necesario, y dar una respuesta adecuada Cuando sea necesario, mejorar la eficacia del SGSI	**SI**	**L0**
5.2.2	**Formación, sensibilización y competencia**		
5.2.2 (a) 5.2.2 (b) 5.2.2 (c) 5.2.2 (d)	Determinar las competencias necesarias para el personal que realiza trabajo efectivo en el SGSI Proporcionar formación o tomar otras acciones para satisfacer estas necesidades Evaluar la efectividad de las acciones llevadas a cabo El mantenimiento de registros de educación/formación/habilidades/experiencia/calificaciones	**SI**	**L0** **L5**
6	**Auditoría Interna del SGSI**		
6 (a) 6 (b) 6 (c) 6 (d) 6 (e) 6 (f)	Cumplir con los requisitos de este Estándar y legislación o reglamentos Cumplir con los requisitos de seguridad de la información identificados Que está efectivamente implementado y mantenido Desempeñe según lo esperado Que sea planificado un programa de auditoría Toman acciones sin demora para eliminar las NC detectadas y sus causas.	**SI**	**L0**
7	**Revisión por la dirección del SGSI**		
7.1	**General**		
7.1 (a)	Información para la Revisión	**SI**	**L0**
7.2	**La información para una revisión incluirá:**		
7.2 (a) 7.2 (b) 7.2 (c) 7.2 (d) 7.2 (e) 7.2 (f) 7.2 (g) 7.2 (h) 7.2 (i)	Resultados de Auditorías y revisiones del SGSI Los comentarios de las partes interesadas Técnicas, productos o procedimientos, para mejorar el rendimiento y la eficacia del SGSI Estado de las acciones preventivas y correctivas Las vulnerabilidades o amenazas no tratadas en la evaluación de riesgos anterior Los resultados de las mediciones de la eficacia Las acciones de seguimiento de revisiones previas de la dirección Todos los cambios que podrían afectar al SGSI Recomendaciones de mejora	**SI**	**L0**
7,3	**Resultados de la Revisión**		

7.3 (a) 7.3 (b) 7.3 (c) 7.3 (d) 7.3 (e)	Mejora de la eficacia del SGSI Actualización del plan de tratamiento de riesgos y evaluación de riesgos Responder a eventos internos o externos que pueden influir en el SGSI modificando de procedimientos y controles Necesidades de Recursos Mejoras de cómo la efectividad de los controles está siendo medida	**SI**	**L0**
8	**Mejora del SGSI**		
8.1	**Mejora continua**		
8.1	Mejorar continuamente la eficacia del SGSI	**SI**	**L0**
8.2	**Acción Correctiva**		
8.2 (a) 8.2 (b) 8.2 (c) 8.2 (d) 8.2 (e) 8.2 (f)	Identificar las no conformidades Determinar las causas de las no conformidades Evaluar la necesidad de adoptar medidas para asegurar que las no conformidades no vuelvan a ocurrir Determinar y aplicar las medidas correctivas necesarias Registrar los resultados de las acciones tomadas Revisar las acciones correctivas tomadas	**SI**	**L0**
8.3	**Acción Preventiva**		
8.3 (a) 8.3 (b) 8.3 (c) 8.3 (d) 8.3 (e)	Identificar no conformidades potenciales y sus causas Evaluar la necesidad de actuar para prevenir la ocurrencia de NC Determinar e implementar las acciones preventivas necesarias Registrar los resultados de las acciones tomadas Revisar las acciones preventivas tomadas	**SI**	**L0**

Tabla I – Análisis diferencial norma ISO 27001

ANEXO III – ANÁLISIS DIFERENCIAL BAJO LA NORMA 27002:05

N1	N2	N3	TITULO	TIPO DE CONTROL			APLICA	VALOR
				J	G	T		
5			**POLÍTICA DE SEGURIDAD**					
5	**1**		**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**					
5	1	1	Documento de política de seguridad de la información	X	X	X	SI	L0
5	1	2	Revisión de la política de seguridad de la información		X		SI	L0
6			**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**					
6	**1**		**ORGANIZACIÓN INTERNA**					
6	1	1	Comité de gestión de la seguridad de la información		X		SI	L0
6	1	2	Coordinación de la seguridad de la información		X		SI	L0
6	1	3	Asignación de responsabilidades en seguridad de la información		X		SI	L0
6	1	4	Proceso de autorización de recursos para la seguridad de la información		X		SI	L0
6	1	5	Acuerdos de confidencialidad	X			SI	L2
6	1	6	Relación con las autoridades		X		SI	L2
6	1	7	Relación con grupos de interés especial		X		SI	L0
6	1	8	Revisión independiente de la seguridad		X		SI	L0
6	**2**		**TERCERAS PARTES**					
6	2	1	Identificación de riesgos relacionados con terceras partes	X	X		SI	L3
6	2	2	Requisitos de seguridad en las relaciones con clientes	X	X		SI	L3
6	2	3	Requisitos de seguridad en los contratos con terceros	X	X		SI	L3
7			**GESTIÓN DE ACTIVOS**					
7	**1**		**RESPONSABILIDAD DE LOS ACTIVOS**					
7	1	1	Inventario de activos	X	X	X	SI	L3
7	1	2	Propietarios de los activos	X	X		SI	L3
7	1	3	Uso aceptable de los recursos	X	X		SI	L3
7	**2**		**CLASIFICACIÓN DE LA INFORMACIÓN**					
7	2	1	Guías de clasificación	X	X		SI	L3
7	2	2	Marcado y tratamiento de la información	X	X	X	SI	L3
8			**SEGURIDAD LIGADA AL PERSONAL**					
8	**1**		**ANTES DE LA RELACIÓN LABORAL**					
8	1	1	Roles y responsabilidades	X	X		SI	L0
8	1	2	Credenciales	X	X		SI	L0
8	1	3	Términos y condiciones del empleo	X	X		SI	L0
8	**2**		**DURANTE LA RELACIÓN LABORAL**					
8	2	1	Responsabilidades de los directores	X	X		SI	L0
8	2	2	Concienciación, formación y capacitación en seguridad de la información	X	X	X	SI	L0
8	2	3	Proceso disciplinario	X			SI	L0
8	**3**		**FINAL O CAMBIO EN LA RELACIÓN LABORAL**					
8	3	1	Responsabilidades al finalizar la relación laboral	X			SI	L0
8	3	2	Devolución de los equipos		X		SI	L2
8	3	3	Supresión de los derechos de acceso		X		SI	L2
9			**SEGURIDAD FÍSICA**					
9	**1**		**ÁREAS SEGURAS**					
9	1	1	Perímetro de seguridad física		X	X	SI	L3
9	1	2	Control físicos de entrada			X	SI	L3
9	1	3	Seguridad de oficinas, despachos y salas		X	X	SI	L3
9	1	4	Protección contra amenazas externas y ambientales			X	SI	L3

9	1	5	Trabajo en áreas seguras		X		SI	L3
9	1	6	Acceso público, zonas de carga y descarga		X	X	SI	L5
9	**2**		**SEGURIDAD DE LOS EQUIPOS**					
9	2	1	Instalación y protección de los equipos		X	X	SI	L2
9	2	2	Servicios de suministro			X	SI	L2
9	2	3	Seguridad del cableado			X	SI	L2
9	2	4	Mantenimiento de los equipos		X		SI	L2
9	2	5	Seguridad de equipos fuera de los locales propios		X		SI	L2
9	2	6	Seguridad en la reutilización o eliminación de equipos		X	X	SI	L2
9	2	7	Sustracciones de equipos	X	X	X	SI	L2
10			**GESTIÓN DE COMUNICACIONES Y OPERACIONES**					
10	**1**		**PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIONES**					
10	1	1	Procedimientos de operaciones documentados		X		SI	L1
10	1	2	Gestión de los cambios		X	X	SI	L1
10	1	3	Segregación de tareas		X		SI	L1
10	1	4	Separación de los entornos de desarrollo, pruebas y explotación		X	X	SI	L1
10	**2**		**GESTIÓN DE LOS NIVELES DE SERVICIOS DE TERCERAS PARTES**					
10	2	1	Niveles de servicio	X	X		SI	L1
10	2	2	Monitorizar y revisar los niveles de servicio		X	X	SI	L1
10	2	3	Gestión de cambios en los niveles de servicio	X	X		SI	L1
10	**3**		**PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS**					
10	3	1	Gestión de capacidades		X		SI	L1
10	3	2	Aceptación de sistemas		X		SI	L1
10	**4**		**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL**					
10	4	1	Controles contra software malicioso		X	X	SI	L1
10	4	2	Controles contra código móvil		X	X	SI	L1
10	**5**		**COPIAS DE RESPALDO**					
10	5	1	Recuperación de la información		X	X	SI	L1
10	**6**		**GESTIÓN DE LA SEGURIDAD DE LA RED**					
10	6	1	Controles de red		X	X	SI	L1
10	6	2	Seguridad de los servicios de red		X	X	SI	L1
10	**7**		**GESTIÓN DE SOPORTES**					
10	7	1	Gestión de soportes extraíbles		X		SI	L1
10	7	2	Eliminación de soportes		X	X	SI	L1
10	7	3	Procedimiento de manejo de soportes		X		SI	L1
10	7	4	Seguridad de la documentación de los sistemas		X	X	SI	L1
10	**8**		**INTERCAMBIO DE INFORMACIÓN**					
10	8	1	Políticas y procedimientos de intercambio de información	X	X		SI	L0
10	8	2	Acuerdos de intercambio	X	X		SI	L0
10	8	3	Soportes físicos en transito			X	SI	L0
10	8	4	Correo electrónico	X	X	X	SI	L0
10	8	5	Sistemas de información de productividad		X	X	SI	L1
10	**9**		**SERVICIOS DE COMERCIO ELECTRONICO**					
10	9	1	Comercio electrónico	X	X	X	NO	
10	9	2	Transacciones interactivas	X	X	X		
10	9	3	Información con acceso publico	X	X	X		
10	**10**		**MONITORIZACIÓN**					
10	10	1	Trazabilidad		X	X	SI	L1
10	10	2	Monitorización del uso de los sistemas			X	SI	L1
10	10	3	Protección de la trazabilidad			X	SI	L1
10	10	4	Trazabilidad de los administradores y operadores			X	SI	L1
10	10	5	Registros de fallos			X	SI	L1
10	10	6	Sincronización de relojes		X	X	SI	L1

11			**CONTROL DE ACCESO**					
11	**1**		**REQUISITO EMPRESARIAL PARA EL CONTROL ACCESO**					
11	1	1	Política de control de acceso		X		SI	L1
11	**2**		**GESTIÓN DEL ACCESO DE LOS USUARIOS**					
11	2	1	Registro de usuarios		X	X	SI	L1
11	2	2	Gestión de privilegios		X	X	SI	L1
11	2	3	Gestión de las contraseñas de los usuarios		X		SI	L1
11	2	4	Revisión de los derechos de accesos		X		SI	L1
11	**3**		**RESPONSABILIDAD DE LOS USUARIOS**					
11	3	1	Uso de las contraseñas		X		SI	L1
11	3	2	Equipo de usuario desatendido		X		SI	L1
11	3	3	Política de puesto de trabajo despejado y bloqueo de pantalla		X		SI	L1
11	**4**		**CONTROL DE ACCESO EN LA RED**					
11	4	1	Política de uso de los servicios de red		X		SI	L1
11	4	2	Autenticación de usuarios para conexiones externas		X	X	SI	L1
11	4	3	Identificación de equipos en la red		X	X	SI	L1
11	4	4	Protección de los puertos de diagnostico remoto y configuración			X	SI	L1
11	4	5	Segregaciones de la red			X	SI	L1
11	4	6	Control de conexión a la red			X	SI	L1
11	4	7	Control de encaminamiento en la red			X	SI	L1
11	**5**		**CONTROL DE ACCESO AL SISTEMA OPERATIVO**					
11	5	1	Procedimiento seguro de login		X	X	SI	L1
11	5	2	Identificación y autenticación de usuario		X	X	SI	L1
11	5	3	Sistema de gestión de contraseñas		X	X	SI	L1
11	5	4	Uso de las utilidades de los sistemas operativos		X		SI	L1
11	5	5	Desconexión automática		X	X	SI	L1
11	5	6	Limitación de las ventanas de conexión		X	X	SI	L1
11	**6**		**CONTROL DE ACCESO A APLICACIONES E INFORMACIÓN**					
11	6	1	Restricción de acceso a la información		X	X	SI	L1
11	6	2	Aislamiento de sistemas sensibles		X		SI	L1
11	**7**		**INFORMÁTICA MÓVIL Y TELETRABAJO**					
11	7	1	Informática móvil y telecomunicaciones		X	X	SI	L1
11	7	2	Teletrabajo	X	X	X	SI	L1
12			**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**					
12	**1**		**REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN**					
12	1	1	Análisis y especificaciones de requisitos de seguridad		X		SI	L1
12	**2**		**PROCESO CORRECTO EN LAS APLICACIONES**					
12	2	1	Validación de los datos de entrada			X	SI	L0
12	2	2	Control del proceso interno			X	SI	L0
12	2	3	Integridad de los mensajes			X	SI	L0
12	2	4	Validación de los datos de salida			X	SI	L0
12	**3**		**CONTROLES CRIPTOGRÁFICOS**					
12	3	1	Política de uso de los controles criptográficos	X	X	X	SI	L0
12	3	2	Gestión de claves		X	X	SI	L0
12	**4**		**SEGURIDAD DE LOS FICHEROS DE LOS SISTEMAS**					
12	4	1	Control del software en explotación		X	X		
12	4	2	Protección de los datos de prueba	X	X	X	NO	
12	4	3	Control de acceso a los fuentes		X	X		
12	**5**		**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**					
12	5	1	Procedimiento de control de cambios		X	X	SI	L1
12	5	2	Revisión técnica de las aplicaciones después de cambios en los SSOO		X		SI	L1
12	5	3	Restricción a los cambios a los paquetes de software		X		SI	L1
12	5	4	Fuga de información		X		SI	L0

12	5	5	Desarrollo externalizado de software	X	X		SI	L0
12	**6**		**GESTIÓN DE VULNERABILIDADES TÉCNICAS**					
12	6	1	Control de vulnerabilidades técnicas		X	X	SI	L1
13			**GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN**					
13	**1**		**REPORTE DE INCIDENCIAS Y DEBILIDADES**					
13	1	1	Reporte de eventos de seguridad de información		X	X	SI	L0
13	1	2	Reporte de debilidades de seguridad		X	X	SI	L0
13	**2**		**GESTIÓN DE INCIDENCIAS DE SEGURIDAD Y MEJORA**					
13	2	1	Responsabilidades y procedimientos	X	X		SI	L0
13	2	2	Aprendiendo de las incidencias		X		SI	L0
13	2	3	Recogida de evidencias	X	X	X	SI	L0
14			**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**					
14	**1**		**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO**					
14	1	1	Incluir la seguridad de la información en el proceso de gestión de la cont. de negocio		X		SI	L0
14	1	2	Continuidad de negocio y análisis de riesgos	X	X	X	SI	L0
14	1	3	Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la info.		X	X	SI	L0
14	1	4	Marco de planificación de la continuidad de negocio		X		SI	L0
14	1	5	Prueba, mantenimiento y revisión de los planes de continuidad de negocio		X		SI	L0
15			**CONFORMIDAD**					
15	**1**		**CONFORMIDAD CON REQUISITOS LEGALES**					
15	1	1	Identificación de la legislación aplicable	X			SI	L3
15	1	2	Derechos de propiedad intelectual	X			SI	L3
15	1	3	Salvaguarda de los registros de la Organización	X			SI	L3
15	1	4	Protección de datos de carácter personal y privacidad	X	X	X	SI	L3
15	1	5	Prevención del mal uso de los recursos informáticos	X			SI	L3
15	1	6	Regulación de controles criptográficos	X			SI	L0
15	**2**		**CONFORMIDAD CON LAS DIRECTRICES DE SEGURIDAD Y REVISIONES TÉCNICAS**					
15	2	1	Conformidad con las políticas de seguridad y estándares	X	X		SI	L0
15	2	2	Comprobación de la conformidad técnica		X	X	SI	L0
15	**3**		**CONSIDERACIONES SOBRE EL AUDIT DE SISTEMAS DE INFORMACIÓN**					
15	3	1	Controles de auditoría de los sistemas de información		X	X	SI	L0
15	3	2	Protección de las herramientas de auditoría de sistemas de información		X		SI	L0

Tabla I – Análisis diferencial norma ISO 27002 y sus 133 controles

ANEXO IV – POLÍTICA DE SEGURIDAD

MASEGO S.A.	DOCUMENTO	CÓDIGO	FECHA REV	REV	REVISADO / MODIFICADO	APROBADO	PROPIETARIO
	POLITICA DE SEGURIDAD	P0L	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página**: 1 de 2

DECLARACIÓN

La información de nuestros clientes es, el activo principal de **MASEGO S.A.** Preservar **la confidencial y la integridad de su información es el objetivo de cara a nuestros clientes, y la disponibilidad de la información lo es para el devenir diario de los procesos dentro de la organización**, mediante la aplicación de las mejores prácticas. El seguimiento estricto de las políticas, normas y procedimientos que conforman el sistema de gestión de la seguridad de la información cerciorarán una seguridad sistemática y continua. Todo lo definido en esta política se concretará y desarrollará en normativas, procedimientos, registros e indicadores del SGSI **integrando, en la medida de lo posible, con otros sistemas de gestión de MASEGO S.A.** (en este caso con el sistema de gestión de la calidad ISO/IEC 9001:2008) compartiendo aquellos recursos para su optimización y la mejora continua de la eficiencia y eficacia de la gestión de los procesos.

PRINCIPIOS

1. **Concienciación:** Los empleados y contratados deben ser conscientes de la necesidad de contar con sistemas de información y redes seguros, así como qué es lo que pueden hacer para promover y fortalecer la seguridad.
2. **Responsabilidad:** Todos los empleados son responsables de la seguridad de los sistemas de información y redes.
3. **Respuesta:** Los empleados deben actuar de manera oportuna y coordinada para prevenir, detectar y responder a incidentes que afecten la seguridad de la información.
4. **Ética:** Los participantes deben respetar los intereses legítimos de los otros.
5. **Democracia:** La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.
6. **Evaluación del riesgo:** Los empleados deben llevar a cabo evaluaciones de riesgo en sus áreas funcionales para: identificarlos y mitigarlos. Tanto activa como proactivamente.
7. **Diseño e implementación de la seguridad:** La seguridad de la información se gestionará como un elemento esencial de los sistemas de información y redes, seleccionando, implantando y utilizando los controles apropiados para el tratamiento efectivo de los riesgos.
8. **Administración:** Los empleados deben adoptar una visión integral de la administración de la seguridad.
9. **Evaluación:** Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y redes, y efectuar las modificaciones apropiadas de las políticas, prácticas, medidas y procedimientos de seguridad.

MASEGO S.A.	**DOCUMENTO**	**CÓDIGO**	**FECHA REV**	**REV**	**REVISADO / MODIFICADO**	**APROBADO**	**PROPIETARIO**
	POLITICA DE SEGURIDAD	P0L	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página**: 2 de 2

DIRECTRICES DE SEGURIDAD

1. La entrada, salida y trabajo de los empleados en la empresa seguirán unas pautas seguras facilitadas por el Responsable de RRHH, PRL & Seguridad Física.
2. Independientemente del cargo ocupado dentro de la organización, todos los empleados aceptarán formalmente el **código ético** de **MASEGO S.A.**
3. Los empleados seguirán las pautas de clasificación de la información de **MASEGO S.A**.
4. El responsable de Seguridad tendrá que gestionar y administrar los riesgos, requisitos, incidencias y mejoras en seguridad mediante un Sistema de Gestión de Seguridad de la Información.
5. Los sistemas y redes informáticas seguirán unas normas de protección adecuadas y actualizadas.
6. Se diseñarán unos procedimientos estándar de intercambio, acceso y almacenamiento seguro de la información, que aseguren el cumplimiento de requisitos eficaces de confidencialidad.
7. Todo el personal recibirá las instrucciones y documentación apropiada para el cumplimiento y buenas prácticas en materia de seguridad de la información. Según su perfil , recibirán documentación sobre:
    - **a)** La propiedad intelectual y el concepto de autorización para el acceso, modificación, cesión, reproducción o comunicación de la información.
    - **b)** Autorización expresa para poder salir con información de carácter confidencial o de cualquier tipo que pueda comprometer dicha información en el exterior.
    - **c)** Las directrices y normas para el cumplimiento de un uso de los recursos de **MASEGO S.A.** adecuado y seguro (redes, hardware, software, telecomunicaciones, correo electrónico, conexiones a internet, etcétera).
8. Cualquier incidencia, vulnerabilidad o mejora en seguridad se debe comunicar para su registro y seguimiento a través de los siguientes medios: **@**: sgsi@masego.cat y, además (del email)para la sede de Madrid y almacenes de Badalona y Madrid: **Teléfono**: 931234567 ó **Fax**: 938901234

La presente política será de aplicación a todo el personal y recursos que se encuentran dentro del alcance del SGSI, se pone en su conocimiento y es comunicada a todas las partes interesadas mediante notificación electrónica y a través de los tablones de anuncios.

FIRMADO: EL DIRECTOR GENERAL En **Barcelona** a día **18** de **Octubre** del **2013**

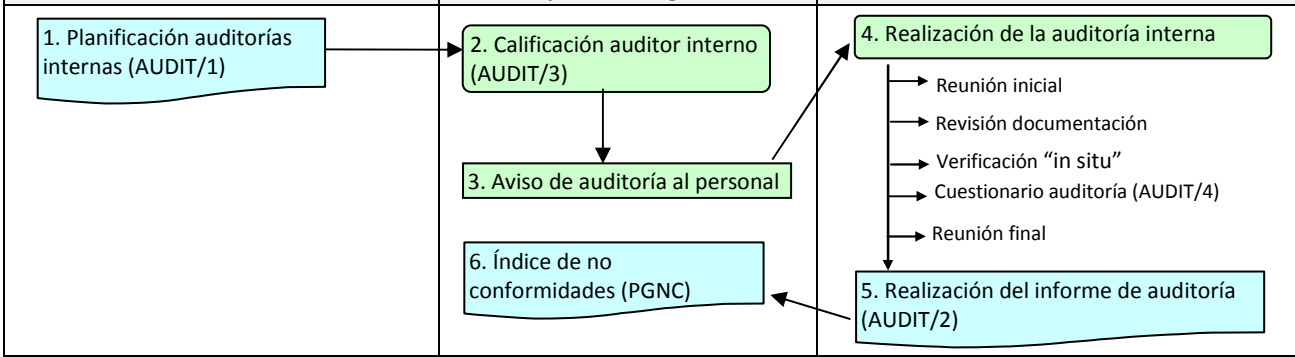
NOTA PARA CONSULTOR: *los principios se extraen del ANEXO B de la norma ISO/IEC 27001: "Los principios de la OCDE y esta norma Internacional"*

ANEXO V – PROCEDIMIENTO DE AUDITORÍA INTERNA

MASEGO S.A.	**PROCEDIMIENTO**	**CÓDIGO**	**FECHA REV**	**REV**	**REVISADO / MODIFICADO**	**APROBADO**	**PROPIETARIO**
	AUDITORÍA INTERNA	AUDIT	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página:** 1 de 1

OBJETO	Definir la metodología para la realización de auditorías para comprobar que todas las actividades relativas a la seguridad de la información cumplen las disposiciones definidas.
ENTRADAS	• Revisión del sistema de gestión de seguridad de la información • Cambios importantes en el sistema • Resultados de otras auditorías

ACTIVIDADES



RESULTADOS	INFORME DE AUDITORÍA (AUDIT/2)

DESCRIPCIÓN

1. Para avaluar las actividades relativas a la seguridad la Dirección define anualmente el PLAN DE AUDITORÍAS (AUDIT/1)
2. Los auditores son designados por la Dirección y no tienen relación directa con el departamento a auditar. Se puede recurrir a auditores externos. Las personas seleccionadas han de cumplir los requisitos de la CALIFICACIÓN DE AUDITOR (AUDIT/3) y serán reconocidas en este mismo registro.
3. La realización de auditorías se avisa al personal afectado mediante email interno con antelación mínima de una semana.
4. La auditoría se realiza de acuerdo al plan definido y consta de les siguientes fases:
   - Reunión inicial, donde se informa con detalle al auditado del objeto, alcance y programa de la auditoría.
   - Disponibilidad y revisión de la documentación aplicable.
   - Verificar el cumplimiento con el que está establecido en la documentación aplicable, comprobando que esta es la idónea.
   - Como ayuda para la realización de la auditoría, el auditor dispone del CUESTIONARIO DE AUDITORÍA (AUDIT/4), aunque puede hacer un cuestionario propio, usando el impreso (AUDIT/5)
   - Reunión final, donde se informa del resultado de la auditoría y se comentan de forma detallada las desviaciones detectadas
5. Después de la realización de la auditoría, el auditor realiza el INFORME DE AUDITORÍA (AUDIT/2) y lo entrega al Responsable de Seguridad, que se encarga de difundirlo a la Dirección y a los responsables de las áreas auditadas.
6. El seguimiento de las posibles no conformidades detectadas se realiza en el ÍNDICE DE NO CONFORMIDADES (PGNC) que abre el responsable del área auditada o responsable de seguridad.

DOCUMENTACIÓN DE REFERENCIA: PGACAP (PROCEDIMIENTO DE ACCIONES CORRECTIVAS Y PREVENTIVAS)

REGISTROS ASOCIADOS

Nombre impreso	Código	Lugar archivo	Responsable archivo	Tiempo archivo
Índice de no conformidades	PGNC	SGSI: INFORMES SEG.	Responsable Seguridad	3 años
Plan de auditorías	AUDIT/1	SGSI: AUDITORÍAS	Responsable. Seguridad	3 años
Informe de auditoría	AUDIT/2	SGSI: AUDITORÍAS	Responsable. Seguridad	3 años
Calificación de auditor	AUDIT/3	SGSI: AUDITORÍAS	Responsable. Seguridad	3 años
Cuestionario de auditoría	AUDIT/4	SGSI: AUDITORÍAS	Responsable. Seguridad	3 años
Plantilla de auditoría	AUDIT/5	SGSI: AUDITORÍAS	Responsable. Seguridad	3 años

NOTA: *no se incluyen los registros asociados*

ANEXO VI – GESTIÓN DE INDICADORES

MASEGO S.A.	**CUADRO DE MANDO INDICADORES ANUAL 2013**	**CÓDIGO**	**FECHA REV**	**REV**	**REVISADO / MODIFICADO**	**APROBADO**	**PROPIETARIO**
		IND	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página:** 1 de 3

ID	CONTROL	INDICADOR	OBJETIVO / DESCRIPCIÓN	FÓRMULA / TOLERANCIA	FRECUENCIA
1	**5.1**	**Política de Seguridad**	Verificar que el documento POL es revisado por la Dirección	Mínimo 1 vez al año	**ANUAL**
2	**6.1**	**Riesgo Interno**	Detectar No Conformidades (NC)	Mínimo 1 NC en cada revisión y que esa NC no se repita 2 años seguidos	**ANUAL**
3	**6.2**	**Riesgo Terceros**	Evaluar la seguridad en las conexiones con terceras partes (compras importantes como un Servidor, etc.)	Comparativa con año anterior. No repetir una misma NC 2 años seguidos	**ANUAL**
4	**7.1**	**Uso de Activos**	Comprobar el correcto uso de los activos y definición de los responsables de cada uno de ellos	No superar el número de incidentes del año anterior	**ANUAL**
5	**7.2**	**Clasificación de la información**	Comprobar la correcta clasificación de la información	No superar el número de incidentes del año anterior	**ANUAL**
6	**8.1**	**RRHH**	Comprobar la eficacia en las operaciones ligadas con RRHH	No superar el número de incidentes del año anterior y en ningún caso superar 2 incidencias graves en 1 año	**ANUAL**
7	**8.2**	**Incidencias con el personal**	Incluye las incidencias de tipo disciplinarias y las de formación	No superar el número de incidentes del año anterior	**ANUAL**
8	**8.3**	**Cese empleados**	Incluye el control de los activos del empleado (controlar la devolución) y la denegación física y lógica de accesos	No superar el número de incidentes del año anterior	**ANUAL**
9	**9.1**	**Seguridad Física**	Registrar todas las incidencias en cada una de las sedes y almacenes respecto a la seguridad física (interna / externa)	No superar el número de incidentes del año anterior	**MENSUAL**
10	**9.2**	**Seguridad Equipos**	Registrar incidencias sobre equipos: retiradas, reutilización, permisos remotos, protección, cableado, suministro eléctrico.	No superar el número de incidentes del año anterior	**ANUAL**
11	**10.1**	**Procedimientos de operación**	Comprobar si existe documentación de procedimientos no documentados	Menos del 5% de los procedimientos operativos pueden no estar documentados	**ANUAL**
			Registrar las versiones generadas en cada procedimiento operativo	Menos del 5% de versiones erróneas como límite	
			Comprobar que el creador de un procedimiento es el mismo que lo prueba	Como mínimo el 90% de la creación y prueba de cada procedimiento lo realiza la misma persona	
12	**10.2**	**Provisión de servicios por terceros**	Comprobar los errores de disponibilidad e incumplimiento de los servicios contratados	<= 5% del total (de errores en los contratos con terceras partes)	**ANUAL**

MASEGO S.A.	**CUADRO DE MANDO INDICADORES ANUAL 2013**	**CÓDIGO**	**FECHA REV**	**REV**	**REVISADO / MODIFICADO**	**APROBADO**	**PROPIETARIO**
		IND	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página:** 2 de 3

13	**10.3**	**Capacidad de los sistemas**	Se comprueba que los sistemas tengan margen de capacidad antes de colapsarse.	No superar el 70% de ocupación de los sistemas en memoria, disco duro y procesador	**MENSUAL**
14	**10.4**	**Infecciones en equipos y servidores**	Se comprueban los LOGS de detecciones de virus (y similares) para verificar el buen funcionamiento de los sistemas de protección	No superar el número de incidentes del mes anterior.	**SEMANAL**
15	**10.5**	**Copias de Seguridad**	Se comprueba la correcta realización de copias de seguridad y pruebas de recuperación de éstas	>= 95% de las copias y pruebas respectivas correctas.	**SEMANAL**
16	**10.6**	**Intrusiones**	Se comprueba que las políticas de acceso a redes definidas en los servidores y equipos son eficientes	No se permite ningún acceso no autorizado.	**SEMANAL**
17	**10.7**	**Gestión de soportes**	Se comprueban las eficacia de las políticas de acceso y manipulación de los soportes fijos y extraíbles	No se permite ningún acceso no autorizado. No se permite ninguna incidencia en la retirada de soportes	**ANUAL**
18	**10.8**	**Intercambio de información**	Número de incumplimientos de la política y procedimientos Incidencias en las compras, en la mensajería electrónica y en el los sistemas de información empresarial	No se permite ningún incumplimiento <= 10 por año y en todo caso, nunca superar las del año anterior	**ANUAL**
19	**10.10**	**Supervisión**	Se comprueba que todos los sistemas estén monitorizados: registrando fallos (registros accesibles) y con los relojes sincronizados. Los accesos a los registros han de estar controlados, evitando accesos no autorizados	El 100% de los sistemas han de estar monitorizados y supervisados. Se permiten incidencias menores: <=5 al año	**ANUAL**
20	**11.2**	**Control de acceso de usuarios**	Son los incumplimientos de la política de control de acceso Revisión de los derechos de acceso de usuario	<=5 por año y en todo caso, nunca superar las del año anterior. Como mínimo 1 al año	**ANUAL**
21	**11.3**	**Responsabilidades del usuario**	Se comprueban no existan incumplimientos en la política de puesto de trabajo despejado y pantalla limpia, el uso correcto de contraseñas, y que los equipos no estén desatendidos	No se permite ningún incumplimiento	**ANUAL**
22	**11.4**	**Control de acceso a la Red**	Registro de cambios en la política de accesos remotos y registro y control de los accesos remotos mediante autentificación de usuario y validación de equipo Control de puertos y conexiones remotas según políticas definidas en los servidores, firewalls y rutas de enrutamiento	Nunca más de 5 errores menores al mes y no se permite ningún incumplimiento para errores mayores	**MENSUAL**
23	**11.5**	**Control de acceso al SSOO**	Registro de los inicios de sesión de usuario y de las desconexiones automáticas en el tiempo establecido.	< 2 al mes y en ningún caso superar el total de incidencias del año anterior	**MENSUAL**

MASEGO S.A.	**CUADRO DE MANDO INDICADORES ANUAL 2013**	**CÓDIGO**	**FECHA REV**	**REV**	**REVISADO / MODIFICADO**	**APROBADO**	**PROPIETARIO**
		IND	18/10/13	0	RESPONSABLE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página:** 3 de 3

24	**11.6**	**Control de acceso a las aplicaciones y a la información**	Se registran los accesos a los sistemas de información, con especial atención a los errores e incidencias sobre éstos accesos	< 10 por año para usuarios registrados y 0 al año para usuarios sin registrar	**MENSUAL**
25	**11.7**	**Control acceso usuarios remotos**	Control de accesos mediante portátiles y equipos, comunicaciones móviles	<=5 por año y en todo caso, nunca superar las del año anterior.	**ANUAL**
26	**12.2**	**Uso correcto de las aplicaciones**	Registrar los errores en la validación de los datos de entrada y salida, el procesamiento interno y la integridad de los mensajes	<=5 por año y en todo caso, nunca superar las del año anterior.	**ANUAL**
27	**12.3**	**Controles criptográficos**	Se comprueba el cumplimiento de la política de su uso, y la gestión de las claves criptográficas existentes	No se permite ninguna incidencia de este tipo	**ANUAL**
28	**12.5**	**Procesos de desarrollo y soporte**	Se comprueba y registran todas las incidencias respecto a la fuga de información así como sus causas	No se permite ninguna incidencia de este tipo	**ANUAL**
			Se evalúa la funcionalidad de todas las aplicaciones tras actualizaciones de los SSOO		
29	**12.6**	**Gestión de las vulnerabilidades técnicas**	De todas las vulnerabilidades encontradas en los sistemas, se pretende gestionar con éxito la gran mayoría de ellas	> 90% de las vulnerabilidades	**ANUAL**
30	**13.1**	**Notificaciones eventos y puntos débiles de la SI**	Se pretende controlar y comprobar la validez de los procesos definidos para la notificación de todos los incidentes detectados	Notificaciones correctas en un >= 90%	**ANUAL**
31	**13.2**	**Incidencias de seguridad**	Se registran todos los incidentes detectados con el fin de mejorar los procesos afectados. Estas mejoras se comprueban al siguiente año para comprobar que esos incidentes no se repitan	No se permite repetir las mismas NC / incidencias detectadas un año antes.	**ANUAL**
32	**14.1**	**Continuidad del Negocio**	Se comprueba la correcta gestión del PCN definido incluyendo: la inclusión de la seguridad de la información en el proceso de CN, la evaluación de riesgos, el desarrollo e implantación del PCN y marco de referencia para su planificación (de la CN)	No se permite ninguna NC	**ANUAL**
			Pruebas, mantenimiento y reevaluación de los PCN	Éxito en >= 95% del total de las pruebas realizadas	
33	**15.1**	**Cumplimiento de los requisitos legales**	A partir de los resultados de las auditorias se comprueban las incidencias en lo referente a cumplimiento de los requisitos legales: legislación aplicable, DPI, protección de documentos de la organización, uso indebido de recursos para el tratamiento de la información y regulación de los controles criptográficos	No se permite ninguna NC.	**ANUAL**
34	**15.2**	**Cumplimiento de las políticas, normas de seguridad y cumplimiento técnico**	Se verifica el correcto cumplimiento.	No se permite ninguna NC.	**ANUAL**
35	**15.3**	**Herramientas para las auditorias del SGSI**	Se comprueban si ha habido accesos no autorizados así como las políticas de acceso sobre las herramientas y registros	No se permite ninguna NC.	**ANUAL**

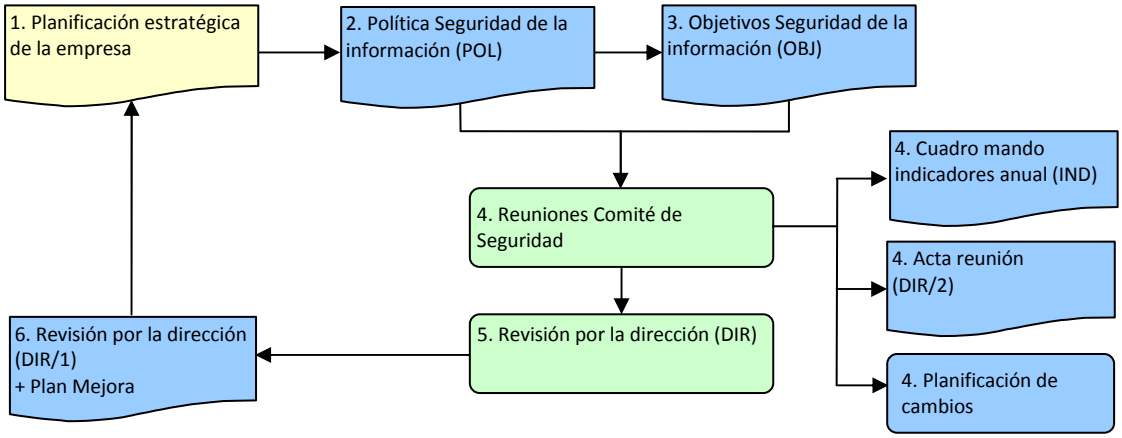
ANEXO VII – PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

MASEGO S.A.	**PROCEDIMIENTO**	**CÓDIGO**	**FECHA**	**REV**	**REVISADO**	**APROBADO**	**PROPIETARIO**
	Planificación estratégica de la SI	DIR	18/10/13	0	RESPONSABLE DE SEGURIDAD	DIRECTOR GENERAL	RESPONSABLE DE SEGURIDAD
	CREADO POR: RESPONSABLE SEGURIDAD				**FECHA CREACIÓN:** 18/10/2013		**Página:** 1 de 2

OBJETO	Definir el proceso para gestionar todas las actividades relacionadas con la dirección estratégica de la seguridad
ENTRADAS	• Exigencias de clientes y reglamentarias • Situación del sector • Resultados de años anteriores

ACTIVIDADES

Director General + Responsables Departamento + Responsable Seguridad de la Información (RSI)



RESULTADOS	POLÍTICA DE SEGURIDAD (POL) OBJETIVOS DE SEGURIDAD (OBJ) INFORME DE REVISIÓN POR LA DIRECCIÓN (DIR/1) ACTAS DE REUNIÓN COMITÉ DE SEGURIDAD (DIR/2) CUADRO DE MANDO DE INDICADORES (IND)

DESCRIPCIÓN

1. La planificación de la calidad es una de las líneas fundamentales de la planificación estratégica de la empresa. La política de la seguridad es uno de los resultados de esta planificación.
2. La Dirección define y aprueba la Política de la Seguridad (POL) que se comunica a todo el personal mediante reuniones internas, el plan de acogida (dentro del cumplimiento de la PRL y Gestión de la Calidad) y su difusión en los cuadros informativos.
3. Anualmente los responsables de los departamentos proponen los objetivos de seguridad, que son aprobados por la Dirección (OBJ).
4. El seguimiento de los objetivos de seguridad se realiza en las reuniones del Comité, y finalmente la valoración global anual se plasma en el informe de revisión del sistema por la Dirección (DIR/1). En las reuniones se analiza también la evolución de los indicadores de los procesos. En el CUADRO DE MANDO DE INDICADORES (IND) se gestiona la evolución de estos con los datos aportados por los propietarios de los mismos. En estas reuniones también se lleva a cabo el seguimiento de:
    a. Resultados auditorías
    b. Retroalimentación clientes
    c. Situación acciones correctivas / preventivas
    d. Planificación nuevos procesos

    El Responsable de Seguridad realiza ACTA DE REUNIÓN (DIR/2) que se distribuye a todos los asistentes. Cuando se detecta la posibilidad de algún cambio importante en el Sistema de Gestión de la Seguridad de la información, éste se planifica en una reunión del Comité de Seguridad en la que se define el cambio, el responsable y la planificación.
5. Una vez al año se realiza una reunión para llevar a cabo la revisión por la dirección en la que se valoran los siguientes puntos:

a. Implantación sistema Gestión de la Seguridad de la información.
b. Revisión política y objetivos
c. Situación acciones correctivas / preventivas
d. Resultado de auditorías
e. Retroalimentación clientes
f. Funcionamiento de los procesos y conformidad servicio
g. Formación del personal
h. Acciones de seguimiento de revisiones anteriores
i. Cambios planificados que podrían afectar al sistema
j. Recomendaciones para la mejora
k. También, se propone el plan de mejora para el ejercicio siguiente con la definición de:
    II. La mejora de la eficacia del sistema de gestión de la seguridad de la información y sus procesos.
    III. La mejora de los servicios en relación con los requisitos del cliente, personal de la empresa y terceras partes.
    IV. Las necesidades de recursos.

6. Los resultados se registran en el informe de REVISIÓN POR LA DIRECCIÓN (DIR/1).

DOCUMENTACIÓN DE REFERENCIA

- POL (POLÍTICA DE SEGURIDAD)
- OBJ (OBJETIVOS DE SEGURIDAD)

REGISTROS ASOCIADOS

Nombre impreso	Código	Lugar archivo	Responsable archivo	Tiempo archivo
Informe revisión Dirección	DIR/1	Carpeta Dirección	Responsable de Seguridad	3 años
Acta de reunión	DIR/2	Carpeta Dirección	Responsable de Seguridad	3 años
Cuadro indicadores Anual	IND	Carpeta Dirección	Responsable de Seguridad	3 años

NOTA PARA CONSULTOR: *no se incluyen los registros asociado, excepto el cuadro de indicadores anual, que se ha visto en el punto anterior.*

ANEXO VIII – GESTIÓN DE ROLES Y RESPONSABILIDADES

Es necesario crear una estructura interna con responsabilidad directa sobre la seguridad de la información. Esta estructura puede variar mucho el sea el tamaño y el tipo de compañía, pero, sea cual sea, **las funciones han de quedar bien definidas y se han de atribuir a personas concretas, con dedicación exclusiva o parcial**. Resulta indispensable que la dirección apruebe la estructura organizativa y la asignación de funciones de seguridad y que de apoyo, para dotar a las personas con responsabilidad en la materia de la autoridad y el tiempo necesario para ejercer sus funciones dentro de la compañía.

1. COMPOSICION DEL COMITÉ DE DIRECCIÓN

Es un órgano existente en la empresa desde sus inicios y **está constituido por**:

- Presidente de la compañía
- Directores
  - Director de General
  - Director de la sede de Madrid
  - Director de sede de Barcelona
  - Director comercial sede Barcelona
  - Director comercial sede Madrid
- Responsables de todas las áreas de la compañía:
  - Responsable almacén de Badalona
  - Responsable almacén de Madrid
  - Responsable de Contabilidad y Finanzas
  - Responsable transporte Nacional
  - Responsable transporte Internacional
  - Responsable TIC
  - Responsable de Calidad

Ahora con la inclusión del SGSI dentro de la organización, este comité mantendrá todos sus miembros como hasta ahora y los roles propios en materia de calidad y de la propia gestión de la compañía. A estas funciones ya existentes se les tendrá que añadir las **funciones inherentes en materia de seguridad de la información,** que son las siguientes:

1. Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
2. Nombrar a los miembros de un Comité de Seguridad de la Información, darles soporte, dotarlo de los recursos necesarios y establecer sus directrices de trabajo.
3. Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.
4. Determinar el umbral de riesgo aceptable en materia de seguridad.
5. Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
6. Aprobar el Plan de seguridad de la información, que recoge los principales proyectos e iniciativas en la materia.

7. Realizar el seguimiento del cuadro de mando de la seguridad de la información.

2. COMPOSICION DEL COMITÉ DE SEGURIDAD

Para poder empezar este proyecto es necesario e imprescindible crear un Comité de Seguridad. Para ello, se ha de contar con la presencia de altos cargos, o cargos intermedios que tengan peso, en mayor o menor grado, en el proceso de implantación, es decir, contar con todos los responsables de departamentos, o de dirección general, en los que los sistemas de la información jueguen un papel vital en el desarrollo diario de sus respectivas áreas. En este caso, y revisando el diagrama organizativo visto en puntos anteriores, la apuesta por **el nuevo Comité de Seguridad queda de la siguiente manera:**

- Presidente de la compañía
- Responsable TIC con nuevo rol de:
  - Responsable de Seguridad
- Responsable de Calidad con nuevo rol de:
  - Representante del Comité de dirección
- Responsable RRHH & PRL con nuevo rol de:
  - Responsable de Seguridad Física del edificio, y asuntos generales
  - Asesor Jurídico
- Directores
  - Director de General
  - Director de la sede de Madrid
  - Director de la sede de Barcelona
  - Director comercial sede Barcelona
  - Director comercial sede Madrid
- Responsables de la resta de áreas de la Organización:
  - Responsable almacén de Badalona
  - Responsable almacén de Madrid
  - Responsable de Contabilidad y Finanzas
  - Responsable transporte Nacional
  - Responsable transporte Internacional

La lista anterior muestra una selección de **miembros permanentes**, pero se podría contar en alguna ocasión, según las necesidades por **miembros invitados**, y por lo tanto, externos a la empresa, como los auditores externos, asesoría jurídica, etcétera. **Es imprescindible que en el Comité de Seguridad se encuentre personal del Comité de Dirección, de esta forma se garantizara su suporte directo.** Algunas de las **funciones y responsabilidades** de esté comité de seguridad serán:

1. Implantar las directrices del Comité de Dirección.
2. Asignar roles y funciones en materia de seguridad.
3. Facilitar al Comité de Dirección las políticas, normas y responsabilidades de la Seguridad de la Información; y esperar su aprobación o cambios propuestos en la documentación.

4. Gestión de riesgos y las salvaguardas propuestas por el responsable de seguridad de la información (RSI).
5. Presentar el Plan director de seguridad de la información para aprobación al Comité de Dirección; supervisar y hacer el seguimiento de su implantación.
6. Crear, desarrollar y mantener del Plan de continuidad de negocio.
7. Asegurar el cumplimiento de la legislación aplicable en materia de seguridad.
8. Concienciación y formación de usuarios en materia de seguridad de la información.
9. Revisar las incidencias más destacadas.
10. Gestionar el cuadro de mando de la seguridad de la información y evolución del SGSI.

3. RESPONSABLE DE SEGURIDAD DE LA INFORMACION

El **responsable TIC** toma el rol de **Responsable de seguridad de la información** (RSI). Sus tareas se corresponden a:

1. Implantar las directrices del Comité de Seguridad de la Información.
2. Crear, promover y mantener una política de seguridad de la información.
3. Crear y actualizar anualmente los objetivos para la seguridad de la información.
4. Crear el marco normativo de seguridad y controlar su cumplimiento.
5. Gestionar la seguridad de la información de forma global.
6. Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo.
7. Controlar la gestión de riesgos de nuevos proyectos.
8. Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas.
9. Crear y gestionar un Plan de continuidad de negocio de la compañía, en base al análisis de riesgo y la importancia de los procesos de negocio.
10. Asegurar el cumplimiento legal de todas las áreas de la organización.
11. Definir la arquitectura de seguridad de los sistemas de información
12. Monitorizar la seguridad y hacer el seguimiento de los incidentes de seguridad.
13. Gestionar un plan de concienciación/formación en seguridad de la información.
14. Coordinar la implantación de herramientas y controles de seguridad de la información
15. Gestión del cuadro de mando de la seguridad.

4. OTRAS RESPONSABILIDADES DISTRIBUIDAS POR LA COMPAÑÍA

Responsables funcionales de la información (directores y responsables)

1. Clasificar la información de la que son responsables según la criticidad que ésta tenga para la compañía en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio, trazabilidad e impacto mediático y determinar el uso que se debe hacer de la información y quién puede acceder.
2. Tener conocimiento de la normativa general o sectorial aplicable a la información de la que son responsables, incluida la normativa vigente en materia de protección de datos de carácter personal.

3. Definir los requisitos de seguridad para el tratamiento de la información, ya sea de forma automatizada o manual, en todo el ciclo de vida de la información (creación, modificación, conservación y destrucción en su caso).
4. Hacer el seguimiento del estado de la seguridad de los sistemas de información que traten la información de que son responsables y gestionar la mitigación de riesgos dentro de su nivel de decisión.
5. Impulsar la elaboración de planes de continuidad de negocio, implicarse y definir procedimientos alternativos en caso de indisponibilidad del sistema o falta de integridad de la información.
6. Colaborar a hacer revisiones y auditorías de seguridad de la información.

Personal en general (mandos intermedios, personal auxiliar)

1. Mantener la confidencialidad de la información.
2. Hacer un buen uso de los equipos y de la información a la que tienen acceso y protegerla de accesos no autorizados.
3. Respetar las normas y los procedimientos vigentes en materia de seguridad de la información y velar por que la respeten terceras partes en prestación de servicios.
4. Utilizar adecuadamente las credenciales de acceso a los sistemas de información. Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra legislación que sea aplicable.
5. Notificar, por la vía establecida, insuficiencias, anomalías o incidencias de seguridad y situaciones sospechosas que pueden poner en peligro la seguridad de la información.
6. Cada área dentro de la compañía debe colaborar con el RSI a desplegar la seguridad en su ámbito de actuación y conseguir trabajar y hacer trabajar la organización de manera segura. Así, pues, también se deben identificar funciones de seguridad en los ámbitos de auditoría, seguros, formación, organización, etc.

Área de tecnologías de la información y comunicaciones (TIC)

1. Cumplir las políticas, las normas y los procedimientos en materia de seguridad de la información. Colaborar con el RSI en definirlos.
2. Implantar en los sistemas de información los controles de seguridad prescritos y las acciones correctoras establecidas y gestionar las vulnerabilidades detectadas.
3. Requerir la participación de la RSI en nuevos proyectos de desarrollo o adaptación o implantación de productos de mercado, especialmente cuando puedan ser críticos en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio y trazabilidad, o puedan tener un impacto mediático importante.
4. Requerir la participación de la RSI en la implantación o gestión de los cambios de hardware y software.
5. Garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos (creación, mantenimiento, conservación y destrucción) y en los procesos de gestión de hardware y software.
6. Adoptar medidas para proteger la información según la clasificación que ha hecho el responsable de la información.
7. Colaborar con el RSI para identificar riesgos ya proponer soluciones, y colaborar en las revisiones o auditorías de seguridad que se lleven a cabo.

Responsable de RRHH y PRL

Se le añade el rol de **Responsable de Seguridad Física del edificio y asuntos generales** y de **Asesor Jurídico.** Para él y sus auxiliares, se crean una serie de necesidades para el cumplimiento en materia de la seguridad de la información, que son:

A. Área de seguridad física

1. Proporcionar los medios técnicos necesarios para la protección física de la información, tanto en lo referente a desastres físicos (incendio, inundación, falladles de suministro eléctrico, etc.) Como accesos no autorizados. La definición de controles que hay que implantar debe hacerse coordinadamente con el RSI.
2. Disponer de medidas de recuperación de la situación normal de operación de acuerdo con los requisitos de continuidad establecidos por el negocio.
3. Conocer e implantar los procedimientos de seguridad establecidos en la política de seguridad de la información.
4. El RSI y el responsable de seguridad física deben reportar mutuamente y tan pronto como puedan las incidencias de seguridad detectadas cuando puedan afectar al ámbito de competencia de la otra parte.
5. Implicar al RSI en los proyectos de obra y rehabilitación de edificios, para tener en cuenta a priori cuestiones de emplazamiento de elementos de red y comunicaciones, protección de equipos, etc.

B. Área de recursos humanos

1. Informar a las unidades gestoras de recursos de información sobre cambios o movimientos de personal para hacer una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría o de funciones, cambios organizativos, etc.
2. Trabajar junto con el RSI para desarrollar la política de seguridad de la información en las cuestiones referentes al personal.
3. Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo

C. Área de asesoría jurídica

1. Colaborar con el RSI a emitir nuevas políticas y normas de seguridad ya investigar y resolver incidencias de seguridad cuando se pueden derivar acciones legales (reclamaciones de terceras partes, acciones contra un trabajador, etc.).
2. Colaborar con el RSI a definir cláusulas específicas de seguridad de la información ya incluirlas en los contratos con terceras partes y contratos de personal externo.
3. Informar el RSI de nueva legislación o cambios en la legislación aplicable, que pueden tener impacto sobre la seguridad de la información, y dar soporte a la hora de interpretarlos.

NOTA PARA EL CONSULTOR: *Extraído del Módulo 4 (Desarrollo de algunos objetivos de control del SGSI) punto 3 (página 29 a 37) de la asignatura "Sistemas de Gestión de la Seguridad de la Información". Dicha información se ha adaptado a nuestro caso.*

ANEXO IX – METODOLOGÍA DEL ANÁLISIS DE RIESGOS

MAGERIT en su tercera versión (V3) es una de las metodologías de análisis de riesgos más utilizadas. El análisis de riesgos **es crucial** en el desarrollo correcto de todo el sistema de gestión de seguridad de la información. **MAGERIT** se basa en la consecución de **7 fases** bien diferenciadas. Podemos ver estas fases y el orden establecido en la siguiente **figura 1**:

Figura 1 – Fases de MAGERIT

FASE 1 – TOMA DE DATOS. PROCESOS DE LA INFORMACION

Esta primera fase se compone de las siguientes tareas:

1. Definición del alcance
2. Estudio de los procesos dentro de la organización
3. Establecer el nivel de detalle al que se quiere llegar

FASE 2 – DIMENSIONAMIENTO. ESTABLECIMIENTO DE PARÁMETROS

En esta segunda fase, una vez establecidos los límites de actuación, se han de identificar los parámetros a usar durante el proceso de análisis de riesgo. Estos parámetros son:

1. **Valor de los activos:** Todos los activos tienen un valor y se éste se puede medir teniendo en cuenta los diferentes escenarios en los cuales un activo puede encontrarse como los son:
    - **La reposición**, como el coste que supone reponer un activo por pérdida o mal funcionamiento.

- **La configuración,** como el coste desde que se adquiere el nuevo activo hasta que está listo para su uso.
- **El uso,** como el coste que supone tener parado un activo para la función que éste desarrolla.
- **Pérdida de oportunidad** es el coste que supone la indisponibilidad de un activo durante cierto tiempo.

Existen **dos maneras de valorar los activos: cuantitativa o cualitativamente.** Los valores definidos, tal y como vemos en la **tabla I** se establecen según un rango preestablecido. La siguiente **tabla I** nos lo muestra un **ejemplo** (en cuanto a los valores cuantitativos numéricos) de valoración de activos:

VALORACION	RANGO	VALOR
Muy Alta	Valor > 200 mil €	300 mil €
Alta	100 mil € < valor > 200 mil €	150 mil €
Media	50 mil € < valor > 100 mil €	75 mil €
Baja	10 mil € < valor > 50 mil €	30 mil €
Muy Baja	Valor < 10 mil €	10 mil €

Tabla I – Valoración de los activos

2. **Vulnerabilidades:** Interpretadas por **MAGERIT** como la frecuencia de ocurrencia de una amenaza, es decir, la frecuencia en la que una organización puede tener una amenaza en concreto. Las vulnerabilidades se calculan mediante una valoración numérica con estimaciones anuales (número de veces al año en el que ocurre):

Vulnerabilidad = Frecuencia estimada / días del año

En la siguiente **tabla II,** podemos ver un ejemplo de clasificación de la Vulnerabilidad, suponiendo que el año tiene 52 semanas y que la frecuencia de ocurrencia es la correcta para este tipo de empresa:

VULNERABILIDAD	RANGO	VALOR
Frecuencia Extrema	1 vez al año	1
Frecuencia Alta	1 vez cada 2 semanas	26/365 = 0,071233
Frecuencia Media	1 vez cada 2 meses	6/365 = 0,016438
Frecuencia Baja	1 vez cada 6 meses	2/365 = 0,005479
Frecuencia Muy Baja	1 vez al año	1/365 = 0,002739

Tabla II – Clasificación de la Vulnerabilidad

3. **Impacto: MAGERIT** entiende por impacto el % del valor del activo que se pierde en caso que haya una incidencia sobre ese activo. Para llevar a cabo esta valoración, es necesario establecer los diferentes valores de impacto a utilizar y luego asignar los valores que se estimen oportunos.

La siguiente **tabla III** muestra estos valores:

IMPACTO	VALOR
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy Bajo	5%

Tabla III – Clasificación impactos

4. **Efectividad del control de seguridad:** el objetivo es reducir, según el control que estemos tratando, su vulnerabilidad y/o el impacto de estos controles. La siguiente **tabla IV** nos muestra la variación Impacto/Vulnerabilidad:

IMPACTO	VALOR
Muy Alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy Bajo	10%

Tabla IV – Efectividad del control

FASE 3 – ANÁLISIS DE ACTIVOS

En esta tercera fase, se pretende identificar todos los activos dentro de la organización y qué necesita para llevar a cabo sus actividades.

La lista de activos resultante variará según el nivel de detalle establecido en la **FASE 1**, siendo ésta más o menos larga. Asimismo, en ningún caso se han de incluir activos que se encuentren fuera de dicho alcance.

Los activos se pueden clasificar según su naturaleza. La siguiente **figura 2** muestra gráficamente el tipo de activos que nos podemos encontrar y clasificar (teniendo en cuenta los valores definidos anteriormente: valor de reposición, de configuración, de uso y de pérdida de oportunidad):

Figura 2 – Tipos de Activos

FASE 4 – ANÁLISIS DE AMENAZAS

Podemos ver en la siguiente **tabla V**, el resumen de la clasificación de amenazas:

CLASIFICACION DE AMENAZAS SEGÚN MAGERIT		
ACCIDENTES	▪ Accidente físico ▪ Avería ▪ Interrupción de los servicios esenciales ▪ Accidentes mecánicos o electromagnéticos	Son situaciones en las que las personas no son responsables voluntariamente, sino que ocurren por causas naturales
ERRORES	▪ Errores en la utilización de los sistemas, provocados por el mal uso ▪ Errores en el diseño conceptual de las aplicaciones ▪ Errores en el desarrollo de las aplicaciones ▪ Errores de actualización o aplicación de parches en los sistemas o aplicaciones ▪ Errores de monitorización ▪ Errores de compatibilidad entre aplicaciones ▪ Errores inesperados (virus, etcétera)	Cometidos de manera involuntaria en el desarrollo diario de las actividades que se desarrollan en la organización. Las causas suelen ser: la distracción, desconocimiento o terceras partes contratadas para trabajar en la organización
AMENAZAS INTENCIONALES PRESENCIALES	▪ Acceso físico no autorizado ▪ Acceso lógico no autorizado ▪ Indisponibilidad de recursos ▪ Filtración de datos a terceros	Acciones provocadas intencionalmente por el personal propio de la organización, conociendo el daño que sus acciones pueden suponer
AMENAZAS INTENCIONALES REMOTAS	▪ Acceso lógico no autorizado ▪ Suplantación del origen ▪ Gusanos (Virus con el fin de propagarse usando los recursos y sistemas del afectado) ▪ Denegación de servicio contra la banda ancha o contra los recursos del sistema	Acciones provocadas intencionalmente por terceras personas externas a la organización que saben el daño que hacen conscientemente

Tabla V – Clasificación de amenazas

FASE 5 – ESTABLECIMIENTO DE VULNERABILIDADES

Es recomendable realizar (y necesario bajo la metodología MAGERIT), tener una lista de vulnerabilidades con el fin de estimar, calcular la frecuencia de ocurrencia de una determinada amenaza sobre un activo.

FASE 6 – VALORACIÓN DE IMPACTOS

Los impactos son las consecuencias que provocan en la organización el hecho que una amenaza, aprovechando una vulnerabilidad, afecte a un activo. Cuando se analizan los impactos se han de tener en cuenta los siguientes aspectos:

- El resultado de la agresión de una amenaza sobre un activo
- El efecto sobre cada activo para agrupar los impactos en cadena según la relación de activos
- El valor económico representativo de las pérdidas producidas en cada activo
- Las pérdidas cuantitativas y cualitativas

FASE 7 – ANÁLISIS DE RIESGO INTRÍNSECO

Llegados a este punto y con los valores calculados en cada una de las situaciones, es momento de realizar los cálculos necesarios para conocer los valores de los riesgos reales que someten a la organización (sin tener en cuenta las futuras medidas de seguridad que se implantarán en fases posteriores con el fin de mitigar esos riesgos). La siguiente fórmula ayudará a calcular dichos valores: **Riesgo = Valor del Activo X Vulnerabilidad X Impacto**

En este momento, la organización deberá decidir qué riesgos se han de aceptar y cuáles no. Es decir, se ha de definir el **nivel aceptable de riesgo**. La siguiente **tabla VI** muestra estos niveles:

NIVEL ACEPTABLE DE RIESGO	VALOR
Alto	75%
Medio	50%
Bajo	25%

Tabla VI – Nivel Aceptable de riesgo

FASE 8 – INFLUENCIA DE LOS CONTROLES DE SEGURIDAD (SALVAGUARDAS)

En esta fase entramos en la gestión de Riesgos propiamente dicha. Se trata de dar una solución a los riesgos encontrados con el fin de mitigarlos (y alcanzar un nivel aceptable de riesgo) o eliminarlos completamente. Estas soluciones o salvaguardas pueden ser de dos tipos:

- **Preventivas**: son las que reducen la frecuencia de ocurrencia de las vulnerabilidades. Una vez aplicada la salvaguarda, se recalcula el valor con la siguiente fórmula: **Nueva vulnerabilidad = Vulnerabilidad X % de disminución de la vulnerabilidad**
- **Correctivas**: son las que reducen el impacto de las amenazas. Una vez aplicada la salvaguarda, se recalcula el valor con la siguiente fórmula: **Nuevo Impacto = Impacto X % de disminución del impacto.**

FASE 9 – ANÁLISIS DE RIESGO EFECTIVO

En esta fase, se estudia cómo, de qué manera las salvaguardas definidas mitigan, reducen los riesgos. En esta fase se calcula el riesgo final y definitivo, dando como resultado el riesgo efectivo que tendrá la organización para cada una de las amenazas identificadas. Los resultados del estudio quedarán de la siguiente manera:

- **Riesgo Intrínseco** → **Valor Activo X Vulnerabilidad X Impacto**
- **Riesgo Efectivo** → Valor Efectivo X Nueva Vulnerabilidad X Nuevo Impacto = Valor Activo X (Vulnerabilidad X Porcentaje de disminución de vulnerabilidad) X (Impacto X Porcentaje de disminución de impacto) = **Riesgo intrínseco X Porcentaje de disminución de vulnerabilidad X Porcentaje de disminución de impacto**

FASE 10 – GESTIÓN DE RIESGOS

La última fase es la de toma de decisiones. Se ha de decidir que salvaguardas y medidas de seguridad se han de escoger (lista de controles de seguridad) con el fin de reducir los riesgos. La consecución de esta fase llega cuando la organización fija todos los riesgos detectados en fases anteriores por debajo del límite definido de riesgos. Asimismo la organización buscará un equilibrio entre esfuerzo y coste económico, tratando de fijar esos riesgos por debajo del límite definido con el menor coste / esfuerzo menor posible. La organización podrá, en el desarrollo de la presente Fase 10, tomar tres tipos diferentes de decisiones:

1. Reducir los riesgos
2. Transferir los riesgos
3. Aceptar los riesgos

Para finalizar esta fase, la organización y el responsable de seguridad en concreto, redactará el **PLAN DE ACCION**. Este plan a de incluir las conclusiones del propio análisis de riesgo, y, las acciones que se llevarán a cabo por la organización para mitigarlos. Este Plan de Acción se compone de la siguiente información:

1. Establecer prioridades
2. Plantear el análisis de Coste / Beneficio
3. Seleccionar controles definitivos
4. Asignar responsabilidades
5. Implantar los controles

NOTA: *Esta documentación se ha elaborado en base al Módulo 2 de la asignatura "Sistemas de Gestión de la Seguridad de la Información" en su punto 4.1. MAGERIT, así como en la propia metodología de MAGERIT V3.*

ANEXO X – DECLARACIÓN DE APLICABILIDAD (SOA)

N1	N2	N3	TITULO	APLICA
5			**POLÍTICA DE SEGURIDAD**	
5	**1**		**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	
5	1	1	Documento de política de seguridad de la información	**SI**
5	1	2	Revisión de la política de seguridad de la información	**SI**
6			**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
6	**1**		**ORGANIZACIÓN INTERNA**	
6	1	1	Comité de gestión de la seguridad de la información	**SI**
6	1	2	Coordinación de la seguridad de la información	**SI**
6	1	3	Asignación de responsabilidades en seguridad de la información	**SI**
6	1	4	Proceso de autorización de recursos para la seguridad de la información	**SI**
6	1	5	Acuerdos de confidencialidad	**SI**
6	1	6	Relación con las autoridades	**SI**
6	1	7	Relación con grupos de interés especial	**SI**
6	1	8	Revisión independiente de la seguridad	**SI**
6	**2**		**TERCERAS PARTES**	
6	2	1	Identificación de riesgos relacionados con terceras partes	**SI**
6	2	2	Requisitos de seguridad en las relaciones con clientes	**SI**
6	2	3	Requisitos de seguridad en los contratos con terceros	**SI**
7			**GESTIÓN DE ACTIVOS**	
7	**1**		**RESPONSABILIDAD DE LOS ACTIVOS**	
7	1	1	Inventario de activos	**SI**
7	1	2	Propietarios de los activos	**SI**
7	1	3	Uso aceptable de los recursos	**SI**
7	**2**		**CLASIFICACIÓN DE LA INFORMACIÓN**	
7	2	1	Guías de clasificación	**SI**
7	2	2	Marcado y tratamiento de la información	**SI**
8			**SEGURIDAD LIGADA AL PERSONAL**	
8	**1**		**ANTES DE LA RELACIÓN LABORAL**	
8	1	1	Roles y responsabilidades	**SI**
8	1	2	Credenciales	**SI**
8	1	3	Términos y condiciones del empleo	**SI**
8	**2**		**DURANTE LA RELACIÓN LABORAL**	
8	2	1	Responsabilidades de los directores	**SI**
8	2	2	Concienciación, formación y capacitación en seguridad de la información	**SI**
8	2	3	Proceso disciplinario	**SI**
8	**3**		**FINAL O CAMBIO EN LA RELACIÓN LABORAL**	
8	3	1	Responsabilidades al finalizar la relación laboral	**SI**
8	3	2	Devolución de los equipos	**SI**
8	3	3	Supresión de los derechos de acceso	**SI**
9			**SEGURIDAD FÍSICA**	
9	**1**		**ÁREAS SEGURAS**	
9	1	1	Perímetro de seguridad física	**SI**
9	1	2	Control físicos de entrada	**SI**
9	1	3	Seguridad de oficinas, despachos y salas	**SI**
9	1	4	Protección contra amenazas externas y ambientales	**SI**
9	1	5	Trabajo en áreas seguras	**SI**
9	1	6	Acceso público, zonas de carga y descarga	**SI**
9	**2**		**SEGURIDAD DE LOS EQUIPOS**	

9	2	1	Instalación y protección de los equipos	SI
9	2	2	Servicios de suministro	SI
9	2	3	Seguridad del cableado	SI
9	2	4	Mantenimiento de los equipos	SI
9	2	5	Seguridad de equipos fuera de los locales propios	SI
9	2	6	Seguridad en la reutilización o eliminación de equipos	SI
9	2	7	Sustracciones de equipos	SI
10			**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
10	**1**		**PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIONES**	
10	1	1	Procedimientos de operaciones documentados	SI
10	1	2	Gestión de los cambios	SI
10	1	3	Segregación de tareas	SI
10	1	4	Separación de los entornos de desarrollo, pruebas y explotación	SI
10	**2**		**GESTIÓN DE LOS NIVELES DE SERVICIOS DE TERCERAS PARTES**	
10	2	1	Niveles de servicio	SI
10	2	2	Monitorizar y revisar los niveles de servicio	SI
10	2	3	Gestión de cambios en los niveles de servicio	SI
10	**3**		**PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS**	
10	3	1	Gestión de capacidades	SI
10	3	2	Aceptación de sistemas	SI
10	**4**		**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL**	
10	4	1	Controles contra software malicioso	SI
10	4	2	Controles contra código móvil	SI
10	**5**		**COPIAS DE RESPALDO**	
10	5	1	Recuperación de la información	SI
10	**6**		**GESTIÓN DE LA SEGURIDAD DE LA RED**	
10	6	1	Controles de red	SI
10	6	2	Seguridad de los servicios de red	SI
10	**7**		**GESTIÓN DE SOPORTES**	
10	7	1	Gestión de soportes extraíbles	SI
10	7	2	Eliminación de soportes	SI
10	7	3	Procedimiento de manejo de soportes	SI
10	7	4	Seguridad de la documentación de los sistemas	SI
10	**8**		**INTERCAMBIO DE INFORMACIÓN**	
10	8	1	Políticas y procedimientos de intercambio de información	SI
10	8	2	Acuerdos de intercambio	SI
10	8	3	Soportes físicos en transito	SI
10	8	4	Correo electrónico	SI
10	8	5	Sistemas de información de productividad	SI
10	**9**		**SERVICIOS DE COMERCIO ELECTRONICO**	
10	9	1	Comercio electrónico	NO
10	9	2	Transacciones interactivas	NO
10	9	3	Información con acceso publico	NO
10	**10**		**MONITORIZACIÓN**	
10	10	1	Trazabilidad	SI
10	10	2	Monitorización del uso de los sistemas	SI
10	10	3	Protección de la trazabilidad	SI
10	10	4	Trazabilidad de los administradores y operadores	SI
10	10	5	Registros de fallos	SI
10	10	6	Sincronización de relojes	SI
11			**CONTROL DE ACCESO**	
11	**1**		**REQUISITO EMPRESARIAL PARA EL CONTROL ACCESO**	
11	1	1	Política de control de acceso	SI

11	**2**		**GESTIÓN DEL ACCESO DE LOS USUARIOS**	
11	2	1	Registro de usuarios	**SI**
11	2	2	Gestión de privilegios	**SI**
11	2	3	Gestión de las contraseñas de los usuarios	**SI**
11	2	4	Revisión de los derechos de accesos	**SI**
11	**3**		**RESPONSABILIDAD DE LOS USUARIOS**	
11	3	1	Uso de las contraseñas	**SI**
11	3	2	Equipo de usuario desatendido	**SI**
11	3	3	Política de puesto de trabajo despejado y bloqueo de pantalla	**SI**
11	**4**		**CONTROL DE ACCESO EN LA RED**	
11	4	1	Política de uso de los servicios de red	**SI**
11	4	2	Autenticación de usuarios para conexiones externas	**SI**
11	4	3	Identificación de equipos en la red	**SI**
11	4	4	Protección de los puertos de diagnostico remoto y configuración	**SI**
11	4	5	Segregaciones de la red	**SI**
11	4	6	Control de conexión a la red	**SI**
11	4	7	Control de encaminamiento en la red	**SI**
11	**5**		**CONTROL DE ACCESO AL SISTEMA OPERATIVO**	
11	5	1	Procedimiento seguro de login	**SI**
11	5	2	Identificación y autenticación de usuario	**SI**
11	5	3	Sistema de gestión de contraseñas	**SI**
11	5	4	Uso de las utilidades de los sistemas operativos	**SI**
11	5	5	Desconexión automática	**SI**
11	5	6	Limitación de las ventanas de conexión	**SI**
11	**6**		**CONTROL DE ACCESO A APLICACIONES E INFORMACIÓN**	
11	6	1	Restricción de acceso a la información	**SI**
11	6	2	Aislamiento de sistemas sensibles	**SI**
11	**7**		**INFORMÁTICA MÓVIL Y TELETRABAJO**	
11	7	1	Informática móvil y telecomunicaciones	**SI**
11	7	2	Teletrabajo	**SI**
12			**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	
12	**1**		**REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN**	
12	1	1	Análisis y especificaciones de requisitos de seguridad	**SI**
12	**2**		**PROCESO CORRECTO EN LAS APLICACIONES**	
12	2	1	Validación de los datos de entrada	**SI**
12	2	2	Control del proceso interno	**SI**
12	2	3	Integridad de los mensajes	**SI**
12	2	4	Validación de los datos de salida	**SI**
12	**3**		**CONTROLES CRIPTOGRÁFICOS**	
12	3	1	Política de uso de los controles criptográficos	**SI**
12	3	2	Gestión de claves	**SI**
12	**4**		**SEGURIDAD DE LOS FICHEROS DE LOS SISTEMAS**	
12	4	1	Control del software en explotación	**NO**
12	4	2	Protección de los datos de prueba	**NO**
12	4	3	Control de acceso a los fuentes	**NO**
12	**5**		**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**	
12	5	1	Procedimiento de control de cambios	**SI**
12	5	2	Revisión técnica de las aplicaciones después de cambios en los SSOO	**SI**
12	5	3	Restricción a los cambios a los paquetes de software	**SI**
12	5	4	Fuga de información	**SI**
12	5	5	Desarrollo externalizado de software	**SI**
12	**6**		**GESTIÓN DE VULNERABILIDADES TÉCNICAS**	
12	6	1	Control de vulnerabilidades técnicas	**SI**

13			**GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN**	
13	**1**		**REPORTE DE INCIDENCIAS Y DEBILIDADES**	
13	1	1	Reporte de eventos de seguridad de información	**SI**
13	1	2	Reporte de debilidades de seguridad	**SI**
13	**2**		**GESTIÓN DE INCIDENCIAS DE SEGURIDAD Y MEJORA**	
13	2	1	Responsabilidades y procedimientos	**SI**
13	2	2	Aprendiendo de las incidencias	**SI**
13	2	3	Recogida de evidencias	**SI**
14			**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**	
14	**1**		**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO**	
14	1	1	Incluir la seguridad de la información en el proceso de gestión de la cont. de negocio	**SI**
14	1	2	Continuidad de negocio y análisis de riesgos	**SI**
14	1	3	Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la info.	**SI**
14	1	4	Marco de planificación de la continuidad de negocio	**SI**
14	1	5	Prueba, mantenimiento y revisión de los planes de continuidad de negocio	**SI**
15			**CONFORMIDAD**	
15	**1**		**CONFORMIDAD CON REQUISITOS LEGALES**	
15	1	1	Identificación de la legislación aplicable	**SI**
15	1	2	Derechos de propiedad intelectual	**SI**
15	1	3	Salvaguarda de los registros de la Organización	**SI**
15	1	4	Protección de datos de carácter personal y privacidad	**SI**
15	1	5	Prevención del mal uso de los recursos informáticos	**SI**
15	1	6	Regulación de controles criptográficos	**SI**
15	**2**		**CONFORMIDAD CON LAS DIRECTRICES DE SEGURIDAD Y REVISIONES TÉCNICAS**	
15	2	1	Conformidad con las políticas de seguridad y estándares	**SI**
15	2	2	Comprobación de la conformidad técnica	**SI**
15	**3**		**CONSIDERACIONES SOBRE EL AUDIT DE SISTEMAS DE INFORMACIÓN**	
15	3	1	Controles de auditoría de los sistemas de información	**SI**
15	3	2	Protección de las herramientas de auditoría de sistemas de información	**SI**

Tabla I – Declaración de Aplicabilidad (SOA)

ANEXO XI – VALORACIÓN DE LAS AMENAZAS

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
HARWARE SERVIDORES	[HW1] [HW7]		FB	100%	50%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FB			100%		
		I.6	FB			50%		
		I.7	FMB			100%		
		E.2	FB	50%	50%	50%		
		E.23	FB			100%		
		E.24	FMB			50%		
		E.25	FMB	100%		100%		
		A.6	FMB	100%	50%	100%		
		A.7	FB	100%	50%	100%		
		A.11	FMB	50%	50%			
		A.23	FMB	50%		50%		
		A.24	FMB			100%		
		A.25	FMB	100%		100%		
		A.26	FB			100%		

Tabla I – Amenazas sobre el HW de Servidores

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
HARWARE EQUIPOS FIJOS	[HW2] [HW3] [HW8] [HW9] [HW13] [HW14] [HW18] [HW19]		FM	100%	20%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FM			100%		
		I.6	FMB			50%		
		I.7	FMB			100%		
		E.2	FB	30%	20%	50%		
		E.23	FB			100%		
		E.24	FMB			50%		
		E.25	FMB	100%		100%		
		A.6	FMB	100%	10%	100%		
		A.7	FM	100%	10%	100%		
		A.11	FMB	30%	10%			
		A.23	FMB	30%		30%		
		A.24	FMB			100%		
		A.25	FMB	100%		100%		
		A.26	FB			100%		

Tabla II – Amenazas sobre el HW de equipos fijos

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
HARWARE PORTÁTIL	[HW23] [HW24]		FM	100%	30%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FM			100%		
		I.6	FMB			50%		
		I.7	FMB			100%		
		E.2	FB	40%	30%	50%		
		E.23	FB			100%		
		E.24	FMB			50%		
		E.25	FMB	100%		100%		
		A.6	FMB	100%	20%	100%		
		A.7	FM	100%	20%	100%		
		A.11	FMB	40%	20%			
		A.23	FMB	40%		40%		
		A.24	FMB			100%		
		A.25	FMB	100%		100%		
		A.26	FB			100%		

Tabla III – Amenazas sobre el HW de equipos portátiles

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
HARWARE RED	[HW4] [HW5] [HW6] [HW10] [HW11] [HW12] [HW15] [HW16] [HW17] [HW20] [HW21] [HW22]		FB	100%	50%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FB			100%		
		I.6	FMB			50%		
		I.7	FMB			100%		
		E.2	FB	50%	50%	50%		
		E.23	FB			100%		
		E.24	FMB			50%		
		E.25	FMB	100%		100%		
		A.6	FMB	100%	50%	100%		
		A.7	FB	100%	50%	100%		
		A.11	FMB	50%	50%			
		A.23	FMB	50%		50%		
		A.24	FMB			100%		
		A.25	FMB	100%		100%		
		A.26	FB			100%		

Tabla IV – Amenazas sobre el HW de red

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
SOFTWARE SERVIDORS			FB	100%	100%	100%	100%	
	[SW1]	I.5	FMB			70%		
	[SW2]	E.1	FB	10%	10%	10%		
	[SW3]	E.2	FB	10%	20%	20%		
	[SW4]	E.8	FMB	10%	20%	20%		
	[SW5]	E.9	FMB	10%	20%	20%		
	[SW6]	E.10	FMB		20%			
	[SW7]	E.15	FMB		10%			
	[SW11]	E.18	FMB			50%		
	[SW12]	E.19	FMB	50%				
	[SW13]	E.20	FMB	20%	20%	20%		
	[SW14]	E.21	FB		20%	20%		
	[SW15]	A.5	FMB	50%	50%		100%	
	[SW16]	A.6	FB	50%	20%	20%		
		A.7	FB	20%	20%	100%		
		A.8	FB	80%	80%	100%		
		A.9	FMB	50%				
		A.10	FMB		50%			
		A.11	FMB	50%	20%			
		A.15	FMB		50%			
		A.18	FMB			50%		
		A.19	FMB	50%				
		A.22	FMB	100%	100%	100%		

Tabla V – Amenazas sobre el SW de Servidores

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
SOFTWARE EQUIPOS			FA	100%	100%	100%	100%	
	[SW8]	I.5	FA			50%		
	[SW9]	E.1	FB	10%	10%	10%		
	[SW10]	E.2	FB	10%	20%	20%		
	[SW17]	E.8	FB	10%	20%	20%		
	[SW18]	E.9	FMB	10%	20%	20%		
	[SW19]	E.10	FMB		20%			
	[SW20]	E.15	FMB		10%			
	[SW21]	E.18	FMB			50%		
	[SW22]	E.19	FMB	50%				
	[SW23]	E.20	FMB	20%	20%	20%		
	[SW24]	E.21	FB		20%	20%		
	[SW25]	A.5	FMB	50%	50%		100%	
	[SW26]	A.6	FB	50%	20%	20%		
	[SW27]	A.7	FB	20%	20%	100%		
	[SW28]	A.8	FM	80%	80%	100%		
	[SW29]	A.9	FB	50%				
	[SW30]	A.10	FB		50%			
	[SW31]	A.11	FB	50%	20%			
		A.15	FB		50%			
		A.18	FB			50%		
		A.19	FM	50%				
		A.22	FM	100%	100%	100%		

Tabla VI – Amenazas sobre el SW de Equipos

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
INSTALACIONES CPD	[L1]		FB	50%	50%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.11	FB			20%		
		E.15	FMB		50%			
		E.18	FMB			50%		
		E.19	FMB	20%				
		A.7	FB	50%	50%	50%		
		A.11	FB	50%	50%			
		A.15	FMB		50%			
		A.18	FMB			100%		
		A.19	FMB	50%				
		A.26	FMB			100%		
		A.27	FMB	50%		100%		

Tabla VII – Amenazas sobre el CPD

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
INSTALACIONES OFICINAS	[L2] [L3] [L4] [L5] [L6] [L7] [L8] [L9] [L10] [L11] [L12] [L13]		FM	50%	50%	100%		
		N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.11	FB			20%		
		E.15	FMB		50%			
		E.18	FMB			50%		
		E.19	FMB	20%				
		A.7	FM	50%	50%	50%		
		A.11	FB	50%	50%			
		A.15	FMB		50%			
		A.18	FMB			100%		
		A.19	FMB	50%				
		A.26	FMB			100%		
		A.27	FMB	50%		100%		

Tabla VIII – Amenazas sobre las oficinas

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
DATOS	[D1] [D2] [D3] [D4] [D5] [D6] [D7] [D8] [D9] [D10] [D11] [D12] [D13] [D14] [D15] [D16] [D17] [D18] [D19] [D20] [D21]		FA	100%	50%	75%	100%	
		E.1	FA	20%	20%	20%		
		E.2	FA	20%	20%	20%		
		E.15	FA		20%			
		E.18	FB			20%		
		E.19	FB	20%				
		A.5	FMB	50%	20%		100%	
		A.6	FB	100%	50%		100%	
		A.11	FMB	100%	50%			

	[D22] [D23] [D24] [D25] [D26] [D27] [D28] [D29] [D30]	A.15	FB		50%			
		A.18	FB			75%		
		A.19	FB	100%				

Tabla IX – Amenazas sobre los datos

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FM	50%	20%	100%	100%	
COMUNICACIONES ISP 2	[COM1]	I.8	FMB			100%		
		E.2	FB	20%	10%	50%		
		E.9	FB	10%				
		E.10	FB		10%			
		E.15	FMB		20%			
		E.18	FB			40%		
		E.19	FMB	10%				
		E.24	FMB			50%		
		A.5	FMB				100%	
		A.6	FB	50%	10%	50%		
		A.7	FM	10%	10%	30%		
		A.9	FMB	10%				
		A.10	FMB		10%			
		A.11	FMB	50%	10%			
		A.12	FMB	30%				
		A.14	FMB	30%				
		A.15	FMB		20%			
		A.19	FMB	40%				
		A.24	FB			50%		

Tabla X – Amenazas sobre las comunicaciones del ISP2

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FM	50%	20%	100%	100%	
COMUNICACIONES ISP 1 (VPN)	[COM2] [COM5] [COM6] [COM9] [COM10] [COM13] [COM14] [COM17]	I.8	FMB			100%		
		E.2	FB	20%	20%	50%		
		E.9	FB	20%				
		E.10	FB		20%			
		E.15	FMB		20%			
		E.18	FB			50%		
		E.19	FMB	20%				
		E.24	FMB			50%		
		A.5	FMB				100%	
		A.6	FB	50%	20%	50%		
		A.7	FM	20%	20%	50%		
		A.9	FMB	20%				
		A.10	FMB		20%			
		A.11	FMB	50%	20%			
		A.12	FMB	50%				
		A.14	FMB	50%				
		A.15	FMB		20%			
		A.19	FMB	50%				
		A.24	FB			50%		

Tabla XI – Amenazas sobre las comunicaciones del ISP1 – VPN

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
COMUNICACIONES VARIAS	[COM3] [COM4] [COM7] [COM8] [COM11] [COM12] [COM15] [COM16]		FM	50%	20%	100%	100%	
		I.8	FB			100%		
		E.2	FB	10%	10%	50%		
		E.9	FB	10%				
		E.19	FMB	10%				
		E.24	FMB			50%		
		A.5	FMB				100%	
		A.6	FB	50%	10%	50%		
		A.7	FM	10%	10%	20%		
		A.10	FMB		10%			
		A.11	FMB	50%	10%			
		A.14	FMB	20%				
		A.15	FMB		20%			
		A.19	FMB	20%				
		A.24	FB			50%		

Tabla XII – Amenazas sobre las comunicaciones varias

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
SERVICIOS VPN	[S2] [S5] [S8] [S11] [S14]		FA	100%	50%	100%	100%	100%
		E.1	FA	20%	10%	10%		
		E.2	FM	20%	20%	20%		
		E.9	FB	10%				
		E.10	FB		10%			
		E.15	FB		20%			
		E.18	FB			50%		
		E.19	FMB	20%				
		E.24	FB			50%		
		A.5	FMB	50%	20%		100%	
		A.6	FMB	20%	50%	20%		
		A.7	FM	10%	10%	100%		
		A.9	FMB	10%				
		A.10	FMB		10%			
		A.11	FMB		10%			
		A.13	FMB		20%			100%
		A.15	FMB		50%			
		A.18	FMB			20%		
		A.19	FMB	100%				
		A.24	FB			100%		

Tabla XIII – Amenazas sobre los servicios VPN

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
SERVICIOS INTERNOS	[S1] [S4] [S7] [S10] [S13]		FA	100%	50%	100%	100%	100%
		E.1	FA	20%	10%	10%		
		E.2	FA	20%	20%	20%		
		E.9	FM	10%				
		E.10	FB		10%			
		E.15	FB		20%			
		E.18	FB			50%		
		E.19	FMB	20%				
		E.24	FB			50%		
		A.5	FMB	50%	20%		100%	

		A.6	FMB	20%	50%	20%		
		A.7	FM	10%	10%	100%		
		A.9	FB	10%				
		A.10	FMB		10%			
		A.11	FMB		10%			
		A.13	FMB		20%			100%
		A.15	FB		50%			
		A.18	FMB			20%		
		A.19	FMB	100%				
		A.24	FB			100%		

Tabla XIV – Amenazas sobre los servicios internos

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FB	100%	50%	100%	100%	100%
SERVICIOS TERCERAS PARTES	[S3] [S6] [S9] [S12] [S15]	E.1	FMB	20%	10%	10%		
		E.2	FB	20%	20%	20%		
		E.10	FB		10%			
		E.15	FB		20%			
		E.18	FB			50%		
		E.19	FMB	20%				
		A.5	FMB	50%	20%		100%	
		A.6	FMB	20%	50%	20%		
		A.7	FMB	10%	10%	100%		
		A.10	FMB		10%			
		A.11	FMB		10%			
		A.13	FMB		20%			100%
		A.15	FMB		50%			
		A.18	FMB			20%		
		A.19	FMB	100%				

Tabla XV – Amenazas sobre los servicios de terceras partes

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FM	100%	50%	100%		
SOPORTES DE INFORMACION: HW	[SI1] [SI2] [SI3] [SI4] [SI6] [SI7] [SI8] [SI9] [SI11] [SI12] [SI13] [SI15] [SI16] [SI17] [SI19] [SI20]	N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FB			50%		
		I.5	FM			50%		
		I.6	FB			50%		
		I.7	FMB			50%		
		I.10	FB			20%		
		E.1	FM	10%	10%	20%		
		E.2	FB	10%	10%	20%		
		E.15	FMB		10%			
		E.18	FB			20%		
		E.19	FMB	20%				
		E.23	FB			50%		
		E.25	FB	10%		50%		
		A.7	FM	100%	50%	100%		
		A.11	FMB	100%	50%			

		A.15	FMB		50%			
		A.18	FMB			50%		
		A.19	FMB	50%				
		A.23	FMB	50%		50%		
		A.25	FMB			100%		
		A.26	FMB			100%		

Tabla XVI – Amenazas sobre los SI para el HW

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FB	50%	50%	100%		
SOPORTES DE INFORMACION: PAPEL	[SI5] [SI10] [SI14] [SI18] [SI21]	N.1	FMB			100%		
		N.2	FMB			100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.7	FMB			50%		
		I.10	FB			50%		
		E.1	FB	20%	50%	50%		
		E.2	FB	20%	50%	50%		
		E.15	FMB		50%			
		E.18	FmB			50%		
		E.19	FMB	20%				
		A.15	FMB		50%			
		A.18	FMB			50%		
		A.19	FMB	50%				
		A.25	FMB			100%		
		A.26	FMB			100%		

Tabla XVII – Amenazas sobre los SI para el papel

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
			FM	50%	50%	100%		
AUXILIAR GENERAL	[AUX1] [AUX2] [AUX3] [AUX4] [AUX6] [AUX7] [AUX8] [AUX9] [AUX10] [AUX12] [AUX13] [AUX14] [AUX15] [AUX16] [AUX19] [AUX20] [AUX21] [AUX22] [AUX23] [AUX26] [AUX27]	N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FM			100%		
		I.6	FB			100%		
		I.7	FB			100%		
		I.9	FB			100%		
		E.23	FM			50%		
		E.25	FB			100%		
		A.7	FMB	10%	20%	20%		
		A.11	FMB	50%	50%			
		A.23	FMB			100%		
		A.25	FMB			100%		
		A.26	FMB			100%		

Tabla XVIII – Amenazas sobre los auxiliares en general

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
AUXILIAR: PARQUE MÓVIL	[AUX5] [AUX11] [AUX17] [AUX24] [AUX28]		FMB	10%		100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FMB			100%		
		I.6	FMB			100%		
		I.7	FMB			100%		
		I.9	FMB			100%		
		A.23	FMB	10%		100%		
		A.25	FMB	10%		100%		
		A.26	FMB	10%		100%		

Tabla XIX – Amenazas sobre los auxiliares: parque móvil

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
AUXILIAR: MAQUINARIA DEL NEGOCIO	[AUX18] [AUX25]		FMB	10%		100%		
		N.*	FMB			100%		
		I.1	FMB			100%		
		I.2	FMB			100%		
		I.*	FMB			100%		
		I.3	FMB			100%		
		I.4	FMB			100%		
		I.5	FMB			100%		
		I.6	FMB			100%		
		I.7	FMB			100%		
		I.9	FMB			100%		
		A.23	FMB	10%		100%		
		A.25	FMB	10%		100%		
		A.26	FMB	10%		100%		

Tabla XX – Amenazas sobre los auxiliares: maquinaria del negocio

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
PERSONAL DIRECTVO	[P1] [P2] [P3] [P4] [P8] [P9]		FMB	20%	20%	100%		
		E.7	FMB			20%		
		E.19	FMB	20%				
		A.28	FMB			100%		
		A.29	FMB	20%	20%	20%		
		A.30	FMB	20%	20%	20%		

Tabla XXI – Amenazas sobre el personal directivo

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
PERSONAL RESPONSABLE	[P5] [P6] [P10] [P12] [P14]		FMB	20%	20%	100%		
		E.7	FMB			20%		
		E.19	FMB	20%				
		A.28	FMB			100%		
		A.29	FMB	20%	20%	20%		
		A.30	FMB	20%	20%	20%		

Tabla XXII – Amenazas sobre el personal responsable

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
PERSONAL AUXILIAR	[P7] [P11] [P13] [P15]		FA	50%	10%	100%		
		E.7	FM			50%		
		E.19	FM	50%				
		A.28	FA			100%		
		A.29	FMB	10%	10%	10%		
		A.30	FMB	10%	10%	10%		

Tabla XXIII – Amenazas sobre el personal auxiliar

TIPO ACTIVO	ID_ACTIVO	ID_AMENAZA	FRECUENCIA	% IMPACTO X DIMENSION				
				C	I	D	A	T
PERSONAL COMERCIALES	[P16]		FB	50%	10%	100%		
		E.7	FMB			10%		
		E.19	FB	50%				
		A.28	FMB			100%		
		A.29	FMB	10%	10%	10%		
		A.30	FMB	10%	10%	10%		

Tabla XXIV – Amenazas sobre los comerciales

ANEXO XII – PROYECTOS PLANTEADOS A LA DIRECCIÓN

MASEGO S.A.	PROYECTO: Elaborar el plan de continuidad del negocio (PCN)					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-01	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/12/2013	**FECHA FIN PROYECTO**	28/02/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		42.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Puesta a punto efectiva de un PCN para asegurar la continuidad del negocio ante cualquier desastre que pueda ocurrir en cualquier momento, y con el mínimo coste posible.
DESCRIPCIÓN	Con el análisis de riesgos implementado y finalizado y mediante gestión directa del comité de seguridad, encabezado por el responsable de Seguridad, se elaborará el presente plan. Este PCN será revisado anualmente por el comité en base a los resultados anuales de las auditorías internas y reglamentarias.
BENEFICIOS	1. Asegura que el negocio continúe en caso de desastre 2. Asegura una mínima y necesaria inyección económica para su cumplimiento 3. Reduce los costes por inactividad (técnicas, de infraestructura, de TI, etc.) en el negocio 4. Personal preparado y formado para actuar en consecuencia 5. Actualización regular del PCN en un entorno cambiante 6. Conocimiento exhaustivo de los entes responsables sobre cada ítem de la organización
REFERENCIA NORMA ISO 27001	14.1
INDICADOR / ES	1. Verificación cumplimiento del PCN con **frecuencia anual**

	Nombre	**Función**	**Fecha**	**Firma**
REALIZADO POR	Marc Serra	Responsable Seguridad	01/11/2013	

MASEGO S.A.	PROYECTO: Tratamiento de la información de RRHH					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-02	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/03/2013	**FECHA FIN PROYECTO**	31/03/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		12.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Crear, mantener y salvaguardar toda la documentación durante todo el ciclo de vida de todos los empleados; concretamente en lo referente al inicio de su contratación, durante la misma y al finalizar el contrato y salida de la empresa.
DESCRIPCIÓN	En toda nueva relación contractual, desde un buen principio se asignarán los roles y responsabilidades, así como los derechos de todo trabajador, informando verbalmente o por escrito a todos los entes relacionados: responsables, comités, etcétera y por supuesto el mismo trabajador. Para la formación se crea un proyecto independiente (PRO-03) que dependerá de este.
BENEFICIOS	1. Procedimientos bien definidos para el departamento de RRHH 2. Asegurar el cumplimiento de la LOPD 3. Definir un proceso disciplinario para todos los escenarios y perfiles de trabajadores 4. Definición clara de los responsables del tratamiento de los datos de RRHH y aseguramiento de la seguridad de los mismos.
REFERENCIA NORMA ISO 27001	8.1 | 8.3
INDICADOR / ES	1. Verificación de las incidencias generadas por empleados con **frecuencia anual** 2. Verificación de anulaciones de accesos a los SI con empleados con el contrato extinguido, con **frecuencia anual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	04/11/2013	

MASEGO S.A.	PROYECTO: Formación y concienciación de seguridad					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-03	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/04/2014	**FECHA FIN PROYECTO**	30/04/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		10.000 €	**VARIACIÓN PRESUPUESTO**	----	**PRO-02**

OBJETIVOS	Crear y mantener un plan de formación, capacitación y concienciación para todos los empleados.
DESCRIPCIÓN	Cada trabajador según su puesto de trabajo tendrá unas responsabilidades y funciones específicas. La mejora de los conocimientos de los empleados en base al desempeño de sus funciones en el trabajo diario dentro de la organización solo puede reportar beneficios. Para todo ello se creará un presupuesto anual para la formación de los empleados.
BENEFICIOS	1. Definir procesos de formación y capacitación continuada para todos los trabajadores. 2. Mejora de la productividad 3. Mejora en el servicio global de la organización hacia los clientes 4. Mejora en las interacciones entre diferentes departamentos de la empresa
REFERENCIA NORMA ISO 27001	8.2
INDICADOR / ES	1. Verificación de las acciones formativas sobre los empleados con **frecuencia anual** 2. Control de presupuestos destinados a la formación de empleados con **frecuencia anual**

	Nombre	**Función**	**Fecha**	**Firma**
REALIZADO POR	Marc Serra	Responsable Seguridad	05/11/2013	

MASEGO S.A.	PROYECTO: Política de Seguridad de la Información					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-04	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/05/2014	**FECHA FIN PROYECTO**	31/05/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		2.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Mejora de la política de la seguridad de la información existente (creada en la FASE 2 del presente plan director)
DESCRIPCIÓN	Con un conocimiento exhaustivo y realista de todos los requerimientos a nivel de negocio dentro de la compañía crear y mantener una política de seguridad de la información. Por último lugar se realizará un proceso de comunicación de la misma a todos los entes dentro de la organización y las terceras partes con las que se tengan relaciones comerciales o de soporte / servicios de cualquier tipo.
BENEFICIOS	1. Definición clara de las responsabilidades en materia de seguridad de la información 2. Definición de procesos básicos para la seguridad de la información 3. Asegurar la información respecto a las terceras partes 4. Reducción de riesgos 5. Reducción de amenazas 6. Ahorro de costes en tratamiento de riesgos y amenazas
REFERENCIA NORMA ISO 27001	5.1
INDICADOR / ES	1. Verificación de implantación de todos los dominios de la norma ISO 27002 con **frecuencia anual** 2. Verificación del cumplimiento de la política de seguridad dentro de la organización con **frecuencia anual en las auditorías internas**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	06/11/2013	

MASEGO S.A.	PROYECTO: Clasificación de la información					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-05	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/06/2014	**FECHA FIN PROYECTO**	31/07/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		1.700 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Asegurar la información en base a las fuentes que la generan.
DESCRIPCIÓN	La información se genera y se trata dentro de la organización a través de las fuentes de información dentro de los sistemas de la organización. Estas fuentes pueden ser de lo más variada, y para cada una de ellas es necesario una serie de medidas de control y seguridad para el aseguramiento de toda la información.
BENEFICIOS	1. Conocimiento exhaustivo del tipo de información existente o Según su valor económico o Según sus requisitos legales o Según su criticidad 2. Definición clara y por niveles de la seguridad de la información
REFERENCIA NORMA ISO 27001	7.2
INDICADOR / ES	1. Verificación la correcta clasificación de todos los activos con **frecuencia anual** 2. Verificación de cualquier incidencia sobre los activos, con **frecuencia mensual**

	Nombre	**Función**	**Fecha**	**Firma**
REALIZADO POR	Marc Serra	Responsable Seguridad	07/11/2013	

MASEGO S.A.	PROYECTO: Gestión efectiva de los incidentes de la SI					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-06	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/08/2014	**FECHA FIN PROYECTO**	30/09/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		2.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Dos objetivos claramente diferenciados: A. Notificación de los incidentes dentro del SGSI B. Registro para el tratamiento de los incidentes con el objetivo de mitigarlos y aprender de éstos
DESCRIPCIÓN	Por una parte se pretende notificar mediante procedimientos bien definidos todas las incidencias detectadas y por otra parte registrar dichas incidencias con definiciones claras de los responsables del tratamiento de éstas así como los procedimientos para su mitigación y aprendizaje.
BENEFICIOS	1. Procedimientos claros para la gestión de incidentes 2. Responsabilidades claras para la gestión de incidentes según el perfil 3. Aprendizaje en base a las incidencias 4. Registrar todas las incidencias = tener evidencias de lo ocurrido 5. Mayor control sobre las incidencias, mejora el tiempo de respuesta y el conocimiento del equipo o personas encargas de subsanarlas.
REFERENCIA NORMA ISO 27001	13.1 | 13.2
INDICADOR / ES	1. Registro de todas las incidencias que afecten al SGSI con **frecuencia mensual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	08/11/2013	

NOTA: *se tiene en cuenta una parada de 1 mes (Agosto) en concepto de vacaciones del personal que ha de realizar e implementar este proyecto. El tiempo estimado para su implementación será de 1 mes real (dos meses si contamos Agosto).*

MASEGO S.A.	PROYECTO: Cumplimiento de los requisitos legales					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-07	18/10/13	----	0	RESPONSABLE SEGURIDAD & RRHH	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/10/2014	**FECHA FIN PROYECTO**	31/10/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		3.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Asegurar el cumplimiento de la LOPD, asegurar el cumplimiento de los requisitos legales a nivel interno y con terceras partes y asegurar la normativa aplicable a los SGSI mediante las auditorias.
DESCRIPCIÓN	La legislación que aplica un SGSI es extensa y variada. En el caso de MASEGO S.A. teniendo en cuenta que su SGSI abarca toda la organización, se deberá asegurar el cumplimiento de los requisitos legales en todos los departamentos. Se comprobará regularmente mediante las auditorias definidas, asegurando de esta manera su cumplimiento.
BENEFICIOS	1. Asegurar el cumplimiento de la legislación que afecta a toda la organización 2. Se registrarán las incidencias por el no cumplimiento para su posterior tratamiento y final cumplimiento 3. Procesos y metodología bien definida para auditar este tipo de información 4. Responsables de cada tipo de requisitos legales por departamento y zona
REFERENCIA NORMA ISO 27001	15.1 | 15.2 | 15.3
INDICADOR / ES	1. Registro de incidencias respecto al cumplimiento de requisitos legales con **frecuencia anual** 2. Registro de las No Conformidades | Acciones Correctivas | Acciones Preventivas (NC | AC | AP) detectadas en las auditorías sobre los requisitos legales con **frecuencia anual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	11/11/2013	

MASEGO S.A.	PROYECTO: Clasificación de los activos					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-08	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/11/2014	**FECHA FIN PROYECTO**	30/11/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		1.000 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Asegurar una correcta clasificación de los activos por tipo, departamento y responsables directos en toda la organización, detectando posibles errores o dependencias mal definidas para su inmediata solución así como la actualización de los mismos cuando estos se modifican, se crean o se eliminan dentro de la organización.
DESCRIPCIÓN	Los activos se clasifican por tipo. Se crean, modifican y eliminan con cierta regularidad según sea la actividad de la organización. En un momento dado, para un proyecto empresarial específico se pueden crear nuevos activos, o modificar algunos existentes para realizar nuevas funcionalidades y al final de dicho proyecto, es más que posible que esos activos se hayan de eliminar, con lo cual, un control efectivo y actualizado de los activos es esencial para un correcto funcionamiento de los mismos por parte de sus responsables asignados.
BENEFICIOS	1. Definición y establecimiento de una Política de gestión de cambios en los activos 2. Inventariado actualizado de los activos en toda la organización 3. Definición clara de los responsables por cada activo 4. Normas y procedimientos para el uso de los activos (interna y externamente)
REFERENCIA NORMA ISO 27001	7.1
INDICADOR / ES	1. Registro del estado y correcta clasificación de los activos con **frecuencia trimestral** 2. Registro de responsables por activo con **frecuencia semestral** 3. Registro de incidencias del uso (interno / externo) de los activos con **frecuencia mensual**

	Nombre	**Función**	**Fecha**	**Firma**
REALIZADO POR	Marc Serra	Responsable Seguridad	12/11/2013	

MASEGO S.A.	PROYECTO: Aspectos organizativos de la SI					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-09	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/12/2014	**FECHA FIN PROYECTO**	31/12/2014	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		2.500 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Se diferencian dos objetivos según sea el ámbito interno o externo (terceras partes): A. Gestionar la seguridad de la información dentro de la organización B. Mantener la seguridad de la información de la organización y de los dispositivos de tratamiento de la información que son objeto de acceso, procesado, comunicación o gestión por terceros
DESCRIPCIÓN	Se debe afianzar el compromiso de la dirección con la seguridad de la información, definir bien los recursos con los que se cuenta para el tratamiento de la información, coordinar el tratamiento de la información en todos los procesos dentro del SGSI y tener un registro actualizado de los recursos dentro de la organización para el tratamiento de dicha información. En referencia a los terceros, es indispensable realizar un control de acceso a los dispositivos de tratamiento de la información realizando una evaluación de riesgos específica para estos casos.
BENEFICIOS	1. Compromiso de la dirección 2. Coordinación bien definida en todos los procesos dentro de la seguridad de la información 3. Definición clara de los recursos dentro de la organización para el tratamiento de la información 4. Procedimientos de altas, modificaciones y bajas de recursos para el tratamiento de la información 5. Acuerdos de confidencialidad con terceras partes 6. Procedimientos bien definidos para contactar con las autoridades competentes 7. Asegurar la confidencialidad, integridad y autenticidad de la información sea cual sea el tipo de acceso a los datos, información (interno, o terceros)
REFERENCIA NORMA ISO 27001	6.1 | 6.2
INDICADOR / ES	1. Registro y control de incidencias internas para el tratamiento de la información con **frecuencia mensual** 2. Registro y control de incidencias para el tratamiento de la información por terceros con **frecuencia mensual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	13/11/2013	

MASEGO S.A.	PROYECTO: Política del control de acceso					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-10	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/01/2015	**FECHA FIN PROYECTO**	29/02/2015	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		3.300 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Control efectivo y procedimental del acceso a la información
DESCRIPCIÓN	Se debe proteger el acceso a los sistemas de servidores y equipos del personal, para garantizar un acceso protegido y capaz de detectar entradas ajenas al sistema, sin permiso ni aviso.
BENEFICIOS	1. Resultados del análisis de riesgos más fieles a la realidad 2. Mayor control y garantía de acceso para Comerciales (teletrabajo) 3. Impedir accesos no autorizados a los sistemas y al robo de la información, tanto crítica como las de más bajo nivel
REFERENCIA NORMA ISO 27001	11.1 | 11.2 | 11.3 | 11.4 | 11.5 | 11.6 | 11.7
INDICADOR / ES	1. Control de acceso de los SI basados en roles con **frecuencia trimestral** 2. Registro de incidencias en los accesos de los SI con **frecuencia trimestral**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	14/11/2013	

MASEGO S.A.	PROYECTO: Política de mantenimiento de los sistemas de información					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-11	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO	01/03/2015	**FECHA FIN PROYECTO**	31/03/2015	**DEPENDENCIAS**	
	PRESUPUESTO INICIAL	6.500 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA	

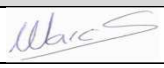
OBJETIVOS	Definición de los aspectos básicos de seguridad en todos los sistemas de información presentes en la organización, con seguimiento en el ciclo de vida de cada uno de ellos, tanto en la adquisición, mantenimiento y retirada de dichos sistemas de información.
DESCRIPCIÓN	Se definirán los procesos y procedimientos de seguridad y los responsables de cada uno de éstos para todos los sistemas de la información. De esta manera se incrementará el nivel de seguridad de los mismos y el buen hacer por parte de sus respectivos responsables.
BENEFICIOS	1. Definición clara de los requisitos en los sistemas de información 2. Tratamiento correcto de las aplicaciones para la entrada / salida de datos 3. Gestión óptima de los controles criptográficos en las aplicaciones que los requieran 4. Procedimientos de control de cambios 5. Revisión de los SI tras cambios en los soportes 6. Restricciones a los cambios en los soportes de información, SW 7. Control y seguridad en las fugas de información 8. Gestión y control óptimo de las vulnerabilidades técnicas 9. La inactividad de los Sistemas de información se reduce considerablemente
REFERENCIA NORMA ISO 27001	12.1 | 12.2 | 12.3 | 12.5 | 12.6
INDICADOR / ES	1. Registro de los sistemas de la información para el cumplimiento de los requisitos de seguridad con **frecuencia trimestral** 2. Registro de incidencias sobre controles criptográficos en uso con **frecuencia trimestral** 3. Registro de incidencias para los soportes de la información **frecuencia trimestral** 4. Registro de incidencias para las vulnerabilidades detectadas en los sistemas de información con **frecuencia mensual** (incluye seguimiento hasta subsanar dichas vulnerabilidades)

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	15/11/2013	

NOTA: *recordemos que el punto **12.4** de la norma no aplica en **MASEGO S.A.***

MASEGO S.A.	PROYECTO: Administración del Software de los equipos personales					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-12	18/10/13	----	0	RESPONSABLE TIC	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/04/2015	**FECHA FIN PROYECTO**	31/07/2015	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		25.500 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Crear procedimientos para la gestión de las operaciones y sus respectivas responsabilidades y responsables de las mismas en base a la dimensión del sistema global (conociendo los límites del mismo). En base a lo anterior, mejorar la seguridad de las aplicaciones de los equipos de trabajo mediante control en la gestión de las redes existentes, incluyendo VPN y el intercambio de información existente entre redes y equipos personales.
DESCRIPCIÓN	De la anterior FASE 3 destaca la falta de seguridad en el SW de los equipos personales, de lo DATOS y SERVICIOS internos y de VPN. Es necesario comenzar con una definición clara de la política y procedimientos para la gestión de operaciones, sus responsables, así como conocer los límites del sistema para poder dar, ofrecer un servicio que de garantías de seguridad. Hasta este momento esto no ha sido así, y el riesgo obtenido para este tipo de activos en la FASE 3 anterior, superaba por mucho el nivel aceptado (<50). Será necesario por tanto proteger el SW de dichos equipos frente al código malicioso y descargable, y además, protección en todos los servicios internos como correo electrónico, entre otros a nivel de redes locales y de VPN para conexión de las sedes por los que corren los DATOS.
BENEFICIOS	1. SSOO seguros 2. Paquetes de SW seguros (Office, Antivirus) 3. Se mejora el nivel de riesgos para el SW de los equipos personales 4. Mejora en la productividad (menos paradas) 5. Resistente a nuevas vulnerabilidades 6. Redes Locales y VPN seguras
REFERENCIA NORMA ISO 27001	10.1 | 10.3 | 10.4 | 10.6 | 10.8
INDICADOR / ES	1. Registro de incidencias SW de servidores y seguimiento con **frecuencia semanal** 2. Registro de incidencias SW de los equipos y seguimiento con **frecuencia mensual** 3. Registro de incidencias tipo: virus, spam, mal/spyware, con **frecuencia mensual** 4. Registro de personal resp. de la seguridad de la información con **frecuencia anual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	18/11/2013	

MASEGO S.A.	PROYECTO: Supervisión de los sistemas de información					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-13	18/10/13	----	0	RESPONSABLE TIC	COMITÉ S.I.
	FECHA INICIO PROYECTO	01/08/2015	**FECHA FIN PROYECTO**	31/08/2015		**DEPENDENCIAS**
	PRESUPUESTO INICIAL	3.700 €	**VARIACIÓN PRESUPUESTO**	----		PRO-12

OBJETIVOS	Mejora del sistema actual de monitorización centralizado en los servidores del CPD con la finalidad de anticiparse a los errores y paradas del sistema a nivel de red (local o VPN)
DESCRIPCIÓN	De la anterior FASE 3 destaca la falta de seguridad en el SW de los equipos personales, de lo DATOS y SERVICIOS internos y de VPN. Con este proyecto se pretende mejorar la monitorización existente de las conexiones de red locales y de VPN para que el departamento de las TIC pueda adelantarse a la caída de los sistemas de información así como determinar el epicentro del error / infección / etc. salvaguardando la seguridad de los datos que navegan por la red y mejorando los servicios existentes. En el PRO-12 marcan los procedimientos, procesos y responsabilidades para estas (monitorización) y otras operaciones (vistas en el PRO-12)
BENEFICIOS	1. Adelantarse a las caídas de los sistemas 2. Procedimientos y responsabilidades bien definidos (PRO-12 según punto 10.1 de la norma) 3. Visualizar en tiempo real y mediante LOGS el origen del problema 4. Mejora del sistema actual de monitorización 5. Centralización del nuevo sistema de monitorización en el CPD 6. Abarca todo el tráfico generado en red interna de todas las sedes y de la VPN 7. Mejora el tiempo de respuesta a paradas no deseadas 8. Mejora por lo tanto la productividad de la organización y empleados
REFERENCIA NORMA ISO 27001	10.10
INDICADOR / ES	1. Registro de incidencias en tiempo real con **frecuencia diaria** 2. Almacenamiento de LOGS para posterior consulta con **frecuencia semanal**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	19/11/2013	

MASEGO S.A.	PROYECTO: Seguridad de los equipos					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-14	18/10/13	----	0	RESPONSABLE TIC	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/09/2015	**FECHA FIN PROYECTO**	30/11/2015	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		2.200 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Evitar cualquier acción dañina sobre los activos y la información que éstos generan o transportan por la red o VPN mediante un control más exhaustivo, relacionando activos con usuarios de manera clara, así como el estado de los mismos.
DESCRIPCIÓN	De la anterior FASE 3 vimos como los SERVICIOS internos y de VPN superaban el valor mínimo de riesgo. Implementando este proyecto, podremos asegurar un mayor control y seguridad en los activos que generan o transportan información vital de la empresa, mitigando riesgos de interceptación de la información en equipos directamente o por red / VPN. Se llevará un control más exhaustivo de los activos asignados al personal, y su estado, con especial atención a la entidad COMERCIALES (que trabajan fuera de las instalaciones: portátiles con conexión 3G para la VPN).
BENEFICIOS	1. Se asegura una protección sobre las amenazas físicas en los equipos 2. Se asegura una protección sobre las amenazas del entorno en los equipos 3. Se asegura la confidencialidad e integridad de la información / datos 4. Se asegura una red libre de amenazas y en todo caso, fácilmente detectable. 5. Se asegura una lista actualizada de activos x empleado, incluyendo el estado de cada uno de esos activos (parado, activo, sustituido, en proceso de destrucción, etcétera) 6. Se asegura un control y verificación de los datos eliminados en equipos a retirar 7. Especial control sobre equipos para el teletrabajo (Comerciales)
REFERENCIA NORMA ISO 27001	9.2
INDICADOR / ES	1. Registro del estado de los equipos con **frecuencia trimestral** 2. Registro de incidencias en los equipos y fuente de las mismas con **frecuencia mensual** 3. Registro de equipos retirados con datos a eliminar y su estado **frecuencia trimestral**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	20/11/2013	

MASEGO S.A.	PROYECTO: Copias de Seguridad					
	CÓDIGO	**FECHA CREACION**	**FECHA REV**	**REV**	**EJECUCIÓN Y DESARROLLO**	**APROBADO POR**
	PRO-15	18/10/13	----	0	RESPONSABLE SEGURIDAD	COMITÉ S.I.
	FECHA INICIO PROYECTO		01/12/2015	**FECHA FIN PROYECTO**	31/12/2015	**DEPENDENCIAS**
	PRESUPUESTO INICIAL		3.500 €	**VARIACIÓN PRESUPUESTO**	----	NINGUNA

OBJETIVOS	Definir una política de copias de seguridad para su ejecución y pruebas de recuperación de las mismas con el fin de asegurar la integridad y disponibilidad de la información.
DESCRIPCIÓN	Se trata de mantener la información integra y disponible en caso de que ocurriera cualquier incidencia, sea leve o grabe. Hasta este momento, los riesgos más importantes se centran en el SW, DATOS y SERVICIOS. Este proyecto, por lo pronto, ayudará a asegurar tanto el SW como los DATOS y por lo tanto a recuperar los SERVICIOS de manera íntegra. Todo ello mediante una política de copias de seguridad bien definida y probada, tanto a nivel de Servidores como Equipos personales y portátiles de Comerciales
BENEFICIOS	12. Asegura la integridad y disponibilidad de los datos 13. Asegura la restauración de sistemas completos de SW y servicios 14. Disminuye el tiempo de inactividad por pérdida de datos 15. Permite mantener el nivel de productividad perdiendo lo mínimo necesario en caso de desastre o emergencia focalizada
REFERENCIA NORMA ISO 27001	10.5
INDICADOR / ES	1. Registro de incidencias en la realización de copias de seguridad **frecuencia trimestral** 2. Registro de incidencias en las restauraciones de prueba con **frecuencia mensual** 3. Registro de incidencias en las restauraciones de emergencia con **frecuencia mensual**

REALIZADO POR	**Nombre**	**Función**	**Fecha**	**Firma**
	Marc Serra	Responsable Seguridad	21/11/2013	

NOTA: *Todos los proyectos definidos se especifican el 18/10/2013 en reunión del comité de seguridad. El responsable de Seguridad los desarrolla en el formato de fichas que acabamos de ver.*

ANEXO XIII – EVALUACIÓN DE LA MADUREZ EN LA AUDITORÍA DE CUMPLIMIENTO

Empezamos con el **5º dominio** de la norma. Podemos ver el resultado en la **tabla I.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
5			**POLÍTICA DE SEGURIDAD**	**0%**	**90%**
5	**1**		**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	**0%**	**90%**
5	1	1	Documento de política de seguridad de la información	0%	**90%**
5	1	2	Revisión de la política de seguridad de la información	0%	**90%**

Tabla I – Valoración madurez 5º dominio de la norma 27002

Seguimos con el **6º dominio** de la norma. Podemos ver el resultado en la **tabla II.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
6			**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**51,25%**	**93,12%**
6	**1**		**ORGANIZACIÓN INTERNA**	**12,5%**	**91,25%**
6	1	1	Comité de gestión de la seguridad de la información	0%	90%
6	1	2	Coordinación de la seguridad de la información	0%	90%
6	1	3	Asignación de responsabilidades en seguridad de la información	0%	90%
6	1	4	Proceso de autorización de recursos para la seguridad de la información	0%	90%
6	1	5	Acuerdos de confidencialidad	50%	95%
6	1	6	Relación con las autoridades	50%	95%
6	1	7	Relación con grupos de interés especial	0%	90%
6	1	8	Revisión independiente de la seguridad	0%	90%
6	**2**		**TERCERAS PARTES**	**90%**	**95%**
6	2	1	Identificación de riesgos relacionados con terceras partes	90%	95%
6	2	2	Requisitos de seguridad en las relaciones con clientes	90%	95%
6	2	3	Requisitos de seguridad en los contratos con terceros	90%	95%

Tabla II – Valoración madurez 6º dominio de la norma 27002

A continuación veremos el **7º dominio** de la norma. Podemos ver el resultado en la **tabla III.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
7			**GESTIÓN DE ACTIVOS**	**90%**	**95%**
7	**1**		**RESPONSABILIDAD DE LOS ACTIVOS**	**90%**	**95%**
7	1	1	Inventario de activos	90%	95%
7	1	2	Propietarios de los activos	90%	95%
7	1	3	Uso aceptable de los recursos	90%	95%
7	**2**		**CLASIFICACIÓN DE LA INFORMACIÓN**	**90%**	**95%**
7	2	1	Guías de clasificación	90%	95%
7	2	2	Marcado y tratamiento de la información	90%	95%

Tabla III – Valoración madurez 7º dominio de la norma 27002

Seguidamente, el **8º dominio** de la norma. Podemos ver el resultado en la **tabla IV.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
8			**SEGURIDAD LIGADA AL PERSONAL**	**16,66%**	**95%**
8	**1**		**ANTES DE LA RELACIÓN LABORAL**	**0%**	**95%**
8	1	1	Roles y responsabilidades	0%	95%
8	1	2	Credenciales	0%	95%
8	1	3	Términos y condiciones del empleo	0%	95%
8	**2**		**DURANTE LA RELACIÓN LABORAL**	0%	**95%**
8	2	1	Responsabilidades de los directores	0%	95%
8	2	2	Concienciación, formación y capacitación en seguridad de la información	0%	95%
8	2	3	Proceso disciplinario	0%	95%
8	**3**		**FINAL O CAMBIO EN LA RELACIÓN LABORAL**	**33,33%**	**95%**
8	3	1	Responsabilidades al finalizar la relación laboral	0%	95%
8	3	2	Devolución de los equipos	50%	95%
8	3	3	Supresión de los derechos de acceso	50%	95%

Tabla IV – Valoración madurez 8º dominio de la norma 27002

Seguimos con el **9º dominio** de la norma. Podemos ver el resultado en la **tabla V.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
9			**SEGURIDAD FÍSICA**	**70,83%**	**93,33%**
9	**1**		**ÁREAS SEGURAS**	**91,66%**	**91,66%**
9	1	1	Perímetro de seguridad física	90%	90%
9	1	2	Control físicos de entrada	90%	90%
9	1	3	Seguridad de oficinas, despachos y salas	90%	90%
9	1	4	Protección contra amenazas externas y ambientales	90%	90%
9	1	5	Trabajo en áreas seguras	90%	90%
9	1	6	Acceso público, zonas de carga y descarga	100%	100%
9	**2**		**SEGURIDAD DE LOS EQUIPOS**	**50%**	**95%**
9	2	1	Instalación y protección de los equipos	50%	95%
9	2	2	Servicios de suministro	50%	95%
9	2	3	Seguridad del cableado	50%	95%
9	2	4	Mantenimiento de los equipos	50%	95%
9	2	5	Seguridad de equipos fuera de los locales propios	50%	95%
9	2	6	Seguridad en la reutilización o eliminación de equipos	50%	95%
9	2	7	Sustracciones de equipos	50%	95%

Tabla V – Valoración madurez 9º dominio de la norma 27002

Toca el **10º dominio** de la norma. Podemos ver el resultado en la **tabla VI.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
10			**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	**9,11%**	**75,64%**
10	**1**		**PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIONES**	**10%**	**95%**
10	1	1	Procedimientos de operaciones documentados	10%	95%
10	1	2	Gestión de los cambios	10%	95%
10	1	3	Segregación de tareas	10%	95%

10	1	4	Separación de los entornos de desarrollo, pruebas y explotación	10%	95%
10	**2**		**GESTIÓN DE LOS NIVELES DE SERVICIOS DE TERCERAS PARTES**	**10%**	**10%**
10	2	1	Niveles de servicio	10%	10%
10	2	2	Monitorizar y revisar los niveles de servicio	10%	10%
10	2	3	Gestión de cambios en los niveles de servicio	10%	10%
10	**3**		**PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS**	**10%**	**95%**
10	3	1	Gestión de capacidades	10%	95%
10	3	2	Aceptación de sistemas	10%	95%
10	**4**		**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL**	**10%**	**95%**
10	4	1	Controles contra software malicioso	10%	95%
10	4	2	Controles contra código móvil	10%	95%
10	**5**		**COPIAS DE RESPALDO**	**10%**	**95%**
10	5	1	Recuperación de la información	10%	95%
10	**6**		**GESTIÓN DE LA SEGURIDAD DE LA RED**	**10%**	**95%**
10	6	1	Controles de red	10%	95%
10	6	2	Seguridad de los servicios de red	10%	95%
10	**7**		**GESTIÓN DE SOPORTES**	**10%**	**10%**
10	7	1	Gestión de soportes extraíbles	10%	10%
10	7	2	Eliminación de soportes	10%	10%
10	7	3	Procedimiento de manejo de soportes	10%	10%
10	7	4	Seguridad de la documentación de los sistemas	10%	10%
10	**8**		**INTERCAMBIO DE INFORMACIÓN**	**2%**	**91%**
10	8	1	Políticas y procedimientos de intercambio de información	0%	90%
10	8	2	Acuerdos de intercambio	0%	90%
10	8	3	Soportes físicos en transito	0%	90%
10	8	4	Correo electrónico	0%	90%
10	8	5	Sistemas de información de productividad	10%	95%
10	**9**		**SERVICIOS DE COMERCIO ELECTRONICO**	**NO APLICA – L6**	
10	9	1	Comercio electrónico		
10	9	2	Transacciones interactivas		
10	9	3	Información con acceso publico		
10	**10**		**MONITORIZACIÓN**	**10%**	**95%**
10	10	1	Trazabilidad	10%	95%
10	10	2	Monitorización del uso de los sistemas	10%	95%
10	10	3	Protección de la trazabilidad	10%	95%
10	10	4	Trazabilidad de los administradores y operadores	10%	95%
10	10	5	Registros de fallos	10%	95%
10	10	6	Sincronización de relojes	10%	95%

Tabla VI – Valoración madurez 10º dominio de la norma 27002

Ahora nos centramos en el **11º dominio** de la norma. Vemos el resultado en la **tabla VII.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
11			**CONTROL DE ACCESO**	**10%**	**95%**
11	**1**		**REQUISITO EMPRESARIAL PARA EL CONTROL ACCESO**	**10%**	**95%**
11	1	1	Política de control de acceso	10%	95%
11	**2**		**GESTIÓN DEL ACCESO DE LOS USUARIOS**	**10%**	**95%**
11	2	1	Registro de usuarios	10%	95%
11	2	2	Gestión de privilegios	10%	95%
11	2	3	Gestión de las contraseñas de los usuarios	10%	95%

11	2	4	Revisión de los derechos de accesos	10%	95%
11	**3**		**RESPONSABILIDAD DE LOS USUARIOS**	**10%**	**95%**
11	3	1	Uso de las contraseñas	10%	95%
11	3	2	Equipo de usuario desatendido	10%	95%
11	3	3	Política de puesto de trabajo despejado y bloqueo de pantalla	10%	95%
11	**4**		**CONTROL DE ACCESO EN LA RED**	**10%**	**95%**
11	4	1	Política de uso de los servicios de red	10%	95%
11	4	2	Autenticación de usuarios para conexiones externas	10%	95%
11	4	3	Identificación de equipos en la red	10%	95%
11	4	4	Protección de los puertos de diagnostico remoto y configuración	10%	95%
11	4	5	Segregaciones de la red	10%	95%
11	4	6	Control de conexión a la red	10%	95%
11	4	7	Control de encaminamiento en la red	10%	95%
11	**5**		**CONTROL DE ACCESO AL SISTEMA OPERATIVO**	**10%**	**95%**
11	5	1	Procedimiento seguro de login	10%	95%
11	5	2	Identificación y autenticación de usuario	10%	95%
11	5	3	Sistema de gestión de contraseñas	10%	95%
11	5	4	Uso de las utilidades de los sistemas operativos	10%	95%
11	5	5	Desconexión automática	10%	95%
11	5	6	Limitación de las ventanas de conexión	10%	95%
11	**6**		**CONTROL DE ACCESO A APLICACIONES E INFORMACIÓN**	**10%**	**95%**
11	6	1	Restricción de acceso a la información	10%	95%
11	6	2	Aislamiento de sistemas sensibles	10%	95%
11	**7**		**INFORMÁTICA MÓVIL Y TELETRABAJO**	**10%**	**95%**
11	7	1	Informática móvil y telecomunicaciones	10%	95%
11	7	2	Teletrabajo	10%	95%

Tabla VII – Valoración madurez 11º dominio de la norma 27002

Vemos ahora el **12º dominio** de la norma. Vemos el resultado en la **tabla VIII.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
12			**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**3,2%**	**91,6%**
12	**1**		**REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN**	**10%**	**95%**
12	1	1	Análisis y especificaciones de requisitos de seguridad	10%	95%
12	**2**		**PROCESO CORRECTO EN LAS APLICACIONES**	**0%**	**90%**
12	2	1	Validación de los datos de entrada	0%	90%
12	2	2	Control del proceso interno	0%	90%
12	2	3	Integridad de los mensajes	0%	90%
12	2	4	Validación de los datos de salida	0%	90%
12	**3**		**CONTROLES CRIPTOGRÁFICOS**	**0%**	**90%**
12	3	1	Política de uso de los controles criptográficos	0%	90%
12	3	2	Gestión de claves	0%	90%
12	**4**		**SEGURIDAD DE LOS FICHEROS DE LOS SISTEMAS**	**NO APLICA – L6**	
12	4	1	Control del software en explotación		
12	4	2	Protección de los datos de prueba		
12	4	3	Control de acceso a los fuentes		
12	**5**		**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**	**6%**	**93%**
12	5	1	Procedimiento de control de cambios	10%	95%
12	5	2	Revisión técnica de las aplicaciones después de cambios en los SSOO	10%	95%
12	5	3	Restricción a los cambios a los paquetes de software	10%	95%
12	5	4	Fuga de información	0%	90%

12	5	5	Desarrollo externalizado de software	0%	90%
12	**6**		**GESTIÓN DE VULNERABILIDADES TÉCNICAS**	**0%**	**90%**
12	6	1	Control de vulnerabilidades técnicas	0%	90%

Tabla VIII – Valoración madurez 12º dominio de la norma 27002

A continuación vemos el **13º dominio** de la norma. Vemos el resultado en la **tabla IX.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
13			**GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN**	**0%**	**95%**
13	**1**		**REPORTE DE INCIDENCIAS Y DEBILIDADES**	**0%**	**95%**
13	1	1	Reporte de eventos de seguridad de información	0%	95%
13	1	2	Reporte de debilidades de seguridad	0%	95%
13	**2**		**GESTIÓN DE INCIDENCIAS DE SEGURIDAD Y MEJORA**	**0%**	**95%**
13	2	1	Responsabilidades y procedimientos	0%	95%
13	2	2	Aprendiendo de las incidencias	0%	95%
13	2	3	Recogida de evidencias	0%	95%

Tabla IX – Valoración madurez 13º dominio de la norma 27002

A punto de acabar, vemos el **14º dominio** de la norma. El resultado en la **tabla X.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
14			**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**	**0%**	**95%**
14	**1**		**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO**	**0%**	**95%**
14	1	1	Incluir la seguridad de la información en el proceso de gestión de la cont. de negocio	0%	95%
14	1	2	Continuidad de negocio y análisis de riesgos	0%	95%
14	1	3	Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la info.	0%	95%
14	1	4	Marco de planificación de la continuidad de negocio	0%	95%
14	1	5	Prueba, mantenimiento y revisión de los planes de continuidad de negocio	0%	95%

Tabla X – Valoración madurez 14º dominio de la norma 27002

Finalmente, vemos el **15º dominio** de la norma. Tenemos el resultado en la **tabla XI.**

N1	N2	N3	TITULO	VALOR FASE 1	VALOR FASE 5
15			**CONFORMIDAD**	**25%**	**95%**
15	**1**		**CONFORMIDAD CON REQUISITOS LEGALES**	**75%**	**95%**
15	1	1	Identificación de la legislación aplicable	90%	95%
15	1	2	Derechos de propiedad intelectual	90%	95%
15	1	3	Salvaguarda de los registros de la Organización	90%	95%
15	1	4	Protección de datos de carácter personal y privacidad	90%	95%
15	1	5	Prevención del mal uso de los recursos informáticos	90%	95%
15	1	6	Regulación de controles criptográficos	0%	95%
15	**2**		**CONFORMIDAD CON LAS DIRECTRICES DE SEGURIDAD Y REVISIONES TÉCNICAS**	**0%**	**95%**
15	2	1	Conformidad con las políticas de seguridad y estándares	0%	95%
15	2	2	Comprobación de la conformidad técnica	0%	95%
15	**3**		**CONSIDERACIONES SOBRE EL AUDIT DE SISTEMAS DE INFORMACIÓN**	**0%**	**95%**
15	3	1	Controles de auditoría de los sistemas de información	0%	95%
15	3	2	Protección de las herramientas de auditoría de sistemas de información	0%	95%

Tabla XI – Valoración madurez 15º dominio de la norma 27002

ANEXO XIV – FICHAS DE NO CONFORMIDAD AUDITORÍA DE CUMPLIMIENTO

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27001:2005		**FECHA**	7 de Enero del 2016
	PERSONA AUDITADA	Manel Folch Flor		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Sede Central & CPD de Barcelona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC01_07012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.2 o 10.2.1 o 10.2.2 o 10.2.3	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. No existe una gestión y procedimientos documentales para comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Manel Folch Flor como responsable de la sede de Barcelona & CPD asume el error, pero justifica este hecho dando a entender que dichos procedimientos los realiza en el día a día, pero que efectivamente no hay registro alguno ni documentos procedimentales que lo sustenten.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se debería comprobar que los **controles de seguridad, las definiciones de los servicios y los niveles de provisión**, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. **2.** Los servicios, informes y registros proporcionados por un tercero **deberían ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorias periódicas** **3.** Se deberían **gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes,** teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	**FECHA REVISION**	10/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	15/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	7 de Enero del 2016
	PERSONA AUDITADA	Manel Folch Flor		**ÁREA**	Tecnologías de la información IT
	LUGAR AUDITADO	Sede Central & CPD de Barcelona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC02_07012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.7 o 10.7.1 o 10.7.2 o 10.7.3 o 10.7.4	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Los soportes deberían ser controlados y protegidos físicamente. Deberían establecerse procedimientos operativos apropiados para proteger los documentos, los soportes informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Manel Folch Flor como responsable de la sede de Barcelona & CPD asume el error, ningún otro tipo de comentario.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían establec**er procedimientos para la gestión de los soportes extraíbles**. **2.** Los soportes deberían ser **retirados de forma segura** cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. **3.** Deberían establecerse **procedimientos para la manipulación y el almacenamiento de la información**, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **4.** La **documentación** del sistema debería estar **protegida contra accesos no autorizados.**	**FECHA REVISION**	10/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	15/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	21 de Enero del 2016
	PERSONA AUDITADA	Julio Cortada Rubio		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Subsede Madrid			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC03_21012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.2 o 10.2.1 o 10.2.2 o 10.2.3	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. No existe una gestión y procedimientos documentales para comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Julio Cortada Rubio como responsable de la subsede de Madrid asume el error pero hace un comentario dando a entender estos procedimientos los realiza en el día a día, pero que efectivamente no hay registro alguno ni documentos procedimentales que lo sustenten.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se debería comprobar que los **controles de seguridad, las definiciones de los servicios y los niveles de provisión**, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. **2.** Los servicios, informes y registros proporcionados por un tercero **deberían ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorias periódicas** **3.** Se deberían **gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes,** teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	**FECHA REVISION**	11/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	22/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	21 de Enero del 2016
	PERSONA AUDITADA	Julio Cortada Rubio		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Subsede Madrid			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC04_21012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.7 o 10.7.1 o 10.7.2 o 10.7.3 o 10.7.4	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Los soportes deberían ser controlados y protegidos físicamente. Deberían establecerse procedimientos operativos apropiados para proteger los documentos, los soportes informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Julio Cortada Rubio como responsable de la subsede de Madrid asume el error. Comenta que la experiencia en su puesto hace que mecánicamente se lleven a cabo estos procedimientos, y que no necesita tenerlos escritos.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían establec**er procedimientos para la gestión de los soportes extraíbles**. **2.** Los soportes deberían ser **retirados de forma segura** cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. **3.** Deberían establecerse **procedimientos para la manipulación y el almacenamiento de la información**, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **4.** La **documentación** del sistema debería estar **protegida contra accesos no autorizados.**	**FECHA REVISION**	11/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	22/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	18 de Enero del 2016
	PERSONA AUDITADA	Josep Girona Trias		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Almacén de Badalona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC05_18012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.2 o 10.2.1 o 10.2.2 o 10.2.3	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. No existe una gestión y procedimientos documentales para comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Josep Girona Trias como responsable del almacén de Badalona asume el error. No entiende ni comparte la necesidad de establecer procedimientos y menos registrar este tipo de actuaciones.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se debería comprobar que los **controles de seguridad, las definiciones de los servicios y los niveles de provisión**, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. **2.** Los servicios, informes y registros proporcionados por un tercero **deberían ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorias periódicas** **3.** Se deberían **gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes,** teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	**FECHA REVISION**	12/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	20/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	18 de Enero del 2016
	PERSONA AUDITADA	Josep Girona Trias		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Almacén de Badalona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC06_18012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.7 o 10.7.1 o 10.7.2 o 10.7.3 o 10.7.4	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Los soportes deberían ser controlados y protegidos físicamente. Deberían establecerse procedimientos operativos apropiados para proteger los documentos, los soportes informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Josep Girona Trias como responsable del almacén de Badalona asume el error. Pero no entiende que necesidad hay para establecer estos procedimientos.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían establecer **procedimientos para la gestión de los soportes extraíbles.** **2.** Los soportes deberían ser **retirados de forma segura** cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. **3.** Deberían establecerse **procedimientos para la manipulación y el almacenamiento de la información**, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **4.** La **documentación** del sistema debería estar **protegida contra accesos no autorizados.**	**FECHA REVISION**	12/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	20/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	26 de Enero del 2016
	PERSONA AUDITADA	Rubén Clarín Martin		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Almacén de Madrid			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC07_26012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.2 o 10.2.1 o 10.2.2 o 10.2.3	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. No existe una gestión y procedimientos documentales para comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Rubén Clarín Martin como responsable del almacén de Madrid asume el error. Hace caso omiso a las explicaciones incluyendo gestos y burlas.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se debería comprobar que los **controles de seguridad, las definiciones de los servicios y los niveles de provisión**, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. **2.** Los servicios, informes y registros proporcionados por un tercero **deberían ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorias periódicas.** **3.** Se deberían **gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes,** teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	**FECHA REVISION** **RESPONSABLE EJECUCION AC** **FIRMA TRAS REVISIÓN**	13/07/2016 Marc Serra Gordo

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	29/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	26 de Enero del 2016
	PERSONA AUDITADA	Rubén Clarín Martin		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Almacén de Madrid			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC08_26012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.7 o 10.7.1 o 10.7.2 o 10.7.3 o 10.7.4	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Los soportes deberían ser controlados y protegidos físicamente. Deberían establecerse procedimientos operativos apropiados para proteger los documentos, los soportes informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Rubén Clarín Martin como responsable del almacén de Madrid asume el error. No entiende las necesidades ni quiere escucharlas.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían establec**er procedimientos para la gestión de los soportes extraíbles**. **2.** Los soportes deberían ser **retirados de forma segura** cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. **3.** Deberían establecerse **procedimientos para la manipulación y el almacenamiento de la información**, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **4.** La **documentación** del sistema debería estar **protegida contra accesos no autorizados.**	**FECHA REVISION**	13/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	29/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	25 de Enero del 2016
	PERSONA AUDITADA	Julio Cortada Gómez		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Comerciales			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC09_25012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.2 o 10.2.1 o 10.2.2 o 10.2.3	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros. No existe una gestión y procedimientos documentales para comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Julio Cortada Gómez como responsable del equipo de comerciales asume el error. Comenta que no tenía conocimiento sobre estas necesidades ni tampoco qué nivel de responsabilidad puede tener en estos temas.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se debería comprobar que los **controles de seguridad, las definiciones de los servicios y los niveles de provisión**, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. **2.** Los servicios, informes y registros proporcionados por un tercero **deberían ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorias periódicas** **3.** Se deberían **gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes,** teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	**FECHA REVISION** **RESPONSABLE EJECUCION AC** **FIRMA TRAS REVISIÓN**	14/07/2016 Marc Serra Gordo

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	25/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	25 de Enero del 2016
	PERSONA AUDITADA	Julio Cortada Gómez		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Comerciales			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC10_25012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	10º Dominio • Punto 10.7 o 10.7.1 o 10.7.2 o 10.7.3 o 10.7.4	**HECHOS Y DATOS ADJUNTOS**	- Índice de documentos entregados - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Los soportes deberían ser controlados y protegidos físicamente. Deberían establecerse procedimientos operativos apropiados para proteger los documentos, los soportes informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Julio Cortada Gómez como responsable del equipo de comerciales asume el error. Comenta que no tenía conocimiento sobre estas necesidades ni tampoco qué nivel de responsabilidad puede tener en estos temas.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían establec**er procedimientos para la gestión de los soportes extraíbles**. **2.** Los soportes deberían ser **retirados de forma segura** cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. **3.** Deberían establecerse **procedimientos para la manipulación y el almacenamiento de la información**, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. **4.** La **documentación** del sistema debería estar **protegida contra accesos no autorizados.**	**FECHA REVISION** **RESPONSABLE EJECUCION AC** **FIRMA TRAS REVISIÓN**	14/07/2016 Marc Serra Gordo

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	25/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	19 de Enero del 2016
	PERSONA AUDITADA	Josep Girona Trias		**ÁREA**	Seguridad Física
	LUGAR AUDITADO	Almacén de Badalona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC11_19012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	9º Dominio • Punto 9.1 o 9.1.6	**HECHOS Y DATOS ADJUNTOS**	- Documentación del SGSI - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	No existe un control de los puntos de acceso tales como las áreas de carga y descarga. Ello implica que el personal no autorizado puede acceder a las instalaciones con impunidad y libertad. Estos puntos de acceso están solapados con las instalaciones de tratamiento de la información (sala del servidor y equipos personales, firewall, etc.) y la circulación de personas sin control alguno.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Josep Girona Trias como responsable del almacén de Badalona no tiene justificación y no entiende como ha ocurrido. Recuerda una reunión que hubo con el comité de seguridad para paliar esta situación pero por alguna razón que desconoce o no recuerda en este momento, no sabe por qué no se han implantado las medidas necesarias.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1.** Se deberían **restringir los accesos al área de carga y descarga desde el exterior** sólo para el personal autorizado e identificado **2.** El área de carga y descarga se debería diseñar de tal manera que los suministros puedan **descargarse sin que el personal de descarga tenga que acceder a otras zonas del edificio** **3.** La **puertas externas** de un área de carga y descara deberían estar **cerradas cuando las puertas internas estén abiertas** **4.** El **material entrante** debería ser **inspeccionado** para evitar amenazas potenciales antes de trasladarlo desde el área de carga y descarga hasta su lugar de utilización **5.** El material entrante debería **registrarse de acuerdo a los procedimientos de gestión de activos** al entrar en la instalación **6.** Cuando sea posible, se debería **separar físicamente la entrada y la salida de envíos.**	**FECHA REVISION**	15/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	20/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Josep Reig Freixes
	NORMATIVA	ISO 27002:2005		**FECHA**	12 de Enero del 2016
	PERSONA AUDITADA	Marc Serra Gordo		**ÁREA**	TIC
	LUGAR AUDITADO	Sede Central & CPD de Barcelona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC12_12012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	7º Dominio • Punto 7.2 o 7.2.2	**HECHOS Y DATOS ADJUNTOS**	- Documentación del SGSI - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Aun con la existencia de los procedimientos para etiquetar y manejar la información en los formatos físicos (esta NC no afecta al formato electrónico), de acuerdo con el esquema de clasificación adoptado por la organización, se constata que el etiquetado es incorrecto, y en la mayoría de los casos inexistente. Así mismo, el registro de control de formatos físicos no concuerda.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Marc Serra Gordo como responsable de las TIC y CPD comenta que está al corriente de este suceso, y que están trabajando en ello. Comenta que desde hace un mes aproximadamente, ha habido actualizaciones de un 35% del total de los soportes físicos y que ha día de hoy queda un 15% por etiquetar. Finalmente acepta la gravedad de esta situación pero ratifica estar al tanto y trabajando sobre ello.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1. Finalizar el etiquetado** lo antes posible. **2. Actualizar el registro** de control para los formatos físicos	**FECHA REVISION**	15/07/2016
		RESPONSABLE EJECUCION AC	Josep Reig Freixes
		FIRMA TRAS REVISIÓN	

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Josep Reig Freixes	Jefe de administradores de Sistemas	15/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	13 de Enero del 2016
	PERSONA AUDITADA	Robert Cau Giralt		**ÁREA**	Seguridad Física de las sedes
	LUGAR AUDITADO	Sede Central & CPD de Barcelona			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC13_13012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	14º Dominio • Punto 14.1 o 14.1.5	**HECHOS Y DATOS ADJUNTOS**	- Planes de Continuidad del Negocio - Verificación visual - Entrevista
DESCRIPCIÓN DE LA/S NC	Los planes de continuidad del negocio deberían **probarse y actualizarse** periódicamente para asegurar que están al día y que son efectivos. Existe plan de pruebas pero no se ha realizado prueba alguna en ninguna de las sedes ni entes (comerciales). No existe un registro.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Robert Cau Giralt como responsable de la Seguridad física y PRL comenta que está perfectamente enterado. Muestra informes con actas de reunión con las fechas asignadas para realizar las pruebas en todas y cada una de las sedes así como los entes de los comerciales. Efectivamente las fechas asignadas son posteriores a la actual; no obstante estas pruebas deberían estar hechas a estas alturas.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1. Realizar las pruebas definidas** en los procedimientos ya establecidos. **2. Cumplir las fechas** dejando el tiempo necesario para una posible reevaluación cuando proceda. **3. Registrar** las pruebas realizadas en todas las sedes.	**FECHA REVISION**	16/07/2016
		RESPONSABLE EJECUCION AC	Marc Serra Gordo
		FIRMA TRAS REVISIÓN	

	NOMBRE	**CARGO**	**FECHA**	**FIRMA**
CREADO POR	Marc Serra Gordo	Responsable Seguridad Información	15/01/2016	

MASEGO S.A.					
	TIPO DE AUDITORÍA	Inicial e Interna		**AUDITOR**	Marc Serra Gordo
	NORMATIVA	ISO 27002:2005		**FECHA**	27 de Enero del 2016
	PERSONA AUDITADA	Javier Soto Mayor		**ÁREA**	Gestión de la Seguridad de la Información
	LUGAR AUDITADO	Almacén de Madrid			
	TIPO DE NC	**MAYOR**	**MENOR**	**ID_NC**	**NC14_27012016_SGSI**

REFERENCIA NORMATIVA NO CUMPLIDA	5º Dominio • Punto 5.1 o 5.1.1	**HECHOS Y DATOS ADJUNTOS**	- Política del SGSI - Entrevista
DESCRIPCIÓN DE LA/S NC	La política de seguridad de la información debería ser comunicada a toda la organización, llegando hasta los destinatarios en una forma que sea apropiada, entendible y accesible al lector al que va dirigida. En este caso el desconocimiento es por parte de los mozos, los responsables saben y muestran correctamente la ubicación y contenido de dicha política de seguridad.		
TESTIMONIO DEL AUDITADO	El auditado, el Sr. Javier Soto Mayor en funciones de mozo de almacén, no puede responder. Busca sin saber donde exactamente. Finalmente asegura que él y sus compañeros desconocen dónde está el documento con la política de seguridad, así como su contendido.		
ACCION/ES CORRECTIVAS PROPUESTAS	**1. Asegurar** por parte de los trabajadores que éstos tienen **acceso inmediato y conocimiento total** de la política de seguridad. **2. Establecer y fijar** físicamente dicha política de seguridad en un **lugar visible y accesible**. **3. Implicar más al personal. Registrar** jornadas de concienciación.	**FECHA REVISION** **RESPONSABLE EJECUCION AC** **FIRMA TRAS REVISIÓN**	17/07/2016 Marc Serra Gordo

CREADO POR	**NOMBRE**	**CARGO**	**FECHA**	**FIRMA**
	Marc Serra Gordo	Responsable Seguridad Información	29/01/2016