# Plan Director de Seguridad de la Información para una compañía de telemarketing

**Nombre estudiante:** Dunia Meler Pascual

**Programa:** Máster Universitario en Seguridad de les Tecnologías de la Información y de las Comunicaciones (MISTIC)

**Nombre Consultor:** Arsenio Tortajada Gallego

**Centro:** Universitat Oberta de Catalunya

**Fecha entrega:** 7 de junio de 2017

**AGRADECIMIENTOS**

*A Jesús,*
*por el apoyo incondicional, por darme constantemente ánimo y creer en mí.*
*Gracias por estar a mi lado.*

*A mi familia,*
*por su compresión durante la duración de este máster.*
*Gracias por vuestra paciencia.*

*A Maribel,*
*por el apoyo, por todos sus buenos consejos, con este máster y en el día a día,*
*te echaré de menos como compañera de trabajo.*
*Gracias amiga.*

*A Roberto,*
*grandísimo compañero de trabajo, por estar siempre ahí intentando ayudar,*
*echaré mucho de menos tu mano amiga siempre cerca.*
*Gracias amigo.*

*A los amigos,*
*por su comprensión y apoyo,*
*y por todos los momentos que han tenido que ser aplazados.*
*Gracias por estar siempre ahí.*

*A Arsenio,*
*consultor de este trabajo.*
*Gracias por tus indicaciones y consejos.*

*Sin todos vosotros hoy este trabajo no sería una realidad.*
*Gracias a todos, de corazón.*

**FICHA DEL TRABAJO FINAL**

| | |
|---|---|
| **Título del trabajo:** | *Plan Director de Seguridad de la Información para una compañía de telemarketing* |
| **Nombre del autor:** | *Dunia Meler Pascual* |
| **Nombre del consultor:** | *Arsenio Tortajada Gallego* |
| **Fecha de entrega (mm/aaaa):** | *06/2017* |
| **Área del Trabajo Final** | *Sistemas de Gestión de la Seguridad de la Información* |
| **Titulación:** | *Máster Universitario en Seguridad de les Tecnologías de la Información y de les Comunicaciones (MISTIC)* |


**Resumen del Trabajo:**

En la actualidad, son numerosos los riesgos a los que los datos y la información de las organizaciones están expuestos a diario en el desarrollo de sus actividades de negocio. Siendo la información uno de los principales activos de las organizaciones, es primordial preservarla para asegurar la continuidad y el desarrollo del negocio, además de cumplir con las exigencias legales, dando credibilidad y garantías a clientes y proveedores.

La implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) es el medio más eficaz para minimizar riesgos, identificar y valorar activos y sus riesgos, considerando el impacto para la organización y poder ejecutar proyectos y planes de acción destinados a reducir el impacto.

Este trabajo describe la realización de un Plan Director de Seguridad, para una compañía de telemarketing (TMK S.A.), basado en la norma internacional, ampliamente reconocida y certificable ISO/IEC 27001:2013 y en la norma ISO/IEC 27002:2013, siendo esta última una guía de buenas prácticas que describe los objetivos de control y controles recomendados.

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, mantener y mejorar un SGSI según el ciclo de Deming (Planificar, Hacer, Verificar y Actuar).

En la compañía TMK S.A. hasta el momento actual se había trabajado en mejorar la seguridad, pero sin implementar un SGSI.

**Abstract:**

Nowadays, there are numerous risks to which organizations' data are exposed daily in the development of their business activities. Since data is one of the main assets of organizations, it is essential not only to protect it in order to ensure business continuity and development, but also to comply with legal requirements, offering credibility and guarantees to customers and suppliers.

Implementing an Information Security Management System (ISMS) is the most effective way of minimizing risks, identifying and assessing assets and their risks, taking into account the impact on the organization, and being able to execute projects and action plans aimed at reducing the impact.

This work describes the elaboration of a Security Master Plan for a telemarketing company (TMK SA), based on the widely known and certifiable international standards ISO/IEC 27001: 2013 and ISO/IEC 27002: 2013, being the latter the best practices guide describing the control objectives and recommended controls.

ISO/IEC 27001 specifies the requirements to establish, implement, maintain and improve an ISMS according to the Deming Cycle (Plan, Do, Check and Act –PDCA-).

Up to date the company TMK S.A. has made efforts to improve security, however, an ISMS has never been implemented.

**Palabras clave**

Sistemas de Gestión de Seguridad de la Información · Plan Director de Seguridad · Norma ISO/IEC 27001 · Norma ISO/IEC 27002 · MAGERIT · Análisis de riesgos · Auditoría

# ÍNDICE



# Lista de figuras

# Lista de tablas

# 1. Introducción

## 1.1. Contexto y justificación del Trabajo

TMK S.A. es una compañía de telemarketing dedicada a prestar servicios de esta índole a clientes. Es de gran importancia la credibilidad en materia de seguridad, puesto que para desarrollar su actividad de negocio se manejan datos e información de terceros proporcionada por los clientes. En ocasiones los datos e información manejada es información de nivel alto de seguridad.

La compañía TMK S.A. ha estado trabajando intensivamente en la seguridad de la información, pero hasta el momento no tiene implementado un Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de asegurar la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad a sus clientes. El primer paso es la implantación del SGSI y posteriormente puede proceder con proceso de certificación.

En este trabajo se ha realizado un Plan Director de Seguridad de la Información para la compañía TMK S.A. con el fin de implantar un SGSI que aportará credibilidad y garantías a los clientes y proveedores. La implantación del SGSI se ha realizado en base a las normas UNE ISO/IEC 27001:2013 y UNE ISO/IEC 27002:2013 de reconocimiento internacional y que aplican a todo tipo de organizaciones.

## 1.2. Objetivos del Trabajo

Este Trabajo Final de Master (especialidad en Sistemas de Gestión de la Seguridad de la Información) tiene como objetivo establecer las bases para la realización del Plan Director de una empresa, basado en el proceso de mejora continua en materia de Seguridad de la Información, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones pertinentes para minimizar el impacto potencial de los riesgos, mejorando la seguridad de la organización de forma global.

La realización de este trabajo conlleva los siguientes objetivos concretos:

- Descripción sintetizada y clara de la compañía objeto de estudio.
- Definición del alcance del SGSI.
- Elaboración de documentos asociados al SGSI.
- Elaboración de análisis diferencial y de riesgos.
- Proposición de proyectos para mejorar la seguridad.
- Realización auditoría interna de cumplimiento.
- Elaboración de un resumen ejecutivo.
- Presentación del trabajo final.

## 1.3. Enfoque y método seguido

Este trabajo se enmarca bajo las normas internacionales ISO/IEC 27001, con el apoyo de los controles de la ISO/IEC 27002. Esta es la normativa de referencia para toda organización que desee alinear sus objetivos y principios de la Seguridad de la Información a la normativa internacional.

En cuanto a la metodología seguida, se ha seguido la división por fases propuesta por el consultor de este trabajo, de forma que finalizada la última fase queda completado el trabajo. La división en fases está basada en el Ciclo de *Deming* o ciclo PDCA (del inglés *Plan-Do-Check-Act*)[1]. Es una estrategia de mejora continua muy utilizada en los SGSI. Los resultados de la implementación del Ciclo de *Deming* permiten a las organizaciones una mejora integral en competitividad, calidad, productividad, etc. reduciendo los costes.

En la fase 3 del trabajo, correspondiente al análisis de riesgos, se ha utilizado la metodología MAGERIT [1] de análisis de riesgos.

## 1.4. Planificación del Trabajo

Las fases en las que se ha dividido el trabajo son las siguientes:

- FASE 1: Situación actual: contextualización, objetivos y análisis diferencial
- FASE 2: Sistema de gestión documental
- FASE 3: Análisis de riesgos
- FASE 4: Propuesta de proyectos
- FASE 5: Auditoría de cumplimiento de la ISO/IEC 27002:2013
- FASE 6: Presentación de resultados y entrega de informes.

## 1.5. Breve sumario de productos obtenidos

Tras la ejecución de cada una de las fases citadas, se han obtenido los siguientes productos:

- Informe de análisis diferencial
- Esquema documental ISO/IEC 27001:2013
- Análisis de riesgos
- Plan de proyectos
- Auditoría de cumplimiento
- Presentación de resultados.

[1] PDCA (*Plan-Do-Check-Act):* Planificar-Hacer-Verificar-Actuar

## 1.6. Breve descripción de los otros capítulos de la memoria

**Capítulo 2: FASE 1: Situación actual: contextualización, objetivos y análisis diferencial**
Introducción al proyecto. Descripción de la empresa objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y análisis diferencial de la empresa respecto las normas ISO/IEC 27001 y ISO/IEC 27002.

**Capítulo 3: FASE 2: Sistema de gestión documental**
Elaboración de la política de seguridad, declaración de aplicabilidad y documentación del SGSI.

**Capítulo 4: FASE 3: 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.

**Capítulo 5: FASE 4: Propuesta de proyectos**
Evaluación de proyectos que es necesario llevar a cabo para alinear la compañía con los objetivos planteados en el Plan Director. Cuantificación económica y temporal.

**Capítulo 6: FASE 5: Auditoría de cumplimiento de la ISO/IEC 27002:2013**
Evaluación de controles, madurez y nivel de cumplimiento.

**Capítulo 7: FASE 6: 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 la Dirección. Entrega del proyecto final.

# 2. FASE 1: Situación actual: contextualización, objetivos y análisis diferencial

## 2.1. Contextualización

**Empresa TMK S.A:** La empresa escogida para la realización de este trabajo se trata de una empresa de telemarketing: TMK S.A (el nombre de la empresa no es real). La empresa TMK es una compañía líder en servicios de *Customer Relationship Management* (CRM) y *Business Process Outsourcing* (BPO).

Breve descripción actual de TMK S.A.

- Las oficinas centrales se encuentran sitas en Madrid.
- Dispone de instalaciones de *Contact Center* en 14 ciudades españolas; Madrid, Barcelona, Sevilla, Valencia, Bilbao, entre otras.
- La plantilla de la compañía la componen más de 10.000 empleados.
- En sus instalaciones dispone de más de 5000 puestos de trabajo físicos.
- Sus clientes proceden de diferentes sectores: banca, compañías de telecomunicaciones, compañías energéticas, compañías petroleras, administraciones públicas, etc.
- La compañía oferta a sus clientes diferentes servicios: Servicios de Atención al Cliente (SAC), Ventas, Recobros, *Back Office,* Soporte Técnico, etc.
- Su Centro de Proceso de Datos (CPD) se encuentra externalizado en un Centro de datos proveedor.

**Organigrama de TMK S.A.**

A continuación se muestra el organigrama de la compañía a alto nivel, mostrando sólo direcciones y gerencias en las que se divide cada dirección debido a la gran extensión de algunas de ellas:

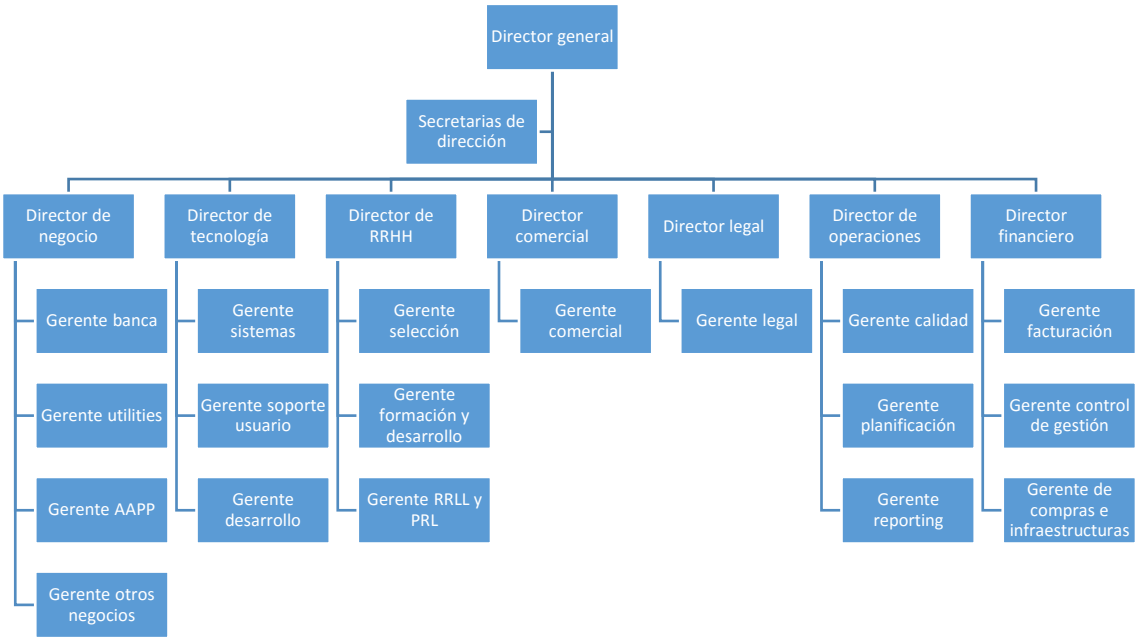


**Figura 1:** Organigrama de la compañía TMK S.A. (Fuente: Propia)

Comité de dirección: el comité de dirección está compuesto por el director general y por todos los directores que dependen de él jerárquica y funcionalmente. El comité de dirección será quien definirá la estrategia de la compañía y tomará las decisiones finales.

Secretarias de dirección: se ocupan de dar soporte y asistencia a los miembros del comité de dirección (director general y directores de áreas).

Dirección de negocio: la dirección de negocio se ocupa de las relaciones con los clientes, y de llevar a cabo los servicios contratados. Cada gerencia se ocupa de un tipo o grupo de clientes.

Dirección de tecnología: la dirección de tecnología gestiona el departamento técnico: soporte a usuarios y clientes, desarrollo de aplicaciones y soluciones, gestión de los sistemas, etc.

Dirección de RRHH: la dirección de recursos humanes gestiona todos los asuntos relacionados con las personas que integran la compañía: selección de personas, formación y desarrollo de las personas, relaciones laborales (RRLL), prevención de riesgos laborales (PRL), etc.

Dirección comercial: la dirección comercial se ocupa de la actividad comercial de la compañía.

Director legal: la dirección legal se ocupa de todos los asuntos legales de la compañía. Tanto internos como con los clientes.

Director de operaciones: gestiona la calidad, reporte y planificación de las operaciones de la compañía.

Director financiero: la dirección de finanzas gestiona la parte financiera de la compañía: presupuestos, compras, infraestructuras, facturación a clientes, etc.

La organización de la compañía es compleja debido a su extensión. A continuación se detalla en el siguiente gráfico la organización de la dirección de tecnología, donde se engloba el departamento de seguridad integrado únicamente por dos personas: el jefe de seguridad y un técnico de seguridad.

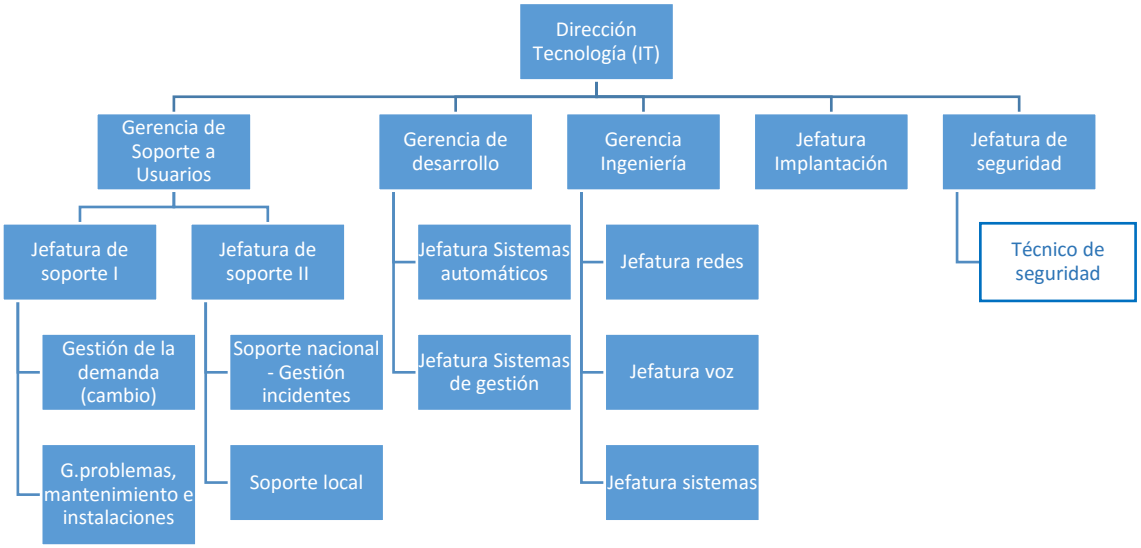


**Figura 2**: Organigrama de la dirección de tecnología de TMK S.A. (Fuente: Propia)

### Ubicaciones físicas

Todos los centros de TMK S.A. cuentan con similar estructura, por lo que se describirá a continuación la estructura tipo según la cual están diseñados todos sus centros de trabajo.

A excepción del edificio en el que se encuentran las oficinas centrales, todos los centros de trabajo están distribuidos en una única planta.

Centros de trabajo:

- Cuentan con un acceso único con un auxiliar de seguridad que hace las funciones de recepcionista a su vez.
- Todos los centros cuentan con alarma conectada con una central de alarmas y con la policía.
- Cada centro dispone de un pequeño Centro de Proceso de Datos (CPD) dedicado a albergar la infraestructura técnica y de telecomunicaciones de cada centro se encuentra restringido el acceso mediante un lector de tarjetas. Sólo el

personal técnica y de seguridad están habilitados a acceder. Junto al CPD se encuentra la sala de trabajo de los técnicos.

- El resto del personal del centro se distribuye en espacios abiertos.
- También hay salas de formación y reuniones.

Edificio de oficinas centrales:

- Sus instalaciones están distribuidas en 6 plantas de un edificio donde hay más empresas.
    - Planta 0, salas de formación y reuniones.
    - Planta 1, se encuentra la recepción y el auxiliar de seguridad. También se encuentra el área técnica y una zona de trabajo de telemarketing
    - Planta 2, 3 y 5, zona exclusiva de trabajo de telemarketing
    - Planta 5, zona de trabajo de personal comercial, RRHH, finanzas, operaciones, legal, etc. en espacios abiertos. También se ubican los despachos de los directores y salas de reuniones.

**Infraestructura técnica**

Los diferentes centros de trabajo de la compañía y el CPD externo se encuentran interconectados mediante red de datos MPLS[2]. La principal infraestructura de Tecnologías de la Información (TI) se concentra en el CPD externo en un entorno de alta disponibilidad TIER IV[3]. En el resto de centros de trabajo residen a parte de los equipos de red locales, equipos de supervivencia en caso de fallo de comunicaciones.

Clasificación TIER: El TIER de un CPD es una clasificación de 4 categorías, en función del nivel de redundancia de los componentes que soportan el Centro de Datos [2].

Los sistemas de la compañía son de última generación y algunas de sus características son:

- Basados en tecnología digital, con sistemas de alta fiabilidad y procesadores duplicados.

[2] MPLS: *Multi Protocol Label Switching* - Conmutación Multi-Protocolo mediante Etiquetas. MPLS está reemplazando rápidamente a *Frame Relay* y ATM (Modo de Transferencia Asíncrona) como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costes generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.

[3] TIER IV: clasificación más exigente, con múltiples redundancias eléctricas y de refrigeración. Disponibilidad del 99,995% (sólo puede dejar de funcionar 26 minutos en un año).

- Sistemas modulares, estructurados, programables, flexibles y ampliables que permite la adaptación a las necesidades de los centros de llamadas.

- Capacidad de gestión de múltiples centros de llamadas, ante la necesidad de interconexión de varias centralitas telefónicas.

- Dispone de licencias ACD[4] disponibles para poder seguir sumando puestos de trabajo.

- Mediante de la funcionalidad de "agente experto", se distribuyen las llamadas a los agentes o grupos de agentes, según *skill* (habilidad) o criterios específicos (idioma, especialidad de llamadas, criterio de Base de Datos, etc.).

- A través de la aplicación de administración del *Call Center* se dispone de la interfaz necesaria para la supervisión y gestión del enrutamiento de las llamadas.

- Se dispone a través del software CMS[5], de un repositorio de datos que permite la gestión de la información para el control y las medidas de explotación del servicio: llamadas recibidas, atendidas, perdidas, desbordadas, etc.

- Todos los puestos de los *Call Center* disponen de conexión a Internet, debidamente protegida a través de sistemas firewall (corta fuegos), facilitando el acceso externo a aplicaciones si fuese necesario.

- Capacidad de grabación y control de costes de todas las llamadas telefónicas.

- Dispone de sistemas IVR[6] que permiten funcionalidades de procesamiento de voz, buzones de voz, gestión de faxes, etc.

- Todos los puestos de teleoperación y trabajo, y sistemas residentes en los CPD locales están protegidos ante sobretensiones y caídas de potencia por un sistema de alimentación ininterrumpida (SAI) y grupos electrógenos accionados por motores diésel.

[4] ACD: *Automatic Call Distributor* – Distribuidor Automático de Llamadas: Proceso por el cual se distribuyen las llamadas que llegan a los sistemas de atención y teleoperadores.

[5] CMS*: Call Management System* – Sistema de Gestión de Llamadas.

[6] IVR: *Interactive Voice Response* – Respuesta de Voz Interactiva: Consiste en un sistema telefónico que es capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz y el reconocimiento de respuestas simples, como "si", "no", u otras. Es un sistema automatizado de respuesta interactiva, orientado a entregar y/o capturar información a través del teléfono, permitiendo el acceso a servicios de información y otras operaciones.

**Hardware**

La compañía cuenta con un parque de 8.000 equipos, en su mayoría PCs de escritorio, portátiles e impresoras, todos ellos conectados a la red corporativa.

El puesto de operador actualmente cuenta con las siguientes características mínimas:

- CPU: Mínimo Intel Core i5 3,1GHz.
- Memoria: Mínimo 4 GB de RAM.
- Disco: 250 GB.
- Tarjeta de red: 10/100 MHz. full dúplex.
- Pantalla: 17”-19”
- Sistema Operativo: Microsoft Windows 7 y Microsoft Windows 10
- Navegador Internet Microsoft Explorer, Firefox y Chrome
- Antivirus

Todos los puestos estarán provistos de terminales telefónicos digitales IP, dotados de *display* (pantalla) para el control de las operaciones previstas, consiguiendo así la mejora de la operativa de los agentes y mayores posibilidades de información al mismo. Todos los puestos están equipados con cascos, con reductor de ruido.

TMK S.A. tanto para sus servicios internos, centrales y dedicados a clientes, dispone de servidores HP Proliant tipo DL380, cuyas características principales son las siguientes:

- Multiprocesador.
- *Cluster*, con cabinas de almacenamiento tipo MSA 500.
- Soporte Raid 1 y 5 para tolerancia a fallos.
- Mantenimiento del fabricante 7x24, tiempo de respuesta en 4 horas.
- Licencia Windows Server.
- Antivirus.
- Dispositivos externos de *backup*.

Las bases de datos están montadas en clúster para su total disponibilidad ante caídas de alguno de los nodos. Copias de *backup* tanto en caliente como en frío dependiendo de si han de ser de alta disponibilidad (24h x 365 días) o no.

Los servidores Web son equipos HP Proliant DL 360, multiprocesador, especialmente diseñados para estas tareas.

Desde hace un tiempo la tendencia no es soportar servicios TI sobre servidores físicos. Hubo un auge importante de utilización de servidores virtuales. Este auge y tendencia también se ha aplicado en TMK S.A. y la gran mayoría de sus servicios están montados en máquinas virtuales. Son claras las ventajas que aporta la virtualización:

- Reutilización de hardware existente y optimización de recursos de hardware.
- Rápida incorporación de nuevos recursos en servidores virtualizados.
- Reducción de costes de espacio, consumo y de hardware.
- Administración global centralizada y más sencilla.
- Facilita la clonación y copia de sistemas, facilitando la creación de entornos de test reales.

- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto.
- Favorece el retorno de la inversión.
- Reduce los tiempos de parada.
- Migración en caliente de máquinas virtuales (sin parada del servicio) de un servidor físico a otro, eliminando paradas planificadas por mantenimiento de servidores físicos.
- En caso de disponer de los servidores físicos en *cluster*: balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el *cluster*, de forma que cada máquina virtual se ejecuta en el servidor físico más adecuado.

TMK S.A. dispone de tres entornos diferenciados, aunque residentes en la misma red: entorno de desarrollo, entorno de preproducción y entorno de producción.

**Centros de Proceso de Datos (CPD)**

Los pequeños CPD de cada centro de trabajo, están dotados de:

- Control de accesos 24 horas.
- Detectores de presencia de humos.
- Sistemas de extinción de incendios.
- Suelo técnico registrable ignifugo y antiestático.
- Toma de tierra debidamente autorizada.
- Equipos de aire acondicionado redundantes y dimensionados para la climatización y control de humedad de todo el CPD, incluso en condiciones extremas de temperatura exterior.
- Tomas de corriente eléctrica independientes con interruptores diferenciales para un máximo de 10 equipos.
- Repartidores de cableado estructurado debidamente etiquetados.
- Acceso de la red telefónica pública en la propia sala y con repartidores de fibra óptica diversificados.

**Red corporativa**

Cada centro de trabajo dispone de una infraestructura de red de área local (LAN) de alto rendimiento basada en conmutadores de red de última generación y principales marcas (Cisco, 3COM y Avaya) y cableado estructurado categoría 5E o superior. La red de comunicaciones está dimensionada para soportar servicios de voz y datos. Actualmente en las nuevas ampliaciones de red en los centros, se instala un único punto de red con electrónica que soporta *Power Over Ethernet* (alimentación a través de Ethernet) para la alimentación de los teléfonos, no siendo necesario de esta forma disponer de puntos de datos y voz diferenciados. La electrónica de red de los centros es *Fast Ethernet* (100 Mbps) y *Giga Ethernet* (1000 Mbps).

A continuación se muestra un diagrama de la red:

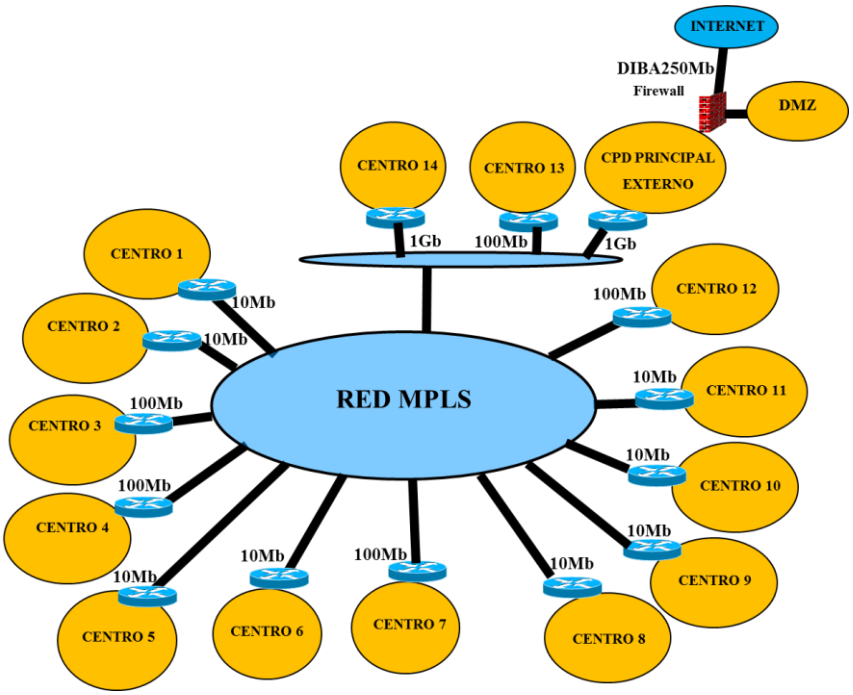


**Figura 3:** Diagrama de red de WAN de TMK S.A. (Fuente: Propia)

En el anterior diagrama de red de la WAN[7] de TMK S.A. podemos observar que todos los centros de trabajo se encuentran interconectados mediante red privada (MPLS). La WAN en todos los centros se encuentra redundada, tanto a nivel de acceso (diversificación de rutas) como en equipos para conseguir un nivel de disponibilidad superior al 99,9%. El acceso a Internet se realiza a través de infraestructura WAN de TMK S.A. Se gestiona mediante diferentes *proxies* dedicados, donde se realiza el filtrado de acceso a contenidos, dependiendo de la configuración definida. Adicionalmente en cada centro hay un dispositivo *(PacketShaper)* dedicado a priorizar y monitorizar el tráfico.

Además de la red corporativa (WAN), existen diferentes conexiones dedicadas que dan cobertura a los diferentes servicios que se prestan, implementadas bajo diferentes tecnologías (MPLS, *Frame Relay*, PaP42, etc.), ajustadas a las necesidades de cada servicio que se presta. Estas conexiones tanto pueden ser titularidad de TMK S.A. como del cliente para el que se presta el servicio.

[7] WAN: *Wide Area Network* – Red de área amplia. Red que abarca varias ubicaciones físicas.

**ACD**[8]

TMK S.A. dispone de un sistema de distribución automático de llamadas (ACD), sistema PABX[9]/ACD, basado en tecnología IP. Existen dos centralitas, en centros de trabajo diferentes, que dan cobertura a todas las plataformas en modo de alta disponibilidad.

Ambos ACD están interconectados de tal modo que permite la transferencia de llamadas entre agentes y servicios de cualquier centro. En todos los centros hay instalados equipos que actúan como pasarela de medios para el tráfico de llamadas y en caso de quedar aislados tienen capacidad de funcionar de forma autónoma.

La distribución automática de llamadas es una función de la centralita que nos permite la manipulación especializada de las llamadas, proporcionando a cada llamada que se recibe el tratamiento óptimo, eficiente y rápido, consiguiendo de esta manera mejorar la calidad del servicio que se ofrece a los clientes.

Algunas de las funciones básicas que proporciona cualquier ACD son las siguientes:

- *Delay announcements* (Anuncios de espera): ofrecer locuciones (anuncios) que darán al cliente cualquier tipo de información y evitarán la pérdida de llamadas.
- *Queue information* (Información de cola): obtener información relacionada con las llamadas que todavía no han podido ser atendidas (permanecen en cola de espera hasta poder ser atendidas).
- *Service Observing* (Servicio de observación): supervisión del trabajo de los agentes, a fin de comprobar si se está ofreciendo el servicio adecuado.
- *Interflow of calls* (flujo interno de llamadas): Gestión interna de las llamadas del sistema.

A través de la vectorización podemos realizar un tratamiento inteligente de las llamadas que entran en nuestro sistema, o las que se hacen internamente en el mismo. Un vector es un algoritmo que gestiona la llamada. Esta característica nos permite manipular cada llamada atendiendo a multitud de factores: número o procedencia de la persona que llama, número de llamadas en la cola de espera, hora y día de la semana, tiempo de espera, etc.

[8] ACD: *Automatic Call Distributor* – Distribuidor Automático de Llamadas

[9] PABX: *Private Automatic Branch eXchange* – Ramal Privado de Conmutación Automática o Central Secundaria Privada Automática; es una centralita telefónica conectada directamente a la red pública de telefonía mediante líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo pertenece a la empresa que lo tiene instalado, no a la compañía telefónica, por eso el adjetivo, “privado” en su denominación.

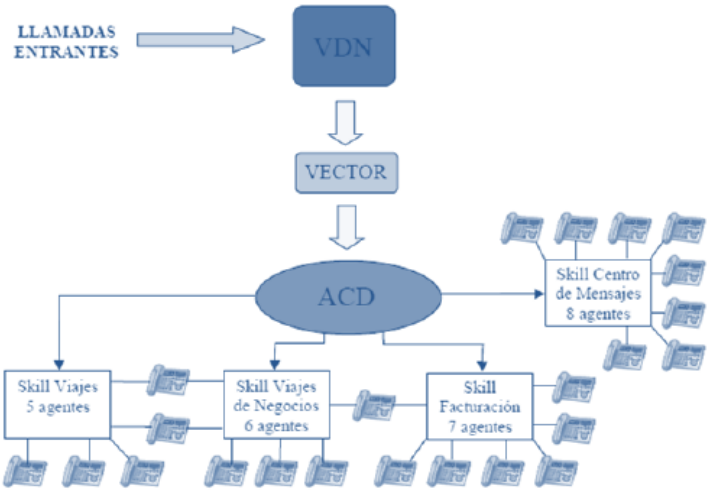


**Figura 4:** Configuración típica y básica de un ACD (Fuente: Propia)

Podemos decir que una configuración básica de un sistema ACD se compone de cuatro elementos:

- Vector: es un conjunto de instrucciones que definen el procesamiento de la llamada. Pudiéndose encadenar o referenciar entre ellos.
- VDN[10]: representa el número telefónico interno (extensión) que dirige una llamada sin atender a un vector, para ser gestionada según la lógica configurada.
- Comandos/instrucciones de vectorización: son aquellos que nos permiten aplicar los diferentes tratamientos a las llamadas, y mediante los cuales definimos la lógica interna del sistema.
- *Skill*: define las habilidades de los agentes. Podemos definir *skill* como conjunto o grupo de agentes específicos preparados para manejar determinado tipo de llamadas. Un mismo agente puede pertenecer a más de un grupo o *skill*.

La centralita incluye un sistema básico de estadísticas de gestión y supervisión del *call cente*r y del sistema. De igual manera, también dispone de salida para conexión de un sistema externo de procesado de estadísticas. En este caso, se utiliza está salida para la conexión a dos sistemas independientes, un tarificador, que permitirá desglosar costes, y el sistema de estadísticas CMS[11], que es un repositorio de datos que permite la gestión de la información para el control y las medidas de explotación del servicio: llamadas recibidas, atendidas, perdidas, desbordadas, etc.

[10] VDN: *Vector Directory Number* – Número del directorio de vectores.
[11] CMS: *Call Management System* – Sistema de gestión de llamadas.

**CMS**

El *Call Management System* (CMS), es el sistema de gestión utilizado para controlar el tráfico de las llamadas de los diferentes servicios. Recoge y almacena los datos de todas las llamadas para poder ser explotados mediante los informes predefinidos o los informes que se pueden diseñar y ajustar a las necesidades específicas.

Es posible disponer de información en tiempo real o pasado (histórico). Algunos de los datos de los que podemos disponer son: llamadas atendidas, llamadas emitidas, llamadas abandonas, llamadas perdidas, tiempos de conversación, tiempos de descanso, tiempos de trabajos administrativos, etc. Todos los datos es posible extraerlos por llamada, por agente, por grupo de agentes, por día, por semana, por mes, etc.

**Tarificador**

Sistema que recoge la información de cada llamada, *Call Detail Recording* (CDR), y la registra en su Base de Datos interna de forma que podamos disponer de los datos de duración, coste, tipo de llamada (interna, entrante o saliente). La información podrá ser consultada mediante informes prediseñados o informes personalizados.

**CTI[12]**

Un sistema CTI es un sistema informático dedicado a la interacción entre una llamada telefónica y un ordenador de forma coordinada (integración de voz y datos). El elemento que hace las funciones de conector entre la centralita y el CTI es el AES[13]. Actualmente dado que los canales de comunicación se han extendido más allá del teléfono, englobando el e-mail, Web, chat, fax, SMS, etc. el término CTI se ha ampliado también a otros canales de comunicación entre la empresa y sus clientes. La tecnología CTI evoluciona hacía integrar todos los canales de comunicación de la empresa y las informaciones que ésta recaba sobre sus clientes o potenciales clientes [3].

El sistema CTI que utiliza la compañía es una solución de gestión de *Contact Center* unificada, modular, basada en IP, que permite implementar nuevos servicios y campañas dentro un único sistema de forma ágil y personalizada.

Es una solución multicanal que permite unificar la gestión de todas las interacciones independientemente del canal que elija el usuario para ponerse en contacto con el servicio: voz (teléfono), e-mail, SMS, Fax, Web, chat, etc.

[12] CTI: *Computer Telephony Integration* – Integración de Telefonía y Datos

[13] AES: *Application Enablement Services* – Servicios de Habilitación de Aplicaciones. Los AES proporcionan una amplia gama de protocolos, aplicaciones de programas, interfaces y servicios que permiten el desarrollo e integración de aplicaciones.

Este sistema permite, durante la gestión del contacto, enviar un e-mail, fax, o SMS al cliente con la información solicitada durante el contacto. Este e-mail, fax o SMS enviado será registrado en el seguimiento de contactos como información enviada.

**Sistemas automáticos**

TMK S.A. dispone de un equipo de trabajo especialista en el diseño, desarrollo e implementación de soluciones de automatización de IVR. Este sistema de desarrollo propio, permite implementar la automatización de servicios a medida para sus clientes con unos costes y plazos muy competitivos, y con gran flexibilidad en cuanto a modificaciones según los requisitos de cada servicio y cliente a lo largo del ciclo de vida del servicio.

El sistema puede interactuar en tiempo real con todo tipo de sistemas clientes, tanto para realizar consultas como para registrar nueva información (Bases de Datos, sistemas CRM, etc.).

Las tecnologías IVR disponibles y con larga experiencia en desarrollo son las siguientes:

- Reconocimiento de dígitos DTMF[14].
- Reconocimiento de números.
- Reconocimiento de palabras clave.
- Reconocimiento de lenguaje natural.
- Emisiones de locuciones y mensajes pregrabados.
- Conversión texto voz.
- Grabación de mensajes y buzones.
- Integración con sistemas de cliente.

**Sistemas de grabación**

Al igual que el sistema de IVR, se dispone de un sistema de un sistema de grabación de desarrollo propio con las siguientes características:

- Chasis de 14 slots con sistema de ventilación redundante.
- Fuentes de alimentación redundantes.
- Grabación de conversaciones en formato GSM, ADPCM o PCM (ocupación aprox. 10 MB por hora/canal - ADPCM -, 3 MB por hora/canal en GSM). Conversión de ficheros a formato WAV y MP3.
- Fácil integración en entorno informático.
- Sistema de fácil uso, basado en aplicaciones estándar Windows.

[14] DTMF: *Dual-Tone Multi-Frequency* – Marcación por tonos o Sistema *Multi-Frecuencial*; Cuando el usuario pulsa en el teclado de su teléfono la tecla correspondiente al dígito que quiere marcar, se envían dos tonos, de distinta frecuencia: uno por columna y otro por fila en la que esté la tecla dispuesta en el teclado telefónico, que la central decodifica a través de filtros especiales, detectando instantáneamente qué dígito se marcó.

- Almacenamiento de conversaciones en disco para recuperación inmediata. La capacidad estándar del sistema es de 70.000 horas de grabaciones on-line, pudiendo aumentarse opcionalmente hasta más de 1 millón de horas de almacenamiento *on line.*
- Configuraciones desde 4 hasta 240 canales por chasis. Gran capacidad de crecimiento: con configuraciones multi-nodo se pueden crear sistemas con varios miles de canales.

Este sistema permite los siguientes tipos de grabación:

- Grabación continua: Permite la grabación de todas las llamadas, tanto de entrada como de salida.
- Grabación selectiva: Permite grabar las conversaciones de centenares de agentes utilizando un reducido número de canales.
- Grabación bajo demanda: Permite que un grupo de agentes compartan un número de canales del sistema, para grabar las partes críticas de las transacciones realizadas. Es el agente de operación o un programa automático, el que activa la grabación.

El sistema incluye un potente sistema de búsqueda de conversaciones, pudiendo localizar y reproducir conversaciones en base de datos tales como código de cliente, identificación del número llamante, agente, fecha y hora,…

**Plataforma SMS**

TMK S.A. cuenta con capacidad de envío de SMS potencialmente hacia cualquier terminal móvil GSM o 3G operado en España o fuera de España. La capacidad de recepción de mensajes está limitada a los terminales móviles GSM o 3G operados en España.

El intercambio de mensajes SMS y de la información relativa al estado de los mismos (confirmaciones de entrega) queda registrado en una Base de Datos. Esta base de datos ofrece gran flexibilidad para el envío de mensajes desde cualquier aplicativo, y proporciona la persistencia y coherencia necesarias en este tipo de servicio ante posibles interrupciones en las líneas de comunicación.

El envío de mensajes desde los puestos de trabajo de TMK S.A. puede realizarse mediante aplicaciones Web desarrolladas para tal fin, o a través de la aplicación corporativa de e-mail, esta última manera facilita disponer de una copia.

## 2.2. Objetivo - Alcance del Plan Director de Seguridad

El objetivo para el Plan Director de Seguridad (PDS) de TMK S.A. se define para el Sistema de Gestión de la Seguridad de la Información de los sistemas de gestión de negocio de la compañía TMK S.A. que comprende los siguientes sistemas: CTI, ACD, CMS, tarificador y puestos de trabajo de operador.

El alcance [4] se limita a la prestación de los servicios contratados por los clientes, incluido la comunicación segura mediante *Virtual Protocol Network (VPN)* que se ofrece a clientes y proveedores.

Queda al margen de este PDS el resto de sistemas de gestión que dan soporte a los procesos de negocio de TMK S.A. Quedarían por tanto excluidos del objetivo algunos SGSI como los siguientes: sistemas de finanzas, sistema de gestión de Recursos Humanos, sistemas de calidad, sistemas TI (correo-e, sistemas web, etc.)

El principal objetivo de Plan Director de Seguridad para TMK S.A. es la de asegurar la máxima fiabilidad en la prestación de servicios a sus clientes. En concreto los objetivos establecidos son:

- Dar fiabilidad y confianza a los clientes, proporcionando como valor añadido un servicio seguro.
- Identificar riesgos que puedan poner en peligro la continuidad del negocio.
- Protección de la información de los clientes.

## 2.3. Análisis diferencial de cumplimiento inicial

En primer lugar, antes de iniciar el proyecto de implantación del SGSI, es necesario realizar un análisis diferencial de las medidas de seguridad y la normativa en la organización. El análisis diferencial se realizará en base a los 114 controles o medidas preventivas (14 áreas y 35 objetivos de control) de la norma ISO/IEC 27002. El análisis nos permitirá conocer de forma global el estado actual de la Organización en relación a la Seguridad de la información.

La valoración para el análisis se realizará en base al Modelo de Madurez de la Capacidad (CMM) y los niveles de valoración se detallan en la siguiente tabla:

| EFECTIVIDAD | CMM | SIGNIFICADO | DESCRIPCIÓN |
|---|---|---|---|
| 0% | L0 | Inexistente | Carencia completa de cualquier proceso reconocido.<br>No se ha reconocido que exista ningún problema a resolver |
| 10% | L1 | Inicial / Ad-hoc | Estado inicial dónde el éxito de las actividades de los procesos se basa la mayor parte de las veces en un esfuerzo personal.<br>Los procedimientos son inexistentes o localizados en áreas concretas.<br>No existen plantillas definidas a nivel corporativo |
| 50% | L2 | Reproducible, pero intuitivo | Los procesos similares se llevan a término de forma similar para diferentes personas con la misma tarea.<br>Se formalizan las "buenas prácticas" en base a la experiencia y al método.<br>No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Depende del grado de conocimiento de cada individuo |
| 90% | L3 | Proceso definido | La organización completa participa en el proceso.<br>Los procesos están implantados, documentados y comunicados. |
| 95% | L4 | Gestionado y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. |
| 100% | L5 | Optimizado | Los procesos están bajo constante mejora.<br>En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |

**Tabla 1:** Modelo de Madurez de la Capacidad (CMM)

En el Anexo I del presente documento podemos encontrar la tabla de análisis diferencial con el análisis detallado para los 114 controles de la norma ISO/IEC 27002.

De una forma más global nos interesa conocer la madurez CMM de los controles analizados y el nivel de cumplimiento de cada área.

En la tabla 2 se muestra la distribución de los 114 controles de la norma ISO/IEC 27002:2013 según el Modelo de Madurez de la Capacidad.

| CMM | Efectividad | Nº Controles |
|---|---|---|
| L0 - Inexistente | 0% | 7 |
| L1 - Inicial | 10% | 22 |
| L2 - Reproducible | 50% | 47 |
| L3 - Proceso definido | 90% | 26 |
| L4 - Gestionado y medible | 95% | 1 |
| L5 - Optimizado | 100% | 11 |

**Tabla 2:** Distribución de los 114 controles ISO/IEC 27002 según CMM

En la siguiente figura podemos apreciar la madurez CMM de los controles ISO de forma gráfica:

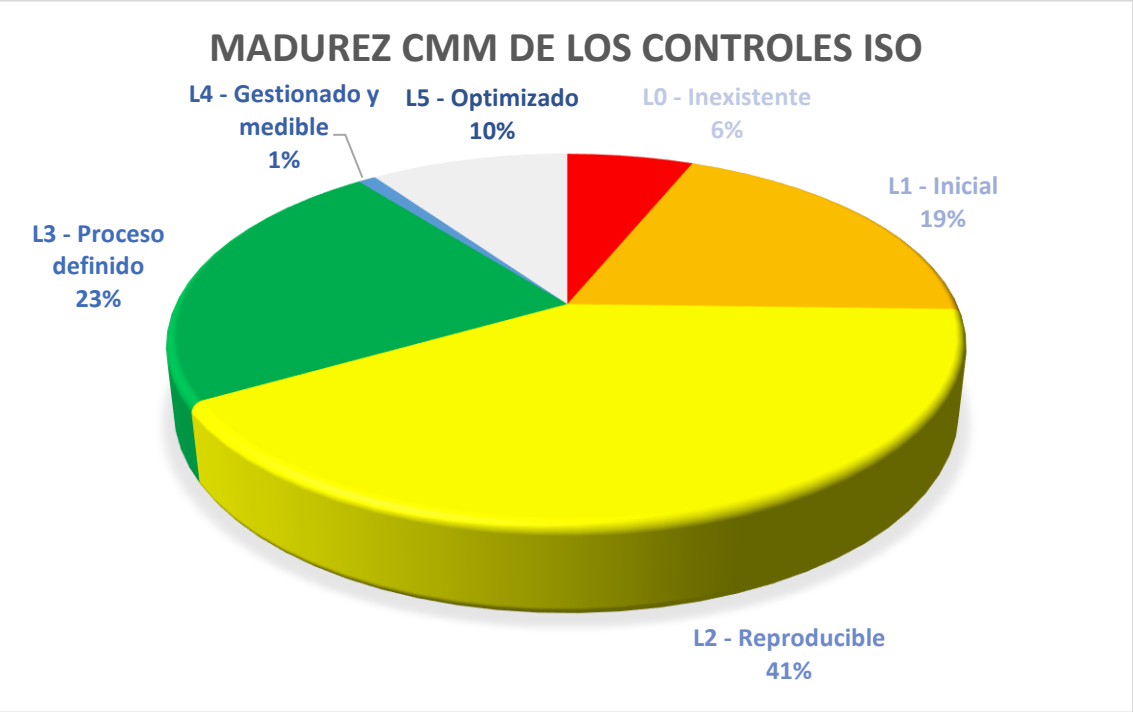


**Figura 5:** Gráfico Modelo de Madurez de la Capacidad (CMM)

En la tabla 3 se presenta el nivel de cumplimiento inicial de cada área de la ISO/IEC 27002:2013:

| Áreas ISO/IEC 27002:2013 | % cumplimiento |
|---|---|
| 5. Política de seguridad de la información | 95% |
| 6. Organización de la seguridad de la información | 50,00% |
| 7. Seguridad ligada a los Recurso Humanos | 61% |
| 8. Administración de activos | 33,33% |
| 9. Control de acceso | 79,17% |
| 10. Criptografía | 0% |
| 11. Seguridad física y del entorno | 68,33% |
| 12. Seguridad de las operaciones | 89,46% |
| 13. Seguridad de las comunicaciones | 46,67% |
| 14. Adquisición, desarrollo y mantenimiento del sistema | 23,33% |
| 15. Relaciones con el proveedor | 50% |
| 16. Gestión de incidentes de seguridad de la información | 27,14% |
| 17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio | 30% |
| 18. Cumplimiento | 66,00% |

**Tabla 3:** Nivel de cumplimiento inicial de cada área de la ISO/IEC 27002:2013

En la siguiente figura muestra gráficamente un Radar del nivel de cumplimiento de cada área:

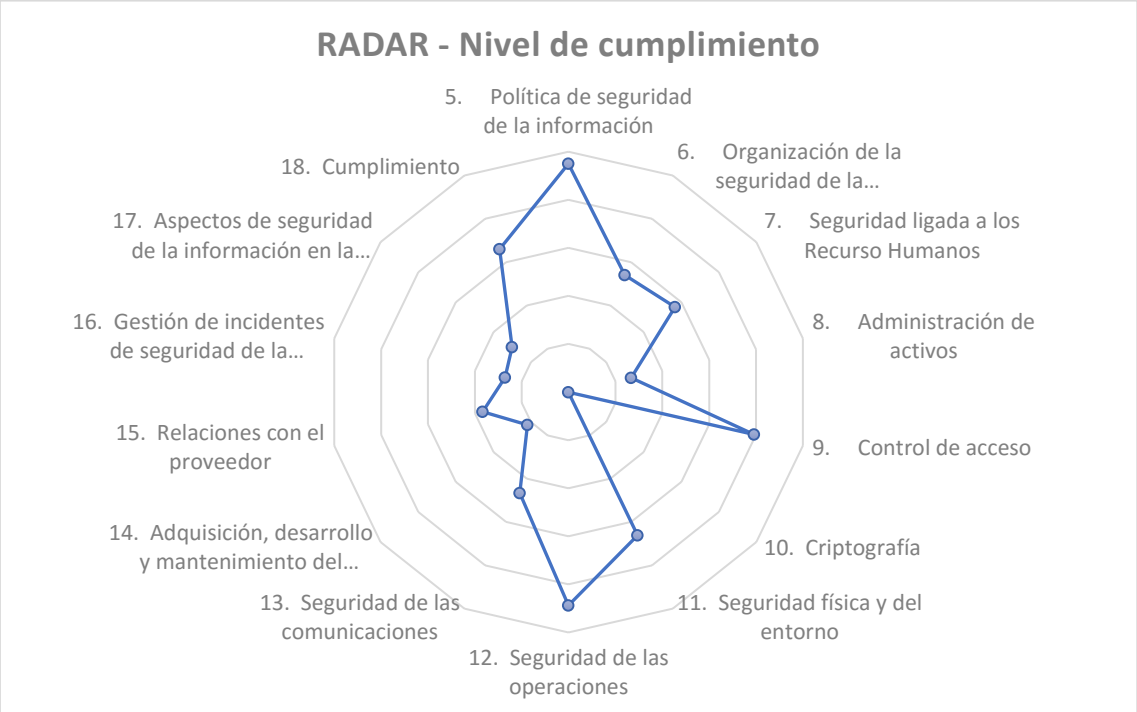


**Figura 6:** Gráfico radar de nivel de cumplimiento

# 3. FASE 2: Sistema de Gestión Documental

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo, lo que significa la necesidad de tener una serie de documentos que dicta la norma ISO/IEC 27001.

El cuerpo documental del SGSI de TMK S.A. se apoya en los siguientes documentos:

**Anexo II: Política de Seguridad**
Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del SGSI. El contenido de la política cubre aspectos relativos al acceso a la información, uso de recursos de la organización, comportamiento en caso de incidentes de seguridad, etc.

**Anexo III: Procedimiento de Auditorías Internas**
Documento que incluye una planificación de las auditorías que se llevarán a cabo durante la vigencia del certificado (una vez obtenido), requisitos que establecerán los auditores internos y definición del modelo de informe de auditoría.

**Anexo IV: Gestión de indicadores**
Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados.

**Anexo V: Procedimiento de Revisión por la Dirección**
La dirección de TMK S.A. debe revisar las cuestiones más importantes que han ido ocurriendo en relación con el SGSI. El procedimiento conforme a la ISO/IEC 27001 define, tanto los puntos de entrada como los de salida que deben obtenerse.

**Anexo VI: Gestión de roles y responsabilidades**
El SGSI tiene un comité de seguridad que debe estar compuesto por un equipo que se encarga de crear, mantener, supervisar y mejorar el sistema. Al menos una persona del Comité de Dirección de la organización forma parte del Comité de Seguridad de forma que las decisiones que se tomen podrán estar aprobadas previamente por un miembro de la dirección.

**Anexo VII: Metodología de Análisis de Riesgos**
Establece la sistemática que se deberá seguir para el cálculo del riesgo y tiene que incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades

**Anexo VIII: Declaración de Aplicabilidad**
Documento que incluye todos los controles de Seguridad establecidos en la organización, con el detalle de aplicabilidad, estado y documentación relacionada.

# 4. FASE 3: Análisis de riesgos

En toda implantación de un SGSI es fundamental realizar un análisis de riesgos. El concepto análisis de riesgos podemos entenderlo como determinar que tiene la organización y estimar que podría ocurrir. Es necesario realizar un evaluación de activos para poderlos proteger, para ello es necesario conocer las dependencias que tienen y realizar una valoración de los mismos.

Existen diferentes metodologías de análisis de riesgos: COBIT, OCTAVE, MAGERIT o DAFP. En este trabajo la metodología utilizada es MAGERIT

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es un método de carácter público elaborado por el Consejo Superior de Informática (CSI), órgano del Ministerio de Administraciones Públicas, encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno de España.

Este método es creado para minimizar los riesgos asociados al uso de sistemas informáticos telemáticos, garantizando la autenticación, confidencialidad, integridad y disponibilidad de los sistemas y generando de este modo confianza en el usuario de los mismos.

Se persigue, por tanto, un doble objetivo:

- Estudiar los riesgos asociados a un sistema de información y su entorno.
- Recomendar las medidas necesarias para conocer, prevenir, impedir, reducir o controlar los riesgos estudiados.

## 4.1. Inventario de activos

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

Se debe disponer de un inventario de activos vinculados a la información. Para MAGERIT en un sistema de información hay dos elementos esenciales: la información que se maneja y los servicios que se prestan.

Subordinados a estos elementos esenciales se identifican otros activos relevantes que recogemos en un inventario según la clasificación propuesta por la metodología escogida (MAGERIT).

- Instalaciones de equipos informáticos y comunicaciones.
- Equipos informáticos *(hardware),* hospedan datos, aplicaciones y servicios
- Aplicaciones *(software)* para manejo de datos
- Datos, que materializan la información.
- Soportes de información, dispositivos de almacenamiento de datos.

- Red, permite intercambio y tráfico de datos
- Servicios auxiliares necesarios
- Equipamiento auxiliar, complementario al equipamiento informático
- Personal, que explota u opera los elementos de esta clasificación.

En el Anexo XIX se muestra el inventario inicial de activos agrupados según MAGERIT en una tabla.

## 4.2. Valoración de los activos

Es importante disponer de una valoración de activos, que en muchos casos será estimada por la enorme dificultad de valorar algunos activos no tangibles como pueden ser la base de datos (cartera) de clientes de una empresa o los *backups* de respaldo. Por ejemplo en el caso de los *backups*, su valoración para la empresa, en caso de pérdida de información va mucho más allá del coste del sistema de *backup* y los soportes sobre los que se realizan.

MAGERIT en el libro III (punto 2.1) propone una clasificación de activos que comprende las siguientes categorías:

- Muy alto
- Alto
- Medio
- Bajo
- Muy bajo

Adicionalmente hay que tener en consideración que los activos dependen unos de otros, es decir están jerarquizados. Un activo superior (jerárquicamente) depende de otro activo inferior cuando la materialización de una amenaza sobre el activo inferior tiene consecuencias perjudiciales sobre el activo superior.

En general el grado de dependencias atendiendo a los grupos de activos identificados por MAGERIT es el siguiente:

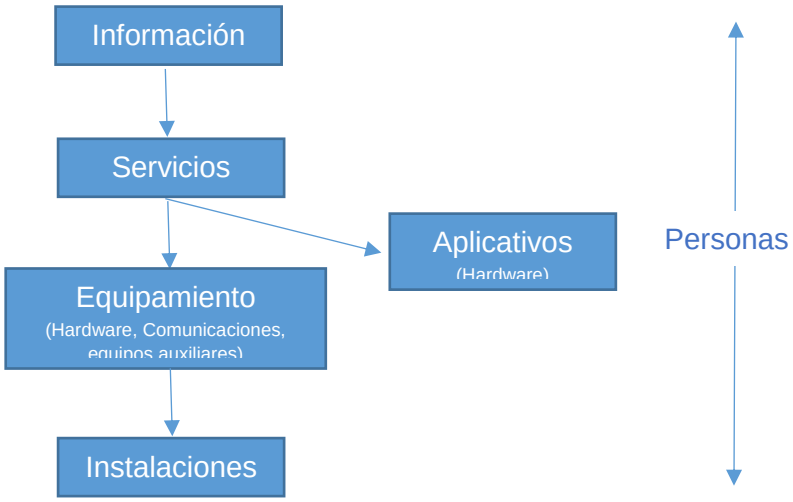


**Figura 7:** Dependencias de los grupos de activos

En el gráfico de dependencias la información aparece como activo superior y a su vez más crítico. Las instalaciones se ubican como activo inferior sin dependencias y el personal aparece como activo transversal a la jerarquía.

La anterior clasificación propuesta por MAGERIT atiende a una clasificación cualitativa, para completar la valoración de los activos también con una clasificación cuantitativa, para cada valor cualitativo (Muy alto; Alto; Medio; Bajo; Muy bajo) se asigna un rango de valores cuantitativos. También para que el modelo nos permita obtener una estimación cuantitativa, se establece para cada rango cuantitativo, un valor medio.

La siguiente tabla refleja la relación cualitativa y cuantitativa:

| Valoración cualitativa | Valoración cuantitativa | |
|---|---|---|
| **Valores** | **Rango económico** | **Valor medio** |
| Muy Alto | >=300.000€ | 500.000€ |
| Alto | >=50.000€ y <300.000€ | 150.000€ |
| Medio | >=10.000€ y <50.000€ | 25.000€ |
| Bajo | >=5.000€ y <10.000€ | 7.500€ |
| Muy Bajo | <5.000€ | 2.500€ |

**Tabla 4:** Relación cualitativa y cuantitativa de los activos

### 4.2.1. Dimensiones de seguridad

Es importante conocer el valor de los activos en varias dimensiones, por ello una vez identificados los activos, estos se valoran según la valoración ACIDA. Esta valoración mide la criticidad en las cinco dimensiones de la seguridad de la información. Esta valoración permite, a posteriori, valorar el impacto que tendrá la materialización de una amenaza sobre la parte del activo expuesto (no cubierto por las medidas preventivas dispuestas para cada una de las dimensiones:

**A**utenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

**C**onfidencialidad: la información debe llegar solo a las personas autorizadas. La confidencialidad es una propiedad de difícil recuperación.

**I**ntegridad: mantenimiento de las características de completitud y corrección de los datos. Los datos no han sido alterados de forma no autorizada.

**D**isponibilidad: disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio.

**A**uditabilidad o Trazabilidad: Característica que asegura de que en todo momento se podrá determinar quién hizo qué y en qué momento

Para valorar las cinco dimensiones (ACIDA), se utilizará la siguiente escala de valoración de diez valores:

| Valor | Criterio |
|---|---|
| 10 | Daño muy grave en la organización |
| 7-9 | Daño grave en la organización |
| 4-6 | Daño importante en la organización |
| 1-3 | Daño menor en la organización |
| 0 | Daño irrelevante en la organización |

**Tabla 5:** Valoración dimensiones de seguridad

En el Anexo X, se muestra la tabla “Valoración de los activos” resumen de valoración en la que se recoge la valoración de activos y los aspectos críticos de estos.

En la citada tabla se valoran los activos según su importancia (Muy Alta; Alta; Media; Baja, Muy baja) y al mismo tiempo se asignará a cada activo para cada dimensión una valoración de 0 a 10.

## 4.3. Análisis de amenazas

Los activos están expuestos a amenazas y estas pueden afectar a diferentes aspectos de la seguridad. Metodológicamente se pretende analizar que amenazas pueden afectar a que activos. Se trata de estimar la vulnerabilidad de cada activo respecto a las amenazas potenciales, así como la frecuencia estimada de las mismas.

La mayoría de metodologías utilizadas para el análisis de riesgos dispone de una tabla de amenazas, como es el caso de nuestra metodología MAGERIT [5].

MAGERIT clasifica las amenazas en las siguientes categorías o grupos:

- Desastres naturales
- De origen industrial
- Errores o fallos no intencionados
- Ataques intencionados

En el Anexo XI – Activos y dimensiones de la seguridad, se muestran las tablas resumen de activos y dimensiones de seguridad, para cada activo determinado. Para cada tipo de activo se analiza la frecuencia con la que se puede materializar la amenaza, así como su impacto en las diferentes dimensiones de la seguridad del activo.

La frecuencia de una amenaza la valoraremos según la siguiente escala:

| Escala de frecuencias ante amenazas | | |
|---|---|---|
| **Frecuencia** | | **Valor** |
| Muy Alta | Semanal | 100 |
| Alta | Mensual | 10 |
| Media | Trimestral | 1 |
| Baja | Anual | 0,1 |
| Muy Baja | >1 año | 0,01 |

**Tabla 6:** Escala de frecuencias ante amenazas

Es fundamental tener claro que el riesgo no es totalmente eliminable, pero si es gestionable.

## 4.4. Impacto potencial

A partir de la tabla de activos y dimensiones de seguridad, y conociendo previamente los valores de los diferentes activos, es posible determinar el impacto potencial que pueden suponer para la organización la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción y a la vez evaluar como se ve modificado el denominado valor una vez se apliquen las contramedidas.

El impacto potencial para cada dimensión de cada activo lo obtenemos mediante la siguiente formula:

**Impacto Potencial = Valor Activo * %Impacto**

| AMBITO | ACTIVO | Valor Activo | | | | | %Impacto | | | | | Impacto Potencial | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | C | I | D | A | A | C | I | D | A | A | C | I | D | A |
| Instalaciones | CPD externo | 9 | 8 | 10 | 10 | 7 | | 80 | 100 | 100 | | 0 | 640 | 1000 | 1000 | 0 |
| | Sedes (14) | 7 | 5 | 3 | 5 | 2 | | 80 | 100 | 100 | | 0 | 400 | 300 | 500 | 0 |
| | CPD sedes | 8 | 7 | 8 | 9 | 6 | | 80 | 100 | 100 | | 0 | 560 | 800 | 900 | 0 |
| Hardware | PCs | 4 | 4 | 5 | 6 | 4 | 100 | 100 | 100 | 100 | | 400 | 400 | 500 | 600 | 0 |
| | Portátiles | 4 | 5 | 5 | 5 | 4 | 100 | 100 | 100 | 100 | | 400 | 500 | 500 | 500 | 0 |
| | Impresoras | 3 | 4 | 3 | 3 | 3 | 100 | 100 | 100 | 100 | | 300 | 400 | 300 | 300 | 0 |
| | Servidores | 9 | 9 | 9 | 9 | 7 | 100 | 100 | 100 | 100 | | 900 | 900 | 900 | 900 | 0 |
| | Centralita | 9 | 9 | 9 | 9 | 7 | 100 | 100 | 100 | 100 | | 900 | 900 | 900 | 900 | 0 |
| | Teléfonos | 4 | 4 | 5 | 6 | 4 | 100 | 100 | 100 | 100 | | 400 | 400 | 500 | 600 | 0 |
| Aplicaciones | Windows server | 4 | 7 | 8 | 8 | 7 | 100 | 100 | 100 | 100 | | 400 | 700 | 800 | 800 | 0 |
| | Windows profesional 7 | 3 | 2 | 2 | 2 | 2 | 100 | 100 | 100 | 100 | | 300 | 200 | 200 | 200 | 0 |
| | Windows profesional 10 | 3 | 2 | 2 | 2 | 2 | 100 | 100 | 100 | 100 | | 300 | 200 | 200 | 200 | 0 |
| | Microsoft Office | 3 | 2 | 2 | 2 | 1 | 100 | 100 | 100 | 100 | | 300 | 200 | 200 | 200 | 0 |
| | Java | 2 | 2 | 2 | 1 | 0 | 100 | 100 | 100 | 100 | | 200 | 200 | 200 | 100 | 0 |
| | Antivirus | 6 | 1 | 4 | 5 | 1 | 100 | 100 | 100 | 100 | | 600 | 100 | 400 | 500 | 0 |
| | UCI Altitude | 6 | 4 | 8 | 9 | 8 | 100 | 100 | 100 | 100 | | 600 | 400 | 800 | 900 | 0 |
| | CRM Microsoft | 6 | 4 | 8 | 9 | 8 | 100 | 100 | 100 | 100 | | 600 | 400 | 800 | 900 | 0 |
| Datos | Bases de Datos de clientes | 7 | 8 | 9 | 7 | 7 | 100 | 100 | 100 | 100 | | 700 | 800 | 900 | 700 | 0 |
| | Código fuente desarrollos | 7 | 8 | 9 | 6 | 6 | 100 | 100 | 100 | 100 | | 700 | 800 | 900 | 600 | 0 |
| | Datos financieros | 4 | 5 | 9 | 6 | 6 | 100 | 100 | 100 | 100 | | 400 | 500 | 900 | 600 | 0 |
| | Backups | 7 | 9 | 10 | 5 | 5 | 100 | 100 | 100 | 100 | | 700 | 900 | 1000 | 500 | 0 |
| | Datos de acceso | 8 | 10 | 10 | 8 | 9 | 100 | 100 | 100 | 100 | | 800 | 1000 | 1000 | 800 | 0 |
| | Datos de configuraciones | 7 | 5 | 9 | 6 | 6 | 100 | 100 | 100 | 100 | | 700 | 500 | 900 | 600 | 0 |
| Red | Cableado de red | 3 | 1 | 7 | 8 | 2 | 100 | 100 | 100 | 100 | | 300 | 100 | 700 | 800 | 0 |
| | Routers | 7 | 7 | 9 | 10 | 5 | 100 | 100 | 100 | 100 | | 700 | 700 | 900 | 1000 | 0 |
| | Switches | 7 | 7 | 9 | 10 | 5 | 100 | 100 | 100 | 100 | | 700 | 700 | 900 | 1000 | 0 |
| | Antenas wifi | 7 | 7 | 9 | 7 | 5 | 100 | 100 | 100 | 100 | | 700 | 700 | 900 | 700 | 0 |
| Servicios | Correo electrónico | 7 | 7 | 8 | 7 | 5 | 100 | 100 | 100 | 100 | 100 | 700 | 700 | 800 | 700 | 500 |
| | Servicios Web | 8 | 7 | 9 | 9 | 6 | 100 | 100 | 100 | 100 | 100 | 800 | 700 | 900 | 900 | 600 |
| Equipamiento auxiliar | SAIs | 0 | 0 | 0 | 10 | 0 | | 10 | 10 | 100 | | 0 | 0 | 0 | 1000 | 0 |
| | Grupos electrógenos | 0 | 0 | 0 | 10 | 0 | | 10 | 10 | 100 | | 0 | 0 | 0 | 1000 | 0 |
| Personal | Responsables de TI | 6 | 6 | 5 | 8 | 5 | | 100 | 25 | 75 | | 0 | 600 | 125 | 600 | 0 |
| | Técnicos de sistemas | 7 | 5 | 8 | 9 | 5 | | 100 | 25 | 75 | | 0 | 500 | 200 | 675 | 0 |
| | Técnicos de desarrollo | 5 | 5 | 8 | 8 | 5 | | 100 | 25 | 75 | | 0 | 500 | 200 | 600 | 0 |

**Tabla 7:** Tabla cálculo impacto potencial

## 4.5. Nivel de riesgo aceptable y riesgo residual

Es necesaria la definición de un límite a partir del cual podemos decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar los controles. El nivel de riesgo

aceptable debe ser aprobado por la dirección de la organización y se deben definir los criterios para establecer este nivel de riesgo.

Aun estableciendo controles, el riesgo se reduce, pero no se elimina, sigue existiendo, pero el objetivo es conseguir reducirlo por debajo del nivel de riesgo aceptable que se ha definido. El riesgo que continua existiendo tras la aplicación de los controles de seguridad se denomina riesgo residual.

**Riesgo = Impacto Potencial * Frecuencia**

| AMBITO | ACTIVO | Impacto Potencial | | | | | Frecuencia | Riesgo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | C | I | D | A | Valor | A | C | I | D | A |
| Instalaciones | CPD externo | 0 | 640 | 1000 | 1000 | 0 | 0,1 | 0 | 64 | 100 | 100 | 0 |
| | Sedes (14) | 0 | 400 | 300 | 500 | 0 | 0,1 | 0 | 40 | 30 | 50 | 0 |
| | CPD sedes | 0 | 560 | 800 | 900 | 0 | 0,1 | 0 | 56 | 80 | 90 | 0 |
| Hardware | PCs | 400 | 400 | 500 | 600 | 0 | 1 | 400 | 400 | 500 | 600 | 0 |
| | Portátiles | 400 | 500 | 500 | 500 | 0 | 1 | 400 | 500 | 500 | 500 | 0 |
| | Impresoras | 300 | 400 | 300 | 300 | 0 | 1 | 300 | 400 | 300 | 300 | 0 |
| | Servidores | 900 | 900 | 900 | 900 | 0 | 1 | 900 | 900 | 900 | 900 | 0 |
| | Centralita | 900 | 900 | 900 | 900 | 0 | 1 | 900 | 900 | 900 | 900 | 0 |
| | Teléfonos | 400 | 400 | 500 | 600 | 0 | 1 | 400 | 400 | 500 | 600 | 0 |
| Aplicaciones | Windows server | 400 | 700 | 800 | 800 | 0 | 1 | 400 | 700 | 800 | 800 | 0 |
| | Windows profesional 7 | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Windows profesional 10 | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Microsoft Office | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Java | 200 | 200 | 200 | 100 | 0 | 1 | 200 | 200 | 200 | 100 | 0 |
| | Antivirus | 500 | 100 | 400 | 500 | 0 | 1 | 500 | 100 | 400 | 500 | 0 |
| | UCI Altitude | 600 | 400 | 800 | 900 | 0 | 1 | 600 | 400 | 800 | 900 | 0 |
| | CRM Microsoft | 600 | 400 | 800 | 900 | 0 | 1 | 600 | 400 | 800 | 900 | 0 |
| Datos | Bases de Datos de clientes | 700 | 800 | 900 | 700 | 0 | 10 | 7000 | 8000 | 9000 | 7000 | 0 |
| | Código fuente desarrollos | 700 | 800 | 900 | 600 | 0 | 10 | 7000 | 8000 | 9000 | 6000 | 0 |
| | Datos financieros | 400 | 500 | 900 | 600 | 0 | 10 | 4000 | 5000 | 9000 | 6000 | 0 |
| | Backups | 700 | 900 | 1000 | 500 | 0 | 10 | 7000 | 9000 | 10000 | 5000 | 0 |
| | Datos de acceso | 800 | 1000 | 1000 | 800 | 0 | 10 | 8000 | 10000 | 10000 | 8000 | 0 |
| | Datos de configuraciones | 700 | 500 | 900 | 600 | 0 | 10 | 7000 | 5000 | 9000 | 6000 | 0 |
| Red | Cableado de red | 300 | 100 | 700 | 800 | 0 | 1 | 300 | 100 | 700 | 800 | 0 |
| | Routers | 700 | 700 | 900 | 1000 | 0 | 1 | 700 | 700 | 900 | 1000 | 0 |
| | Switches | 700 | 700 | 900 | 1000 | 0 | 1 | 700 | 700 | 900 | 1000 | 0 |
| | Antenas wifi | 700 | 700 | 900 | 700 | 0 | 1 | 700 | 700 | 900 | 700 | 0 |
| Servicios | Correo electrónico | 700 | 700 | 800 | 700 | 500 | 0,1 | 70 | 70 | 80 | 70 | 50 |
| | Servicios Web | 800 | 700 | 900 | 900 | 600 | 0,1 | 80 | 70 | 90 | 90 | 60 |
| Equipamiento auxiliar | SAIs | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| | Grupos electrógenos | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| Personal | Responsables de TI | 0 | 600 | 125 | 600 | 0 | 1 | 0 | 600 | 125 | 600 | 0 |
| | Técnicos de sistemas | 0 | 500 | 200 | 675 | 0 | 1 | 0 | 500 | 200 | 675 | 0 |
| | Técnicos de desarrollo | 0 | 500 | 200 | 600 | 0 | 1 | 0 | 500 | 200 | 600 | 0 |

**Tabla 8:** Tabla cálculo riesgo

# 5. FASE 4: Propuesta de proyectos

Tras la fase de análisis de riesgos somos conscientes de los riesgos actuales de la Organización y en base a ello se plantearán proyectos de mejora para aumentar la seguridad de la Organización. Se priorizarán los proyectos relacionados con los activos identificados con mayor riesgo.

| AMBITO | ACTIVO | Impacto Potencial | | | | | Frecuencia | Riesgo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | C | I | D | A | Valor | A | C | I | D | A |
| Instalaciones | CPD externo | 0 | 640 | 1000 | 1000 | 0 | 0,1 | 0 | 64 | 100 | 100 | 0 |
| | Sedes (14) | 0 | 400 | 300 | 500 | 0 | 0,1 | 0 | 40 | 30 | 50 | 0 |
| | CPD sedes | 0 | 560 | 800 | 900 | 0 | 0,1 | 0 | 56 | 80 | 90 | 0 |
| Hardware | PCs | 400 | 400 | 500 | 600 | 0 | 1 | 400 | 400 | 500 | 600 | 0 |
| | Portátiles | 400 | 500 | 500 | 500 | 0 | 1 | 400 | 500 | 500 | 500 | 0 |
| | Impresoras | 300 | 400 | 300 | 300 | 0 | 1 | 300 | 400 | 300 | 300 | 0 |
| | Servidores | 900 | 900 | 900 | 900 | 0 | 1 | 900 | 900 | 900 | 900 | 0 |
| | Centralita | 900 | 900 | 900 | 900 | 0 | 1 | 900 | 900 | 900 | 900 | 0 |
| | Teléfonos | 400 | 400 | 500 | 600 | 0 | 1 | 400 | 400 | 500 | 600 | 0 |
| Aplicaciones | Windows server | 400 | 700 | 800 | 800 | 0 | 1 | 400 | 700 | 800 | 800 | 0 |
| | Windows profesional 7 | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Windows profesional 10 | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Microsoft Office | 300 | 200 | 200 | 200 | 0 | 1 | 300 | 200 | 200 | 200 | 0 |
| | Java | 200 | 200 | 200 | 100 | 0 | 1 | 200 | 200 | 200 | 100 | 0 |
| | Antivirus | 500 | 100 | 400 | 500 | 0 | 1 | 500 | 100 | 400 | 500 | 0 |
| | UCI Altitude | 600 | 400 | 800 | 900 | 0 | 1 | 600 | 400 | 800 | 900 | 0 |
| | CRM Microsoft | 600 | 400 | 800 | 900 | 0 | 1 | 600 | 400 | 800 | 900 | 0 |
| Datos | Bases de Datos de clientes | 700 | 800 | 900 | 700 | 0 | 10 | 7000 | 8000 | 9000 | 7000 | 0 |
| | Código fuente desarrollos | 700 | 800 | 900 | 600 | 0 | 10 | 7000 | 8000 | 9000 | 6000 | 0 |
| | Datos financieros | 400 | 500 | 900 | 600 | 0 | 10 | 4000 | 5000 | 9000 | 6000 | 0 |
| | Backups | 700 | 900 | 1000 | 500 | 0 | 10 | 7000 | 9000 | 10000 | 5000 | 0 |
| | Datos de acceso | 800 | 1000 | 1000 | 800 | 0 | 10 | 8000 | 10000 | 10000 | 8000 | 0 |
| | Datos de configuraciones | 700 | 500 | 900 | 600 | 0 | 10 | 7000 | 5000 | 9000 | 6000 | 0 |
| Red | Cableado de red | 300 | 100 | 700 | 800 | 0 | 1 | 300 | 100 | 700 | 800 | 0 |
| | Routers | 700 | 700 | 900 | 1000 | 0 | 1 | 700 | 700 | 900 | 1000 | 0 |
| | Switches | 700 | 700 | 900 | 1000 | 0 | 1 | 700 | 700 | 900 | 1000 | 0 |
| | Antenas wifi | 700 | 700 | 900 | 700 | 0 | 1 | 700 | 700 | 900 | 700 | 0 |
| Servicios | Correo electrónico | 700 | 700 | 800 | 700 | 500 | 0,1 | 70 | 70 | 80 | 70 | 50 |
| | Servicios Web | 800 | 700 | 900 | 900 | 600 | 0,1 | 80 | 70 | 90 | 90 | 60 |
| Equipamiento auxiliar | SAIs | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| | Grupos electrógenos | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| Personal | Responsables de TI | 0 | 600 | 125 | 600 | 0 | 1 | 0 | 600 | 125 | 600 | 0 |
| | Técnicos de sistemas | 0 | 500 | 200 | 675 | 0 | 1 | 0 | 500 | 200 | 675 | 0 |
| | Técnicos de desarrollo | 0 | 500 | 200 | 600 | 0 | 1 | 0 | 500 | 200 | 600 | 0 |

**Tabla 9:** Tabla de cálculo de riesgo (con riesgo alto y medio coloreado)

Se dividirán los proyectos en dos, en función del riesgo determinado en la fase anterior. La dirección ha decidido establecer el umbral de riesgo en 500, siendo este valor de riesgo el que determinará la necesidad de acometer proyectos de mejora. Hasta el nivel de riesgo 500 la organización ha decidido asumir el riesgo. En un principio se ha decidido acometer con prioridad los proyectos orientados a mitigar el riesgo de los activos que se ha cuantificado riesgo mayor a 1000. A continuación en la tabla de riesgo se muestra coloreado los activos con riesgo mayor a 500 (mayor de 500 y hasta 1000 en amarillo; mayor de 1000 en rojo).

Como podemos observar los activos más vulnerables son los relacionados con los datos, todos presentan un nivel de riesgo superior a 1000 en las dimensiones Autenticidad, Confidencialidad, Integridad y Disponibilidad. Los datos son fundamentales para la actividad de la empresa TMK S.A. por ello es lógico que sean los activos más vulnerables. Por ejemplo podría ser fatal para la actividad de la empresa perder una Base de Datos de clientes puesto que suele ser un activo fundamental en su actividad de negocio (telemarketing).

Los proyectos de mejora propuestos para mitigar los riesgos de los activos de Datos son los siguientes:

- PR1: Plan de Continuidad del Negocio
- PR2: Política de Backups
- PR3: Formaciones continúas y de actualización en materia de seguridad
- PR4: Procedimiento de destrucción de soportes

Estos proyectos no sólo contribuirán a mitigar el riesgo para los activos de Datos, indudablemente el Plan de Continuidad del Negocio contribuirá a mitigar riesgos en otros activos, pero será prioritario por afectar a los activos de Datos.

Otros grupos de activos para los que hay que acometer mejoras son: hardware, aplicaciones y red, los proyectos propuestos para mejorar la seguridad son los siguientes:

- PR5: Gestión de activos
- PR6: Plan de renovación de hardware (Servidores, PCs y portátiles)
- PR7: Mejora en la gestión de los incidentes de seguridad
- PR8: Plan de renovación y actualización de elementos de red
- PR9: Alta disponibilidad para aplicaciones que soportan el negocio
- PR10: Política de dispositivos móviles

En el Anexo XII se muestra para cada proyecto una ficha detallada que recoge: descripción del proyecto, objetivos, riesgos a mitigar, coste, temporalidad e indicadores definidos.

En la ficha de cada proyecto se ha detallado el coste estimado y presupuestado, así como la temporalidad estimada. A continuación en la tabla 10 se muestra un resumen de estos datos:

| Proyecto | Coste | | Temporalidad | |
|---|---|---|---|---|
| **PR1: Plan de Continuidad del Negocio** | 30.000€ | 32.800€ | 6 meses | 6 meses |
| **PR2: Política de *backups*** | 1.000€ | | 1 mes | |
| **PR3: Formaciones continúas y de actualización en materia de seguridad** | 1.500€ | | 1 mes | |
| **PR4: Procedimiento de destrucción de soportes** | 300€ | | 1 mes | |
| **PR5: Gestión de activos** | 0€ | 550.000€ | 1 mes | 12 meses |
| **PR6: Plan de renovación de hardware (Servidores, PCs y portátiles)** | 300.000€ | | 12 meses | |
| **PR7: Mejora en la gestión de los incidentes de seguridad** | 0€ | | 12 meses | |
| **PR8: Plan de renovación y actualización de elementos de red** | 100.000€ | | 12 meses | |
| **PR9: Alta disponibilidad para aplicaciones que soportan el negocio** | 150.000€ | | 12 meses | |
| **PR10: Política de dispositivos móviles** | 0€ | | 1 mes | |

**Tabla 10:** Tabla resumen coste y temporalidad

Como podemos observar, la temporalidad de los proyectos no es la suma de los tiempos de cada proyecto porque algunos proyectos serán ejecutados en paralelo. A Continuación en el diagrama de Gantt se representa de forma gráfica la planificación para los proyectos.

| Proyecto | Fecha inicio | Fecha final | Duración (días) |
|---|---|---|---|
| PR1 | 01/06/2017 | 28/11/2017 | 180 |
| PR2 | 01/07/2017 | 31/07/2017 | 30 |
| PR3 | 01/09/2017 | 01/10/2017 | 30 |
| PR4 | 01/10/2017 | 31/10/2017 | 30 |
| PR5 | 01/06/2017 | 01/07/2017 | 30 |
| PR6 | 01/06/2017 | 01/06/2018 | 365 |
| PR7 | 01/11/2017 | 01/12/2017 | 30 |
| PR8 | 01/06/2017 | 01/06/2018 | 365 |
| PR9 | 01/06/2017 | 01/06/2018 | 365 |
| PR10 | 01/12/2017 | 31/12/2017 | 30 |

**Tabla 11:** Fechas y duración de los proyectos.

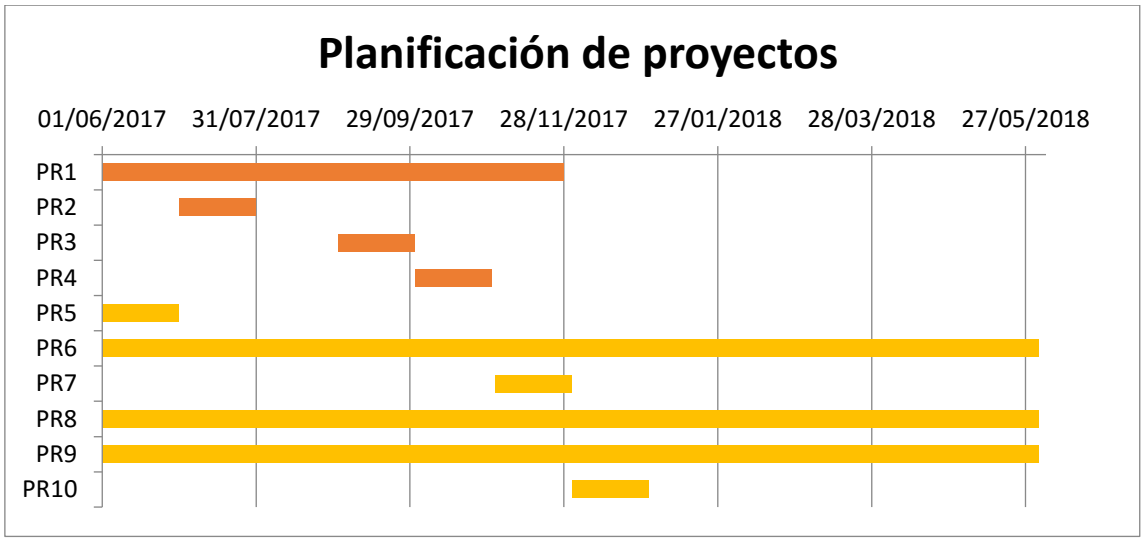


**Figura 8:** Diagrama de Gantt planificación proyectos

Todos los proyectos propuestos contribuyen a una mejora del riesgo de la Organización, el riesgo evoluciona de forma positiva, reduciendo la frecuencia de las amenazas y por tanto el riesgo al que están expuestos los activos.

En la siguiente tabla podemos observar el impacto sobre la seguridad que han tenido los proyectos propuestos:

| AMBITO | ACTIVO | Impacto Potencial | | | | | Frecuencia | Riesgo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | C | I | D | A | Valor | A | C | I | D | A |
| Instalaciones | CPD externo | 0 | 640 | 1000 | 1000 | 0 | 0,1 | 0 | 64 | 100 | 100 | 0 |
| | Sedes (14) | 0 | 400 | 300 | 500 | 0 | 0,1 | 0 | 40 | 30 | 50 | 0 |
| | CPD sedes | 0 | 560 | 800 | 900 | 0 | 0,1 | 0 | 56 | 80 | 90 | 0 |
| Hardware | PCs | 400 | 400 | 500 | 600 | 0 | 0,1 | 40 | 40 | 50 | 60 | 0 |
| | Portátiles | 400 | 500 | 500 | 500 | 0 | 0,1 | 40 | 50 | 50 | 50 | 0 |
| | Impresoras | 300 | 400 | 300 | 300 | 0 | 0,1 | 30 | 40 | 30 | 30 | 0 |
| | Servidores | 900 | 900 | 900 | 900 | 0 | 0,1 | 90 | 90 | 90 | 90 | 0 |
| | Centralita | 900 | 900 | 900 | 900 | 0 | 0,1 | 90 | 90 | 90 | 90 | 0 |
| | Teléfonos | 400 | 400 | 500 | 600 | 0 | 0,1 | 40 | 40 | 50 | 60 | 0 |
| Aplicaciones | Windows server | 400 | 700 | 800 | 800 | 0 | 0,1 | 40 | 70 | 80 | 80 | 0 |
| | Windows profesional 7 | 300 | 200 | 200 | 200 | 0 | 0,1 | 30 | 20 | 20 | 20 | 0 |
| | Windows profesional 10 | 300 | 200 | 200 | 200 | 0 | 0,1 | 30 | 20 | 20 | 20 | 0 |
| | Microsoft Office | 300 | 200 | 200 | 200 | 0 | 0,1 | 30 | 20 | 20 | 20 | 0 |
| | Java | 200 | 200 | 200 | 100 | 0 | 0,1 | 20 | 20 | 20 | 10 | 0 |
| | Antivirus | 600 | 100 | 400 | 500 | 0 | 0,1 | 60 | 10 | 40 | 50 | 0 |
| | UCI Altitude | 600 | 400 | 800 | 900 | 0 | 0,1 | 60 | 40 | 80 | 90 | 0 |
| | CRM Microsoft | 600 | 400 | 800 | 900 | 0 | 0,1 | 60 | 40 | 80 | 90 | 0 |
| Datos | Bases de Datos de clientes | 700 | 800 | 900 | 700 | 0 | 0,1 | 70 | 80 | 90 | 70 | 0 |
| | Código fuente desarrollos | 700 | 800 | 900 | 600 | 0 | 0,1 | 70 | 80 | 90 | 60 | 0 |
| | Datos financieros | 400 | 500 | 900 | 600 | 0 | 0,1 | 40 | 50 | 90 | 60 | 0 |
| | Backups | 700 | 900 | 1000 | 500 | 0 | 0,1 | 70 | 90 | 100 | 50 | 0 |
| | Datos de acceso | 800 | 1000 | 1000 | 800 | 0 | 0,1 | 80 | 100 | 100 | 80 | 0 |
| | Datos de configuraciones | 700 | 500 | 900 | 600 | 0 | 0,1 | 70 | 50 | 90 | 60 | 0 |
| Red | Cableado de red | 300 | 100 | 700 | 800 | 0 | 0,1 | 30 | 10 | 70 | 80 | 0 |
| | Routers | 700 | 700 | 900 | 1000 | 0 | 0,1 | 70 | 70 | 90 | 100 | 0 |
| | Switches | 700 | 700 | 900 | 1000 | 0 | 0,1 | 70 | 70 | 90 | 100 | 0 |
| | Antenas wifi | 700 | 700 | 900 | 700 | 0 | 0,1 | 70 | 70 | 90 | 70 | 0 |
| Servicios | Correo electrónico | 700 | 700 | 800 | 700 | 500 | 0,1 | 70 | 70 | 80 | 70 | 50 |
| | Servicios Web | 800 | 700 | 900 | 900 | 600 | 0,1 | 80 | 70 | 90 | 90 | 60 |
| Equipamiento auxiliar | SAIs | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| | Grupos electrógenos | 0 | 0 | 0 | 1000 | 0 | 0,1 | 0 | 0 | 0 | 100 | 0 |
| Personal | Responsables de TI | 0 | 600 | 125 | 600 | 0 | 0,1 | 0 | 60 | 12,5 | 60 | 0 |
| | Técnicos de sistemas | 0 | 500 | 200 | 675 | 0 | 0,1 | 0 | 50 | 20 | 67,5 | 0 |
| | Técnicos de desarrollo | 0 | 500 | 200 | 600 | 0 | 0,1 | 0 | 50 | 20 | 60 | 0 |

**Tabla 12:** Tabla cálculo de riesgo tres la ejecución de los proyectos.

Al mismo tiempo los proyectos propuestos también contribuyen a mejorar el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002.

En el Anexo XIII se recoge el detalle del análisis diferencial posterior a la implementación de los proyectos, que nos permite conocer el nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002:2013.

En el siguiente gráfico, se muestra la evolución en el nivel de cumplimiento, que ha ido evolucionado hacía un nivel de madurez optimizado en la mayoría de dominios que no alcanzaban este nivel.

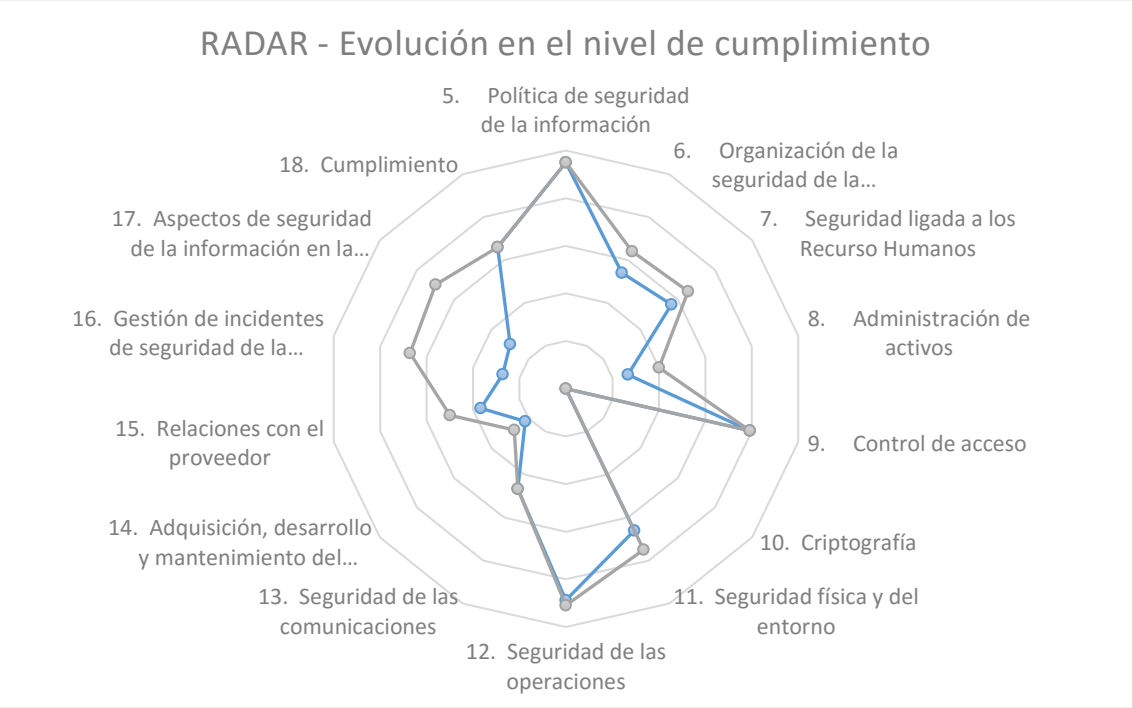


**Figura 9:** Gráfico radar evolución en el nivel de cumplimiento tres ejecución de proyectos.

# 6. FASE 5: Auditoría de cumplimiento de ISO/IEC 27002:2013

Tras el trabajo previo realizado en las fases anteriores, llega el momento de evaluar la seguridad actual de la compañía, para ello se procederá a realizar una auditoría en el marco de la ISO/IEC 27002:2013, que tiene por cometido determinar el nivel de cumplimiento de la compañía TMK S.A. con la norma de referencia.

La auditoría se basará en las 14 áreas y 35 objetivos de control de la ISO.

Tras finalizar la ejecución de proyectos (fase 4), se volvió a realizar el análisis diferencial (Anexo XIII)

| EFECTIVIDAD | CMM | SIGNIFICADO |
|---|---|---|
| (0%-10%) | L0 | Inexistente |
| [10%-50%) | L1 | Inicial / Ad-hoc |
| [50%-90%) | L2 | Reproducible, pero intuitivo |
| [90%-95%) | L3 | Proceso definido |
| [95%-100%) | L4 | Gestionado y medible |
| 100% | L5 | Optimizado |

**Tabla 13:** Tabla leyenda Modelo de Madurez de la Capacidad (CMM)

| Áreas ISO/IEC 27002:2013 | Fase 1 | Fase 5 |
|---|---|---|
| 5. Política de seguridad de la información | 95% | 95% |
| 6. Organización de la seguridad de la información | 54,00% | 64,00% |
| 7. Seguridad ligada a los Recurso Humanos | 57% | 66% |
| 8. Administración de activos | 26,67% | 40,00% |
| 9. Control de acceso | 79,17% | 79,17% |
| 10. Criptografía | 0% | 0% |
| 11. Seguridad física y del entorno | 66,11% | 75,00% |
| 12. Seguridad de las operaciones | 88,75% | 90,89% |
| 13. Seguridad de las comunicaciones | 46,67% | 46,67% |
| 14. Adquisición, desarrollo y mantenimiento del sistema | 21,85% | 27,78% |
| 15. Relaciones con el proveedor | 37% | 50% |
| 16. Gestión de incidentes de seguridad de la información | 27,14% | 67,14% |
| 17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio | 30% | 70% |
| 18. Cumplimiento | 66,00% | 66,00% |

**Tabla 14:** Tabla resumen evolución en el nivel de cumplimiento.

En referencia a los controles, tal y como podemos apreciar en el gráfico siguiente, aproximadamente el 50% han alcanzado un nivel de madurez superior a L3 (según la

clasificación CMM). Actualmente el 46% de los controles han alcanzado un grado de madurez L3 o superior, frente al 34% inicial. Si nos fijamos en el los controles que quedan en un nivel inferior a L3, la mayoría de los controles (40% de 54%), se encuentran en un nivel L2 (reproducible).

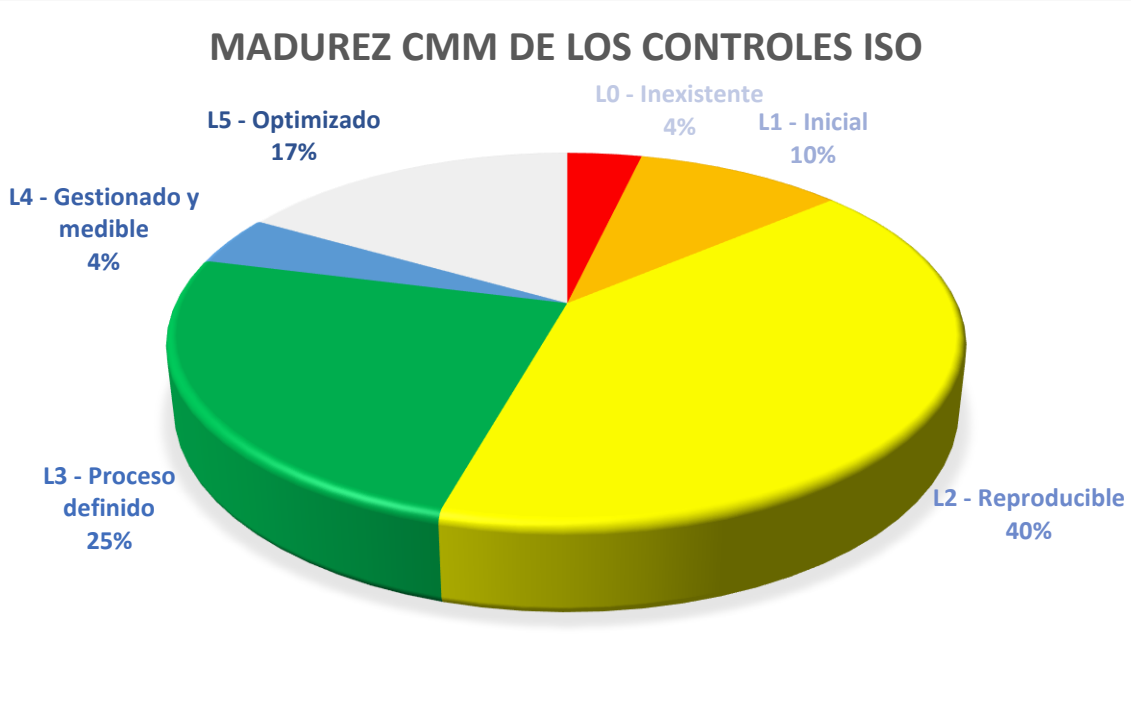


**Figura 10:** Gráfico madurez CMM de los controles ISO

Hay que tener en cuenta que el trabajo no finaliza aquí y que será necesario seguir mejorando la seguridad basándonos en la mejora continua.

En el Anexo XIV, se encuentra disponible el informe completo de la auditoría llevada a cabo tras la completa ejecución de todos los proyectos definidos y planificados en la fase 4 de este Plan Director de Seguridad de la Información para la compañía TMK S.A. Puesto que se presupone que la auditoría es llevada a cabo tras la ejecución de todos los proyectos, y estos finalizan el 31 de mayo de 2018, la auditoría tendrá lugar a continuación durante el mes de junio del año 2018.

# 7. FASE 6: Presentación de resultados y entrega de informes

Llegados a este punto se han completado todas las fases, previamente establecidas, para poner en marcha el Plan de Implementación de un SGSI para la compañía TMK S.A.

Esta última fase tiene como cometido proceder con la presentación del trabajo realizado, que comprende la siguiente documentación a entregar:

- Resumen ejecutivo.
- Memoria del Trabajo Final de Máster (presente documento).
- Video de presentación del Trabajo Final de Máster.
- Presentación del Trabajo Final de Máter *(Power Point)*

# 8. Conclusiones

Llegados a este punto tras haber desarrollado todas las fases planteadas, estamos en disposición de citar las conclusiones extraídas:

- Se ha evidenciado que el trabajo anteriormente realizado por TMK en materia de seguridad de la información, ha contribuido positivamente en la implantación de este PDS, partiendo de un nivel de cumplimiento superior al que se suele partir generalmente por primera vez.

- La seguridad de la compañía TMK S.A. ha mejorado con el Plan Director de Seguridad realizado en este trabajo como se evidencia al observar la evolución del nivel de cumplimiento.

- El trabajo realizado ha contribuido a mejorar el compromiso de la dirección respecto a la Seguridad de la Información y a incrementar la concienciación entre la dirección y empleados.

- Tras la realización del PDS podemos decir que la seguridad de TMK S.A. está "más ordenada". Hasta el momento se había invertido trabajo y esfuerzo en mejorar la seguridad pero de una forma no demasiado sistematizada o procedimentada. El seguimiento de las normas internacionales ISO/IEC 27001 y 27002 han contribuido muy favorablemente a la evolución de la seguridad de la compañía, y por tanto a posicionar a la compañía dentro del mercado del telemarketing.

**Futuras líneas de trabajo:**

- A partir del trabajo realizado y basado en la mejora continua, se propone iniciar otro Plan Director de Seguridad con el fin de seguir evolucionando el nivel de cumplimiento y por tanto la seguridad de TMK S.A.

- Este trabajo es el inicio para poder disponer en la compañía TMK S.A. de un Sistema de Gestión de Seguridad de la Información certificado conforme a la norma ISO/IEC 27001:2013.

# 9. Glosario

SGSI Sistema de Gestión de Seguridad de la Información

CRM *Customer Relationship Management* – Gestión de la relación con el cliente

BPO *Business Process Outsourcing* – Externalización de procesos de negocio

SAC Servicio de Atención al Cliente

CPD Centro de Proceso de Datos

TI Tecnologías de la Información

PDS Plan Director de Seguridad

CMM *Capacity Maturity Model* – Modelo de Madurez de la Capacidad

# 10. Bibliografía

[1] URL disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WTAcemjyi00
Consultado: 28/02/2017.

[2] URL disponible en: http://www.ticbeat.com/tecnologias/que-es-un-centro-de-datos-tier-iv-y-cuales-hay-en-espana/
Consultado: 03/03/2017.

[3] URL disponible en: http://es.wikipedia.org/wiki/Computer_Telephony_Integration
Consultado: 10/03/2017

[4] URL disponible en: http://secugest.blogspot.com.es/2006/10/definiendo-el-alcance-del-sgsi.html
Consultado: 12/03/2017

[5] URL disponible en: https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_catalogo%20de%20elementos_es_NIPO_630-12-171-8.pdf
Consultado: 23/03/2017

## 11. Anexos

# ANEXOS

# ANEXO I:

## Análisis diferencial inicial

| CONTROLES | Estado |
|---|---|
| **5. Política de seguridad de la información** | **95%** |
| 5.1. **Política de seguridad de la información** | **95%** |
| 5.1.1. Documento de política de seguridad de la información | 100% |
| 5.1.2. Revisión de la política de seguridad | 90% |
| **6. Organización de la seguridad de la información** | **54,00%** |
| 6.1. **Organización interna** | **58%** |
| 6.1.1. Roles y responsabilidades de la seguridad de la información | 90% |
| 6.1.2. Segregación de funciones | 50% |
| 6.1.3. Contacto con autoridades | 50% |
| 6.1.4. Contacto con grupos especiales de interés | 50% |
| 6.1.5. Seguridad de la información en la gestión del proyecto | 50% |
| 6.2. **Dispositivos móviles y trabajo remoto** | **50%** |
| 6.2.1. Política de dispositivos móviles | 10% |
| 6.2.2. Trabajo remoto | 90% |
| **7. Seguridad ligada a los Recurso Humanos** | **56,67%** |
| 7.1. **Previo al empleo** | **30%** |
| 7.1.1. Selección | 10% |
| 7.1.2. Términos y condiciones de la relación laboral | 50% |
| 7.2. **Durante el empleo** | **50%** |
| 7.2.1. Responsabilidad de la dirección | 90% |
| 7.2.2. Concienciación, educación y formación en seguridad de la información | 50% |
| 7.2.3. Proceso disciplinario | 10% |
| 7.3. **Desvinculación y cambio de empleo** | **90%** |
| 7.3.1. Responsabilidades en la desvinculación o cambio de empleo | 90% |
| **8. Administración de activos** | **26,67%** |
| 8.1. **Responsabilidad por los activos** | **20%** |
| 8.1.1. Inventario de activos | 10% |
| 8.1.2. Propiedad de los activos | 10% |
| 8.1.3. Uso aceptable de los activos | 10% |
| 8.1.4. Devolución de activos | 50% |
| 8.2. **Clasificación de la información** | **10%** |
| 8.2.1. Clasificación de la información | 10% |
| 8.2.2. Etiquetado de la información | 10% |
| 8.2.3. Manejo de activos | 10% |
| 8.3. **Manejo de los medios** | **50%** |
| 8.3.1. Gestión de los medios removibles | 50% |
| 8.3.2. Eliminación de los medios | 50% |
| 8.3.3. Transferencia física de medios | 50% |
| **9. Control de acceso** | **79,17%** |
| 9.1. **Requisitos de negocio para el control de acceso** | **90%** |
| 9.1.1. Política de control de acceso | 90% |
| 9.1.2. Accesos a las redes y a los servicios de red | 90% |
| 9.2. **Gestión de acceso del usuario** | **56,67%** |
| 9.2.1. Registro y cancelación de registro de usuarios | 50% |
| 9.2.2. Asignación de acceso de usuario | 10% |
| 9.2.3. Gestión de derechos de acceso privilegiados | 50% |
| 9.2.4. Gestión de información secreta de autenticación de usuarios | 50% |
| 9.2.5. Revisión de los derechos de acceso de usuario | 90% |
| 9.2.6. Eliminación o ajuste de los derechos de acceso | 90% |
| 9.3. **Responsabilidades del usuario** | **90%** |
| 9.3.1. Uso de información de autenticación secreta | 90% |

| | |
|---|---|
| 9.4. **Control de acceso al sistema y aplicaciones** | **80%** |
| 9.4.1. Restricción de acceso a la información | 50% |
| 9.4.2. Procedimientos de inicio de sesión seguro | 50% |
| 9.4.3. Sistema de gestión de contraseñas | 100% |
| 9.4.4. Uso de programas con privilegios de sistema | 100% |
| 9.4.5. Control de acceso al código fuente de los programas | 100% |
| **10. Criptografía** | **0%** |
| 10.1. **Controles criptográficos** | **0%** |
| 10.1.1. Política sobre el uso de controles criptográficos | 0% |
| 10.1.2. Gestión de claves | 0% |
| **11. Seguridad física y del entorno** | **66,11%** |
| 11.1. **Áreas seguras** | **73,33%** |
| 11.1.1. Perímetro de seguridad física | 100% |
| 11.1.2. Controles de acceso físico | 100% |
| 11.1.3. Seguridad de oficinas, salas e instalaciones | 90% |
| 11.1.4. Protección contra amenazas externas y del entorno | 50% |
| 11.1.5. Trabajo en áreas seguras | 50% |
| 11.1.6. Áreas de entrega y carga | 50% |
| 11.2. **Equipamiento** | **58,89%** |
| 11.2.1. Ubicación y protección del equipamiento | 90% |
| 11.2.2. Elementos de soporte | 90% |
| 11.2.3. Seguridad en el cableado | 10% |
| 11.2.4. Mantenimiento del equipamiento | 50% |
| 11.2.5. Retiro de activos | 50% |
| 11.2.6. Seguridad del equipamiento y los activos fuera de las instalaciones | 50% |
| 11.2.7. Seguridad en la reutilización o descarte de equipos | 50% |
| 11.2.8. Equipo de usuario desatendido | 90% |
| 11.2.9. Política de escritorio y pantalla limpios | 50% |
| **12. Seguridad de las operaciones** | **88,75%** |
| 12.1. **Procedimientos operacionales y responsabilidades** | **83,75%** |
| 12.1.1. Procedimientos de operación documentados | 50% |
| 12.1.2. Gestión de cambios | 100% |
| 12.1.3. Gestión de la capacidad | 95% |
| 12.1.4. Separación de los ambientes de desarrollo, prueba y operacionales | 90% |
| 12.2. **Protección contra código malicioso** | **90%** |
| 12.2.1. Controles contra código malicioso | 90% |
| 12.3. **Respaldo** | **90%** |
| 12.3.1. Respaldo de la información | 90% |
| 12.4. **Registro y monitoreo** | **62,50%** |
| 12.4.1. Registro de evento | 50% |
| 12.4.2. Protección de la información de registros | 50% |
| 12.4.3. Registros del administrador y el operador | 50% |
| 12.4.4. Sincronización de relojes | 100% |
| 12.5. **Control de software de operación** | **100%** |
| 12.5.1. Instalación del software en sistemas operaciones | 100% |
| 12.6. **Gestión de la vulnerabilidad técnica** | **95%** |
| 12.6.1. Gestión de las vulnerabilidades técnicas | 100% |
| 12.6.2. Restricciones sobre la instalación de software | 90% |
| 12.7. **Consideraciones de la auditoría de los sistemas de información** | **100%** |
| 12.7.1. Controles de auditoría de sistemas de información | 100% |

| | |
|---|---|
| **13. Seguridad de las comunicaciones** | **46,67%** |
| 13.1. **Gestión de la seguridad de red** | **33,33%** |
| 13.1.1. Controles de red | 50% |
| 13.1.2. Seguridad de los servicios de red | 50% |
| 13.1.3. Separación en las redes | 0% |
| 13.2. **Transferencia de información** | **60%** |
| 13.2.1. Políticas y procedimientos de transferencia de información | 50% |
| 13.2.2. Acuerdos sobre transferencia de información | 50% |
| 13.2.3. Mensajería electrónica | 50% |
| 13.2.4. Acuerdos de confidencialidad o no divulgación | 90% |
| **14. Adquisición, desarrollo y mantenimiento del sistema** | **22%** |
| 14.1. **Requisitos de seguridad de los sistemas de información** | **3,33%** |
| 14.1.1. Análisis y especificación de requisitos de seguridad de la información | 10% |
| 14.1.2. Aseguramiento de servicios de aplicación en redes públicas | 0% |
| 14.1.3. Protección de las transacciones de servicios de aplicación | 0% |
| 14.2. **Seguridad en procesos de desarrollo y soporte** | **62,22%** |
| 14.2.1. Política de desarrollo seguro | 50% |
| 14.2.2. Procedimientos de control de cambios del sistema | 90% |
| 14.2.3. Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación | 50% |
| 14.2.4. Restricciones en los cambios a los paquetes de software | 90% |
| 14.2.5. Principios de ingeniería de sistema seguro | 50% |
| 14.2.6. Entorno de desarrollo seguro | 50% |
| 14.2.7. Desarrollo externalizado | 0% |
| 14.2.8. Prueba de seguridad del sistema | 90% |
| 14.2.9. Prueba de aprobación del sistema | 90% |
| 14.3. **Datos de prueba** | **0%** |
| 14.3.1. Protección de datos de prueba | 0% |
| **15. Relaciones con el proveedor** | 37% |
| 15.1. **Seguridad de la información en las relaciones con el proveedor** | **23%** |
| 15.1.1. Política de seguridad de la información para las relaciones con el proveedor | 10% |
| 15.1.2. Abordar la seguridad dentro de los acuerdos del proveedor | 10% |
| 15.1.3. Cadena de suministro de tecnologías de la información y comunicaciones | 50% |
| 15.2. **Gestión de entrega del servicio del proveedor** | **50%** |
| 15.2.1. Supervisión y revisión de los servicios del proveedor | 50% |
| 15.2.2. Gestión de cambios a los servicios del proveedor | 50% |
| **16. Gestión de incidentes de seguridad de la información** | **27,14%** |
| 16.1. **Gestión de incidentes de seguridad de la información y mejoras** | **27,14%** |
| 16.1.1. Responsabilidades y procedimientos | 50% |
| 16.1.2. Informe de eventos de seguridad de la información | 50% |
| 16.1.3. Informe de las debilidades de seguridad de la información | 50% |
| 16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información | 10% |
| 16.1.5. Respuesta ante incidentes de seguridad de la información | 10% |
| 16.1.6. Aprendizaje de los incidentes de seguridad de la información | 10% |
| 16.1.7. Recolección de evidencia | 10% |
| **17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio** | 30% |
| 17.1. **Continuidad de la seguridad de la información** | **10%** |
| 17.1.1. Planificación de la continuidad de la seguridad de la información | 10% |
| 17.1.2. Implementación de la continuidad de la seguridad de la información | 10% |

| | |
|---|---|
| 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información | 10% |
| 17.2. **Redundancias** | **50%** |
| 17.2.1. Disponibilidad de las instalaciones de procesamiento de la información | 50% |
| **18. Cumplimiento** | **66,00%** |
| 18.1. **Cumplimiento con los requisitos legales y contractuales** | **42%** |
| 18.1.1. Identificación de la legislación vigente y los requisitos contractuales | 50% |
| 18.1.2. Derechos de propiedad intelectual | 50% |
| 18.1.3. Protección de los registros | 50% |
| 18.1.4. Privacidad y protección de la información de identificación personal | 50% |
| 18.1.5. Regulación de los controles criptográficos | 10% |
| 18.2. **Revisiones de seguridad de la información** | **90%** |
| 18.2.1. Revisión independiente de la seguridad de la información | 90% |
| 18.2.2. Cumplimiento con las políticas y normas de seguridad | 90% |
| 18.2.3. Verificación del cumplimiento técnico | 90% |

# ANEXO II:

## DOC-01-SEG Política de Seguridad

| **Documento** | | DOC-01-SEG Política de seguridad | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

# 1. Objeto

TMK S.A. es una compañía dedicada a los *Contact Center* y plenamente consciente de la importancia que tiene la seguridad de la información en el desarrollo de su negocio, en el marco de la implantación de un Sistema de Gestión de Seguridad de la Información suscribe la presente política.
En este documento se redacta la política de seguridad de la compañía enmarcada en la norma internacional ISO/IEC 27001.

# 2. Alcance

La política de seguridad es de aplicación a todo el personal y activos de TMK S.A., la dirección es responsable de ponerla en su conocimiento y de comunicarla a todas las partes interesadas.

# 3. Política de Seguridad de la Información

## 3.1. Objetivos de Seguridad

TMK S.A. establece, define y revisa unos objetivos para todos sus activos físicos y lógicos de información de la compañía, encaminados a mejorar su seguridad, comprometiéndose con la conservación de la confidencialidad, disponibilidad e integridad de su información así como de los sistemas que la soportan, aumentando la confianza de clientes y otras partes interesadas; sumado con el cumplimiento de todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

## 3.2. Funciones y áreas de responsabilidad

La dirección de la compañía tiene la responsabilidad de la gestión de los valores de TMK S.A. de forma eficaz y satisfactoria de acuerdo con las leyes actuales, los requisitos y los contratos.

El director de TI es el propietario de la política de seguridad tiene la responsabilidad de la seguridad de la información en TMK S.A. de acuerdo a la política de seguridad. Todo cambio en la política de seguridad debe ser aprobado por el director de TI. Es el responsable de publicar las políticas y normativas relacionadas con la seguridad de la información.

El responsable de seguridad de la información de la compañía reporta al director de TI. También es el responsable de auditorías de TI y de protección de datos. Entre sus funciones tiene la de responsabilizarse de la edición y revisión de la política.
Los propietarios de los sistemas, que son a su vez sus administradores junto a sus equipos, están claramente identificados y tienen identificados los grupos de usuarios

para gestión de los accesos a la información. Gestionan las características de las políticas de acceso a los sistemas y datos.
Los usuarios de los sistemas de información son responsables del adecuado uso de estos de acuerdo a la política de seguridad de la información.

# 4. Acceso a la información

## 4.1. Por parte de las personas

La compañía TMK S.A. exigirá la firma de un acuerdo de confidencialidad a sus empleados, empresas proveedoras y otros usuarios que deban tener acceso a información sensible o interna, en el momento que se inicie su relación contractual u operativa.
Empleados y proveedores serán formados e informados en relación a la política de seguridad y procedimientos internos de la compañía.
El no cumplimiento de la política de seguridad de la información podrá dar lugar a sanciones contempladas por la legislación vigente y el convenio del sector del telemarketing.
Los sistemas de información y datos propiedad de TMK S.A. no podrán ser utilizados fuera del marco de la compañía. No se permite el uso personal de los activos de la compañía, salvo que sea expresamente autorizado su uso.
Al finalizar la relación contractual u operativa entre empleados o proveedores y TMK S.A. los activos físicos o de información deberán ser entregados y TMK S.A. procederá a la eliminación o baja de los accesos a la información vigentes.

## 4.2. Seguridad física

Los sistemas y la información que requiere protección deberán ubicarse en zonas físicamente seguras con control de acceso restringido únicamente a personal con autorización de acceso y existirá un registro de accesos.
Las zonas seguras deben localizarse identificadas y documentadas y tendrán un propietario que será el encargado de autorizar el acceso a las mismas.
Los empleados y visitantes en los edificios de la compañía tienen obligación a portar de forma visible los elementos identificativos que se les ha proporcionado. Estos elementos identificativos son de uso personal e intransferible.

## 4.3. Acceso a los sistemas

Todo sistema de TMK S.A. requiere previa autenticación para poder acceder. La autenticación se realiza mediante usuarios individuales y únicos con contraseña. Los usuarios tienen deber de mantener en secreto su contraseña y es responsable del posible mal uso que se realice con sus credenciales de acceso a los sistemas.

Las contraseñas de acceso de los usuarios serán cambiadas periódicamente y deberán cumplir una serie de requisitos de seguridad como longitud mínima, uso de diferentes caracteres, complejidad, etc.
Todo usuario tiene la obligación de reportar los incidentes en materia de seguridad utilizando las directrices establecidas por TMK S.A.
Los usuarios serán creados previa solicitud por personal autorizado (personal de recursos humanos o responsables de cada área de la compañía con autorización). Se deberá especificar el uso o limitaciones de los usuarios.

### 4.4. Accesos remotos

Para que se autoricen accesos remotos a sistemas de información de TMK S.A. será necesario confirmar que se ha leído y entendido la política de seguridad de TMK.S.A, para ello deberá ser aceptada de forma explícita.
Únicamente se permite acceso remoto a la red de TMK S.A. mediante soluciones de seguridad certificadas y aprobadas por el departamento de TI.

## 5. Gestión de incidentes

Se tratarán como incidentes de seguridad todo incumplimiento de la política de seguridad, mal uso de sistemas de información y comportamientos que pongan en riesgo la seguridad.
Los empleados deben reportar los incidentes de seguridad del mismo modo que comunican cualquier otro incidente que acontece en su día a día y estos en función de su criticidad serán reportados a los responsables de seguridad.
Los incidentes de seguridad relevantes serán tratados por el Comité de Seguridad de la Información, el cual contará entre sus integrantes al Director de TI (como miembro de la dirección) y el responsable de seguridad de la información.

## 6. Referencias

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

# ANEXO III:

PR-01-SEG Procedimiento de auditorías internas

| **Documento** | | PR-01-SEG Procedimiento de auditorías internas | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

# 1. Objetivo

Documento que establece el procedimiento de auditorías internas a llevar a cabo en la compañía TMK S.A. Incluye planificación de las auditorías, requisitos que establecerán los auditores internos y el modelo de informe final de la auditoría.

# 2. Alcance

El procedimiento aplica a las auditorías internas a realizar en el marco del Sistema de Gestión de la Seguridad de la Información de la compañía TMK S.A.

# 3. Plan de auditoría

El plan de auditoría será definido por el responsable de seguridad de la información de TMK S.A. y se establece una periodicidad anual para las mismas.
El plan de auditoría incluirá los puntos a auditar y áreas a auditar y establecerá una agenda prevista (fecha y hora) para cada área a auditar.
También detallará el equipo que llevará a cabo la auditoría interna. El personal puede ser propio o externo a la compañía pero en ambos casos deberá mostrar independencia con los procesos a auditar.

## 3.1. Previo a la auditoría

Una vez aprobado el plan de auditoría, esta deberá ser comunicada a todos los implicados con la suficiente antelación (al menos 10 días laborables).
El auditor o auditores deberán contar con la cualificación adecuada para llevar a cabo a auditoría. Deberá acreditar certificación de auditor para la norma ISO/IEC 27001.

## 3.2. Realización auditoría

El objetivo de la auditoría es determinar el grado de cumplimiento del SGSI con la norma ISO/IEC 27001, por lo que se procederá a la revisión de los puntos que contempla la norma, así como sus controles asociados (ISO/IEC 27002).

Con el fin de revisar todos los puntos y controles de la normativa, el equipo auditor mantendrá reuniones con las diferentes áreas convocadas a la auditoría en las que se entrevistará con los implicados. En estas reuniones el equipo auditor requerirá documentación, revisará evidencias, realizará inspecciones visuales, etc. El área auditada deberá facilitar el trabajo del equipo auditor con disposición de atender todos sus requerimientos.
El auditor tomará nota de la inspección realizada y en el informe final dejará de forma clara y explícita las no conformidades (respecto la norma) encontradas, así como los puntos a mejorar, u observaciones.

Finalmente se realizará una reunión final de resumen en el que se comentarán las no conformidades encontradas y se dispondrá de la fecha en que se entregará el informe

de la auditoría (al final de este documento se encuentro una plantilla tipo con la información que debe incluir el informe, el formato puede variar).

### 3.3. Resultado de auditoría

Una vez entregado el informe de la auditoría este será analizado por el responsable de seguridad y por el comité de seguridad a fin de establecer un plan de acción a llevar a cabo para solucionar las no conformidades, si las ha habido, los puntos identificados como mejora y las observaciones realizadas.

## 4. Plan de acción

El plan de acción a llevar a cabo estará dividido en actividades acotadas y bien definidas, con una persona responsable, y el tiempo en que debe ser cada actividad completada.

## 5. Referencias

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

## 6. Informe de auditoría interna

### INFORME DE AUDITORÍA

**Control de Versiones**

| Versión | Modificaciones |
|---|---|
| | |

**Datos de la auditoría y compañía auditada**

| |
|---|
| **Fecha de la auditoría:** |
| **Ubicación (lugar) de la auditoría:** |
| **Organización/Compañía auditada:** |

**Equipo auditor:**

| |
|---|
| |

**Áreas y personal auditado:**

| |
|---|
| |

| Plan de auditoría | | | | 5 Políticas de seguridad de la información | 6 Organización de la seguridad de la información | 7 Seguridad relativa a los recursos humanos | 8 Gestión de activos | 9 Control de acceso | 10 Criptografía | 11 Seguridad física y del entorno | 12 Seguridad de las operaciones | 13 Seguridad de las comunicaciones | 14 Adquisición, desarrollo y mantenimiento de los sistemas de información | 15 Relación con proveedores | 16 Gestión de incidentes de seguridad de la información | 17Aspectos de seguridad de la información para la gestión de la continuidad del negocio | 18 Cumplimiento |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DIA | CENTRO | HORA | ÁREA / DEPARTAMENTO / RESPONSABLE | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

**Objetivo**

**Alcance**

**Normas de referencia:**

## RESULTADOS

### Controles

| Objetivos de control | Descripción | Resultado (OK/AM/NOK) | Comentarios |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**No Conformidad Menor:** Desviación mínima en relación con requisitos normativos, propios de la organización y/o legales y no afecta a la eficiencia e integridad del sistema de Gestión.

**No Conformidad Mayor:** Incumplimiento de un requisito normativo, propio de la organización y/o legal, que vulnera o pone en serio riesgo la integridad del sistema de gestión. Puede corresponder a la no aplicación de una cláusula de una norma (requerida por la organización), el desarrollo de un proceso sin control, ausencia consistente de registros declarados por la organización o exigidos por la norma, o la repetición permanente y prolongada a través del tiempo de pequeños incumplimientos asociados a un mismo proceso o actividad.

| No Conformidades Mayores | No Conformidades Menores | Observaciones |
|---|---|---|
| | | |

**Resumen auditoría**

**Conclusiones finales**

# ANEXO IV:

## DOC-02-SEG Gestión de indicadores

| **Documento** | | DOC-02-SEG Gestión de indicadores | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

## 1. Objetivo

El objetivo del documento de gestión de indicadores es la definición de indicadores para medir la eficacia de los controles de seguridad implantados.

## 2. Alcance

Aplica a los controles del SGSI, correspondientes a la norma ISO/IEC 27002:2013.

## 3. Definición de indicadores

Se deberán definir indicadores para cada punto de la norma ISO/IEC 27001. Para cada indicador se definirá un límite máximo que determinará el cumplimiento del indicador.
Cada indicador tendrá un responsable y será identificado de forma única y se acompañará de una pequeña descripción que ayude a su interpretación
A continuación se indican algunos parámetros que ayudan a definir los diferentes indicadores:

- Frecuencia
- Valor mínimo y/o máximo
- Valor obtenido o resultado

## 4. Informe

El resultado de los indicadores debe quedar registrado en un único documento para cada ciclo establecido a modo de informe.

## 5. Referencias

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

# ANEXO IV:

PR-02-SEG Procedimiento de revisión por la dirección

| **Documento** | | DOC-02-SEG Procedimiento de revisión por la dirección | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

## 1. Objetivo

El presente procedimiento describe la revisión anual que debe ser realizada por la dirección de TMK S.A. Deben revisarse las cuestiones más importantes que han ido sucediendo en relación al Sistema de Gestión de la Seguridad de la Información.

## 2. Alcance

El alcance está enmarcado en el SGSI de TMK S.A.

## 3. Revisión

La revisión debe contemplar las oportunidades de mejora identificadas y las necesidades de cambio en el SGSI, incluyendo la política y los objetivos de seguridad de la información. Los resultados de las revisiones deben quedar documentados y mantener los registros.
Se presentará a la dirección de TMK S.A. un informe de revisión que incluirá los siguientes apartados:

- Resultados de auditorías y revisiones de SGSI.
- Comentarios provenientes de las partes interesadas (empleados, clientes, proveedores, responsable de seguridad, etc.)
- Técnicas, productos o procedimientos que podrían utilizarse dentro de la organización para mejorar el comportamiento y la eficacia del SGSI.
- Vulnerabilidades o amenazas no abordadas en la evaluación de riegos previa;
- Cumplimiento de los objetivos de seguridad de la información (resultados y mediciones)
- Estado de las acciones realizadas desde la última revisión de la Dirección
- Actualización de la política de seguridad
- Cambios que pudiesen afectar el SGSI;
- Oportunidades y mejoras detectadas

Tras la revisión realizada con la dirección se emitirá una actualización del informe presentado en el que se incluirá cualquier decisión y acción relativa a:

- Mejora de la eficacia del SGSI;

- Actualización de la evaluación de riesgos y plan de tratamiento de riesgos
- Modificación de los procedimientos y controles que afectan a la seguridad de la información cuando sea necesario para responder a los eventos internos o externos que pueden afectar al SGSI, incluyendo cambios en:
    - Requisitos de negocio
    - Requisitos de seguridad
    - Procesos de negocio que afectan a los requisitos de negocio existentes.
    - Requisitos legales o reglamentarios
    - Obligaciones contractuales
    - Niveles de riesgo y/o criterios de aceptación de los riesgos
- Necesidades de recursos
- Mejora en las métricas de los controles

## 4. Referencias

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

# ANEXO VI:

DOC-03-SEG Gestión de roles y responsabilidades

| **Documento** | | DOC-03-SEG Gestión de roles y responsabilidades | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

# 1. Objetivo

El objetivo del presente documento es documentar los roles y responsabilidades en materia de seguridad, del personal relacionado con el SGSI.

# 2. Alcance

Las directrices y normas descritas en el presente documento aplican al personal relacionado con el SGSI de la compañía.

# 3. Modelo organizativo

La responsabilidad con la seguridad de la información recae en todos los integrantes de la organización. Se definen tres roles: propietario, custodio y usuario.

## 3.1. Roles

- Propietario: es responsable de definir el uso correcto de los activos de los que es propietario. Los propietarios son personal interno (empleados) y preferentemente tendrán un puesto directivo o de responsabilidad.

  En materia de seguridad el propietario de un activo es el responsable de mantenerlo, determinar su criticidad y clasificación, establecer los requerimientos de protección y conceder o eliminar permisos de acceso a los usuarios.

  Todo propietario debe definir y revisar periódicamente la clasificación de sus activos y las restricciones de acceso a cada uno de ellos.

  Los propietarios deben asegurar que tanto la información, como los activos asociados con los recursos para su tratamiento, son utilizados según las normas vigentes aplicables a la clasificación de la información.

  Los propietarios pueden delegar tareas rutinarias, pero nunca la responsabilidad.

  Por tanto, el propietario de la información tendrá las siguientes funciones:

  - Conocer cómo se usa su información dentro y fuera de la organización, entendiendo también los problemas potenciales asociados al uso de esta información.

  - Clasificar la información basándose en su sensibilidad y criticidad. Las escalas de sensibilidad y criticidad no son desarrolladas por el Propietario, sino por el Área de Seguridad de la Información.

- Aprobar todos los requisitos de acceso a la información de la que ha sido designado.

- Los custodios de los activos son los encargados de establecer y mantener los controles adecuados para proteger la información de acuerdo al nivel de protección requerido por el propietario.

  Tienen las siguientes funciones:

  - Salvaguardar el almacenamiento y procesamiento seguro de la información, como puede ser el respaldo diario de la información y la administración de los sistemas de control de accesos.
  - Cumplir las instrucciones del propietario de la información.
  - Gestionar diariamente la información que le ha sido encomendada, incluyendo el soporte técnico.
  - Informar periódicamente al propietario sobre todo el que tenga acceso a la información en cuestión.
  - Proveer asesoramiento técnico sobre las mejores formas de proteger la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información.

- El rol usuario es aquel que tiene acceso a la información y/o sistemas de la organización. Podrán ser clientes, empleados, personal temporal o personal externo. Sus permisos de acceso deberán ser revocados cuando cese la necesidad de acceder a una información en concreto.

  Funciones para el usuario:

  - Solicitar al correspondiente propietario los accesos a la información y sistemas.
  - Utilizar la información únicamente para el propósito para el que ha sido autorizado por parte del propietario.
  - Manejar de forma segura la información a la que se la ha concedido acceso.
  - Informar al propietario o a su superior inmediato, de los errores o anomalías en la información a la cual tiene acceso.
  - Consultar de inmediato a los especialistas en seguridad cuando se produzca una incidencia sospechosa o fallo de seguridad.

## 4. Actividades de seguridad

- Definición de la seguridad:
    - Establecer los requisitos y necesidades de seguridad detectados mediante las peticiones realizadas por el usuario.
    - Definir las Normativas de Seguridad de la Información.
    - Definir la tecnología de la Seguridad de la Información.
    - Definir la Estrategia de la Seguridad de la Información.
    - Definir las Responsabilidades de la Seguridad de la Información.

- Implantación de la seguridad:
    - Satisfacer los requisitos de seguridad definidos.
    - Asegurar el pase a producción óptimo de aplicaciones/sistemas.
    - Entregar a la unidad de gestión, el sistema o módulo implantado para su supervisión.
    - Detectar y reportar al Área de Seguridad de la Información cualquier anomalía en la implantación que afecte al cumplimiento de los requisitos definidos.
    - Dar soporte en todo el ciclo de vida de los sistemas o módulos de seguridad de la Información a las áreas responsables de su explotación y administración.
- Gestión de la seguridad
    - Mantener y supervisar la operación satisfactoria del sistema o módulo de seguridad implantado.
    - Acometer todas las tareas de operación, administración y explotación de los sistemas o módulos de seguridad implantados.
    - Satisfacer los requisitos de seguridad definidos.
- Auditoría de la seguridad
    - Recopilar los requisitos de seguridad definidos en estudios previos de la aplicación o sistema y verificar/contrastar su cumplimiento, tanto en la fase de implantación, como durante el resto de vida de la aplicación o sistema.

- Informar al Comité de Dirección de los resultados de la auditoría realizada sobre el cumplimiento de la política de seguridad.

## 5. Comité de seguridad

El principal objetivo del comité de seguridad es la de promover la seguridad de la información con el compromiso de la dirección de la compañía. También son objetivos del comité de seguridad (en adelante CSI), coordinador y velar por el alineamiento de los objetivos de seguridad con los objetivos del negocio de la compañía y establecer una vía de comunicación con el comité de dirección de TMK S.A.

El CSI estará constituido por representantes de áreas competentes en materia de seguridad, además de un responsable de la dirección:

- Presidente del comité, director de TI (miembro de la dirección de TMK S.A.).
- Responsable del comité, responsable de seguridad de la información.
- Responsable de desarrollo.
- Responsable sistemas IT.
- Responsable RRHH-
- Responsable de cumplimiento legal y normativo.
- Responsable infraestructuras y seguridad física.
- Responsables de negocio.

El CSI estará liderado por el director IT, miembro de la dirección de TMK S.A. y le corresponden las funciones:

- Representación del CSI en los comités de dirección de TMK S.A.
- Legitimar con su aprobación las decisiones del CSI.
- Visado de actas en las reuniones.

Al responsable de seguridad le corresponden las funciones:

- Convocar al CSI
- Dirigir las reuniones del CSI

### 5.1. Reuniones del Comité

El Responsable de Seguridad propondrá la convocatoria del mismo siempre que:

- Aparezcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad que requieran la participación de las distintas áreas que forman el CSI.

- Periódicamente, normalmente cada mes. Nunca se dilatará más de tres meses el periodo entre la celebración de un CSI y el siguiente.

Cuando la materia de los asuntos a tratar así lo requiera, el Responsable de Seguridad podrá invitar a las reuniones, con voz, pero sin voto, a aquellas personas que por sus conocimientos o experiencia estime conveniente para el mejor asesoramiento del CSI.

### 5.1.1. Acta

De cada sesión se levantará un acta, indicando los asistentes, un resumen de los asuntos tratados, las decisiones acordadas, así como cualquier otro tema que los miembros del CSI soliciten expresamente.

### 5.1.2. Reporte

El Responsable del CSI reportará al Comité Directivo de la Organización. Los reportes tratarán la situación actual, las decisiones tomadas por el CSI y aquellas cuestiones para las cuales el Comité no tenga potestad suficiente para decidir.

## 5.2. Funciones del Comité de Seguridad de la Información

El CSI desempeñará las funciones en relación a la seguridad de la información que se le citan a continuación:

- Revisión y propuesta de la Política de Seguridad de la Información, para su aprobación en el Comité de Dirección.
- Fijar las directrices y responsabilidades principales en materia de seguridad que garanticen la disponibilidad, integridad, auditabilidad, autenticidad y confidencialidad de la información.
- Formalizar y mantener el cuerpo normativo de seguridad, orientado al cumplimiento de los estándares de seguridad ISO/IEC 27001:2013 y ISO/IEC 27002, así como la legislación aplicable.
- Coordinar los esfuerzos de todas las áreas con responsabilidades sobre la seguridad de la información, para asegurar que los esfuerzos sean consistentes y se evitan duplicidades.
- Coordinar todos los proyectos de mejora o cambio de la seguridad de la información, en cualquier ámbito.
- Promover mecanismos para asegurar la concienciación, educación y formación en materia de seguridad de todo el personal.
- Participar en la evaluación de riesgos para determinar el impacto de las amenazas sobre los activos de la Organización.
- Supervisar y controlar los cambios significativos en la exposición de los activos de información a las amenazas principales, así como las incidencias ocurridas.

- Promover la mejora continua del sistema de gestión de la seguridad de la información poniendo los recursos necesarios para ello, respaldando las iniciativas y acciones de mejora de la seguridad en los sistemas de información y promoviendo los proyectos que se requieran para la implantación de las medidas y acciones de seguridad acordes con el nivel de riesgo.

- Coordinar y promover las acciones necesarias, relacionadas con el cumplimiento legal y normativo, en temas relacionados con la seguridad de la información.

- Revisar los Planes de Contingencias y Continuidad de Negocio desarrollados, a fin de asegurar que se cumplen los estándares de la Organización y que se han integrado todas las prácticas de planificación recomendadas.

# 6. Roles y funciones de seguridad

## 6.1. Presidente del Comité

El rol del Presidente del CSI, máximo responsable de seguridad de la información dentro de la Organización, dirige, coordina, planifica y organiza las actividades de seguridad de la información en toda la organización.

En ausencia del presidente delegará sus funciones en un responsable de su dirección y también miembros del CSI: responsable de desarrollo, o responsable de sistemas IT.
En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará al Comité de Dirección.

Funciones y Responsabilidades:

- Entender los principales servicios prestados por la Organización y, supervisar y coordinar las soluciones propuestas para proteger la información de dichos servicios, en todos los ámbitos de la seguridad de la información.

- Supervisar los Análisis de Riesgos periódicos que se lleven a cabo.

- Colaborar con el Responsable de Seguridad en la identificación del nivel de riesgo aceptable e identificar la mejor forma de reducir el riesgo hasta ese nivel.

- Aprobar un Plan de Tratamiento de Riesgo como propuesta a futuro de la gestión de la seguridad de la información, considerando todas las propuestas de los miembros del CSI.

- Definir las responsabilidades de seguridad de la información que cada individuo tiene, alineadas con los objetivos de negocio de la Organización.

- Aprobar planes de acción, priorizando las acciones propuestas por los diferentes miembros del Comité relacionados con la seguridad de la información, para la alineación con los objetivos del negocio de la Organización.
- Informar al Comité de Dirección de comunicados urgentes que puedan poner en riesgo la seguridad de la información, de forma que puedan efectuarse las acciones correctivas inmediatas.

## 6.2. Responsable del Comité

El Responsable de Seguridad de la Información tiene como objetivo asesorar y orientar a los miembros del CSI en todos los temas relacionados con la seguridad de la información.

En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará al Responsable del CSI.

Funciones y Responsabilidades:

- Entender los principales servicios prestados por la Organización y proponer soluciones para proteger la información de dichos servicios en su ámbito.
- Colaborar en la definición y refinamiento de los procedimientos para la identificación de activos de información y su clasificación.
- Participar en las evaluaciones periódicas de riesgos que se lleven a cabo en la Organización.
- Colaborar en la definición de las responsabilidades sobre la seguridad de la información que cada individuo tiene; asegurando el cumplimiento de las políticas y estándares establecidos.
- Proponer recomendaciones para proteger la información y los sistemas de información.
- Colaborar en la selección de herramientas que permitan monitorizar o asegurar el cumplimiento de las políticas y estándares de seguridad, apoyando los procesos de implantación.
- Definir un Plan de Tratamiento de Riesgo como propuesta a futuro de la gestión de la seguridad de la información, considerando todas las propuestas de los miembros del CSI.
- Definir planes de acción, priorizando las acciones propuestas por los diferentes miembros del Comité relacionados con la seguridad de la información, para la alineación con los objetivos del negocio de la Organización.

- Realizar controles internos sobre el estado de la seguridad.
- Documentar y realizar el seguimiento de todas las incidencias reportadas sobre aspectos relacionados con la seguridad lógica.
- Diseñar y gestionar procedimientos para la detección, investigación, corrección, acciones disciplinarias y/o denuncia, relacionados con las violaciones e incidentes de seguridad de la información.
- Dirigir el desarrollo de cuestionarios u otras herramientas que ayuden a los responsables de área a determinar el grado de conformidad con los requerimientos de seguridad lógica de la información dentro de sus respectivas áreas.
- Estar informado acerca de los avances más recientes en el campo de la seguridad de la información, incluyendo nuevos productos y servicios.
- Evaluar los informes de errores de los sistemas de información, informes de ataques publicados, y otras noticias de seguridad enviadas por proveedores, agencias del gobierno, universidades, asociaciones profesionales, etc.; realizando recomendaciones para tomar las medidas preventivas oportunas.
- Colaborar con el Comité en la resolución de incidentes de seguridad lógica y especialmente en aquellos que puedan dar origen a delitos y faltas tipificados en el derecho Penal, Civil, Convenios internacionales, etc.
- Colaborar con Recursos Humanos para llevar a la práctica mecanismos aprobados por el Comité para asegurar la concienciación, educación y formación en materia de seguridad de todo el personal y colaboradores.
- Comunicar a los responsables de las áreas auditadas los resultados de las auditorías, con el objetivo de que puedan resolver las no conformidades identificadas.
- Realizar un seguimiento sobre la resolución por parte de las áreas responsables de las no conformidades comunicadas.

## 6.3. Responsable de desarrollo y de servicios IT.

Son encargados de la operación efectiva de la seguridad lógica, estando al frente de la implantación de las soluciones diseñadas propias de seguridad o de aquellas cuestiones relativas a la infraestructura tecnológica que afecten a la seguridad.

En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará al Responsable del CSI.

Funciones y Responsabilidades:

- Participar en las evaluaciones periódicas de riesgos que se lleven a cabo en la Organización, en lo relativo a los aspectos tecnológicos de la seguridad.
- Definir soluciones para resolver los riesgos de seguridad tecnológicos identificados en los análisis de riesgos, así como proteger la información en la implantación de los nuevos sistemas.
- Implementar los controles de seguridad necesarios conforme a las directrices de la Política de Seguridad de la Información, incluyendo: sistemas de detección de virus, cortafuegos, monitorización de sistemas y de la red, control de accesos, copias de seguridad, herramientas de cifrado, etc.; coordinando los trabajos con los distintos responsables involucrados.
- Asistir al Responsable del Comité para analizar y gestionar los riesgos de la infraestructura tecnológica, determinar sus vulnerabilidades y establecer las medidas de salvaguarda que garanticen la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de la información de acuerdo a un riesgo residual asumido por la organización.

## 6.4. Responsables de Negocio

Máximos responsables de Negocio (Gerentes de Negocio).
En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reporta al Responsable del CSI.

Funciones y Responsabilidades:

- Entender los principales servicios prestados por la Organización y, supervisar y coordinar las soluciones propuestas para proteger la información de dichos servicios, en todos los ámbitos de la seguridad de la información.
- Participar en las evaluaciones periódicas de riesgos que se lleven a cabo.
- Determinar cuál es el nivel de riesgo aceptable en las operaciones de negocio.
- Analizar y realizar una evaluación del coste-beneficio de las soluciones de seguridad que afectan directamente a Operaciones.
- Velar por el cumplimiento de la Política de Seguridad de la Información en el ámbito de sus competencias y entre el personal de Operaciones.
- Definir e implantar Planes de Continuidad de Negocio para poder continuar operando en caso de desastre, desarrollando la metodología de evaluación de impactos ante desastres.

## 6.5. Responsable de Infraestructuras y seguridad física

Máximo responsable de la Seguridad Física en la Organización. En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará al Responsable del CSI.

Funciones y Responsabilidades:

- Entender los principales servicios prestados por la Organización y proponer soluciones para proteger la información de dichos servicios en su ámbito.
- Definir recomendaciones para minimizar amenazas sobre aspectos de seguridad física (fuego, tormentas de viento, inundación, terremoto, robo, secuestro, asalto, vandalismo y accidentes industriales).
- Participar en las evaluaciones periódicas de riesgos que se lleven a cabo.
- Supervisar la instalación, mantenimiento y operación de los sistemas de seguridad físicos.
- Realizar periódicamente revisiones físicas para determinar si las instalaciones están debidamente protegidas contra robo, vandalismo, explosión, fuego, inundación, terremoto, tormentas de viento y otras amenazas.
- Diseñar y supervisar la instalación y operación de sistemas de control de ambiente para las oficinas y otras áreas de la Organización, como aire acondicionado, calefacción, ventilación, drenaje, prevención eléctrica, etc.
- Supervisar el mantenimiento de los dispositivos de detección y extinción de incendios.
- Establecer y mantener el sistema de control de acceso físico que ayude a asegurar que los presentes en las instalaciones están autorizados y que se registran los accesos.
- Establecer y supervisar el grupo de guardias privados que mantienen la seguridad.
- Gestionar las llaves de puertas y armarios que protejan la información y la propiedad de la Organización. Distribuir estas llaves al personal autorizado y mantener copias de las mismas.
- Evaluar las propuestas de reformas en oficinas e instalaciones para asegurar que las medidas de seguridad han sido incluidas en el diseño.
- Investigar los últimos adelantos en seguridad física y protección ejecutiva, y recomendará productos y servicios específicos si son para beneficio de la Organización.

## 6.6. Responsable de Recursos Humanos

Es el máximo responsable de los RRHH en la Organización. En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará al Responsable del CSI.

Funciones y Responsabilidades:

- Definir los procesos de selección del personal, así como los perfiles funcionales dentro de la organización.
- Proporcionar la formación adecuada, en materia de seguridad de la información, y hacer llegar las actualizaciones regulares del marco normativo a empleados y colaboradores.
- Notificar a las áreas implicadas todas aquellas altas, bajas o modificaciones de personal a efectos de que se realicen las operaciones necesarias en los sistemas.
- Definir los procedimientos disciplinarios para los empleados que violen las políticas y procedimientos de seguridad de la organización.

## 6.7. Responsable del Cumplimiento Legal y Normativo

El Responsable de Cumplimiento legal es la persona encargada de velar que en la organización se observen los requerimientos legales en materia de seguridad de la información, asesorando y/o resolviendo sobre el conjunto de aspectos legales que inciden o pueden incidir sobre las tecnologías de la información y comunicaciones.

En el ámbito de las actividades relacionadas con la seguridad de la información y con el fin de que estas actividades se coordinen de forma centralizada, reportará funcionalmente al Responsable del CSI.

Funciones y Responsabilidades:

- Revisar y evaluar la legislación vigente dentro de la jurisdicción en la que se encuentra la Organización, recomendando las actuaciones pertinentes.
- Evaluar la responsabilidad legal que pueda recaer sobre la Dirección como consecuencia de incumplimientos legales o contractuales en materia de seguridad de la información. Así mismo, realizar las recomendaciones que sean necesarias.
- Participar, cuando sea necesario, en las evaluaciones periódicas de riesgos que se lleven a cabo.

- Efectuar recomendaciones para prevenir que la Organización asuma riesgos excesivos con implicaciones legales por el uso de las tecnologías.
- Actuar de vínculo con los organismos públicos de seguridad, como la Policía Nacional, la Guardia Civil o la Agencia Española de Protección de Datos.
- Colaborar en la definición del sistema de clasificación de la información y de los correspondientes controles que protejan la información sensible de la organización.
- Asistir en la redacción y revisión de documentos legales referentes a temas legislativos y normativos relacionados con la seguridad de la información, incluyendo las cláusulas de contratos del personal y con proveedores.
- Establecer y mantener un programa de conformidad para asegurar el cumplimiento con las leyes y regulaciones vigentes, y que con este programa se pueda demostrar dicha conformidad.
- Asesorar a los Responsables de los ficheros con datos de carácter personal sobre sus obligaciones en relación a las inscripciones de ficheros en la Agencia de Protección de Datos y la elaboración de los Documentos de Seguridad.
- Colaborar en la coordinación y control de las medidas de seguridad definidas para la protección de los ficheros y sistemas de información con datos de carácter personal; estas medidas serán las que hayan sido definidas en los documentos de seguridad por los responsables de los ficheros.
- Colaborar en la definición de las responsabilidades sobre la seguridad de la información que cada individuo tiene; asegurando el cumplimiento legal y normativo.
- Asesorar a RRHH para divulgar entre todos los empleados las directrices a tener en cuenta para asegurar el cumplimiento de la normativa vigente en cada momento.

## 7. Referencias

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

# ANEXO VII:

DOC-04-SEG Metodología de análisis de riesgos

| **Documento** | | DOC-04-SEG Metodología de análisis de riesgos | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

## 1. Objetivo

El presente documento define el enfoque para el análisis y evaluación de riesgos de seguridad de la información. El análisis de riesgos permite determinar que tiene la organización y estimar lo que podría ocurrir.

## 2. Alcance

Aplica al alcance del SGSI.

## 3. Análisis de riesgos

El análisis de riesgos considera los siguientes elementos:

1. Activos, que son los elementos del SGSI o íntimamente relacionados, que soportan el negocio.
2. Amenazas, que son las cosas que pueden pasar a los activos causando perjuicio en la organización
3. Salvaguardas, que son las medidas de protección desplegadas para que las amenazas no causen daño o para minimizarlo.

El análisis de riesgos permite analizar estos elementos metódicamente para llegar a conclusiones fundadas y proceder a la fase de tratamiento.

## 4. MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos que fue elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para el análisis de riesgos derivados del uso de las tecnologías de la información y comunicaciones (en adelante TIC) para así implementar las medidas de control adecuadas que permitan minimizar los riesgos.

Esta metodología presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.

## 5. Metodología

El análisis de riesgos determina el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, teniendo en cuenta el coste que supondría su degradación
2. Determinar a qué amenazas están expuestos los activos.

3. Determinar las salvaguardas existentes y si son eficaces frente al riesgo
4. Estimación del impacto (daño sobre el activo si se produce la amenaza)
5. Estimación del riesgo (en función de la expectativa de materialización)

El análisis de riesgos se lleva a cabo mediante las siguientes áreas:
**MAR – Método de Análisis de Riesgos**
MAR 1 – Caracterización de los activos
MAR 11 – Identificación de los activos
MAR12 – Dependencias entre activos
MAR 13 – Valoración de activos
MAR 2 – Caracterización de las amenazas
MAR 21 – Identificación de las amenazas
MAR 22 – Valoración de las amenazas
MAR 3 – Caracterización de las salvaguardas
MAR 31 – Identificación de las salvaguardas pertinentes
MAR 32 – Valoración de las salvaguardas
MAR 4 - Estimación del estado del riesgo
MAR 41 – Estimación del impacto
MAR 42 – Estimación del riesgo

## 5.1. Documentación

Así como se van completando tareas se va generando documentación intermedia (entrevistas, inventarios, informes, evaluaciones, etc.). Al completar todas las tareas la documentación final del análisis de riesgos que tenemos:

- Modelo de valor: informe de activos, con sus dependencias, dimensiones en que son valiosos y estimación de su valor en cada dimensión.
- Mapa de riesgos: informe que detalla las amenazas significativas sobre cada activo, caracterizadas por la frecuencia de ocurrencia y por la degradación que causaría la materialización sobre el activo.
- Declaración de aplicabilidad: informe que recoge las contramedidas que se consideran apropiadas para defender el SGSI.
- Evaluación de salvaguardas: Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.
- Informe de vulnerabilidades: detalla las salvaguardas necesarias pero ausentes o insuficientes
- Estado de riesgo: informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza

## 5.2. Lista de control

| √ | Actividad | Tarea |
|---|---|---|
| | Se han identificado los activos esenciales: información que se trata y servicios que se prestan | MAR. 11 |
| | Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad | MAR. 13 |
| | Se han identificado los demás activos del sistema | MAR. 11 |
| | Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, median identificación de las dependencias) | MAR. 12 |
| | Se han identificado las amenazas posibles obre los activos | MAR. 21 |
| | Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas | MAR. 22 |
| | Se ha estimado la probabilidad de que dichas amenazas se materialicen | MAR. 23 |
| | Se han estimado los impactos y riesgos potenciales, inherentes al sistema | MAR. 4 |
| | Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales | MAR. 31 |
| | Se ha valorado el despliegue de las salvaguardas identificadas | MAR. 32 |
| | Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas | MAR. 4 |

# 6. Referencias

- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro I – Método)
- UNE-ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información (SGSI).
- UNE-ISO/IEC 27002:2013 - Código de buenas prácticas para la Gestión de la Seguridad de la Información.

# ANEXO VIII:

DOC-05-SEG Declaración de aplicabilidad

| **Documento** | | DOC-05-SEG Declaración de aplicabilidad | | |
|---|---|---|---|---|
| **Uso** | | Interno | | |
| **Fecha** | **Versión** | **Realizado por** | **Revisado por** | **Cambios** |
| 20/03/17 | 1.00 | Responsable seguridad | Director IT | Documento inicial |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# ÍNDICE

# 1. Objetivo

El presente documento define el enfoque para el análisis y evaluación de riesgos de seguridad de la información. El análisis de riesgos permite determinar que tiene la organización y estimar lo que podría ocurrir. El análisis de riesgos

# 2. Alcance

El alcance de este documento aplica en el contexto del SGSI.

# 3. Declaración de aplicabilidad

| CONTROLES | Aplica | Estado | Documentación |
|---|---|---|---|
| **5. Política de seguridad de la información** | | | |
| 5.1. **Política de seguridad de la información** | | | |
| 5.1.1. Documento de política de seguridad de la información | Si | 100% | Política de seguridad |
| 5.1.2. Revisión de la política de seguridad | Si | 90% | Revisión por la dirección<br>Comité de seguridad |
| **6. Organización de la seguridad de la información** | | | |
| 6.1. **Organización interna** | | | |
| 6.1.1. Roles y responsabilidades de la seguridad de la información | Si | 90% | Definición de los puestos de trabajo<br>Gestión de roles y responsabilidad |
| 6.1.2. Segregación de funciones | Si | 50% | No documentado, existen equipos de trabajo diferenciados |
| 6.1.3. Contacto con autoridades | Si | 50% | Función del departamento legal |
| 6.1.4. Contacto con grupos especiales de interés | Si | 50% | No documentado |
| 6.1.5. Seguridad de la información en la gestión del proyecto | Si | 50% | Contratos de clientes<br>Ofertas comerciales |
| 6.2. **Dispositivos móviles y trabajo remoto** | | | |
| 6.2.1. Política de dispositivos móviles | Si | 10% | No documentado. Portátiles cifrados |
| 6.2.2. Trabajo remoto | Si | 90% | Cláusula de teletrabajo en contratos |
| **7. Seguridad ligada a los Recurso Humanos** | | | |
| 7.1. **Previo al empleo** | | | |
| 7.1.1. Selección | Si | 10% | No documentado |
| 7.1.2. Términos y condiciones de la relación laboral | Si | 50% | Contrato de trabajo<br>Cláusula de confidencialidad |
| 7.2. **Durante el empleo** | | | |
| 7.2.1. Responsabilidad de la dirección | Si | 90% | Política de Seguridad<br>Formación en seguridad<br>Acuerdo protección datos empleado y confidencialidad |
| 7.2.2. Concienciación, educación y formación en seguridad de la información | Si | 50% | Formaciones a empleados<br>Difusión de información de seguridad |
| 7.2.3. Proceso disciplinario | Si | 10% | Convenio del sector |
| 7.3. **Desvinculación y cambio de empleo** | | | |

| | | | |
|---|---|---|---|
| 7.3.1. Responsabilidades en la desvinculación o cambio de empleo | Si | 90% | Procedimiento, documento altas y bajas |
| **8. Administración de activos** | | | |
| 8.1. **Responsabilidad por los activos** | | | |
| 8.1.1. Inventario de activos | Si | 10% | Herramientas de inventario automáticas |
| 8.1.2. Propiedad de los activos | Si | 10% | No documentado formalmente |
| 8.1.3. Uso aceptable de los activos | Si | 10% | Política de seguridad |
| 8.1.4. Devolución de activos | Si | 50% | Procedimiento, documento altas y bajas |
| 8.2. **Clasificación de la información** | | | |
| 8.2.1. Clasificación de la información | Si | 10% | No procedimentado |
| 8.2.2. Etiquetado de la información | Si | 10% | No procedimentado |
| 8.2.3. Manejo de activos | Si | 10% | No procedimentado |
| 8.3. **Manejo de los medios** | | | |
| 8.3.1. Gestión de los medios removibles | Si | 50% | No procedimentado, existen buenas prácticas |
| 8.3.2. Eliminación de los medios | Si | 50% | No procedimentado, existen buenas prácticas |
| 8.3.3. Transferencia física de medios | Si | 50% | No procedimentado, existen buenas prácticas |
| **9. Control de acceso** | | | |
| 9.1. **Requisitos de negocio para el control de acceso** | | | |
| 9.1.1. Política de control de acceso | Si | 90% | Política control de acceso |
| 9.1.2. Accesos a las redes y a los servicios de red | Si | 90% | Política control de acceso |
| 9.2. **Gestión de acceso del usuario** | | | |
| 9.2.1. Registro y cancelación de registro de usuarios | Si | 50% | No procedimentado, existen buenas prácticas |
| 9.2.2. Asignación de acceso de usuario | Si | 10% | No procedimentado |
| 9.2.3. Gestión de derechos de acceso privilegiados | Si | 50% | No procedimentado, existen buenas prácticas |
| 9.2.4. Gestión de información secreta de autenticación de usuarios | Si | 50% | No procedimentado, existen buenas prácticas |
| 9.2.5. Revisión de los derechos de acceso de usuario | Si | 90% | Revisiones periódicas |
| 9.2.6. Eliminación o ajuste de los derechos de acceso | Si | 90% | Revisiones periódicas |
| 9.3. **Responsabilidades del usuario** | | | |
| 9.3.1. Uso de información de autenticación secreta | Si | 90% | Política usuarios y contraseñas |
| 9.4. **Control de acceso al sistema y aplicaciones** | | | |
| 9.4.1. Restricción de acceso a la información | Si | 50% | Todo acceso requiere de autenticación |
| 9.4.2. Procedimientos de inicio de sesión seguro | Si | 50% | Directorio activo |
| 9.4.3. Sistema de gestión de contraseñas | Si | 100% | Política usuarios y contraseñas y política de directorio |
| 9.4.4. Uso de programas con privilegios de sistema | Si | 100% | Política usuarios y contraseñas |
| 9.4.5. Control de acceso al código fuente de los programas | Si | 100% | Política usuarios y contraseñas |
| **10. Criptografía** | | | |
| 10.1. **Controles criptográficos** | | | |
| 10.1.1. Política sobre el uso de controles criptográficos | Si | 0% | Solo en portátiles |

| | | | |
|---|---|---|---|
| 10.1.2. Gestión de claves | Si | 0% | Sólo en portátiles |
| **11. Seguridad física y del entorno** | | | |
| 11.1. **Áreas seguras** | | | |
| 11.1.1. Perímetro de seguridad física | Si | 100% | Procedimiento de acceso a CPDs<br>Accesos controlados por acceso con tarjeta |
| 11.1.2. Controles de acceso físico | Si | 100% | Procedimiento de acceso a CPDs<br>Accesos controlados por acceso con tarjeta |
| 11.1.3. Seguridad de oficinas, salas e instalaciones | Si | 90% | Accesos controlados por acceso con tarjeta |
| 11.1.4. Protección contra amenazas externas y del entorno | Si | 50% | Gestionado por la propiedad del edificio |
| 11.1.5. Trabajo en áreas seguras | Si | 50% | Procedimiento de acceso a CPDs<br>Accesos controlados por acceso con tarjeta |
| 11.1.6. Áreas de entrega y carga | Si | 50% | Accesos controlados por acceso con tarjeta |
| 11.2. **Equipamiento** | | | |
| 11.2.1. Ubicación y protección del equipamiento | Si | 90% | Procedimiento de acceso a CPDs<br>Accesos controlados por acceso con tarjeta |
| 11.2.2. Elementos de soporte | Si | 90% | Doble sistema de alimentación de soporte |
| 11.2.3. Seguridad en el cableado | Si | 10% | No procedimentado, buenas prácticas |
| 11.2.4. Mantenimiento del equipamiento | Si | 50% | No procedimentado, buenas prácticas. Alta disponibilidad. |
| 11.2.5. Retiro de activos | Si | 50% | Guías de buenas prácticas |
| 11.2.6. Seguridad del equipamiento y los activos fuera de las instalaciones | Si | 50% | Política de seguridad<br>VPN y Cifrado de portátiles |
| 11.2.7. Seguridad en la reutilización o descarte de equipos | Si | 50% | Formateo de equipos |
| 11.2.8. Equipo de usuario desatendido | Si | 90% | Bloqueo automático por inactividad<br>Política de seguridad del empleado |
| 11.2.9. Política de escritorio y pantalla limpios | Si | 50% | Política de seguridad del empleado |
| **12. Seguridad de las operaciones** | | | |
| 12.1. **Procedimientos operacionales y responsabilidades** | | | |
| 12.1.1. Procedimientos de operación documentados | Si | 50% | Repositorios de documentación |
| 12.1.2. Gestión de cambios | Si | 100% | Proceso gestión de cambios (ITIL) |
| 12.1.3. Gestión de la capacidad | Si | 95% | Proceso gestión de la capacidad (ITIL) |
| 12.1.4. Separación de los ambientes de desarrollo, prueba y operacionales | Si | 90% | No procedimentado, guías de buenas prácticas |
| 12.2. **Protección contra código malicioso** | | | |
| 12.2.1. Controles contra código malicioso | Si | 90% | Antivirus<br>Restricción instalar software |
| 12.3. **Respaldo** | | | |
| 12.3.1. Respaldo de la información | Si | 90% | Política de backups |
| 12.4. **Registro y monitoreo** | | | |
| 12.4.1. Registro de evento | Si | 50% | Para datos de nivel alto de seguridad (LOPD) |
| 12.4.2. Protección de la información de registros | Si | 50% | Existe *backup* |
| 12.4.3. Registros del administrador y el operador | Si | 50% | Existen registros |

| | | | |
|---|---|---|---|
| 12.4.4. Sincronización de relojes | Si | 100% | Sincronizado con servidor NTP |
| 12.5. **Control de software de operación** | | | |
| 12.5.1. Instalación del software en sistemas operaciones | Si | 100% | Proceso de Gestión de cambios |
| 12.6. **Gestión de la vulnerabilidad técnica** | | | |
| 12.6.1. Gestión de las vulnerabilidades técnicas | Si | 100% | Actualizaciones de seguridad |
| 12.6.2. Restricciones sobre la instalación de software | Si | 90% | Instalación de software restringida |
| 12.7. **Consideraciones de la auditoría de los sistemas de información** | | | |
| 12.7.1. Controles de auditoría de sistemas de información | Si | 100% | Auditorías internas |
| **13. Seguridad de las comunicaciones** | | | |
| 13.1. **Gestión de la seguridad de red** | | | |
| 13.1.1. Controles de red | Si | 50% | Firewall, IPS, antivirus |
| 13.1.2. Seguridad de los servicios de red | Si | 50% | Firewall, IPS, antivirus |
| 13.1.3. Separación en las redes | No | 0% | No hay separación de redes |
| 13.2. **Transferencia de información** | | | |
| 13.2.1. Políticas y procedimientos de transferencia de información | Si | 50% | No procedimentado, buenas prácticas |
| 13.2.2. Acuerdos sobre transferencia de información | Si | 50% | No procedimentado, buenas prácticas |
| 13.2.3. Mensajería electrónica | Si | 50% | No procedimentado, buenas prácticas |
| 13.2.4. Acuerdos de confidencialidad o no divulgación | Si | 90% | Cláusulas confidencialidad empleados y proveedores |
| **14. Adquisición, desarrollo y mantenimiento del sistema** | | | |
| 14.1. **Requisitos de seguridad de los sistemas de información** | | | |
| 14.1.1. Análisis y especificación de requisitos de seguridad de la información | Si | 10% | No procedimentado |
| 14.1.2. Aseguramiento de servicios de aplicación en redes públicas | No | 0% | |
| 14.1.3. Protección de las transacciones de servicios de aplicación | No | 0% | |
| 14.2. **Seguridad en procesos de desarrollo y soporte** | | | |
| 14.2.1. Política de desarrollo seguro | Si | 50% | No procedimentado |
| 14.2.2. Procedimientos de control de cambios del sistema | Si | 90% | Gestión de cambios |
| 14.2.3. Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación | Si | 50% | Gestión de cambios |
| 14.2.4. Restricciones en los cambios a los paquetes de software | Si | 90% | Gestión de cambios |
| 14.2.5. Principios de ingeniería de sistema seguro | Si | 50% | No procedimentado, buenas prácticas |
| 14.2.6. Entorno de desarrollo seguro | Si | 50% | Buenas prácticas |
| 14.2.7. Desarrollo externalizado | No | 0% | |
| 14.2.8. Prueba de seguridad del sistema | Si | 90% | Gestión de cambios |
| 14.2.9. Prueba de aprobación del sistema | Si | 90% | Gestión de cambios |
| 14.3. **Datos de prueba** | | | |
| 14.3.1. Protección de datos de prueba | No | 0% | |
| **15. Relaciones con el proveedor** | | | |
| 15.1. **Seguridad de la información en las relaciones con el proveedor** | | | |

| | | | |
|---|---|---|---|
| 15.1.1. Política de seguridad de la información para las relaciones con el proveedor | Si | 10% | Contratos |
| 15.1.2. Abordar la seguridad dentro de los acuerdos del proveedor | Si | 10% | Contratos |
| 15.1.3. Cadena de suministro de tecnologías de la información y comunicaciones | Si | 50% | Contratos |
| 15.2. **Gestión de entrega del servicio del proveedor** | | | |
| 15.2.1. Supervisión y revisión de los servicios del proveedor | Si | 50% | No procedimentado |
| 15.2.2. Gestión de cambios a los servicios del proveedor | Si | 50% | Gestión del cambio |
| **16. Gestión de incidentes de seguridad de la información** | | | |
| 16.1. **Gestión de incidentes de seguridad de la información y mejoras** | | | |
| 16.1.1. Responsabilidades y procedimientos | Si | 50% | Gestión de incidentes |
| 16.1.2. Informe de eventos de seguridad de la información | Si | 50% | Gestión de incidentes – herramienta incidentes |
| 16.1.3. Informe de las debilidades de seguridad de la información | Si | 50% | Gestión de incidentes |
| 16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información | Si | 10% | Gestión de incidentes |
| 16.1.5. Respuesta ante incidentes de seguridad de la información | Si | 10% | Gestión de incidentes |
| 16.1.6. Aprendizaje de los incidentes de seguridad de la información | Si | 10% | Gestión de incidentes |
| 16.1.7. Recolección de evidencia | Si | 10% | Gestión de incidentes |
| **17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio** | | | |
| 17.1. **Continuidad de la seguridad de la información** | | | |
| 17.1.1. Planificación de la continuidad de la seguridad de la información | Si | 10% | Planes continuidad negocio |
| 17.1.2. Implementación de la continuidad de la seguridad de la información | Si | 10% | Planes continuidad negocio |
| 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Si | 10% | Planes continuidad negocio |
| 17.2. **Redundancias** | | | |
| 17.2.1. Disponibilidad de las instalaciones de procesamiento de la información | Si | 50% | Planes continuidad negocio |
| **18. Cumplimiento** | | | |
| 18.1. **Cumplimiento con los requisitos legales y contractuales** | | | |
| 18.1.1. Identificación de la legislación vigente y los requisitos contractuales | Si | 50% | Buenas prácticas |
| 18.1.2. Derechos de propiedad intelectual | Si | 50% | Buenas prácticas |
| 18.1.3. Protección de los registros | Si | 50% | Buenas prácticas |
| 18.1.4. Privacidad y protección de la información de identificación personal | Si | 50% | Auditorías LOPD |
| 18.1.5. Regulación de los controles criptográficos | Si | 10% | No procedimentado |
| 18.2. **Revisiones de seguridad de la información** | | | |
| 18.2.1. Revisión independiente de la seguridad de la información | Si | 90% | Auditorías LOPD |
| 18.2.2. Cumplimiento con las políticas y normas de seguridad | Si | 90% | Política de seguridad |
| 18.2.3. Verificación del cumplimiento técnico | Si | 90% | Política de seguridad |

## 4. Referencias

- UNE-ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información (SGSI).
- UNE-ISO/IEC 27002:2013 - Código de buenas prácticas para la Gestión de la Seguridad de la Información.

# ANEXO IX:

## Inventario de activos

| AMBITO | ACTIVO |
|---|---|
| **Instalaciones** | CPD externo |
| | Sedes (14) |
| | CPD sedes |
| **Hardware** | PCs |
| | Portátiles |
| | Impresoras |
| | Servidores |
| | Centralita |
| | Teléfonos |
| **Aplicaciones** | Windows server |
| | Windows profesional 7 |
| | Windows profesional 10 |
| | Microsoft Office |
| | Java |
| | Antivirus |
| | UCI Altitude |
| | CRM Microsoft |
| **Datos** | Bases de Datos de clientes |
| | Código fuente desarrollos |
| | Datos financieros |
| | *Backups* |
| | Datos de acceso |
| | Datos de configuraciones |
| **Red** | *Routers* |
| | *Switches* |
| | Antenas wifi |
| **Servicios** | Correo electrónico |
| | Servicios Web |
| **Equipamiento auxiliar** | SAIs |
| | Grupos electrógenos |
| **Personal** | Responsables de TI |
| | Técnicos de sistemas |
| | Técnicos de desarrollo |

# ANEXO X:

## Valoración de los activos

| AMBITO | ACTIVO | VALOR | ASPECTOS CRÍTICOS | | | | |
|---|---|---|---|---|---|---|---|
| | | | A | C | I | D | A |
| Instalaciones | CPD externo | Muy Alto | 9 | 8 | 10 | 10 | 7 |
| | Sedes (14) | Alto | 7 | 5 | 3 | 5 | 2 |
| | CPD sedes | Alto | 8 | 7 | 8 | 9 | 6 |
| Hardware | PCs | Medio | 4 | 4 | 5 | 6 | 4 |
| | Portátiles | Medio | 4 | 5 | 5 | 5 | 4 |
| | Impresoras | Bajo | 3 | 4 | 3 | 3 | 3 |
| | Servidores | Muy Alto | 9 | 9 | 9 | 9 | 7 |
| | Centralita | Muy Alto | 9 | 9 | 9 | 9 | 7 |
| | Teléfonos | Medio | 4 | 4 | 5 | 6 | 4 |
| Aplicaciones | Windows server | Alto | 4 | 7 | 8 | 8 | 7 |
| | Windows profesional 7 | Bajo | 3 | 2 | 2 | 2 | 2 |
| | Windows profesional 10 | Bajo | 3 | 2 | 2 | 2 | 2 |
| | Microsoft Office | Bajo | 3 | 2 | 2 | 2 | 1 |
| | Java | Bajo | 2 | 2 | 2 | 1 | 0 |
| | Antivirus | Bajo | 5 | 1 | 4 | 5 | 1 |
| | UCI Altitude | Alto | 6 | 4 | 8 | 9 | 8 |
| | CRM Microsoft | Alto | 6 | 4 | 8 | 9 | 8 |
| Datos | Bases de Datos de clientes | Muy Alto | 7 | 8 | 9 | 7 | 7 |
| | Código fuente desarrollos | Medio | 7 | 8 | 9 | 6 | 6 |
| | Datos financieros | Alto | 4 | 5 | 9 | 6 | 6 |
| | *Backups* | Muy Alto | 7 | 9 | 10 | 5 | 5 |
| | Datos de acceso | Muy Alto | 8 | 10 | 10 | 8 | 9 |
| | Datos de configuraciones | Alto | 7 | 5 | 9 | 6 | 6 |
| Red | Cableado de red | Medio | 3 | 1 | 7 | 8 | 2 |
| | *Routers* | Alto | 7 | 7 | 9 | 10 | 5 |
| | *Switches* | Alto | 7 | 7 | 9 | 10 | 5 |
| | Antenas wifi | Alto | 7 | 7 | 9 | 7 | 5 |
| Servicios | Correo electrónico | Alto | 7 | 7 | 8 | 7 | 5 |
| | Servicios Web | Alto | 8 | 7 | 9 | 9 | 6 |
| Equipamiento auxiliar | SAIs | Alto | 0 | 0 | 0 | 10 | 0 |
| | Grupos electrógenos | Alto | 0 | 0 | 0 | 10 | 0 |
| Personal | Responsables de TI | Medio | 6 | 6 | 5 | 8 | 5 |
| | Técnicos de sistemas | Alto | 7 | 5 | 8 | 9 | 5 |
| | Técnicos de desarrollo | Medio | 5 | 5 | 8 | 8 | 5 |

# ANEXO XI:

## Activos y dimensiones de seguridad

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Instalaciones** | | | | | | |
| CPD externo | | | 80% | 100% | 100% | |
| Sedes (14) | | | 80% | 100% | 100% | |
| CPD sedes | | | 80% | 100% | 100% | |
| [N.1] Fuego | 0,01 | | | | 100% | |
| [N.2] Daños por agua | 0,01 | | | | 100% | |
| [I.1] Fuego | 0,01 | | | | 100% | |
| [I.2] Daños por agua | 0,1 | | | | 100% | |
| [E.15] Alteración accidental de la información | 0,1 | | | 25% | | |
| [E.18] Destrucción de información | 0,1 | | | 100% | 50% | |
| [E.19] Fugas de información | 0,1 | | 50% | | | |
| [A.11] Acceso no autorizado | 0,1 | | 50% | 50% | | |
| [A.15] Modificación deliberada de la información | 0,01 | | | 80% | | |
| [A.18] Destrucción de información | 0,01 | | | | 80% | |
| [A.19] Divulgación de información | 0,01 | | 80% | | | |
| [A.26] Ataque destructivo | 0,01 | | | | 100% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Hardware** | | | | | | |
| PCs | | | 100% | 50% | 100% | |
| Portátiles | | | 100% | 50% | 100% | |
| Impresoras | | | 100% | 50% | 100% | |
| Servidores | | | 100% | 50% | 100% | |
| Centralita | | | 100% | 50% | 100% | |
| Teléfonos | | | 100% | 50% | 100% | |
| [N.1] Fuego | 0,01 | | | | 100% | |
| [N.2] Daños por agua | 0,01 | | | | 100% | |
| [I.1] Fuego | 0,01 | | | | 100% | |
| [I.2] Daños por agua | 0,01 | | | | 100% | |
| [I.3] Contaminación mecánica | 0,01 | | | | 100% | |
| [I.4] Contaminación electromagnética | 0,01 | | | | 100% | |
| [I.5] Avería de origen físico o lógico | 1 | | | | 100% | |
| [I.6] Corte del suministro eléctrico | 1 | | | | 100% | |
| [I.7] Condiciones inadecuadas de temperatura o humedad | 0,1 | | | | 60% | |
| [E.2] Errores del administrador | 0,1 | | 25% | 25% | 50% | |
| [E.23] Errores de mantenimiento/actualización de equipos (hardware) | 0,1 | | | | 100% | |
| [E.24] Caída del sistema por agotamiento de recursos | 0,1 | | | | 100% | |
| [E.25] Pérdida de equipos | 0,01 | | 50% | | 100% | |
| [A.6] Abuso de privilegios de acceso | 0,01 | | 50% | 50% | 50% | |
| [A.7] Uso no previsto | 0,1 | | 50% | 50% | 50% | |
| [A.11] Acceso no autorizado | 0,01 | | 75% | 50% | | |
| [A.23] Manipulación de los equipos | 0,01 | | 25% | | 25% | |
| [A.24] Denegación de servicio | 0,01 | | | | 100% | |
| [A.25] Robo | 0,01 | | 100% | | 100% | |
| [A.26] Ataque destructivo | 0,01 | | | | 100% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Aplicaciones** | | | | | | |
| Windows server | | 100% | 100% | 100% | 100% | |
| Windows profesional 7 | | 100% | 100% | 100% | 100% | |
| Windows profesional 10 | | 100% | 100% | 100% | 100% | |
| Microsoft Office | | 100% | 100% | 100% | 100% | |
| Java | | 100% | 100% | 100% | 100% | |
| Antivirus | | 100% | 100% | 100% | 100% | |
| UCI Altitude | | 100% | 100% | 100% | 100% | |
| CRM Microsoft | | 100% | 100% | 100% | 100% | |
| [I.5] Avería de origen físico o lógico | 0,1 | | | | 50% | |
| [E.1] Errores de los usuarios | 1 | | 5% | 10% | 20% | |
| [E.2] Errores del administrador | 0,1 | | 25% | 25% | 50% | |
| [E.8] Difusión de software dañino | 0,1 | | 25% | 40% | 50% | |
| [E.9] Errores de re-encaminamiento | 0,01 | | 20% | | | |
| [E10] Errores de secuencia | 0,01 | | | 10% | | |
| [E15] Alteración accidental de la información | 0,01 | | | 10% | | |
| [E.18] Destrucción de la información | 0,01 | | | | 50% | |
| [E.19] Fugas de información | 0,01 | | 25% | | | |
| [E.20] Vulnerabilidades de los programas (software) | 0,1 | | 25% | 25% | 50% | |
| [E.21]Errores de mantenimiento/actualización de equipos | 0,01 | | | 25% | 50% | |
| [A.5] Suplantación de la identidad del usuario | 0,1 | 100% | 75% | 75% | | |
| [A.6] Abuso de privilegios de acceso | 0,01 | | 50% | 25% | 25% | |
| [A.7] Uso no previsto | 0,1 | | 10% | 10% | 25% | |
| [A.8] Difusión de software dañino | 0,1 | | 75% | 75% | 100% | |
| [A.9] Re-encaminamiento de mensajes | 0,01 | | 50% | | | |
| [A.10] Alteración de secuencia | 0,01 | | | 50% | | |
| [A.11] Acceso no autorizado | 0,01 | | 100% | 75% | | |
| [A.15] Modificación deliberada de la información | 0,01 | | | 100% | | |
| [A.18] Destrucción de información | 0,01 | | | | 100% | |
| [A.19] Divulgación de la información | 0,01 | | 100% | | | |
| [A.22] Manipulación de programas | 0,01 | | 50% | 50% | 50% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| Datos | | | | | | |
| Bases de Datos de clientes | | 100% | 100% | 100% | 100% | |
| Código fuente desarrollos | | 100% | 100% | 100% | 100% | |
| Datos financieros | | 100% | 100% | 100% | 100% | |
| Backups | | 100% | 100% | 100% | 100% | |
| Datos de acceso | | 100% | 100% | 100% | 100% | |
| Datos de configuraciones | | 100% | 100% | 100% | 100% | |
| [E.1] Errores de los usuarios | 10 | | 10% | 10% | 25% | |
| [E.2] Errores del administrador | 0,1 | | 25% | 25% | 50% | |
| [E.15] Alteración accidental de la información | 0,1 | | | 25% | | |
| [E.18] Destrucción de información | 0,01 | | | 50% | | |
| [E.19] Fugas de información | 0,01 | | | 25% | | |
| [A.5] Suplantación de la identidad del usuario | 0,1 | 100% | 75% | 25% | | |
| [A.6] Abuso de privilegios de acceso | 0,01 | | 75% | 25% | 25% | |
| [A.11] Acceso no autorizado | 0,01 | | 75% | 25% | | |
| [A.15] Modificación deliberada de información | 0,01 | | | 100% | | |
| [A.18] Destrucción de información | 0,01 | | | | 100% | |
| [A.19] Divulgación de información | 0,01 | | 100% | | | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Red** | | | | | | |
| Cableado de red | | 100% | 100% | 100% | 100% | |
| Routers | | 100% | 100% | 100% | 100% | |
| Switches | | 100% | 100% | 100% | 100% | |
| Antenas wifi | | 100% | 100% | 100% | 100% | |
| [I.8] Fallo de servicios de comunicaciones | 1 | | | | 100% | |
| [E.2] Errores del administrador | 0,1 | | 25% | 25% | 50% | |
| [E.9] Errores de re-encaminamiento | 0,01 | | 25% | | | |
| [E.10] Errores de secuencia | 0,01 | | | 25% | | |
| [E.15] Alteración accidental de la información | 0,01 | | | 25% | | |
| [E.18] Destrucción de información | 0,01 | | | | 75% | |
| [E.19] Fugas de información | 0,01 | | 25% | | | |
| [E.24] Caída del sistema por agotamiento de recursos | 0,1 | | | | 100% | |
| [A.5] Suplantación de la identidad de usuario | 0,01 | 100% | 50% | 25% | | |
| [A.6] Abuso de privilegios de acceso | 0,01 | | 25% | 25% | 25% | |
| [A.7] Uso no previsto | 0,01 | | 25% | 25% | 50% | |
| [A.9] Re-encaminamiento de mensajes | 0,01 | | 50% | | | |
| [A.10] Alteración de secuencia | 0,01 | | | 50% | | |
| [A.11] Acceso no autorizado | 0,01 | | | 50% | | |
| [A.12] Análisis de tráfico | 0,01 | | 25% | | | |
| [A.14] Interceptación de información (escucha) | 0,01 | | 75% | | | |
| [A.15] Modificación deliberada de la información | 0,01 | | | 100% | | |
| [A.19] Divulgación de información | 0,01 | | 100% | | | |
| [A.24] Denegación de servicio | 0,01 | | | | 100% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Servicios** | | | | | | |
| Correo electrónico | | 100% | 100% | 100% | 100% | 100% |
| Servicios Web | | 100% | 100% | 100% | 100% | 100% |
| [E.1] Errores de los usuarios | 0,1 | | 25% | 25% | 25% | |
| [E.2] Errores del administrador | 0,01 | | 50% | 50% | 50% | |
| [E.9] Errores de re-encaminamiento | 0,01 | | 50% | | | |
| [E.10] Errores de secuencia | 0,01 | | | 25% | | |
| [E.15] Alteración accidental de la información | 0,01 | | | 75% | | |
| [E.18] Destrucción de información | 0,01 | | | 75% | | |
| [E.19] Fugas de información | 0,01 | | | | 50% | |
| [E.24] Caída del sistema por agotamiento de recursos | 0,1 | | | | 100% | |
| [A.5] Suplantación de la identidad del usuario | 0,01 | 100% | 75% | 25% | | |
| [A.6] Abuso de privilegios de acceso | 0,01 | | 25% | 25% | 25% | |
| [A.7] Uso no previsto | 0,01 | | 25% | 25% | 25% | |
| [A.9] Re-encaminamiento de mensajes | 0,01 | | 25% | | | |
| [A.10] Alteración de secuencia | 0,01 | | | 25% | | |
| [A.11] Acceso no autorizado | 0,01 | | 75% | 25% | | |
| [A.13] Repudio | 0,01 | | | | | 100% |
| [A.15] Modificación deliberada de la información | 0,01 | | | 100% | | |
| [A.18] Destrucción de información | 0,01 | | | | 100% | |
| [A.19] Divulgación de información | 0,01 | | 100% | | | |
| [A.24] Denegación de servicio | 0,01 | | | | 100% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Equipamiento auxiliar** | | | | | | |
| SAIs | | | 10% | 10% | 100% | |
| Grupos electrógenos | | | 10% | 10% | 100% | |
| [N.1] Fuego | 0,01 | | | | 100% | |
| [N.2] Daños por agua | 0,01 | | | | 100% | |
| [I.1] Fuego | 0,01 | | | | 100% | |
| [I.2] Daños por agua | 0,01 | | | | 100% | |
| [I.3] Contaminación mecánica | 0,01 | | | | 100% | |
| [I.4] Contaminación electromagnética | 0,01 | | | | 100% | |
| [I.5] Avería de origen físico o lógico | 0,01 | | | | 100% | |
| [I.7] Condiciones inadecuadas de temperatura o humedad | 0,1 | | | | 100% | |
| [I.9] Interrupción de otros servicios y suministros esenciales | 0,01 | | | | 100% | |
| [E.23] Errores de mantenimiento/actualización de equipos (hardware) | 0,1 | | | | 100% | |
| [E.25] Pérdida de equipos | 0,01 | | 10% | | 100% | |
| [A.7] Uso no previsto | 0,01 | | 10% | 10% | 10% | |
| [A.11] Acceso no autorizado | 0,01 | | 10% | 10% | | |
| [A.23] Manipulación de los equipos | 0,01 | | 10% | | 100% | |
| [A.25] Robo | 0,01 | | 10% | | 100% | |
| [A.26] Ataque destructivo | 0,01 | | | | 100% | |

| Activo | Frecuencia | A | C | I | D | A |
|---|---|---|---|---|---|---|
| **Personal** | | | | | | |
| Responsables de TI | | | 100% | 25% | 75% | |
| Técnicos de sistemas | | | 100% | | | |
| [E.19] Fugas de información | 0,01 | | 100% | | | |
| [E.28] Indisponibilidad del personal | 0,1 | | | | 10% | |
| [A.28] Indisponibilidad del personal | 0,1 | | | | 75% | |
| [A.29] Extorsión | 0,01 | | 25% | 25% | 50% | |
| [A.30] Ingeniería social (picaresca) | 0,01 | | 25% | 25% | 25% | |

# ANEXO XII:

## Proyectos

| PR1: Plan de Continuidad del Negocio |
|---|
| **Descripción:** |
| Plan práctico de cómo TMK.S.A. debe recuperarse y restaurar sus funciones críticas ante una interrupción total o parcial en un determinado tiempo ante una interrupción no deseada o un desastre. En el plan de Continuidad del Negocio (PCN) se deberán contemplar los riesgos analizados así como aquellos activos con mayor valor para TMK S.A. El PCN deberá detallar las acciones a llevar a cabo para la recuperación, especificando responsables.<br>Este plan deberá ser revisado de forma periódica, se propone cada 6 meses, y ajustarlo a las necesidades y circunstancias de cada momento. |
| **Equipo de trabajo** |
| - Responsable de seguridad<br>- Responsables TI (Soporte a usuarios, Ingeniería y Desarrollo) |
| **Objetivos** |
| - Recuperar las funciones críticas en el menor tiempo posible, asegurando la continuidad.<br>- Tener documentado y preparado el proceso de recuperación/restauración.<br>- Reducir al mínimo las pérdidas económicas por indisponibilidad del negocio. |
| **Riesgos a mitigar:** |
| - Inactividad total o parcial de TMK S.A. |
| **Coste:** |
| El coste es alto porque implica que algunos sistemas sean redundados. Actualmente la mayoría de sistemas de TMK S.A. cuentan con redundancia pero no todos.<br>Se estima un coste de 30.000€ |
| **Temporalidad:** |
| Teniendo en cuenta que aparte de la documentación del plan, hay que proveer hardware, y posteriormente este deberá ser configurado como redundante, el proyecto se extenderá durante un periodo de 6 meses. Medio plazo. |
| **Indicadores:** |
| - Revisión semestral del PCN, incluyendo pruebas de redundancia de sistemas en horario de bajo impacto. |

**PR2: Política de *backups***

**Descripción:**

Actualmente en TMK S.A. se realizan *backups* de diferentes sistemas, de los cuales son varios los responsables. El proyecto definirá e implantará una única política de *backups*, que garantizará la confidencialidad, disponibilidad e integridad de los datos.
En TMK S.A. se realizan backups de sistemas (configuraciones), bases de datos y datos alojados en unidades de red.
Se definirá una política de backups diarios a disco y semanales a cinta siendo estos últimos externalizados. Actualmente existe una empresa con la que se externalizan *backups*, pero no todos. Los *backups* en cinta deberán ser encriptados y estar correctamente registrados e inventariados para poder ser localizados en caso de necesidad.
Antes de externalizar el *backup* deberá ser comprobada su recuperación, realizando alguna recuperación aleatoria.
Los backups diarios (disco) serán sobrescritos semanalmente y los backups semanales (cinta) serán recuperados del lugar de custodia y sobrescritos trimestralmente (12 semanas).
Toda restauración de datos solicitada de *backup* deberá ser solicitada mediante herramienta de comunicación de incidentes.

**Equipo de trabajo**

- Responsable de seguridad
- Responsables TI (Soporte a usuarios, Ingeniería y Desarrollo)

**Objetivos**

- Recuperación de datos ante problemas de integridad y/o disponibilidad de los mismos.
- Contribuir a la restauración/recuperación ante desastres.
- Evita pérdidas irreparables.

**Riesgos a mitigar:**

- Pérdida de datos.
- Pérdida de configuraciones.

**Coste:**

Se estima que únicamente será necesario comprar algunas cintas de *backup* adicionales. No es necesaria más infraestructura de la que actualmente se dispone. El contrato de externalización de *backups* con el proveedor se encuentra vigente.
Coste: 1000€

**Temporalidad:**

El trabajo de este proyecto reside principalmente en la unificación de *backups* que ya actualmente se están realizando y en la creación de una política única.
Corto plazo. 1 mes

**Indicadores:**

- Chequeo y registro de revisión de *backups* diarios (disco).
- Chequeo y registro de revisión de *backups* semanales (cinta).
- Registro de restauraciones solicitadas.
- Registro de peticiones de *backups* a proveedor externo para restauraciones.

| PR3: Formaciones continúas y de actualización en materia de seguridad |
|---|
| **Descripción:** |
| Es fundamental que los empleados estén formados y concienciados en materia de seguridad. Para ello es necesario realizar continúas formaciones y actualizaciones de las mismas<br>Se deberán realizar formaciones a empleados nuevos ajustadas a su perfil y actualizaciones periódicas (al menos una vez al año). Se reforzará la formación y concienciación con comunicados y píldoras informativas. El proyecto implica la realización de un calendario de formaciones anual. |
| **Equipo de trabajo** |
| - Responsable de seguridad |
| **Objetivos** |
| - La formación y concienciación contribuye al incremento de la seguridad.<br>- Los empleados desarrollan la actividad en su puesto de trabajo con garantías. |
| **Riesgos a mitigar:** |
| - Incidentes de seguridad que ocurren por desconocimiento. |
| **Coste:** |
| El mayor coste para llevar a cabo este proyecto reside en la necesidad de desplazamiento del formador a algunos centros a impartir la formación, aunque también podrá ser formación en formato virtual.<br>Coste: 1500€/año |
| **Temporalidad:** |
| Corto plazo. Un mes. |
| **Indicadores:** |
| - Chequeo y registro de revisión de *backups* diarios (disco).<br>- Chequeo y registro de revisión de *backups* semanales (cinta).<br>- Registro de restauraciones solicitadas.<br>- Registro de peticiones de *backups* a proveedor externo para restauraciones. |

| PR4: Procedimiento de destrucción de soportes |
| --- |
| **Descripción:** |
| El procedimiento de destrucción de soportes físicos con información (discos duros, CD/DVDs, cintas, etc.) deberá realizarse con garantías. El procedimiento deberá detallar como proceder al fin de la vida útil de un soporte: deberá quedar registrado y será destruido por una empresa proveedora que expedirá certificado de destrucción a tal efecto. |
| **Equipo de trabajo** |
| - Responsable de seguridad |
| **Objetivos** |
| - Garantizar la correcta eliminación de soportes obsoletos |
| **Riesgos a mitigar:** |
| - Evitar fugas de información<br>- Evitar uso fraudulento |
| **Coste:** |
| Básicamente el coste del proyecto es el de contratar una empresa de destrucción de soportes<br>Coste: 300€ |
| **Temporalidad:** |
| Corto plazo. Un mes. |
| **Indicadores:** |
| - Registro de eliminación de soportes |

| PR5: Gestión de activos |
| --- |
| **Descripción:** |
| Todos los activos de la compañía TMK S.A. deben estar correctamente identificados, asignados e inventariados. Revisión y actualización del inventario actual |
| **Equipo de trabajo** |
| - Responsable de seguridad<br>- Responsables TI (Soporte a Usuarios e Ingeniería) |
| **Objetivos** |
| - Inventario correcto y actualizado<br>- Mayor control y seguridad sobre los activos |
| **Riesgos a mitigar:** |
| - Pérdida o no localización de activos.<br>- Activos no inventariados, son activos no controlados e inseguros |
| **Coste:** |
| Se puede contemplar la contratación de una herramienta para gestión de activos, pero por el momento no se contempla por lo que no tendrá coste este proyecto para la empresa.<br>Coste 0€. |
| **Temporalidad:** |
| Corto plazo. Un mes. |
| **Indicadores:** |
| - Revisión bimensual de inventarios de activos |

| PR6: Plan de renovación de hardware (Servidores, PCs, portátiles y teléfonos) |
|---|
| **Descripción:** |
| Una vez esté revisado el inventario de activos, se planificará la renovación de equipos hardware más antiguos (servidores, PCs y portátiles). En el negocio del telemarketing el trabajo del operador depende del PC y teléfono, si estos no están disponibles la empresa está perdiendo dinero. |
| **Equipo de trabajo** |
| - Responsables TI (Soporte a Usuarios e Ingeniería) |
| **Objetivos** |
| - Disminución de incidentes que provocan indisponibilidad<br>- Renovación del parque de equipos. |
| **Riesgos a mitigar:** |
| - Indisponibilidad de equipos hardware. |
| **Coste:** |
| El coste de llevar a cabo este proyecto es alto debido al coste de los equipos. Año a año se deberían ir renovando los equipos más antiguos. Se estima el coste anual para renovación de equipos.<br>300.000€ |
| **Temporalidad:** |
| Largo plazo. Un año. |
| **Indicadores:** |
| - Registro de equipos renovados<br>- Registro de equipos pendientes de renovación |

| PR7: Mejora en la gestión de los incidentes de seguridad |
|---|
| **Descripción:** |
| Mejorar y optimizar la gestión de los incidentes de seguridad. Actualmente se comunican los incidentes de seguridad gracias a la concienciación entre los empleados, pero se debe establecer un canal único de comunicación que será la herramienta de comunicación de incidencias para que de este modo queden registrados. Se definirá el procedimiento de actuación ante la comunicación de un incidente de seguridad, así como para la identificación, recolección, adquisición y conservación de información que pueda servir de evidencia. También es necesario definir un proceso disciplinario formal que será comunicado a los empleados, que recogerá las acciones a tomar ante empleados que comentan una infracción en materia de seguridad de la información. |
| **Equipo de trabajo** |
| - Responsable de seguridad<br>- Responsable TI (Soporte a Usuarios) |
| **Objetivos** |
| - Gestión procedimentada<br>- Disponer de un registro único de incidentes y su resolución.<br>- Incidentes de seguridad atendidos según procedimiento documentado |
| **Riesgos a mitigar:** |
| - Evitar diferentes modos de proceder ante los incidentes de seguridad |
| **Coste:** |
| Este proyecto no tiene coste asociado para la compañía, puesto que la herramienta de registro ya se dispone de ella.<br>0€ |
| **Temporalidad:** |
| Corto plazo. Un mes. |
| **Indicadores:** |
| - Registro de incidencias de seguridad |

| PR8: Plan de renovación y actualización de elementos de red |
|---|
| **Descripción:** |
| Una vez esté revisado el inventario de activos, se planificará la renovación de elementos de red más antiguos (*switches*, *routers*, cableado, etc.). En el negocio de TMK S.A. las comunicaciones tanto internas como externas son fundamentales para el desarrollo su actividad. |
| **Equipo de trabajo** |
| - Responsables TI (Soporte a Usuarios e Ingeniería) |
| **Objetivos** |
| - Disminución de incidentes que provocan indisponibilidad<br>- Renovación del parque de equipos. |
| **Riesgos a mitigar:** |
| - Indisponibilidad de elementos de red. |
| **Coste:** |
| El coste de llevar a cabo este proyecto es alto debido al coste de los equipos. Año a año se deberían ir renovando los equipos más antiguos. Se estima el coste anual para renovación de equipos.<br>100.000€ |
| **Temporalidad:** |
| Largo plazo. Un año. |
| **Indicadores:** |
| - Registro de equipos renovados<br>- Registro de equipos pendientes de renovación |

| PR9: Alta disponibilidad para aplicaciones que soportan el negocio |
|---|
| **Descripción:** |
| Este proyecto deberá analizar las mejores opciones para disponer de las aplicaciones que soportan en negocio en alta disponibilidad (UCI, CRM). Será necesario la compra de hardware adicional y el soporte de los proveedores para llevarlo a cabo. |
| **Equipo de trabajo** |
| - Responsables TI (Soporte a Usuarios e Ingeniería) |
| **Objetivos** |
| - Disminución de incidentes que provocan indisponibilidad<br>- Evitar interrupciones parciales o totales de los sistemas de negocio.<br>- Aplicaciones en alta disponibilidad |
| **Riesgos a mitigar:** |
| - Indisponibilidad de aplicaciones |
| **Coste:** |
| El coste de llevar a cabo este proyecto implica compra de equipos y soporte de proveedores. 150.000€ |
| **Temporalidad:** |
| Largo plazo. Un año. |
| **Indicadores:** |
| - Registro de indisponibilidad de aplicaciones<br>- Registro de incidentes relacionados con las aplicaciones en alta disponibilidad, provoquen o no indisponibilidad. |

| PR8: Política de dispositivos móviles |
| --- |
| **Descripción:** |
| En la compañía se utiliza un número importante de dispositivos móviles y actualmente no existe ningún procedimiento o política al respecto. Si está regulado el uso de ordenadores portátiles, pero no el de otros dispositivos. Este proyecto elaborará una política global para los dispositivos móviles (ordenadores portátiles, teléfonos móviles, tabletas, etc.). La política incluirá la obligatoriedad de entregar dispositivos móviles cifrados a los usuarios. |
| **Equipo de trabajo** |
| - Responsable de Seguridad<br>- Responsables TI (Soporte a Usuarios e Ingeniería)<br>- Responsables RRHH |
| **Objetivos** |
| - Regular el uso de los dispositivos móviles.<br>- Determinar el perfil de usuario con acceso a dispositivos móviles. |
| **Riesgos a mitigar:** |
| - Riesgos propios de la utilización de dispositivos móviles. |
| **Coste:** |
| Este proyecto no tendrá coste asociado, puesto que la política será elaborada internamente y no requiere de recursos.<br>0€ |
| **Temporalidad:** |
| Corto plazo. Un mes. |
| **Indicadores:** |
| - Registro de dispositivos móviles y asignación.<br>- Registro de cifrado |

# ANEXO XIII:

## Análisis diferencial post-implementación de proyectos

| CONTROLES | Estado inicial | Estado post-impl. |
|---|---|---|
| **5. Política de Seguridad de la Información** | **95%** | **95%** |
| 5.1. **Política de seguridad de la información** | **95%** | **95%** |
| 5.1.1. Documento de política de seguridad de la información | 100% | 100% |
| 5.1.2. Revisión de la política de seguridad | 90% | 90% |
| **6. Organización de la seguridad de la información** | **54,00%** | **64,00%** |
| 6.1. **Organización interna** | **58%** | **58%** |
| 6.1.1. Roles y responsabilidades de la seguridad de la información | 90% | 90% |
| 6.1.2. Segregación de funciones | 50% | 50% |
| 6.1.3. Contacto con autoridades | 50% | 50% |
| 6.1.4. Contacto con grupos especiales de interés | 50% | 50% |
| 6.1.5. Seguridad de la información en la gestión del proyecto | 50% | 50% |
| 6.2. **Dispositivos móviles y trabajo remoto** | **50%** | **70%** |
| 6.2.1. Política de dispositivos móviles | 10% | 50% |
| 6.2.2. Trabajo remoto | 90% | 90% |
| **7. Seguridad ligada a los Recurso Humanos** | **56,67%** | **65,56%** |
| 7.1. **Previo al empleo** | **30%** | **30%** |
| 7.1.1. Selección | 10% | 10% |
| 7.1.2. Términos y condiciones de la relación laboral | 50% | 50% |
| 7.2. **Durante el empleo** | **50%** | **77%** |
| 7.2.1. Responsabilidad de la dirección | 90% | 90% |
| 7.2.2. Concienciación, educación y formación en seguridad de la información | 50% | 90% |
| 7.2.3. Proceso disciplinario | 10% | 50% |
| 7.3. **Desvinculación y cambio de empleo** | **90%** | **90%** |
| 7.3.1. Responsabilidades en la desvinculación o cambio de empleo | 90% | 90% |
| **8. Administración de activos** | **26,67%** | **40,00%** |
| 8.1. **Responsabilidad por los activos** | **20%** | **60%** |
| 8.1.1. Inventario de activos | 10% | 50% |
| 8.1.2. Propiedad de los activos | 10% | 50% |
| 8.1.3. Uso aceptable de los activos | 10% | 50% |
| 8.1.4. Devolución de activos | 50% | 90% |
| 8.2. **Clasificación de la información** | **10%** | **10%** |
| 8.2.1. Clasificación de la información | 10% | 10% |
| 8.2.2. Etiquetado de la información | 10% | 10% |
| 8.2.3. Manejo de activos | 10% | 10% |
| 8.3. **Manejo de los medios** | **50%** | **50%** |
| 8.3.1. Gestión de los medios removibles | 50% | 50% |
| 8.3.2. Eliminación de los medios | 50% | 50% |
| 8.3.3. Transferencia física de medios | 50% | 50% |
| **9. Control de acceso** | **79,17%** | **79,17%** |
| 9.1. **Requisitos de negocio para el control de acceso** | **90%** | **90%** |
| 9.1.1. Política de control de acceso | 90% | 90% |
| 9.1.2. Accesos a las redes y a los servicios de red | 90% | 90% |
| 9.2. **Gestión de acceso del usuario** | **56,67%** | **56,67%** |
| 9.2.1. Registro y cancelación de registro de usuarios | 50% | 50% |
| 9.2.2. Asignación de acceso de usuario | 10% | 10% |
| 9.2.3. Gestión de derechos de acceso privilegiados | 50% | 50% |
| 9.2.4. Gestión de información secreta de autenticación de usuarios | 50% | 50% |
| 9.2.5. Revisión de los derechos de acceso de usuario | 90% | 90% |

| | | |
|---|---|---|
| 9.2.6. Eliminación o ajuste de los derechos de acceso | 90% | 90% |
| 9.3. **Responsabilidades del usuario** | **90%** | **90%** |
| 9.3.1. Uso de información de autenticación secreta | 90% | 90% |
| 9.4. **Control de acceso al sistema y aplicaciones** | **80%** | **80%** |
| 9.4.1. Restricción de acceso a la información | 50% | 50% |
| 9.4.2. Procedimientos de inicio de sesión seguro | 50% | 50% |
| 9.4.3. Sistema de gestión de contraseñas | 100% | 100% |
| 9.4.4. Uso de programas con privilegios de sistema | 100% | 100% |
| 9.4.5. Control de acceso al código fuente de los programas | 100% | 100% |
| **10. Criptografía** | **0%** | **0%** |
| 10.1. **Controles criptográficos** | **0%** | **0%** |
| 10.1.1. Política sobre el uso de controles criptográficos | 0% | 0% |
| 10.1.2. Gestión de claves | 0% | 0% |
| **11. Seguridad física y del entorno** | **66,11%** | **75,00%** |
| 11.1. **Áreas seguras** | **73,33%** | **73,33%** |
| 11.1.1. Perímetro de seguridad física | 100% | 100% |
| 11.1.2. Controles de acceso físico | 100% | 100% |
| 11.1.3. Seguridad de oficinas, salas e instalaciones | 90% | 90% |
| 11.1.4. Protección contra amenazas externas y del entorno | 50% | 50% |
| 11.1.5. Trabajo en áreas seguras | 50% | 50% |
| 11.1.6. Áreas de entrega y carga | 50% | 50% |
| 11.2. **Equipamiento** | **58,89%** | **76,67%** |
| 11.2.1. Ubicación y protección del equipamiento | 90% | 90% |
| 11.2.2. Elementos de soporte | 90% | 90% |
| 11.2.3. Seguridad en el cableado | 10% | 50% |
| 11.2.4. Mantenimiento del equipamiento | 50% | 90% |
| 11.2.5. Retiro de activos | 50% | 90% |
| 11.2.6. Seguridad del equipamiento y los activos fuera de las instalaciones | 50% | 50% |
| 11.2.7. Seguridad en la reutilización o descarte de equipos | 50% | 90% |
| 11.2.8. Equipo de usuario desatendido | 90% | 90% |
| 11.2.9. Política de escritorio y pantalla limpios | 50% | 50% |
| **12. Seguridad de las operaciones** | **88,75%** | **90,89%** |
| 12.1. **Procedimientos operacionales y responsabilidades** | **83,75%** | **93,75%** |
| 12.1.1. Procedimientos de operación documentados | 50% | 90% |
| 12.1.2. Gestión de cambios | 100% | 100% |
| 12.1.3. Gestión de la capacidad | 95% | 95% |
| 12.1.4. Separación de los ambientes de desarrollo, prueba y operacionales | 90% | 90% |
| 12.2. **Protección contra código malicioso** | **90%** | **90%** |
| 12.2.1. Controles contra código malicioso | 90% | 90% |
| 12.3. **Respaldo** | **90%** | **95%** |
| 12.3.1. Respaldo de la información | 90% | 95% |
| 12.4. **Registro y monitoreo** | **62,50%** | **62,50%** |
| 12.4.1. Registro de evento | 50% | 50% |
| 12.4.2. Protección de la información de registros | 50% | 50% |
| 12.4.3. Registros del administrador y el operador | 50% | 50% |
| 12.4.4. Sincronización de relojes | 100% | 100% |
| 12.5. **Control de software de operación** | **100%** | **100%** |

| | | |
|---|---|---|
| 12.5.1. Instalación del software en sistemas operaciones | 100% | 100% |
| 12.6. **Gestión de la vulnerabilidad técnica** | **95%** | **95%** |
| 12.6.1. Gestión de las vulnerabilidades técnicas | 100% | 100% |
| 12.6.2. Restricciones sobre la instalación de software | 90% | 90% |
| 12.7. **Consideraciones de la auditoría de los sistemas de información** | **100%** | **100%** |
| 12.7.1. Controles de auditoría de sistemas de información | 100% | 100% |
| **13. Seguridad de las comunicaciones** | **46,67%** | **46,67%** |
| 13.1. **Gestión de la seguridad de red** | **33,33%** | **33,33%** |
| 13.1.1. Controles de red | 50% | 50% |
| 13.1.2. Seguridad de los servicios de red | 50% | 50% |
| 13.1.3. Separación en las redes | 0% | 0% |
| 13.2. **Transferencia de información** | **60%** | **60%** |
| 13.2.1. Políticas y procedimientos de transferencia de información | 50% | 50% |
| 13.2.2. Acuerdos sobre transferencia de información | 50% | 50% |
| 13.2.3. Mensajería electrónica | 50% | 50% |
| 13.2.4. Acuerdos de confidencialidad o no divulgación | 90% | 90% |
| **14. Adquisición, desarrollo y mantenimiento del sistema** | **22%** | **28%** |
| 14.1. **Requisitos de seguridad de los sistemas de información** | **3,33%** | **16,67%** |
| 14.1.1. Análisis y especificación de requisitos de seguridad de la información | 10% | 50% |
| 14.1.2. Aseguramiento de servicios de aplicación en redes públicas | 0% | 0% |
| 14.1.3. Protección de las transacciones de servicios de aplicación | 0% | 0% |
| 14.2. **Seguridad en procesos de desarrollo y soporte** | **62,22%** | **66,67%** |
| 14.2.1. Política de desarrollo seguro | 50% | 50% |
| 14.2.2. Procedimientos de control de cambios del sistema | 90% | 90% |
| 14.2.3. Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación | 50% | 90% |
| 14.2.4. Restricciones en los cambios a los paquetes de software | 90% | 90% |
| 14.2.5. Principios de ingeniería de sistema seguro | 50% | 50% |
| 14.2.6. Entorno de desarrollo seguro | 50% | 50% |
| 14.2.7. Desarrollo externalizado | 0% | 0% |
| 14.2.8. Prueba de seguridad del sistema | 90% | 90% |
| 14.2.9. Prueba de aprobación del sistema | 90% | 90% |
| 14.3. **Datos de prueba** | **0%** | **0%** |
| 14.3.1. Protección de datos de prueba | 0% | 0% |
| **15. Relaciones con el proveedor** | 37% | 50% |
| 15.1. **Seguridad de la información en las relaciones con el proveedor** | **23%** | **50%** |
| 15.1.1. Política de seguridad de la información para las relaciones con el proveedor | 10% | 50% |
| 15.1.2. Abordar la seguridad dentro de los acuerdos del proveedor | 10% | 50% |
| 15.1.3. Cadena de suministro de tecnologías de la información y comunicaciones | 50% | 50% |
| 15.2. **Gestión de entrega del servicio del proveedor** | **50%** | **50%** |
| 15.2.1. Supervisión y revisión de los servicios del proveedor | 50% | 50% |
| 15.2.2. Gestión de cambios a los servicios del proveedor | 50% | 50% |
| **16. Gestión de incidentes de seguridad de la información** | **27,14%** | **67,14%** |
| 16.1. **Gestión de incidentes de seguridad de la información y mejoras** | **27,14%** | **67,14%** |
| 16.1.1. Responsabilidades y procedimientos | 50% | 90% |
| 16.1.2. Informe de eventos de seguridad de la información | 50% | 90% |
| 16.1.3. Informe de las debilidades de seguridad de la información | 50% | 90% |

| | | |
|---|---|---|
| 16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información | 10% | 50% |
| 16.1.5. Respuesta ante incidentes de seguridad de la información | 10% | 50% |
| 16.1.6. Aprendizaje de los incidentes de seguridad de la información | 10% | 50% |
| 16.1.7. Recolección de evidencia | 10% | 50% |
| **17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio** | 30% | 70% |
| 17.1. **Continuidad de la seguridad de la información** | **10%** | **50%** |
| 17.1.1. Planificación de la continuidad de la seguridad de la información | 10% | 50% |
| 17.1.2. Implementación de la continuidad de la seguridad de la información | 10% | 50% |
| 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información | 10% | 50% |
| 17.2. **Redundancias** | **50%** | **90%** |
| 17.2.1. Disponibilidad de las instalaciones de procesamiento de la información | 50% | 90% |
| **18. Cumplimiento** | **66,00%** | **66,00%** |
| 18.1. **Cumplimiento con los requisitos legales y contractuales** | **42%** | **42%** |
| 18.1.1. Identificación de la legislación vigente y los requisitos contractuales | 50% | 50% |
| 18.1.2. Derechos de propiedad intelectual | 50% | 50% |
| 18.1.3. Protección de los registros | 50% | 50% |
| 18.1.4. Privacidad y protección de la información de identificación personal | 50% | 50% |
| 18.1.5. Regulación de los controles criptográficos | 10% | 10% |
| 18.2. **Revisiones de seguridad de la información** | **90%** | **90%** |
| 18.2.1. Revisión independiente de la seguridad de la información | 90% | 90% |
| 18.2.2. Cumplimiento con las políticas y normas de seguridad | 90% | 90% |
| 18.2.3. Verificación del cumplimiento técnico | 90% | 90% |

# ANEXO XIV:

Informe de auditoría interna TMK S.A.
ISO/IEC 27001:2013

# ÍNDICE

| TMK S.A | Informe de auditoría interna | |
|---|---|---|
| | Fecha: 08/06/2017 | Versión 1.00 |

## INFORME DE AUDITORÍA

**Control de Versiones**

| Versión | Modificaciones |
|---|---|
| 0.00 | Borrador |
| 1.00 | Informe de auditoría interna del SGSI gestionado por TMK S.A. |

**Datos de la auditoría y compañía auditada**

| |
|---|
| **Fecha de la auditoría: 0**4/06/2018 – 06/06/2018 |
| **Ubicación (lugar) de la auditoría:** Oficinas centrales TMK S.A. (Madrid) |
| **Organización/Compañía auditada:** TMK S.A. |

**Equipo auditor:**

| |
|---|
| Dunia Meler Pascual – Auditor responsable. |

**Áreas y personal auditado:**

- Dirección de tecnología:
  - Gerencia de soporte a usuarios
  - Gerencia de sistemas
  - Gerencia de desarrollo
  - Responsable de seguridad
- Dirección de RRHH
  - Gerencia de RRHH
- Dirección de finanzas
  - Gerencia infraestructuras
- Dirección legal
  - Gerencia legal

| Plan de auditoría | | | | 5 Políticas de seguridad de la información | 6 Organización de la seguridad de la información | 7 Seguridad relativa a los recursos humanos | 8 Gestión de activos | 9 Control de acceso | 10 Criptografía | 11 Seguridad física y del entorno | 12 Seguridad de las operaciones | 13 Seguridad de las comunicaciones | 14 Adquisición, desarrollo y mantenimiento de los sistemas de información | 15 Relación con proveedores | 16 Gestión de incidentes de seguridad de la información | 17Aspectos de seguridad de la información para la gestión de la continuidad del negocio | 18 Cumplimiento |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DIA | CENTRO | HORA | ÁREA / DEPARTAMENTO / RESPONSABLE | | | | | | | | | | | | | | |
| 4/06 | Madrid | 09:30-12:00 | Resp. Seguridad / RRHH | X | X | X | | | | | | | | | | | |
| 4/06 | Madrid | 12:00 -14:00 | Seguridad / Sistemas / Infraestructuras | | | | X | X | | X | | | | | | | |
| 5/06 | Madrid | 09:30-12:00 | Resp. Seguridad / Sistemas / Soporte usuarios | | | | | | X | | X | X | | | | | |
| 5/06 | Madrid | 12:00-14:00 | Seguridad / Desarrollo / Sistemas | | | | | | | | | | X | X | | | |
| 6/06 | Madrid | 09:30-11:30 | Seguridad / Sop. Usuarios | | | | | | | | | | | | X | X | |
| 6/06 | Madrid | 11:30-14:00 | Seguridad / legal | | | | | | | | | | | | | | X |

| TMK S.A | Informe de auditoría interna | |
|---|---|---|
| | Fecha: 08/06/2017 | Versión 1.00 |

**Objetivo**

Los objetivos de la auditoría interna son:

- Determinar el grado de cumplimiento del Sistema de Gestión de Seguridad de la Información de TMK S.A. de acuerdo a los requisitos de la norma UNE-ISO/IEC 27001:2007.
- Comprobar el grado de implantación de los Objetivos de Control y Controles, de acuerdo a la Declaración de Aplicabilidad y en base a los requisitos de la norma UNE-ISO/IEC 27002:2013, en TMK S.A.

**Alcance**

La auditoría se ha realizado a los sistemas de gestión que soportan el negocio de TMK S.A. (CTI, ACD, CMS, tarificador), puestos de trabajo de operador y red de comunicaciones.

**Normas de referencia:**

ISO/IEC 27001:2013
ISO/IEC 27002:2013

## RESULTADOS

### Controles

| Objetivos de control | Descripción | Resultado (OK/AM/NOK) | Comentarios |
|---|---|---|---|
| **5. Política de seguridad de la información** | | | |
| **5.1. Política de seguridad de la información** | | | |
| 5.1.1 Políticas para la seguridad de la información | Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes. | OK | Política de Seguridad de la Información. DOC-01-SEG Política de Seguridad |
| 5.1.2 Revisión de las políticas para la seguridad de la información | Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. | OK | Revisión por la dirección (anual) Actas comité de seguridad. |
| **6. Organización de la seguridad de la información** | | | |
| **6.1. Organización interna** | | | |
| 6.1.1. Roles y responsabilidades en seguridad de la información | Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas | OK | Las responsabilidades se encuentran asignadas en la documentación del SGSI: DOC-03-SEG Gestión de roles y responsabilidades |
| 6.1.2 Segregación de tareas | Las funciones y áreas de responsabilidad deben segregarse para reducir la | OK | Existen grupos de trabajo diferenciados |

| | | | |
|---|---|---|---|
| | posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización | | |
| 6.1.3 Contacto con las autoridades | Deben mantenerse los contactos apropiados con las autoridades pertinentes. | OK | Función del departamento legal. |
| 6.1.4 Contacto con grupos de interés especial | Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializadas en seguridad. | OK | Socios de la Asociación Española de *Contact Center*<br>Reuniones y seminarios AEPD<br>Fabricantes *software* y *hardware* |
| 6.1.5 Seguridad de la información en la gestión de proyectos | La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto. | OK | Se trata la seguridad de la información en contratos de clientes y ofertas comerciales. |
| **6.2. Los dispositivos móviles y el teletrabajo** | | | |
| 6.2.1 Política de dispositivos móviles | Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles. | OK | Portátiles cifrados con *bitlocker* |
| 6.2.2 Teletrabajo | Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo. | OK | Cláusula de teletrabajo firmada en contratos. |
| **7. Seguridad relativa a los recursos humanos** | | | |
| **7.1. Antes del empleo** | | | |
| 7.1.1. Selección | Se debe verificar los antecedentes de todos los candidatos al empleo, de acuerdo a las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida y los riesgos percibidos | NOK – No OK<br>No Conformidad Menor | Por LOPD no es legal investigar sin autorización. Actualmente solo se pide curriculum, no se pide autorización y por tanto no se realiza investigación. Se debe valorar solicitar titulaciones compulsadas y realizar algún test. |
| 7.1.2 Términos y condiciones del empleo | Como parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el | OK | Contrato de trabajo (empleados) y proveedores incluyen cláusula de confidencialidad. |

| | | | |
|---|---|---|---|
| | empleado como hacia la organización. | | |
| **7.2. Durante el empleo** | | | |
| 7.2.1 Responsabilidades de gestión | La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. | OK | Política de seguridad<br>Formación en seguridad<br>Acuerdo protección de datos empleado y confidencialidad |
| 7.2.2 Concienciación, educación y capacitación en seguridad de la información. | Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo. | OK | Formación a empleados<br>Difusión de información de seguridad. |
| 7.2.3 Proceso disciplinario | Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad. | OK | Convenido del sector para el *Contact Center* |
| **7.3. Finalización del empleo o cambio en el puesto de trabajo** | | | |
| 7.3.1 Responsabilidades ante la finalización o cambio | Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir. | OK | Procedimiento de altas y bajas |
| **8. Gestión de activos** | | | |
| **8.1. Responsabilidad sobre los activos** | | | |
| 8.1.1 Inventario de activos | Los activos asociados a la información, y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. | OK | Inventario de activos del SGSI |
| 8.1.2 Propiedad de los activos | Todos los activos que figuran en el inventario deben tener un propietario. | NOK – No OK<br>No Conformidad Menor | Los auditados refieren que todo activo tiene un propietario pero no está documentado. Se debe documentar. |
| 8.1.3 Uso aceptable de los activos | Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los | OK | Política de seguridad. |

| | | | |
|---|---|---|---|
| | recursos para el tratamiento de la información. | | |
| 8.1.4 Devolución de activos | Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo. | OK | Procedimiento de altas y bajas |
| **8.2. Clasificación de la información** | | | |
| 8.2.1. Clasificación de la información | La información debe ser clasificada en términos legales, de valor, criticidad y sensibilidad para la divulgación o modificación sin autorización | NOK – No OK No Conformidad Menor | Se realiza clasificación, pero no existe una forma común de proceder. Debe unificarse y procedimentarse el proceso y asignar responsabilidades. |
| 8.2.2. Etiquetado de la información | Desarrollo e implementación conjunto de procedimientos para el etiquetado de la información de acuerdo al esquema de clasificación establecido por la compañía | NOK – No OK No Conformidad Menor | No existe una forma común de proceder. Debe unificarse y procedimentarse el proceso y asignar responsabilidades. |
| 8.2.3. Manejo de activos | Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización. | NOK – No OK No Conformidad Menor | No existe una forma común de proceder. Debe unificarse y procedimentarse el proceso y asignar responsabilidades. |
| **8.3. Manipulación de los soportes** | | | |
| 8.3.1 Gestión de soportes extraíbles | Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización | OK | Política de *backups* |
| 8.3.2 Eliminación de soportes | Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales. | OK | Los soportes son eliminados de forma segura. Existen registros de eliminación. Procedimiento de destrucción de soportes. |
| 8.3.3 Soportes físicos en tránsito | Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. | OK | Lo soportes viajan cifrados y en maletines seguros con candados con código de seguridad de cuatro dígitos. |
| **9. Control de acceso** | | | |
| **9.1. Requisitos de negocio para el control de acceso** | | | |
| 9.1.1 Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de | OK | Política de control de acceso Procedimiento de altas y bajas. |

| | | | |
|---|---|---|---|
| | negocio y de seguridad de la información. | | |
| 9.1.2 Acceso a las redes y a los servicios de red | Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados. | OK | Todos los accesos a redes y servicios de red solicitados deben ser autorizados de forma expresa por el responsable del recurso. Existen registros. |
| **9.2. Gestión de acceso de usuario** | | | |
| 9.2.1 Registro y baja de usuario | Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso. | OK | Procedimiento de altas y bajas. |
| 9.2.2. Asignación de acceso de usuario | Debe existir procedimiento formal de asignación de acceso de usuario para asignar o revocar derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios. | AM – A Mejorar | Existe una forma de proceder para la asignación y revocación de usuarios, pero no está documentado formalmente como procedimiento |
| 9.2.3 Gestión de privilegios de acceso | La asignación y el uso de privilegios de acceso debe estar restringida y controlada | OK | Todas las asignaciones quedan registradas y está restringida. |
| 9.2.4 Gestión de la información secreta de autenticación de los usuarios | La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión. | OK | Se entregan contraseñas temporales que el sistema obliga a cambiar al usuario de forma obligatoria y secreta. |
| 9.2.5 Revisión de los derechos de acceso de usuario | Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares | OK | Se realizan revisiones periódicas por los propietarios que quedan registradas. |
| 9.2.6 Retirada o reasignación de los derechos de acceso | Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio. | OK | Se realizan revisiones periódicas de los usuarios activos e inactivos.<br>Seguridad de la información envía recordatorios de revisión<br>Procedimiento de altas y bajas. |
| **9.3. Responsabilidades del usuario** | | | |
| 9.3.1 Uso de la información secreta de autenticación | Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación. | OK | Configuración de políticas y usuarios en el Directorio Activo de la compañía. |
| **9.4. Responsabilidades del usuario** | | | |
| 9.4.1 Restricción del acceso a la información | Se debe restringir el accesos la información y a las funciones de las aplicaciones, de acuerdo con | OK | Todo acceso requiere de autenticación. |

| | | | |
|---|---|---|---|
| | la política de control de acceso definida. | | |
| 9.4.2 Procedimientos seguros de inicio de sesión | Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión. | OK | Inicio de sesión sincronizado con Directorio Activo. |
| 9.4.3 Sistema de gestión de contraseñas | Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas. | OK | Configuración de políticas y usuarios en el Directorio Activo de la compañía |
| 9.4.4 Uso de utilidades con privilegios del sistema | Se debe restringir y controlar rigurosamente el uso de utilidades que puedan invalidar los controles del sistema y de la aplicación. | OK | Política de usuarios y contraseñas. |
| 9.4.5 Control de acceso al código fuente de los programas | Se debe restringir el acceso al código fuente de los programas. | OK | Política de usuarios y contraseñas.<br>Los usuarios sólo tienen los permisos necesarios para su trabajo. |
| **10. Criptografía** | | | |
| **10.1. Controles criptográficos** | | | |
| 10.1.1. Política sobre el uso de controles criptográficos | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información | AM – A Mejorar | Hasta el momento sólo se encriptan las copias de seguridad *(backup)* que viajan fuera de las instalaciones de la compañía y los portátiles. Debe ser desarrollada una política y analizar si hay otros activos a encriptar. |
| 10.1.2. Gestión de claves | Se debe desarrollar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil. | NOK – No OK<br>No Conformidad Mayor | Sólo se usan claves criptográficas en el cifrado de portátiles, pero no hay una política formal ni una vida útil definida. |
| **11. Seguridad física y del entorno** | | | |
| **11.1. Áreas seguras** | | | |
| 11.1.1 Perímetro de seguridad física | Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información | OK | Procedimiento de acceso a CPDs y acceso mediante lector de tarjeta. |
| 11.1.2 Controles físicos de entrada | Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado | OK | Procedimiento de acceso a CPDs y acceso mediante lector de tarjeta |

| | | | |
|---|---|---|---|
| 11.1.3 Seguridad de oficinas, despachos y recursos | Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física. | OK | Accesos controlados mediante lector de tarjeta. |
| 11.1.4 Protección contra las amenazas externas y ambientales | Se debe diseñar y aplicar protección física contra desastres naturales, ataques provocados por el hombre o accidentes. | OK | Medidas gestionadas por la propiedad del edificio. |
| 11.1.5 El trabajo en áreas seguras | Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras. | OK | Procedimiento de acceso a CPDs y acceso mediante lector de tarjeta. |
| 11.1.6 Áreas de carga y descarga | Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados | OK | Accesos controlados mediante lector de tarjeta. |
| **11.2. Seguridad en los equipos** | | | |
| 11.2.1 Emplazamiento y protección de equipos | Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados. | OK | Procedimiento de acceso a CPDs y acceso mediante lector de tarjeta |
| 11.2.2 Instalaciones de suministro | Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro. | OK | Doble sistema de alimentación de soporte. |
| 11.2.3 Seguridad del cableado | El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. | OK | El cableado de red y eléctrico se encuentra protegido. |
| 11.2.4 Mantenimiento de los equipos | Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas. | OK | Mantenimientos contratados con proveedores.<br>Alta disponibilidad.<br>Revisiones diarias y sistema de alertas. |
| 11.2.5 Retirada de | Sin autorización previa, los equipos, la información o el | OK | Se requiere autorización para sacar fuera de las |

| | | | |
|---|---|---|---|
| materiales propiedad de la empresa | software no deben sacarse de las instalaciones. | | instalaciones información, equipos o *software*. |
| 11.2.6 Seguridad de los equipos fuera de las instalaciones | Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones. | OK | Política de seguridad VPN y cifrado de portátiles. |
| 11.2.7 Reutilización o eliminación segura de equipos | Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos. | OK | Los equipos o soportes son formateados previamente a su reutilización o eliminación. |
| 11.2.8 Equipo de usuario desatendido | Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada. | OK | Bloqueo automático por inactividad<br>Política de seguridad del empleado. |
| 11.2.9 Política de puesto de trabajo despejado y pantalla limpia | Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información. | OK | Política de seguridad del empleado |
| **12. Seguridad de las operaciones** | | | |
| **12.1. Procedimientos y responsabilidades operacionales** | | | |
| 12.1.1 Documentación de procedimientos de los operación | Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten | OK | Los documentos y procedimientos están en repositorios de información en la intranet. |
| 12.1.2 Gestión de cambios | Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados | OK | Proceso de gestión de cambios (ITIL) |
| 12.1.3 Gestión de capacidades | Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema. | OK | Proceso de gestión de la capacidad (ITIL) |
| 12.1.4 Separación de los recursos de | Deben separarse los recursos de desarrollo, | OK | Existen entornos de desarrollo, |

| | | | |
|---|---|---|---|
| desarrollo, prueba y operación | pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción. | | preproducción y producción diferenciados y con accesos restringidos. |
| **12.2. Protección contra software malicioso *(malware)*** | | | |
| 12.2.1 Controles contra el código malicioso | Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario. | OK | Antivirus<br>Restricciones instalación de software |
| **12.3. Copias de seguridad** | | | |
| 12.3.1 Copias de seguridad de la información | Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada. | OK | Política de backups. |
| **12.4. Registros y supervisión** | | | |
| 12.4.1 Registro de eventos | Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. | OK | Existe registro para datos de nivel alto de seguridad (LOPD) |
| 12.4.2 Protección de la información de registro | Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados. | OK | Existe copia de seguridad del registro. |
| 12.4.3 Registros de administración y operación | Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema. | OK | Existen registros de actividad que se revisan. |
| 12.4.4 Sincronización del reloj | Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo. | OK | Sincronizado con servidor NTP |
| **12.5. Control del software en explotación** | | | |

| | | | |
|---|---|---|---|
| 12.5.1 Instalación del software en explotación | Se deben implementar procedimientos para controlar la instalación del software en explotación. | OK | Proceso Gestión del cambio (ITIL) |
| **12.6. Gestión de la vulnerabilidad técnica** | | | |
| 12.6.1 Gestión de las vulnerabilidades técnicas | Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado. | OK | Actualizaciones de seguridad distribuidas de forma automática. |
| 12.6.2 Restricción en la instalación de software | Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios | OK | Instalación de software restringida para usuarios. |
| **12.7. Consideraciones sobre la auditoria de sistemas de información** | | | |
| 12.7.1 Controles de auditoría de sistemas de información | Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio | OK | Existe documentación para realización de *checklist*.<br>Las auditorías son planificadas y acordadas. |
| **13. Seguridad de las comunicaciones** | | | |
| **13.1. Gestión de la seguridad de redes** | | | |
| 13.1.1 Controles de red | Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones. | OK | Firewall<br>IPS<br>Antivirus |
| 13.1.2 Seguridad de los servicios de red | Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan. | OK | Firewall<br>IPS<br>Antivirus |

| | | | |
|---|---|---|---|
| 13.1.3 Segregación en redes | Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas. | No aplica a TMK S.A. | |
| **13.2. Transferencia de información** | | | |
| 13.2.1 Políticas y procedimientos de intercambio de información | Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación. | OK | Utilización VPN |
| 13.2.2 Acuerdos de intercambio de información | Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros. | OK | Utilización VPN |
| 13.2.3 Mensajería electrónica | La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida. | OK | La mensajería electrónica es sólo de uso interno. |
| 13.2.4 Acuerdos de confidencialidad o no revelación | Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación | OK | Clausulas confidencialidad empleados y proveedores. |
| **14. Adquisición, desarrollo y mantenimiento de los sistemas de información.** | | | |
| **14.1. Requisitos de seguridad en sistemas de información** | | | |
| 14.1.1 Análisis de requisitos y especificaciones de seguridad de la información | Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes. | AM – A Mejorar | Los requisitos se tienen en cuenta en sistemas nuevos o en las mejoras, pero no está documentado.<br>Se aconseja documentarlos.<br>Están sujetos al proceso de gestión del cambio. |
| 14.1.2 Asegurar los servicios de aplicaciones en redes públicas | La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas. | No aplica a TMK S.A. | |
| 14.1.3 Protección de las transacciones de servicios de | La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para | No aplica a TMK S.A. | |

| | | | |
|---|---|---|---|
| aplicaciones | prevenir la transmisión incompleta, errores de enrutamiento, 'alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas. | | |
| **14.2. Seguridad en el desarrollo y en los procesos de soporte** | | | |
| 14.2.1 Política de desarrollo seguro | Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas | AM – A Mejorar | Se siguen reglas de desarrollo seguro pero no se encuentran documentadas. Se recomienda documentarlas. |
| 14.2.2 Procedimiento de control de cambios en sistemas | La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios. | OK | Procedimiento de gestión del cambio (ITIL) |
| 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio criticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización. | OK | Procedimiento de gestión del cambio (ITIL).<br>Existen entornos de pruebas (desarrollo y pre-producción) |
| 14.2.4 Restricciones a los cambios en los paquetes de software | Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso. | OK | Procedimiento de gestión del cambio (ITIL). |
| 14.2.5 Principios de ingeniería de sistemas seguros | Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información. | OK | Existen maquetas seguras y probadas para la implementación de nuevos sistemas de información. |
| 14.2.6 Entorno de desarrollo seguro | Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que | OK | Existe entorno de desarrollo. |

| | | | |
|---|---|---|---|
| | cubren todo el ciclo de vida de desarrollo del sistema. | | |
| 14.2.7 Externalización del desarrollo de software | El desarrollo de software externalizado debe ser supervisado y controlado por la organización. | No aplica a TMK S.A. | |
| 14.2.8 Pruebas funcionales de seguridad de sistemas | Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo | OK | Procedimiento de gestión del cambio (ITIL). |
| 14.2.9 Pruebas de aceptación de sistemas | Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones. | OK | Procedimiento de gestión del cambio (ITIL). |
| **14.3. Datos de prueba** | | | |
| 14.3.1 Protección de los datos de prueba | Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados. | No aplica a TMK S.A. | |
| **15. Relación con proveedores** | | | |
| **15.1. Seguridad en las relaciones con proveedores** | | | |
| 15.1.1 Política de seguridad de la información en las relaciones con los proveedores | Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos deben acordarse con el proveedor y quedar documentados | OK | Contratos con proveedores |
| 15.1.2 Requisitos de seguridad en contratos con terceros | Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT | OK | Contratos con proveedores |
| 15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones | Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la | OK | Contratos con proveedores |

| | | | |
|---|---|---|---|
| | cadena de suministro de productos. | | |
| **15.2. Gestión de la provisión de servicios del proveedor** | | | |
| 15.2.1 Control y revisión de la provisión de servicios del proveedor | Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor | OK | Se revisan las condiciones contractuales de los servicios contratados. |
| A15.2.2 Gestión de cambios en la provisión del servicio del proveedor | Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos. | OK | Procedimiento de gestión del cambio (ITIL) |
| **16. Gestión de incidentes de seguridad de la información.** | | | |
| **16.1. Gestión de incidentes de seguridad de la información y mejoras** | | | |
| 16.1.1 Responsabilidades y procedimientos | Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información. | OK | Proceso de gestión de incidentes (ITIL)<br>Proceso gestión de incidentes de seguridad |
| 16.1.2 Notificación de los eventos de seguridad de la información | Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible. | OK | Proceso de gestión de incidentes (ITIL)<br>Proceso gestión de incidentes de seguridad |
| 16.1.3 Notificación de puntos débiles de la seguridad | Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios. | OK | Proceso de gestión de incidentes (ITIL)<br>Proceso gestión de incidentes de seguridad |
| 16.1.4 Evaluación y decisión sobre los eventos de seguridad de información | Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información. | OK | Proceso de gestión de incidentes (ITIL)<br>Proceso gestión de incidentes de seguridad |

| | | | |
|---|---|---|---|
| 16.1.5 Respuesta a incidentes de seguridad de la información | Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados. | OK | Proceso de gestión de incidentes (ITIL) Proceso gestión de incidentes de seguridad |
| 16.1.6 Aprendizaje de los incidentes de seguridad de la información | El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro. | OK | Proceso de gestión de incidentes (ITIL) Proceso gestión de incidentes de seguridad |
| 16.1.7 Recopilación de evidencias | La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia. | OK | Proceso de gestión de incidentes (ITIL) Proceso gestión de incidentes de seguridad |
| **17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio** | | | |
| **17.1. Continuidad de la seguridad de la información.** | | | |
| 17.1.1 Planificación de la continuidad de la seguridad de la información | La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre | OK | Plan de continuidad de negocio |
| 17.1.2 Implementar la continuidad de la seguridad de la información | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa. | OK | Plan de continuidad de negocio |
| 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas. | OK | Plan de continuidad de negocio |
| **17.2. Redundancias** | | | |

| | | | |
|---|---|---|---|
| 17.2.1 Disponibilidad de los recursos de tratamiento de la información | Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad | OK | Plan de continuidad de negocio |
| **18. Cumplimiento** | | | |
| **18.1. Gestión de la seguridad de redes** | | | |
| 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales | Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización. | OK | El departamento legal se ocupa tanto de la identificación de la legislación aplicable como de los requisitos contractuales con proveedores y los mantiene documentados. |
| 18.1.2 Derechos de propiedad intelectual (DPI) | Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados | OK | Los usuarios no pueden instalar libremente *software*.<br>La instalación de software es controlada por los administradores y por la gestión del cambio. |
| 18.1.3 Protección de los registros de la organización | Los registros deben estar protegidos contra la pérdida destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio | OK | Política de *backups.* |
| 18.1.4 Protección privacidad de la información de carácter personal | Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables. | OK | Auditoría LOPD<br>Política de seguridad |
| 18.1.5. Regulación de los controles criptográficos | Se deben utilizar controles criptográficos que cumplan los acuerdos, leyes y regulaciones pertinentes. | NOK – No OK<br>No Conformidad Mayor | No hay evidencias de controles criptográficos. |
| **18.2. Revisiones de la seguridad de la información** | | | |

| | | | |
|---|---|---|---|
| 18.2.1 Revisión independiente de la seguridad de la información | El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad. | OK | Auditoría de cumplimiento |
| 18.2.2 Cumplimiento de las políticas y normas de seguridad | Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable | OK | Política de seguridad |
| 18.2.3 Comprobación del cumplimiento técnico | Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización. | OK | Política de seguridad |

**No Conformidad Menor:** Desviación mínima en relación con requisitos normativos, propios de la organización y/o legales y no afecta a la eficiencia e integridad del sistema de Gestión.

**No Conformidad Mayor:** Incumplimiento de un requisito normativo, propio de la organización y/o legal, que vulnera o pone en serio riesgo la integridad del sistema de gestión. Puede corresponder a la no aplicación de una cláusula de una norma (requerida por la organización), el desarrollo de un proceso sin control, ausencia consistente de registros declarados por la organización o exigidos por la norma, o la repetición permanente y prolongada a través del tiempo de pequeños incumplimientos asociados a un mismo proceso o actividad.

| No Conformidades Mayores | No Conformidades Menores | Observaciones |
|---|---|---|
| 2 | 5 | 4 |

**Resumen auditoría**

Se ha realizado la Auditoría Interna a los Sistemas de Gestión de la Seguridad de TMK S.A., de acuerdo a las revisiones establecidas en el Sistema de Gestión y en base al Plan de Auditoría.

Se ha comprobado la implantación del mismo respecto a los requisitos especificados en la norma de referencia: UNE-ISO/IEC 27001:2013 “Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos”.

La revisión se ha realizado en los departamentos de la empresa que figuran en el Listado de Personal Entrevistado, incluido en este informe.

A lo largo de la auditoría se ha realizado la comprobación de la documentación del SGSI y revisado el Análisis y Evaluación de riesgos.

El Análisis y la Valoración de Riesgos realizados se han realizado en base a la metodología MAGERIT. La revisión de controles se ha realizado en base a la Declaración de Aplicabilidad de fecha 27/03/2017.

El emplazamiento auditado ha sido la sede central de TMK S.A. sita en Madrid.

**Conclusiones finales**

El sistema de Gestión de Seguridad de la se encuentra en un grado de implantación avanzado. No obstante en cuanto a la Implantación de controles y a su eficacia se refiere, se han detectado algunos aspectos que han de ser revisados y corregidos utilizando los procedimientos establecidos por el SGSI.