laSalle ENG
Ramon Llull University

Escola Tècnica Superior d'Enginyeria Electrònica i Informàtica La Salle

Treball Final de Màster

Màster Universitari en Enginyeria de Telecomunicació

Plan Director de Seguridad

Alumne

Guillermo Martínez-Ubierna de Evan

Professor Ponent

Jaume Abella Fuentes

ACTA DE L'EXAMEN
DEL TREBALL FI DE CARRERA

Reunit el Tribunal qualificador en el dia de la data, l'alumne

D. Guillermo Martínez-Ubierna de Evan

va exposar el seu Treball de Fi de Màster, el qual va tractar sobre el tema següent:

Plan Director de Seguridad

Acabada l'exposició i contestades per part de l'alumne les objeccions formulades pels Srs. membres del tribunal, aquest valorà l'esmentat Treball amb la qualificació de

Barcelona,

VOCAL DEL TRIBUNAL VOCAL DEL TRIBUNAL

PRESIDENT DEL TRIBUNAL

Resumen

En el actual documento se presenta el estudio de la infraestructura tecnológica de la empresa GUIMARUBI y su posterior plan de acción de mejora a realizar en los próximos tres años. Este proyecto se ha focalizado en la securización de los sistemas con la intención de definir los próximos pasos en el ámbito de los sistemas elaborando un Plan Director de Seguridad.

El Plan Director de Seguridad es una necesidad para la organización que ha de estar integrado en los procesos de negocio. No es únicamente un análisis de riesgo, ni un diagnóstico/auditoría de seguridad, es un documento "vivo" que contiene un conjunto de actuaciones alineadas con la estrategia de la operación con la finalidad de proporcionar un entorno seguro de operaciones para el negocio.

Los objetivos del presente Plan Director de Seguridad son:

1. Definir un Modelo de Seguridad Corporativo, adaptando los estándares internacionales (referencias) a las necesidades específicas de la Compañía, y alineado con su Plan Estratégico.
2. Identificar el nivel de Seguridad existente en los sistemas de información de la Compañía, en base a sus necesidades de negocio y a los servicios que ésta ofrece.
3. Definir y planificar el conjunto de acciones a realizar (a corto, medio y largo plazo) en el ámbito temporal establecido, a raíz de la diferencia existente entre el nivel de seguridad objetivo de la Compañía y del nivel de seguridad actual.
4. Conocer y cuantificar las inversiones y costes necesarios para alcanzar el nivel de seguridad adecuado a las necesidades de negocio de la Compañía.

Esta memoria ofrece una visión global de la infraestructura de la Compañía y un análisis para su posterior actualización siguiendo un plan de acción definido para los próximos 3 años.

Palabras Clave

Ciberseguridad, Análisis de Riesgos, Sistemas TI, ISO, MAGERIT, OCTAVE, NIST, CMMI, vulnerabilidades, amenazas, impacto, activos y riesgos de TI.

Resum

A l'actual document es presenta l'estudi de la infraestructura tecnològica de l'empresa GUIMARUBI i el seu posterior pla d'acció de millora a realitzar en els propers tres anys. Aquest projecte s'ha focalitzat en la securització dels sistemes amb la intenció de definir els propers passos en l'àmbit dels sistemes elaborant un Pla Director de Seguretat.

El Pla Director de Seguretat és una necessitat per a l'organització que ha d'estar integrat en els processos de negoci. No és únicament una anàlisi de risc, ni un diagnòstic/auditoria de seguretat, és un document "viu" que conté un conjunt d'actuacions alineades amb l'estratègia de l'operació amb la finalitat de proporcionar un entorn segur d'operacions per al negoci.

Els objectius del present Pla Director de Seguretat són:

1. Definir un Model de Seguretat Corporatiu, adaptant els estàndards internacionals (referències) a les necessitats específiques de la Companyia, i alineat amb el seu Pla Estratègic.
2. Identificar el nivell de Seguretat existent en els sistemes d'informació de la Companyia, sobre la base de les seves necessitats de negoci i als serveis que aquesta ofereix.
3. Definir i planificar el conjunt d'accions a realitzar (a curt, mitjà i llarg termini) en l'àmbit temporal establert, arran de la diferència existent entre el nivell de seguretat objectiu de la Companyia i del nivell de seguretat actual.
4. Conèixer i quantificar les inversions i costos necessaris per aconseguir el nivell de seguretat adequat a les necessitats de negoci de la Companyia.

Aquesta memòria ofereix una visió global de la infraestructura de la Companyia i una anàlisi per a la seva posterior actualització seguint un pla d'acció definit per als propers 3 anys.

Paraules Clau

Ciberseguretat, Anàlisi de Riscos, Sistemes TI, ISO, MAGERIT, OCTAVE, NIST, CMMI, vulnerabilitats, amenaces, impacte, actius i riscos de TI.

Abstract

The current document sets forth the study of the technological infrastructure of the GUIMARUBI Company and his action plan of improvement to execute in the next three years. This project has focused in the securization of the IT systems with the intention to define the next steps in the field of IT systems elaborating a “Safety Director Plan”.

The “Safety Director Plan” is a need for the organization that has to be integrated in the business process. It is not only a risk analysis, a security diagnostic/audit, it is a “live” document that it contains a group of tasks aligned with the strategy of the operation in order to provide a secure operating environment for the business.

The objectives of the “Security Director Plan” are as follows:

1. Define a Model of Corporate Security, adapting the international standards (references) to the specific needs of the Company, and aligned with his Strategic Plan.
2. Identify the level of existent Security in the information systems of the Company, on the base of his needs of business and to the services that this offers.
3. Define and schedule the group of actions to execute (at short, average and long term) established, as a result of the existent difference between the level of objective security of the Company and of the level of current security.
4. Identify and quantify the future investments and necessary costs to achieve the level of suitable security to the needs of business of the Company.

This project offers a global vision of the infrastructure of the Company and a detailed analysis for its update following an action plan defined for the next 3 years

Key words

Cybersecurity, Risk Analysis, IT Systems, ISO, MAGERIT, OCTAVE, NIST, CMMI, vulnerabilities, threats, impact, assets and IT Risks.

Agradecimientos

Agradezco a todas las personas que me han ayudado a hacer posible el desarrollo de este proyecto, especialmente a Ignacio Pérez y Albert Castellanos, compañeros de trabajo y amigos. También quiero agradecer a mi tutor del trabajo, Jaume Abella, por la ayuda prestada en el proyecto. Por último, me gustaría agradecer a Sandra todo el apoyo que me ha dado desde el primer momento y por haberme aguantado en los momentos difíciles y haberme dado ánimos.

Contenido

Tabla de Figuras

Acrónimos

AARR: Análisis de Riesgos
APT: *Advanced Persistent Threat*
BIA: *Business Impact Analysis*
BSI: *British Standards Institution*
CERT: *Computer Emergency Response Team*
CMMI: *Capability Maturity Model Integration*
CNPIC: Comité Nacional de Protección de Infraestructuras Críticas
CPD: Centro de Procesado de Datos
DAFO: Debilidades Amenazas Fortalezas Oportunidades
DLP: *Data Loss Prevention*
DoS: *Denial of Service*
E-DRM: *Electronic Discovery Reference Model*
EY: *Ernst&Young*
FTE: *Full-Time Equivalent*
FW: *FireWal*l
IDS: *Intrusion Detection System*
IEC: *International Electrotechnical Commission*
IoT: *Internet of Things*
IPS: *Intrusion Prevention System*
ISO: *International Organization for Standardization*
ITIL: *Information Technology Infrastructure Library*
LOPD: Ley Orgánica de Protección de Datos
LPIC: Ley de Protección de Infraestructuras Críticas
MS: Microsoft
NIST: *National Institute of Standards and Technology*
OCTAVE: *Operationally Critical Threat, Asset and Vulnerability Evaluation*
OGC: *Office of Government Commerce*
PCI-DSS: *Payment Card Industry - Data Security Standard*
PCN: Plan de Continuidad de Negocio
PDSI: Plan Director de Seguridad de la Información
RGPD: Reglamento General de Protección de Datos
SGA: Sistema de Gestión de Almacenes
SGSI: Sistema de Gestión de Seguridad de la Información
SI: Sistema de Información
SLA: *Service Level Agreement*
SO: Sistema Operativo
S-SDLC: *Secure Software Development Life Cycle*
SSO: *Single Sign On*
TI: Tecnologías de la Información
USB: *Universal Serial Bus*
VNC: *Virtual Network Computing*

1 Introducción

El presente Trabajo Final de Master describe el trabajo realizado durante la ejecución de un Plan Director de Seguridad para una empresa del sector *retail*. Este trabajo se ha realizado como un proyecto real de consultoría en la empresa EY, ofreciendo sus servicios a la empresa GUIMARUBI.

Como resultado de este proyecto, se obtendrá el estado actual de cobertura tecnológica de GUIMARUBI y se hará una propuesta de visión tecnológica futura (3 años) y el detalle de los programas y proyectos tecnológicos necesarios a abordar con el fin de conseguirlo. El Plan Director de Seguridad permitirá a GUIMARUBI definir y planificar las directrices de actuación necesarias en materia de seguridad de la información para ofrecer confianza sobre los servicios y procesos que éstos soportan. Este Plan Director deberá dar respuesta a las siguientes preguntas:

1. ¿Hacia Dónde?: Definir un Modelo de Seguridad Corporativo (Políticas, Organización, Controles y Arquitectura Tecnológica), adaptando los estándares internacionales (ISO/IEC 27002) a las necesidades específicas de GUIMARUBI.
2. ¿Qué?: Identificar el nivel de Seguridad Existente en los sistemas de información de GUIMARUBI y el *gap* existente con el nivel de Seguridad Objetivo, definido en base a los objetivos de negocio y a los servicios que ofrece GUIMARUBI.
3. ¿Cómo?: Definir y planificar el conjunto de acciones a realizar (a corto, medio y largo plazo) en el ámbito temporal establecido, a raíz de la diferencia existente entre el nivel de seguridad objetivo y el nivel de seguridad actual.
4. ¿Cuánto?: Conocer y cuantificar las inversiones y costes necesarios para alcanzar el nivel de seguridad adecuado a las necesidades de negocio de GUIMARUBI

El éxito de un Plan Director de pasa por considerar las cuatro dimensiones que afectan directamente al nivel de seguridad de la información en una Organización:

1. Estrategia
2. Procesos
3. Tecnología
4. Personas

El Plan Director deberá proporcionar soluciones adecuadas en estos cuatro ámbitos, logrando a través de ellas alcanzar el nivel de seguridad deseado.

El Plan Director debe proporcionar también las métricas necesarias para calcular el nivel de seguridad y analizar la evolución del mismo conforme avanza la implantación de las acciones identificadas en el Plan:

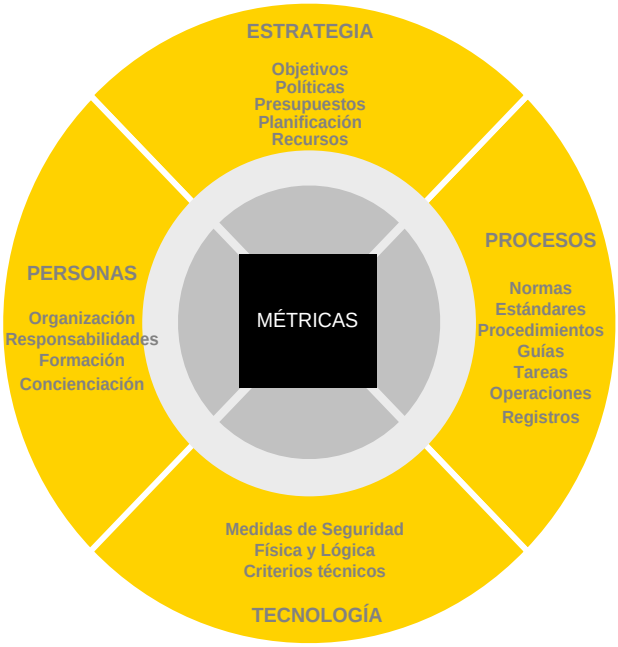


Figura 1: Dimensiones que afectan directamente al nivel de seguridad de la información en una Organización

1.1 Estructura del documento

Inicialmente el documento expondrá los antecedentes de la empresa sobre la cual se ha realizado el presente Plan Director de Seguridad para entender el mercado en el que se encuentra. Adicionalmente, para poner en contexto el actual proyecto se explicará la historia de la ciberseguridad a lo largo de los últimos años y la relevancia que tiene hoy en día en todas las empresas de cualquier tamaño.

Posteriormente se expondrán los fundamentos teóricos necesarios para el entendimiento y la ejecución del presente proyecto. Se definirán los términos más importantes que aparecen a lo largo del documento, se expondrán los diferentes tipos de Análisis de Riesgos y la posterior gestión del riesgo una vez obtenidos los resultados del análisis para, con ello, trazar un plan a corto, medio y largo plazo.

Seguidamente se explicará el alcance del proyecto realizado en la empresa GUIMARUBI, exponiendo el trabajo que se realizará en el presente documento.

A continuación se enumerarán las metodologías y marcos de referencia más importantes al realizar un análisis de riesgos y un Plan Director de Seguridad y se detallarán. Dichas metodologías y marcos de referencia serán utilizadas para realizar el actual proyecto.

Continuadamente se describirá el trabajo realizado en GUIMARUBI, detallando todo el proceso seguido durante el proyecto y los resultados obtenidos, así como el plan propuesto para la mejora del nivel de seguridad para GUIMARUBI.

Consecutivamente se detallará la planificación del proyecto, así como su coste, tanto en tiempo como económico y finalmente, se redactarán las líneas de futuro de este proyecto, exponiendo la continuación del mismo para los próximos 3 años.

2 Antecedentes

Se expondrá la importancia de que una empresa realice un proyecto como el descrito en este documento, para ello se introducirá el contexto de la empresa y la importancia de la ciberseguridad hoy en día.

2.1 Quien es GUIMARUBI y qué hace

GUIMARUBI es la primera empresa mayorista de España del sector de la distribución alimentaria. Con más de 85 años de experiencia, cuenta con diferentes líneas de negocio:

- Franquicias de supermercados.
- *Import* & *Export*.
- Venta mayorista.
- Restauración organizada.

Para alcanzar la actual posición de liderazgo en el mercado mayorista, durante los últimos años, GUIMARUBI ha impulsado múltiples iniciativas estratégicas que han ido transformado la organización, los procesos operativos y sus sistemas de información soporte. Todo este proceso de transformación ha podido ocasionar la aparición de nuevos escenarios de riesgos asociados a la seguridad de la información no contemplados hasta el momento; es por ello, que la Compañía cree necesario realizar un análisis de esos posibles escenarios para minimizar los potenciales riesgos asociados a la seguridad de la información.

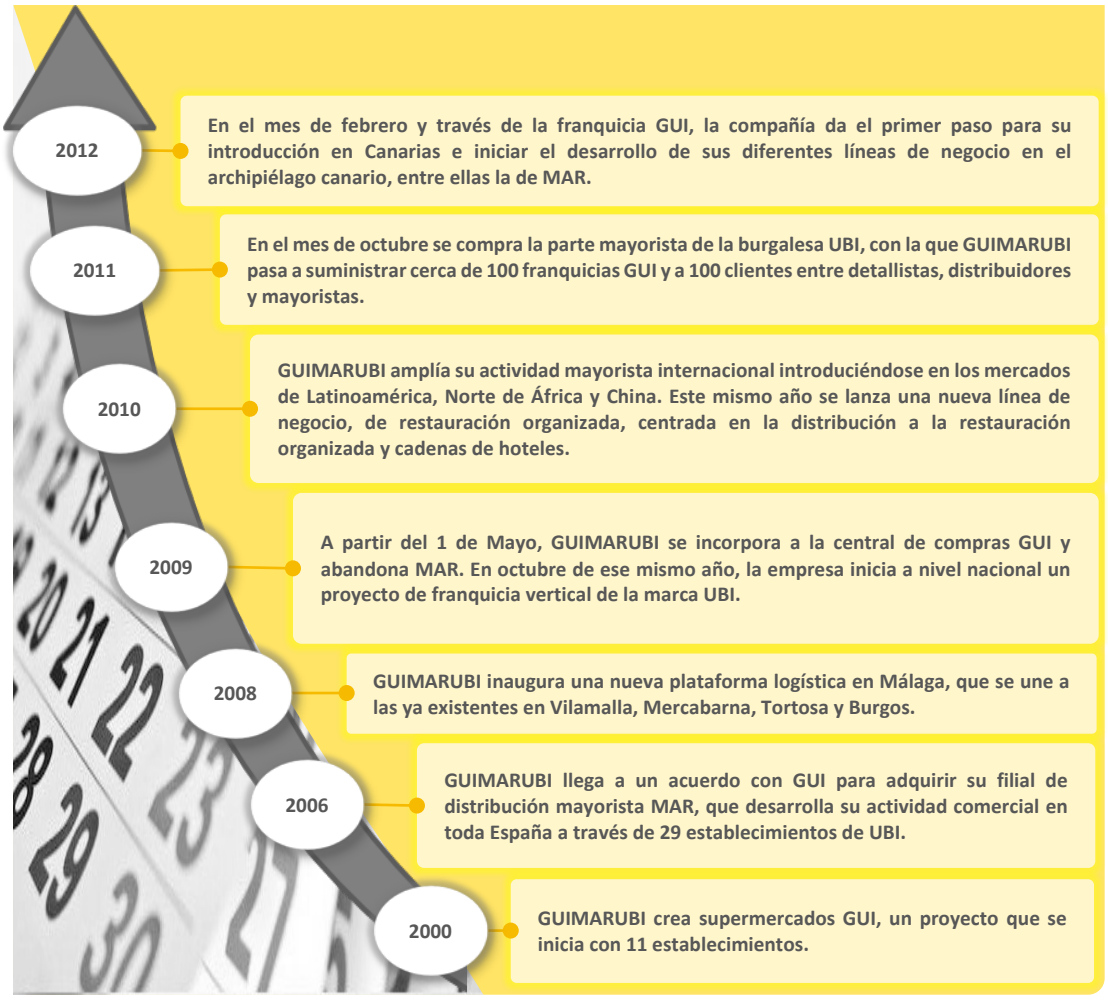


Figura 2: Historia de GUIMARUBI

2.2 Importancia de la Ciberseguridad en el siglo XXI

La seguridad informática o ciberseguridad, se define como el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en un ordenador o circulante a través de las redes de ordenadores. (1). La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse

En el mundo online de hoy en día, cada organización es digital por defecto, con las culturas de trabajo, tecnologías y procesos de la era de internet. Adicionalmente, en el mundo conectado y convergente entregado por IoT, el paisaje digital es amplio, con todos los activos de información utilizados por las organizaciones que representan a otro nodo en la red. Nunca ha sido más difícil para las organizaciones no sólo entender su entorno cibernético, pero también establecer estructuras de gobierno, instituir procesos, desarrollar comportamientos e implementar herramientas adecuadas para protegerse, defenderse y responder a los ataques de seguridad cibernética.

Mantener confianza nunca ha sido más difícil. Las amenazas cibernéticas se han trasladado de ataques a las instituciones a los ataques contra el sistema financiero en general. En respuesta, los reguladores se centran principalmente en los riesgos cibernéticos y el contagio a través de

las empresas y terceros. Los reguladores también esperan que las instituciones financieras mejoren las protecciones contra la privacidad en nombre de los clientes, quienes exigen que su información confidencial se guarde de manera segura.

Hoy en día las organizaciones cuentan cada vez más con las tecnologías adheridas a sus procesos de negocio, y actualmente, en un mayor grado, debido a la irrupción de las tecnologías de carácter móvil y al "*cloud computing*", que dotan a las empresas de una mayor movilidad y escalabilidad, convirtiéndose en un área clave de las mismas, y por consiguiente, la protección de la información que mediante el uso de estos dispositivos se gestiona.

Por todo ello, es muy importante que una empresa esté a la vanguardia de la tecnología, para poder evitar posibles ataques contra ella y que no impacten sobre su negocio, debido a esta razón, es necesario que las empresas dispongan de un Plan Director de Seguridad que permita identificar el estado actual de la seguridad y permita trazar un plan de acción para estar protegido ante las posibles amenazas existentes.

3 Objetivos

El objetivo del presente proyecto se centra en actualizar la infraestructura tecnológica de la empresa GUIMARUBI con el fin de mejorar su seguridad llevando a cabo un análisis de riesgos de la misma para determinar un plan de acción a realizar para mejorar la seguridad. Por ende, por una parte se explicará el objetivo del Plan Director de Seguridad y por otra, el objetivo de realizar un análisis de riesgos.

3.1 Plan Director de Seguridad

El objetivo principal del PDSI es la definición de las directrices de seguridad de la información que deberán ser implantadas en GUIMARUBI conforme a los objetivos de negocio, que permitan mantener un nivel de riesgo adecuado a las necesidades actuales y futuras de la organización. Para conseguir dicho objetivo principal, se deberán cubrir los siguientes aspectos:

- Consolidar la información de proyectos existentes y planificar la ejecución de sus planes de acción. Consolidar e integrar de manera ordenada toda la información de seguridad de la información de proyectos existentes (por ej. PCN, Análisis de Riesgos, PCI-DSS, LOPD, SGSI…) unificando la información relativa a inventarios de activos, diagnósticos/análisis de situación, análisis de riesgos y planes de acción resultantes. Toda esta información se verá alimentada a lo largo de este proyecto con actividades de diagnóstico y análisis.
- Involucrar a la Dirección en la gestión de la seguridad de la información. Establecer los mecanismos necesarios para involucrar a la Dirección y las unidades de negocio en la gestión de la seguridad de acuerdo a una gestión de riesgos adecuada. Para ello se establecerá un Comité Técnico de Seguridad definiendo funciones, responsabilidades y canales de comunicación.
- Realizar un análisis de seguridad cubriendo la estrategia, la organización, los procesos, la tecnología y las personas para identificar las debilidades tanto técnicas como organizativas que puedan resultar en un impacto económico, de imagen o legal para el negocio de GUIMARUBI.
- Identificación y evaluación de los riesgos. Para todos los activos de GUIMARUBI que dan soporte a los procesos de negocio, se identificarán y evaluará los riesgos de seguridad de la información asociados, decidiendo en cada caso la mejor estrategia posible.
- Priorizar la seguridad en la información o recursos críticos de GUIMARUBI garantizando un nivel adecuado de seguridad. Focalizar la seguridad de la información, planificando acciones correctivas y de seguridad, en aquellos activos de información que pueden afectar gravemente las operaciones o la imagen de la compañía. Esta priorización tendrá en cuenta los resultados obtenidos en la evaluación de riesgos.
- Marcar las directrices para garantizar la seguridad en las diferentes ubicaciones geográficas. Definir y planificar las acciones necesarias para garantizar la seguridad de la información en activos de información o recursos (soportes) cuya gestión no se realiza de manera centralizada.
- Analizar la situación de la organización respecto a buenas prácticas internacionalmente reconocidas como la ISO 27001/2:2013 identificando debilidades de seguridad y riesgos.
- Revisar el nivel de cumplimiento en materia de protección de datos de carácter personal Reglamento (UE) 2016/679, evaluando el cumplimiento de las medidas de seguridad requeridas en su reglamento de desarrollo RD 1720/2007.
- Realizar revisiones técnicas de seguridad representativas (interna, *pentest* externo, *wifi* y revisión CPDs y una delegación) que permitan obtener una imagen de los riesgos existentes en la infraestructura, CPDs y delegaciones de GUIMARUBI.

- Revisar el nivel de protección de la organización frente a nuevas amenazas y riesgos innovadores respecto las tendencias del sector de la seguridad como podría ser *Big Data*, APTs, cibercrimen, Seguridad en Servicios Externalizados, Social Media, etc.
- Realizar un análisis de riesgos que esté alineado con las prioridades y un lenguaje del negocio en términos de impacto para las operaciones del negocio. El mapa de riesgos resultante ha de permitir proponer un plan de gestión determinando el nivel de riesgo aceptable para la organización.
- Definir un modelo de seguridad objetivo que incluya tanto un modelo de organización como el estado de seguridad objetivo en base al nivel de riesgo aceptable.
- A partir del nivel de Seguridad actual y el Modelo de Seguridad Objetivo, se determinará el gap existente identificando las iniciativas necesarias para alcanzar el modelo objetivo.
- Priorización de las iniciativas necesarias identificadas en función de un criterio beneficio vs coste, criterio que será expresado en términos de mitigación de riesgos y coste asociado a las medidas planteadas.
- Proveer de un plan de proyectos de seguridad, organizados en *quickwins*, a corto, medio y largo, priorizado en base al coste, esfuerzo y beneficio de la implantación, con suficiente grado de detalle que permita la toma la toma de decisiones para corregir fallos de seguridad y evaluar el riesgo que tendría la no ejecución de los mismos en cuanto a seguridad se refiere.
- Garantizar la implantación y el control del Plan de Acción definido. Definir los mecanismos necesarios para controlar y seguir la adecuada implantación de la seguridad en la compañía.

El Plan Director de Seguridad debe ser la hoja de ruta que lleve desde donde está la compañía hasta dónde quiere llegar. El destino debe estar definido por los objetivos de seguridad que dimanan, a su vez, de los objetivos de negocio.

Un Plan Director de Seguridad se basa principalmente en un análisis de riesgo, el cual deriva en un plan de necesidades. Dicho análisis de riesgos es la base para poder identificar las acciones o proyectos que se deberán llevar a cabo.

3.2 Análisis de Riesgos

Un análisis de riesgos es el proceso de identificar los riesgos de la seguridad, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda o controles para poder reducir el riesgo existente hasta un nivel que sea aceptable para la compañía.

El análisis de riesgos intenta que los criterios en los que se apoya la seguridad sean más objetivos

- Introduce un grado importante de objetividad.
- Permite a la organización gestionar los riesgos por sí mismos.
- Apoyar la toma de decisiones basándose en los riesgos propios.
- Centrarse en proteger activos importantes.
- Formar y comunicar los aspectos de seguridad necesarios.

A partir del análisis y evaluación de riesgos la empresa conocerá los riesgos que afectan a sus sistemas de información, permitiendo adoptar medidas y técnicas que los prevengan, impidan o controlen.

Por otra parte, permitirá auditar el grado de seguridad del sistema y adaptar los mecanismos de control según avancen las técnicas o se descubran nuevos riesgos.

El objetivo de un análisis de riesgos es saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabildades para,

posteriormente, reducir el riesgo existente hasta un nivel que sea aceptable para la Organización. Los principales motivos que llevan a su elaboración son los siguientes:

- Identificar riesgos de la seguridad de la información que podrían impedir a la organización lograr sus objetivos.
- Selección de salvaguardas en función del riesgo detectado.
- Diseño, implantación, y certificación de un SGSI basado en la Norma ISO 27001:2013.
- Creación de Planes de Contingencia en previsión de las amenazas detectadas.
- Creación de un Plan Director.
- Conocimiento de los costes derivados de la falta de control de riesgo.

4 Fundamentos teóricos de un AARR

Un Análisis de Riesgos es un procedimiento de ayuda a la decisión. Sus resultados constituyen una guía para que la organización pueda tomar decisiones sobre si es necesario implantar nuevos mecanismos de seguridad y qué controles o procesos de seguridad serán los más adecuados.

Una vez conocidos los riesgos, la organización puede decidir qué medidas tomar dependiendo de una serie de factores (costes de la implantación de controles que reduzcan los riesgos vs. costes derivados de las consecuencias de la materialización de estos riesgos):

1. Mitigar el riesgo, mediante la implantación y mantenimiento de controles de seguridad que minimicen estos riesgos y los mantengan a un nivel aceptable (lo cual implica inversiones económicas)
2. Asumir ciertos riesgos a los que está expuesta la organización ya que las consecuencias acarrean un coste económico y estratégico menor que el coste que sería necesario aportar para reducir dichos riesgos
3. Transferir estos riesgos, bien a un prestador de servicios especializado mediante un SLA o bien mediante la contratación de una póliza de riesgo electrónico.
4. Eliminar o evitar los riesgos, modificando características básicas del activo.

4.1 Definiciones

- **Activo**: Recurso, proceso, producto, infraestructura informática o cualquier "cosa" que la Organización ha establecido que debe protegerse. El valor de un activo está asociado a los siguientes elementos de un activo: creación, desarrollo, soporte, reposición, credibilidad, costes asociados y valor de propiedad. Ejemplos de activos:
  - Información y datos
  - Hardware
  - Software
  - Servicios
  - Documentos
  - Personal
  - Edificios
  - Inventario
  - Tesorería
  - Imagen / Reputación
- **Amenaza**: La ocurrencia de cualquier evento que causa un impacto no deseable sobre la Organización. Ejemplos de amenazas:
  - Errores
  - Daño intencional / ataque
  - Fraude
  - Robo
  - Falla de equipo / software
  - Desastres naturales
- **Vulnerabilidad**: La ausencia o debilidad del control. Ejemplos de vulnerabilidades:
  - Falta de conocimientos del usuario
  - Falta de funcionalidad de la seguridad
  - Elección deficiente de contraseñas
  - Tecnología no probada
  - Transmisión por comunicaciones no protegidas

- **Control, salvaguarda o contramedida**: Mecanismo que se emplea con el fin de reducir el riesgo asociado a una o varias amenazas. Hay diferentes tipos de controles:
    - Preventivos:
        - Política de seguridad
        - Formación del usuario
        - Controles de acceso
        - Cortafuegos
        - Segregación de funciones
    - Detectivos:
        - Registro de *logs*, sistemas de auditoría
        - IDS
    - Correctivos:
        - Copias de respaldo (*back-ups*)
        - Plan de contingencias y continuidad de negocio
- **Impacto**: Consecuencia de la materialización de una amenaza sobre un activo. Ejemplos de impactos:
    - Pérdidas económicas
    - Pérdida de oportunidades de negocio
    - Pérdida de imagen de la empresa / reputación
    - Pérdida de eficiencia
    - Pérdida de vidas humanas
    - Sanción por violación de la legislación
    - Interrupción de la actividad de la empresa
- **Riesgo**: Posibilidad de daño o pérdida.
- **Riesgo inherente**: Riesgo existente en el activo, por el simple hecho de existir, y pertenecer a una determinada categoría.
- **Riesgo intrínseco**: Es la posibilidad de que se produzca un impacto determinado en un activo o en un grupo de activos.
- **Riesgo global**: Impacto x probabilidad.
- **Riesgo residual**: Riesgo que queda tras la aplicación de salvaguardas o una vez que los controles han sido aplicados.
- **Evaluación del riesgo**: Es el proceso de comparar el riesgo estimado contra un criterio de riesgos para determinar su importancia relativa y detectar áreas de mejora.
- **Tratamiento del riesgo**: Es el proceso de selección e implantación de medidas para modificar el nivel de riesgo. Es el proceso de definir un plan de gestión de seguridad basado en la evaluación del riesgo.
- **Gestión de riesgos**: Es el proceso global de identificar, controlar y eliminar o minimizar determinados eventos que pueden afectar a los sistemas de información.

Figura 3: Definición visual de riesgos, amenazas y controles.

4.2 Relaciones existentes

Los anteriores conceptos teóricos están relacionados entre sí, tal y como se puede observar en la siguiente figura:

Figura 4: Relación de los conceptos teóricos de un AARR.

El mapa conceptual de un análisis de riesgos quedaría de la siguiente manera:

Figura 5: Mapa conceptual de un AARR.

4.3 Tipos de análisis de riesgos

1. **Análisis de riesgos cuantitativos**: Pretenden asignar de forma objetiva un valor numérico (ej. coste monetario) a los componentes del análisis de riesgos y a las pérdidas potenciales. Cuando todos los elementos (valor de los activos, impacto, probabilidad de amenaza, efectividad de contramedidas, coste de contramedidas, incertidumbre y probabilidad) son cuantificados, el proceso se considera totalmente cuantitativo. No es posible realizar un enfoque puramente cuantitativo, puesto que las medidas cuantitativas deben ser aplicadas a elementos cualitativos.
2. **Análisis de riesgos cualitativos**: Pretenden asignar de forma objetiva un valor cualitativo (ej. alto-medio-bajo) a los componentes del análisis de riesgos y a las pérdidas potenciales. Nos sirve para poder comparar los valores asignados a los activos. No es posible realizar un enfoque puramente cualitativo, puesto que siempre hay que medir y es difícil hacerlo sin enfoque cuantitativo.
3. **Análisis de riesgos semi-cuantitativo**: Pretenden asignar de forma objetiva un valor cualitativo (ej. 0-1-2-…8-9-10) a los componentes del análisis de riesgos y a las pérdidas potenciales. Nos sirve para poder comparar los valores asignados a los activos y es el más utilizado.
4. **Análisis de riesgos automatizados**: El objetivo de estos es minimizar el esfuerzo manual necesario para realizar el análisis de riesgos. Para ello, previamente ha de crearse una base de datos. Las ventajas son las siguientes:
    - Se pueden ejecutar varios análisis con diferentes parámetros (¿qué pasa si...?)
    - Los cálculos se procesan rápidamente
    - Estimación de pérdidas potenciales esperadas
    - Determinar el beneficio de medidas de seguridad implantadas

4.4 Gestión de riesgos

Para poder controlar y gestionar el riesgo, el primer paso es evaluar si el riesgo requiere medidas para su tratamiento o no, es decir, si el nivel de riesgo es aceptable, y por tanto únicamente se vigilarán las condiciones para mantener el nivel obtenido, o no, en cuyo caso se seleccionarán e implantarán las correspondientes medidas de seguridad. Para ello, es necesario evaluar los resultados del riesgo efectivo (valor medio) obtenido en el Análisis de Riesgos.

El Nivel de Riesgo Aceptable resulta del equilibrio entre:

- **El coste de seguridad** (coste de las medidas de medidas de seguridad)
- **El coste del riesgo** (coste que tendría si el riesgo se hiciera realidad):
  - La degradación existente en caso de desastre
  - La frecuencia de suceso de la amenaza

A partir de los resultados de la evaluación de riesgos y teniendo en cuenta el nivel de riesgo aceptable establecido, el Comité de Seguridad de la organización (o el responsable en su defecto si no existe un Comité) decide qué tratamiento va a dar a los riesgos no aceptables, que puede ser:

- **Reducir el riesgo** (reducir amenazas, vulnerabilidades, posibles impactos, etc.) implantando los controles apropiados.
- **Asumir el riesgo** (no es necesario tratarlos).
- **Evitar el riesgo** (eliminar el uso del activo involucrado, servicio, proceso o fuente de amenaza).
- **Transferir el riesgo a terceros** (póliza de seguro que cubra el nivel de riesgo no aceptable o subcontratar servicio / proceso, etc.).

El riesgo se asumirá si:

- Está por debajo del Nivel de Riesgo Aceptable.
- El impacto es despreciable.
- El coste de las salvaguardas es desproporcionado en comparación al impacto y riesgo a mitigar.

Sobre los riesgos que se ha decidido reducir, el Responsable de Seguridad junto con el responsable del proceso / activo correspondiente, establece aquellos controles o salvaguardas que protejan efectivamente contra los riesgos detectados y no aceptados.

Dichos controles pueden surgir de:

- Norma ISO/IEC 27002:2005
- Magerit v3.0
- Cualquier otro que considere el personal implicado.

Además de que es necesario que haya un equilibrio entre:

- Controles organizativos (seguridad física, personas, administrativa, etc.).
- Controles Técnicos (configuración, testeo, etc.).
- Controles de Infraestructura (hardware, software, comunicaciones etc.).

Adicionalmente, se tendrán en cuenta los requisitos asociados al activo sobre tres aspectos:

1. Requisitos de negocio (cumplimiento de política y normas de seguridad, cumplimiento de estándares del sector, coordinación de actividades de seguridad, etc.).
2. Requisitos del resultado del análisis de riesgo (fallos de seguridad, incidentes y fallos, mal uso, cambios no autorizados, etc.).
3. Requisitos legales, reglamentarios y contractuales.

Tras conocer los requerimientos de seguridad, el responsable del proceso está en disposición de identificar y seleccionar los controles de seguridad a aplicar, los cuales podrán ser:

- Controles **implantados**, en los que se valorará el grado de madurez con respecto al riesgo a mitigar
- Controles **nuevos** que afectan al riesgo y que no están implantados

Una vez seleccionados los controles, para comprobar que el control es efectivo, es necesario aplicar el grado de cumplimiento o efectividad requerido y volver a calcular el riesgo efectivo para comprobar que el nivel obtenido es aceptable.

- Si resulta satisfactorio, se aceptará el control.
- Si no lo es, se volverá a analizar la situación hasta dar con los controles necesarios que mitiguen el riesgo hasta los niveles aceptables para la organización.

Es importante reseñar que un mismo control puede afectar a varios riesgos, por lo que al probarlo, se debe hacer teniendo en cuenta todos los escenarios en los que participa.

Una vez seleccionados los controles y el estado requerido para reducir el riesgo hasta nivel aceptable, el Responsable de Seguridad con el apoyo del personal implicado en los procesos, confeccionan el Plan de Gestión del Riesgo en el cual:

1. Planifican la implantación de los controles establecidos.
2. Identifican los indicadores o parámetros que informen sobre el la eficacia del control implantado.
3. Definen los responsables de realizar el seguimiento y medición de los controles establecidos.
4. Establecen los criterios de aceptación/rechazo y las acciones a emprender si los resultados no son satisfactorios.
5. Realiza una evaluación periódica del cumplimiento de la legislación, reglamentación y otros requisitos suscritos.
6. Verifican que los controles funcionan y que están siendo utilizados de la forma prevista.

Por tanto, en el Plan de Gestión del Riesgo se contemplan los siguientes datos:

- Acción Correctiva (número, descripción y tipo: organizativo, técnico o infraestructura)
- Control/es relacionado/s para reducir el riesgo.
- Prioridad (alta, media o baja).
- Inversión.
- Fecha estimada de inicio y fin de la implantación de la acción correctiva.
- Responsable de su realización (interno u organismo externo, si está contratado).
- Nivel requerido, teniendo en cuenta los requerimientos de negocio, de reducción del riesgo y requisitos legales u otros requisitos, que deben cumplirse.

El Responsable de Seguridad es la función encargada de la modificación del Plan de Gestión del Riesgo, que deberá realizar siempre que haya cambios respecto a:

- Las condiciones en las que se desarrollan los procesos objeto de alcance del SGSI.
- Análisis de riesgos que justifiquen cambios en las salvaguardas implantadas.
- Los criterios de análisis de riesgos.
- Requisitos legales u otros requisitos aplicables.

En dicho caso, el Responsable de Seguridad las modificaciones introducidas y un nuevo "Plan de Gestión del riesgo".

Adicionalmente al Plan de Gestión de Riesgo, el Responsable de Seguridad define un Plan de Seguimiento y Medición de los controles para asegurar los controles son implantados y los

controles reducen los riesgos a los niveles establecidos como aceptables (efectividad requerida) o realizar las acciones oportunas en caso de no ser así.

Dicho Plan contiene la siguiente información:

- Indicadores para medir la eficacia del control implantado.
- Periodicidad de medición.
- Efectividad requerida.
- Responsable de medición.
- Resultado de las mediciones (fecha y resultado: conforme o no conforme).

5 Alcance del proyecto

Para realizar el Análisis de Situación Actual del PDSI se realizarán un conjunto de evaluaciones técnicas de seguridad, teniendo en cuenta los resultados de los trabajos de revisión de seguridad técnica. Para determinar el alcance de las auditorias técnicas de seguridad quedan incluidos en el proyecto los siguientes puntos:

- Análisis detallado de los resultados de los trabajos de revisión técnica de seguridad realizados en los diferentes ámbitos (externas, internas, aplicaciones, comunicaciones, etc.).
- Identificación de auditorías técnicas de seguridad y las tendencias de amenazas y riesgos actuales.
- Priorización de las diferentes auditorias técnicas identificadas de acuerdo al riesgo que resultan para GUIMARUBI así como de acuerdo a las prioridades de la organización.
- Realización durante el Plan Director de las auditorias consideradas prioritarias o críticas de manera alineada a los esfuerzos y dedicaciones contratadas.
- Diseño de un Plan de Auditorías de Seguridad considerando el listado de auditorías.
- Revisión y asesoramiento en el proceso de auditoría de GUIMARUBI.

Respecto a las aplicaciones, de forma particular en los entornos SAP:

- Se detectarán las debilidades existentes en temas de seguridad, tanto en las vías de cómo acceden a los sistemas los diferentes usuarios, como en los perfiles, roles y permisos que tienes asignados éstos.
- Se realizará el análisis para implementar a futuro una correcta segregación de funciones en los sistemas de la información que permita a la compañía reducir el riesgo de fraude, intencionado o no, o un uso fraudulento de sus operaciones de negocio.

Por último, se contempla la realización de actividades en el ámbito del "*hacking* ético"; concretamente:

- Test de intrusión interno (4 clases C[1]).
- Test de intrusión externo (1 clase C).

El proyecto se focalizará en los activos de información de GUIMARUBI, incluyendo todos aquellos sistemas de negocio propios de GUIMARUBI: SAP R/3, SAP BI, SISLOG (SGA),…etc.

En los entornos SAP, al ser los productos de mayor relevancia y donde más usuarios acceden, se requiere evaluar el grado de seguridad y de segregación de tareas en base al puesto de trabajo.

[1] Una IP de clase C es una dirección utilizada para identificar un dispositivo dentro de una red privada. Las direcciones IP abarcan desde 192.0.0.0 hasta 223.255.255.255, , dejando 21 bits para la dirección de red real.

6 Marcos de referencia y metodologías

Existen diversas metodologías para realizar un análisis de riesgos, de las cuales, las más estandarizadas y reconocidas se exponen seguidamente, junto con los marcos de referencia para realizar un análisis de riesgos.

6.1 SGSI y Familia ISO 27.000

Un SGSI, según la concepción que establece la Norma ISO/IEC 27.001:2013 (2), siendo ésta extrapolable a otros marcos de gobierno de TI, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información, ello significa que se va a dejar de operar de una manera intuitiva, y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización, lo cual, permitirá conocer mejor la organización, cómo funciona ésta y qué se puede hacer para que la situación mejore.

La norma específica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos, es decir, tanto la documentación de soporte como las tareas que se realizan, de esta manera, se puede afirmar que los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, aspecto que no sucedería si se confía en un traspaso de información verbal informal.

Según la ISO, la normalización es la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado, que puede ser tecnológico, político o económico, con lo que se hace necesario adoptar, unos marcos de gobierno como los que venimos exponiendo, en este caso en el ámbito tecnológico, tales como la ISO/IEC 27.000, que será la examinada en el presente apartado.

Con lo cual, un buen Gobierno de TI, debe de apoyarse en este marco de estándares y normas de cumplimiento, que aunque en algunos casos no sea necesaria su adopción, siempre es preceptiva, con el objetivo de garantizar que todas las tecnologías que gestiona una organización, estén orientadas hacia la consecución de sus objetivos de negocio, así como que estén ajustadas a los requerimientos individuales que se susciten, para aunar los esfuerzos hacia la consolidación de unas mejores prácticas en el ámbito implicado.

De tal manera, se encuentran una multitud de estándares que están interrelacionados con el concepto de gobierno de TI, y la implementación que se realiza de las nuevas tecnologías y la seguridad de la información que se viene estableciendo, es por ello que deviene tarea imposible citarlos individualmente, con lo cual, se expondrán a continuación, aquellos considerados como más relevantes:

- **ITIL**; es un marco de trabajo publicado por la OGC del Reino Unido, basado en mejores prácticas TI para el gobierno tecnológico de las organizaciones, integrándolas de acuerdo con los objetivos de negocio que éstas ostenten, adoptando un punto de vista estratégico en el ámbito de la gestión de servicios TI.

- **ISO/IEC 27.000**; es un marco de trabajo publicado por y por IEC, derivado de la norma BS 7799 del gobierno británico, que proporciona un marco de gestión de la seguridad

de la información, utilizable por cualquier tipo de organización, independientemente de su tamaño y naturaleza.

Siguiendo con lo hasta ahora expuesto, cabe mencionar que existen marcos de trabajo que tratan de una manera específica, determinados aspectos relacionados con el gobierno de las TI, entre los que cabe destacar:

- **Val IT**; se trata de gestionar un portfolio de iniciativas orientadas en el campo de las nuevas tecnologías, que permita generar valor en la organización y controlar la inversión destinada.

- ***Risk IT***; se trata de gestionar un marco de trabajo orientando a identificar y gestionar los riesgos que están relacionados con las organizaciones, respecto del uso que se hace en ellas de las nuevas tecnologías.

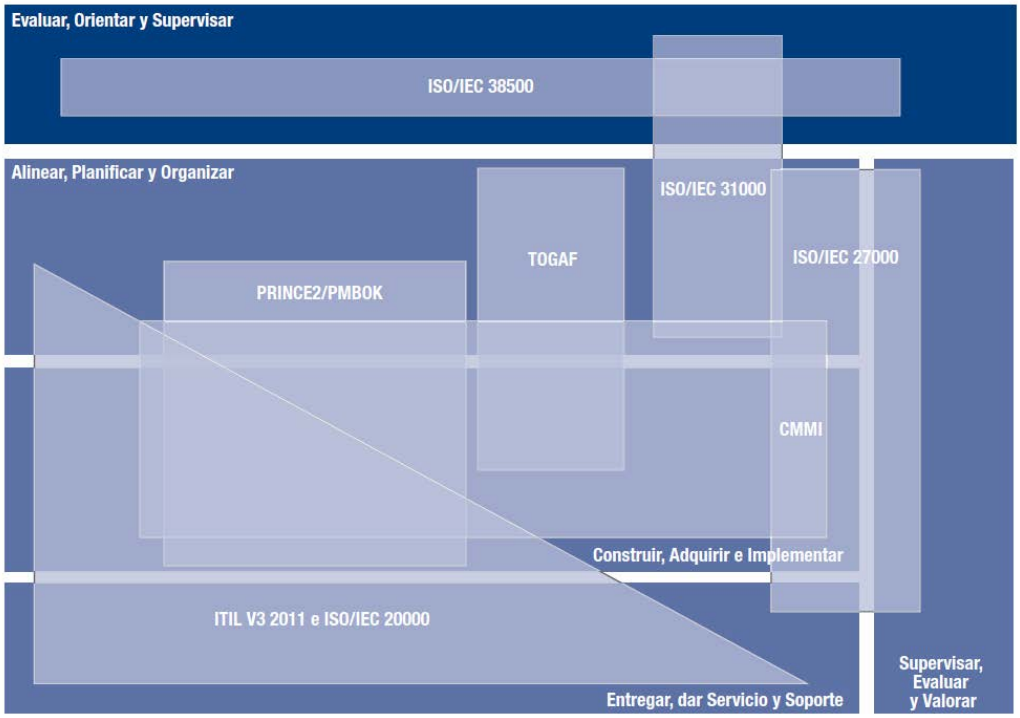


Figura 6: Mapa conceptual que diversifica el campo de actuación de los principales estándares y marcos de trabajo TI, dentro de los procesos que forman el marco de gobierno de COBIT 5 (Fuente: ISACA, 2012)

Se puede definir como un conjunto de marcos de trabajo desarrollados por ISO e IEC, que proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de organización, independientemente de su tamaño o naturaleza jurídica, dentro de los más importantes de esta serie, encontramos: ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006, entre otras.

Para el propósito de este trabajo, se toman como enfoque de análisis de la serie ISO 27000, en concreto, las normas ISO 27001 e ISO 27002, por un lado, la norma ISO 27001, la cual tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI), sustituyendo a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

Figura 7: Eje temporal que muestra la evolución de la Norma ISO 27000. (Fuente: http://www.ISO27000.es)

Esta norma abarca todo tipo de organizaciones, tal y como anteriormente se ha comentado, debido a que ha sido elaborada con el fin de proporcionar a éstas, un modelo que permita operar mediante la implementación de un SGSI, este enfoque basado en procesos enunciado en parágrafos anteriores, estimula a los usuarios a hacer énfasis en[2]:

- Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información.
- Implementar y operar controles para mejorar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización.
- El seguimiento y revisión del desempeño y eficacia del SGSI.
- La mejora continua basada en la medición de objetivos.

Por el otro lado, está el estándar ISO/IEC 27002:2013 (3), renombrada ISO/IEC 17799:2005 desde el 1 de julio de 2007, está considerada como una código guía de buenas prácticas comúnmente aceptadas, donde se describen las finalidades de control recomendables para desarrollar y mantener las normas necesarias de seguridad y gestión de la información, en una determinada organización, ayudando a los responsables que deseen implantarla, para dotarla de rigor y confianza en la materia.

La fuente histórica para el estándar fue BS 7799-1, cuyas partes esenciales fueron tomadas en el desarrollo de la Norma ISO/IEC 17799:2005, anteriormente mencionada, bajo la rúbrica; Tecnología de la Información - Código de Prácticas para la Gestión de Seguridad de la Información, dicho estándar fue desarrollado y publicado por la BSI, denominado como BS 7799-1:1999.

No obstante, la norma ha sido revisada desde todos los ángulos a fecha de octubre de 2013 (ISO/IEC 27002:2013), y define 114 controles de seguridad, repartidos en 35 categorías de seguridad, que a su vez, están organizados bajo 14 dominios o capítulos de seguridad, que se pueden enumerar de la manera siguiente:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. La seguridad ligada a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.

[2] Basado en la Norma ISO/IEC 27.001:2013. Sistema de Gestión de la Seguridad de la Información. AENOR 2014.

7. La seguridad física y del entorno.
8. Seguridad en las operaciones.
9. Seguridad en las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas de información.
11. Las relaciones con los proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14. Cumplimiento.

Una vez alcanzado este punto, cabe reseñar el funcionamiento básico que esboza la norma que se pretende analizar, no siendo otra que la serie ISO/IEC 27002:2013, la cual contiene varias categorías de seguridad, que engloban los objetivos de control que se pretenden consolidar, así como los controles que se deben de llevar a cabo para consolidar las finalidades de control previstas, no obstante, estos controles conllevan aparejada una breve descripción, que pretenderá guiar al responsable de adopción del estándar de la organización en su implementación, es por ello, que se detalla de una manera intrínseca, las actividades que se deben de llevar a cabo para la consecución del fin previsto.

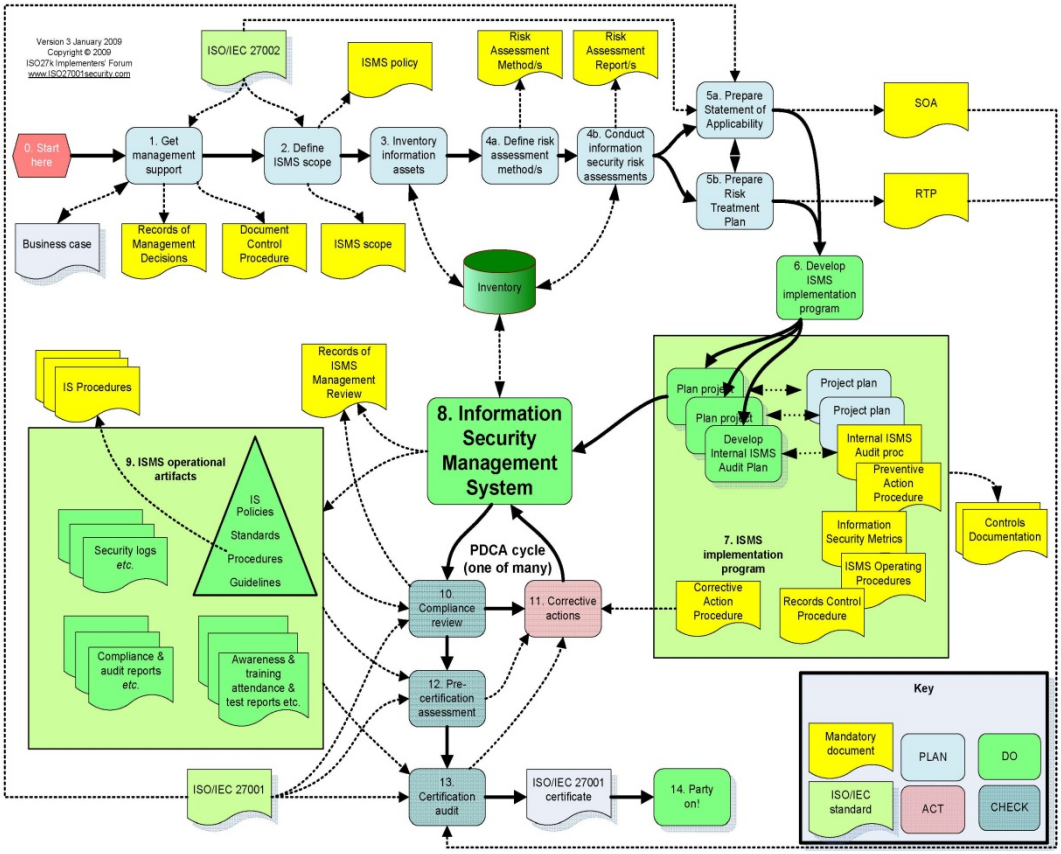


Figura 8: Mapa conceptual que esboza el proceso de implementación de la certificación ISO/IEC 27002:2013. (Fuente: Fuente: http://www.ISO27000.es)

6.2 OCTAVE

El método OCTAVE (4) fue encargado por el CERT a la universidad de *Carnegie Mellon* (SEI). Se liberó en 2Q02 y desde entonces se han producido varias revisiones.

Su objetivo es permitir a las organizaciones:

1. Gestionar por sí mismos los análisis de riesgos de seguridad de la información.
2. Tomar las mejores decisiones posibles basándose en la situación real de sus propios riesgos.
3. Centrar los objetivos de seguridad en proteger los activos más relevantes.
4. Comunicar de forma efectiva la información relativa a seguridad de la información.

Algunos aspectos importantes de OCTAVE:

- Garantizar la continuidad de negocio
- Definir amenazas y riesgos en función de los activos más críticos
- Gestión de riesgos y estrategias de protección basada en la realidad de la organización
- Metodología de la recolección de datos
- Orientada a toda la organización

Los enfoques actuales en GRSI suelen ser incompletos por las siguientes razones:

1. Muchas organizaciones crean estrategias de protección empezando por analizar las vulnerabilidades de la infraestructura técnica. Esto entorpece el desarrollo de acciones eficaces por dos motivos:
    i. Es difícil cualificar la información importante
    ii. Se crean divergencias en los requerimientos de seguridad de los departamentos de negocio (y operativos) y el área de TI.

2. Fruto de una mala comunicación entre negocio y sistemas, en materia de seguridad, las organizaciones pueden estar asumiendo, sin ser plenamente conscientes de ello, un alto nivel de riesgo con relación a la protección de sus activos de información. En esta situación, es frecuente que no quede claro si la información importante se protege adecuadamente o si los recursos destinados a seguridad se dedican a proteger información de importancia relativa o menor.

3. Además, muchas organizaciones delegan la evaluación de riesgos en seguridad de la información en terceros, lo cual puede tener serias contrapartidas:
    - Las organizaciones no tienen forma de saber si la evaluación del riesgo es adecuada o no.
    - Para los expertos externos es muy difícil, si no imposible, asumir las perspectivas de la organización.
    - Después de la evaluación, los expertos se van. Lo que debería ser una gestión continua se convierte en auditorias puntuales.

Las ventajas de utilizar OCTAVE, frente a otros métodos conocidos (como es el caso de MAGERIT en el sector público español) son principalmente las siguientes:

1. **Es un método operativo, orientado a resultados**: Después de la primera iteración (2-3 meses) se obtiene un plan a corto y un plan estratégico, para mitigar los riesgos detectados. En la siguiente iteración (después de 6 meses o un año) se parte de los resultados de la implantación de las acciones anteriores.

2. **Se dirige desde el negocio a los sistemas y no al revés**, proponiendo un equipo de trabajo mixto entre usuarios de negocio y personal técnico. El conocimiento sobre los riesgos lo tienen los usuarios del negocio y las vulnerabilidades se miden y se cubren desde los sistemas.
3. **Propone una metodología muy bien detallada**, con unos pasos muy claros y definidos, proporcionando el suficiente material de soporte (plantillas, ejemplos, etc.), y asumiendo todas las buenas prácticas de las normas y estándares actuales.
4. **Las empresas pueden asumir las actividades de seguimiento con autonomía**, después de un soporte en la primera iteración.

El objeto de un proyecto de este tipo es el desarrollo de una metodología propia que permita realizar una gestión de riesgo continua y controlada de sus activos. Dentro de las metodologías existentes se suele adoptar OCTAVE por los siguientes motivos:

i. OCTAVE es una metodología que incluye elementos tecnológicos y de negocio.

ii. OCTAVE permite la relación de alto nivel entre áreas funcionales heterogéneas.

iii. OCTAVE tiene la capacidad de incorporar catálogos de amenazas y salvaguardas.

La adaptación requiere de los siguientes pasos:

1. **Activos**: Los activos relevantes son los procesos, a alto y bajo nivel y la información.

2. **Requerimientos**: Las fuentes de requerimientos son la legislación aplicable, pudiendo variar en función del país y la jurisdicción y la política de seguridad corporativa. Se aplicará también elementos de buenas prácticas en la gestión de riesgos.

3. **Amenazas y Salvaguardas**: El catálogo de Amenazas y Salvaguardas tomará como base de riesgos y salvaguardas el "*IT Baseline Protection Manual*" y los controles adicionales de ISO-27002.

4. **Estrategia e Implantación**: Finalmente se considerarán las estrategias empleadas por la entidad para gestionar los riesgos y proporcionar los elementos necesarios para la toma de decisiones incluyendo la gravedad del riesgo y el retorno esperado de la inversión de seguridad.

El método OCTAVE define los componentes esenciales para una gestión del riesgo en la seguridad de la información integral, sistemática, contextual y autónoma. Siguiendo el método OCTAVE, cualquier organización podrá tomar decisiones sobre la protección de la información sobre la base de los riesgos en la confidencialidad, integridad y disponibilidad de los activos de información críticos. Durante todo el proceso, las unidades operativas o de negocio y el área de TI trabajan conjuntamente para descubrir los requerimientos de seguridad.

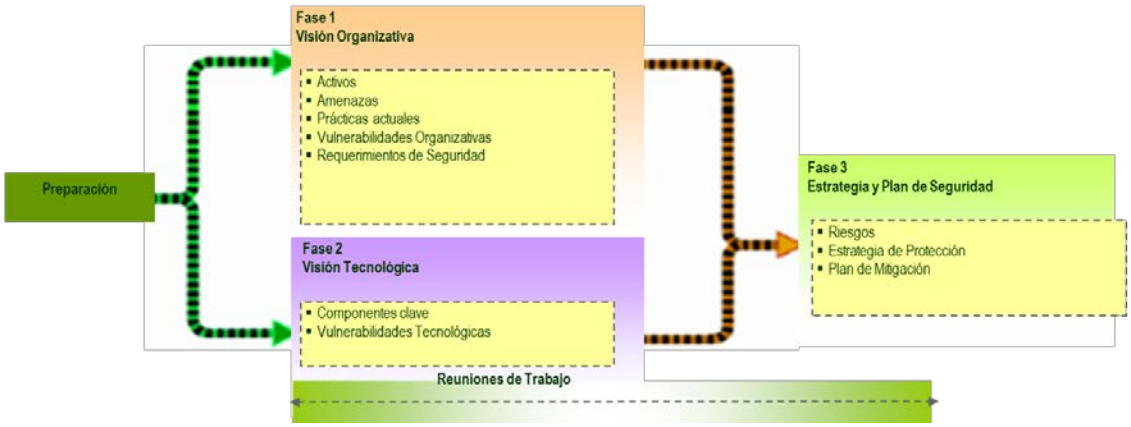


Figura 9: Fases de la metodología OCTAVE

A través de tres fases, similares a las fases de cualquier proyecto de IT, el método OCTAVE propone un análisis tecnológico y organizativo para integrar las necesidades de seguridad de la organización:

- **Fase 1: Aspectos Organizativos / Construcción de los Patrones de Amenaza**. Evaluación de la organización. Se examinan las áreas clave de experiencia en la organización para recabar el conocimiento relevante sobre los activos de información: las amenazas a las que están sometidos, los requerimientos de seguridad, las prácticas de protección actuales de la organización (estrategia actual en prácticas de protección), y las debilidades en las políticas y prácticas organizativas (vulnerabilidades organizativas). Hay que lograr las distintas visiones que la organización tiene de activos críticos, amenazas, áreas a estudiar, requerimientos de seguridad, procesos, vulnerabilidades organizativas, etc. Para obtener el punto de vista de:
  - Dirección
  - Operaciones
  - Personal en general

  Con esta información se elaboran los perfiles de riesgos de la organización.
  Se consideran como activos:
  - Información
  - Sistemas
  - Software
  - Hardware
  - Personas

  Hay que elaborar los perfiles de amenazas para cada escenario:
  - Activo
  - Tipo de acceso
  - Actor / origen
  - Motivación
  - Resultado
- **Fase 2: Aspectos Tecnológicos / Identificación de las Vulnerabilidades de Infraestructura.** Evaluación de la infraestructura de la información. Se examinan las debilidades (vulnerabilidades tecnológicas) de los componentes clave de la infraestructura técnica, que pueden desencadenar acciones no autorizadas. Es necesario identificar los componentes técnicos o tecnológicos críticos para los procesos de negocio, se evalúan estos componentes técnicos para identificar sus vulnerabilidades

y, tras la identificación de los componentes tecnológicos a evaluar, hay que seleccionar las herramientas a utilizar (*scanners* de SO., *scanners* de red, *checklists*…).

- **Fase 3: Desarrollo de la Estrategia y Plan de Seguridad.** En esta fase se analizan los riesgos. Se analiza la información generada en la evaluación de la organización y de la infraestructura técnica (fases 1 y 2) para identificar los riesgos para la organización y para evaluar los riesgos basados en su impacto para los objetivos de la organización. Adicionalmente, se desarrolla la estrategia de protección y el plan de mitigación para los riesgos de mayor prioridad. En esta fase se llevan a cabo los siguientes puntos:
  - Desarrollar el análisis de riesgos para los activos críticos.
  - Evaluar el impacto y la probabilidad de cada escenario identificado en términos de Alto / Medio / Bajo.

  Se consideran los siguientes tipos de impacto a evaluar:
  - Imagen / Confianza de los clientes
  - Salud o vidas humanas
  - Legal o regulatorio
  - Financiero
  - Otros

  A partir de esta información hay que determinar que escenarios producen pérdidas bajas, medias o elevadas para la organización. Adicionalmente, en esta fase se genera un plan para los diferentes ámbitos expuestos:
  - Formación y concienciación
  - Estrategia general de seguridad
  - Gestión de seguridad
  - Políticas y procedimientos de seguridad
  - Soporte de la dirección
  - Plan de continuidad / contingencias / recuperación de desastres
  - Seguridad física
  - Seguridad de IT
  - Seguridad de la plantilla en general

De esta manera, los entregables del análisis de riesgos siguiendo ésta metodología quedarían de la siguiente manera:

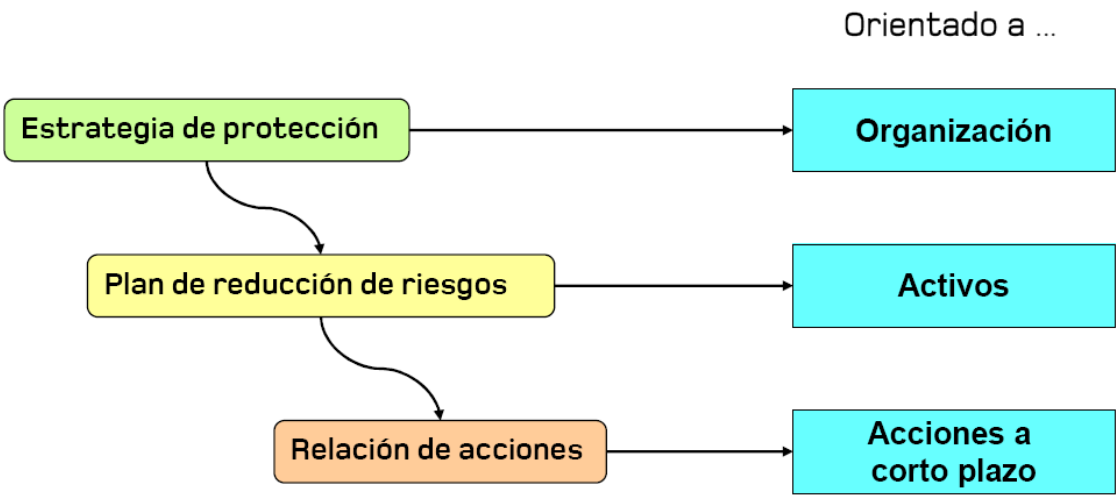


Figura 10: Entregables de la tercera Fase de OCTAVE

6.3 Magerit v3

Es una metodología de Análisis y Gestión de Riesgos de los sistemas de información desarrollada por el Ministerio de Administraciones Públicas Español. Permite profundizar en el análisis hasta el grado necesario y realizar una valoración estimada. Está basada en el estándar internacional: ITSEC.

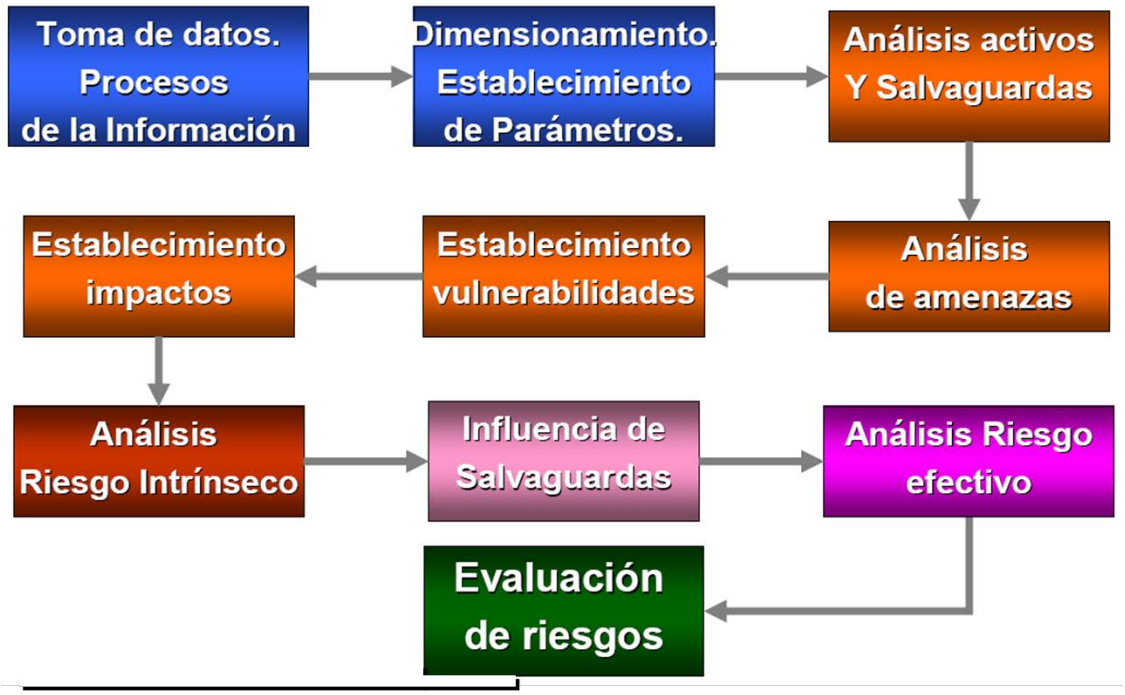


Figura 11: Fases de la metodología Magerit v3

Existen 9 fases para realizar un análisis de riesgos MAGERIT (5) (6) (7):

1. **Identificación de activos:** El primer paso para realizar un análisis de riesgos completo es identificar todos los activos de la organización implicados en el alcance del SGSI. Para garantizar que todos los activos son tenidos en cuenta, se clasifican en las siguientes categorías:
    - La Información que maneja el sistema. MAGERIT lo considera el activo esencial.
    - Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
    - Las aplicaciones informáticas (*software*) que permiten manejar los datos.
    - Los equipos informáticos (*hardware*) y que permiten hospedar datos, aplicaciones y servicios.
    - Los soportes de información que son dispositivos de almacenamiento de datos.
    - Las redes y equipos de comunicaciones que permiten intercambiar datos.
    - Las instalaciones que acogen equipos informáticos y de comunicaciones.
    - Las personas que explotan u operan todos los elementos anteriormente citados.

    A partir de dicha clasificación, el Responsable de Seguridad junto con los propietarios de los activos, identifica los siguientes datos:
    - Activo
    - Área de negocio involucrada
    - Responsable o propietario del activo
    - Descripción breve del activo
    - Plataforma tecnológica que soporta el activo

2. **Valoración de activos:** Una vez identificados los activos, los responsables los valoran para conocer su criticidad. Dicha valoración se realiza en base a sus requerimientos de seguridad de negocio. Los requerimientos de seguridad se engloban bajo las siguientes dimensiones de valoración:
    - Confidencialidad: Característica que asegura que sólo quienes estén autorizados pueden acceder a la información.
    - Integridad: Característica que asegura que la información no es alterada de forma incontrolada. Garantiza la exactitud y completitud de la información y los métodos de procesamiento de la misma.
    - Disponibilidad: Característica que asegura que los usuarios autorizados disponen de acceso a la información cuando lo requieren.
    - Autenticidad (no repudio): Característica que asegura que se pueda asociar una acción con un individuo u organización de forma fehaciente.
    - Trazabilidad: Característica que asegura la existencia de un registro o traza en la ocurrencia de un evento o transacción.

3. **Agrupación de activos:** Con objeto de disponer de datos que se puedan manejar de manera coherente y dada la amplitud del listado de activos, una vez identificados y valorados los activos, es necesario definir los dominios de riesgo. Esto es, agrupar los activos resultantes en grupos homogéneos de similares características que permita estandarizar la posterior gestión del riesgo, implantación de salvaguardas y controles por dominios agilizando esta tarea.

4. **Dependencias entre activos:** Siguiendo los criterios establecidos por la metodología MAGERIT, se debe contemplar la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior. Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

5. **Identificación de amenazas:** A partir de los Dominios de Riesgo definidos, es preciso identificar y evaluar las amenazas que pueden comprometer la seguridad de los Activos de Información que los conforman. Cada amenaza es un evento que potencialmente puede desencadenar otras amenazas. Por ejemplo, MAGERIT tipifica las amenazas en 4 grupos:
    - Desastres Naturales
    - De Origen Industrial
    - Errores y Fallos No Intencionados
    - Ataques Deliberados

    A su vez estos cuatro grandes grupos se componen de diferentes subgrupos, como por ejemplo, dentro del grupo Desastres Naturales existen: Fuego, Daños por agua y Desastres naturales.

    Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:
    - Degradación: cuán perjudicado resultaría el activo
    - Frecuencia: cada cuánto se materializa la amenaza

6. **Impacto y riesgo intrínseco:**
   - Impacto**:** El Impacto, visto como una característica del activo, recoge el cambio en el estado de seguridad del activo; es decir, permite conocer el alcance del daño sobre el activo derivado de la materialización de amenazas.
     Impacto (I) = f (importancia del activo, gravedad de la vulnerabilidad)
   - Riesgo Intrínseco: El siguiente paso consiste en realizar el cálculo del nivel de riesgo. Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

$$Riesgo\ (R) = \sqrt{Impacto\ (I)^2 x\ Probabilidad\ (P)^2}$$

7. **Identificación de salvaguardas:** Se debe proceder a identificar las funciones o servicios de salvaguarda existentes que reducirán ese riesgo, y a estimar su eficacia para lograr dicha reducción. Para ello, todo el personal responsable de los activos es entrevistado para conocer el grado de cumplimiento de los controles que le aplican. Se estimará un grado de eficacia real de cada salvaguarda en cada caso concreto, entre un 0% para aquellas salvaguardas que no reducen el riesgo y el 100% para aquellas que son perfectas. A partir de la información obtenida en las entrevistas acerca del grado de implantación de los controles en los distintos entornos tecnológicos, el Responsable de Seguridad realiza una estimación de su efectividad en la reducción de los elementos integrantes del riesgo (ocurrencia e impacto).

8. **Nivel de riesgo efectivo:** Tras determinar la efectividad de las salvaguardas existentes, debe definirse el nivel de riesgo efectivo restante.

6.4 NIST SP 800-30

El NIST es una agencia federal fundada en 1901 para la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. El NIST discute el proceso de gestión de riesgos y cómo las evaluaciones son una parte importante de ese proceso. La publicación de la NIST (8) es una guía enfocada a las organizaciones para la realización de evaluaciones de riesgos de los sistemas de información. El objetivo principal es asegurar los sistemas de información que traten información, además de la optimización de la administración de riesgos a partir del resultado de un AARR.

Los fundamentos expuestos en esta norma, relacionados con los métodos de evaluación de riesgos intentan ser similares a los procesos y enfoques descritos por la ISO y la IEC. La reutilización de los resultados de la evaluación permite reducir la carga sobre las organizaciones que deben cumplir con las normas ISO/IEC y NIST.

La norma NIST proporciona una guía para la realización de cada una de las tres fases del proceso de evaluación de riesgos. NIST plantea una metodología apoyada en los siguientes pasos:

1. **Determinación del Sistema**:
   i. Determinar el sistema a analizar:
      - Alcance
      - Servicios y funciones soportadas por el sistema
      - Criticidad
      - Nivel de protección requerido

ii. Identificar:
- Hardware
- Software
- Interfaces del sistema
- Datos e información
- Personal
- Misión del sistema

2. Identificación de vulnerabilidades:

i. Para determinar vulnerabilidades se usa:
- Fuentes o bases de datos de vulnerabilidades
- Chequeos de seguridad del sistema
- *Checklists* de requisitos de seguridad

ii. Se identificarán vulnerabilidades:
- Política de seguridad
- Procedimientos de seguridad
- Requerimientos de los sistemas
- Análisis de productos
- Salvaguardas técnicas
- Chequeos de vulnerabilidades
- *Test* de penetración

3. Identificación de amenazas:

i. Las fuentes que pueden originar amenazas son:
- Naturales: Riadas, terremotos, tormentas…
- Humanas: Errores, ataques, virus, robos…
- Entorno: Incendios, cortes de suministros…

ii. A la hora de analizar amenazas humanas hay que considerar:
- El origen de la amenaza: hackers, espionaje industrial…
- La motivación: reto personal, ventajas competitivas…
- La acción: ingeniaría social, intrusiones, robo…

4. Estudio de salvaguardas:

Categorías de las salvaguardas:
- Prevención
- Detección
- Contención
- Corrección
- Evaluación

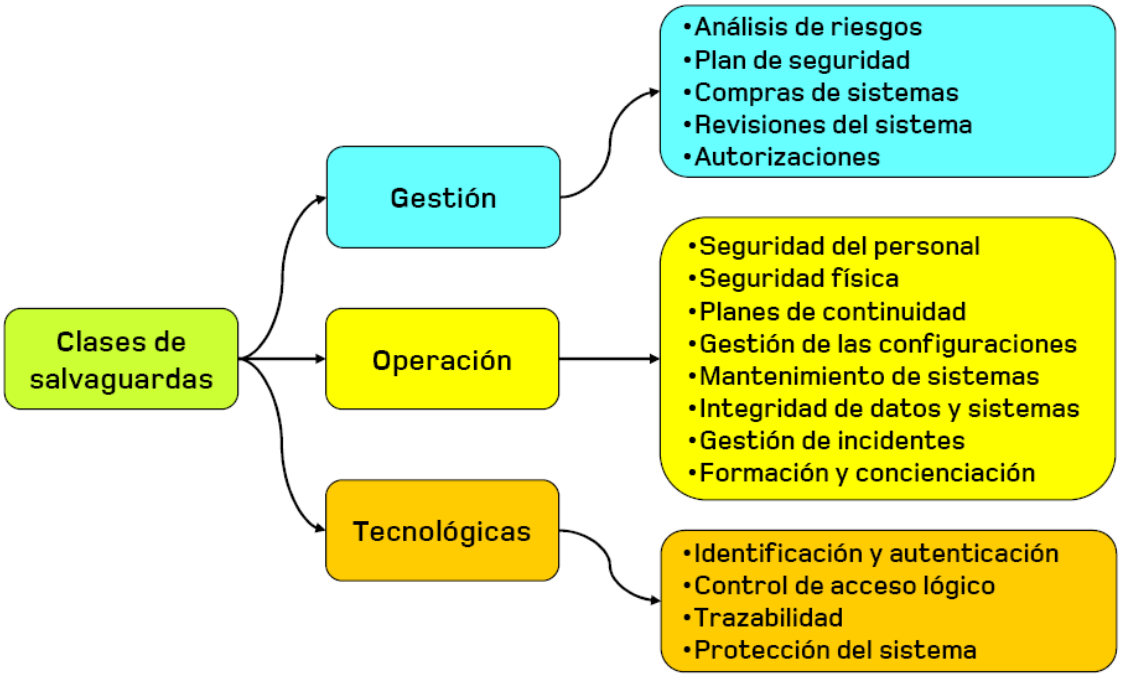


Figura 12: Clases de salvaguardas (NIST SP 800-30)

5. **Determinación de la probabilidad:**
   i. Hay que determinar la probabilidad de que un ataque se materialice teniendo en cuenta:
      - Motivación y capacidad del origen de la amenaza.
      - Tipo de vulnerabilidad.
      - Salvaguardas existentes.
   ii. La probabilidad será:
      - Alta, si el origen de la amenaza está motivado y tiene capacidad y no existen salvaguardas adecuadas.
      - Media, si el origen de la amenaza está motivado y tiene capacidad y si existen salvaguardas adecuadas.
      - Baja, si el origen de la amenaza no está motivado o no tiene capacidad y si existen salvaguardas adecuadas.

6. **Análisis del impacto:**
   i. El impacto de un incidente se determina en función de:
      - Las funcionalidades soportadas por el sistema
      - La criticidad de los datos y el sistema
      - Los niveles de protección requeridos
   ii. El incidente puede comprometer:
      - Confidencialidad
      - Integridad
      - Disponibilidad
   iii. El impacto se clasificará como:
      - Bajo, si las consecuencias son limitadas
      - Medio, si las consecuencias son serias
      - Alto, si las consecuencias son graves

7. **Análisis del riesgo:**
   i. El Riesgo para cada amenaza / vulnerabilidad es una función de:
      - La probabilidad
      - El impacto
      - Las salvaguardas existentes
   ii. Se asignan unos coeficientes a impactos y probabilidades
      - Bajo: 1 → 10
      - Medio: 10 → 50
      - Alto: 50 → 100

RIESGO		Impacto		
		Bajo	Medio	Alto
Probabilidad		10	50	100
Alta	1	10	50	100
Media	0,5	5	25	50
Baja	0,1	0,5	2,5	5

Figura 13: Varemos del riesgo en función del Impacto y la Probabilidad

6.5 CMMI

Los modelos CMMI (9) describen las que han sido consideradas como mejores prácticas que las organizaciones han encontradas productivas y útiles para conseguir sus objetivos de negocio.

Independientemente del tipo de organización, para aplicar estas prácticas se debe usar un criterio profesional para interpretarlas según la situación, las necesidades y los objetivos de negocio.

Aunque las áreas de proceso describen las características de una organización comprometida con la mejora de procesos, éstas se deben interpretar a la luz de un conocimiento profundo de la organización, del entorno de negocio y de las circunstancias específicas involucradas.

Los modelos CMMI no prescriben explícitamente ni implican procesos particulares. En su lugar, CMMI describe los criterios mínimos necesarios para planificar e implementar los procesos seleccionados por la organización para la mejora, basándose en objetivos de negocio.

El CMMI es un modelo que permite evaluar la madurez en la mejora de los procesos. Consiste en las mejores prácticas que tratan las actividades de desarrollo y de mantenimiento que cubren el ciclo de vida del producto, desde la concepción a la entrega y el mantenimiento.

El modelo general del CMMI se organiza en tres ámbitos principales (llamados constelaciones):

- CMMI-DEV: Modelo orientado al desarrollo y mantenimiento
- CMMI-ACQ: Orientado a la gestión de las adquisiciones
- CMMI-SRV: Centrado en la gestión de los servicios

Las tres constelaciones comparten el esquema general de definición y elementos, y gran parte de las áreas de proceso:

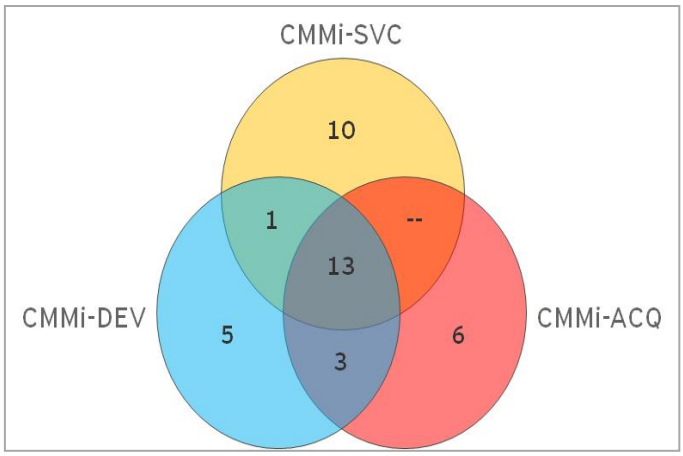


Figura 14: Constelaciones del CMMI

Figura 15: Elementos del modelo CMMI

El nivel de madurez de una organización proporciona una manera de predecir su futuro rendimiento.

Para el CMMI, un nivel de madurez es una etapa en la evolución de la mejora de los procesos y consiste en un conjunto predefinido de áreas. Cada nivel de madurez estabiliza una parte importante de los procesos de la organización.

Los modelos CMMI identifican cinco niveles de madurez:

1. Inicial
2. Gestionado
3. Definido
4. Gestionado cuantitativamente
5. En optimización

La asignación a un nivel de madurez se mide por el logro de las metas específicas y genéricas que se aplican a cada conjunto predefinido de áreas de proceso.

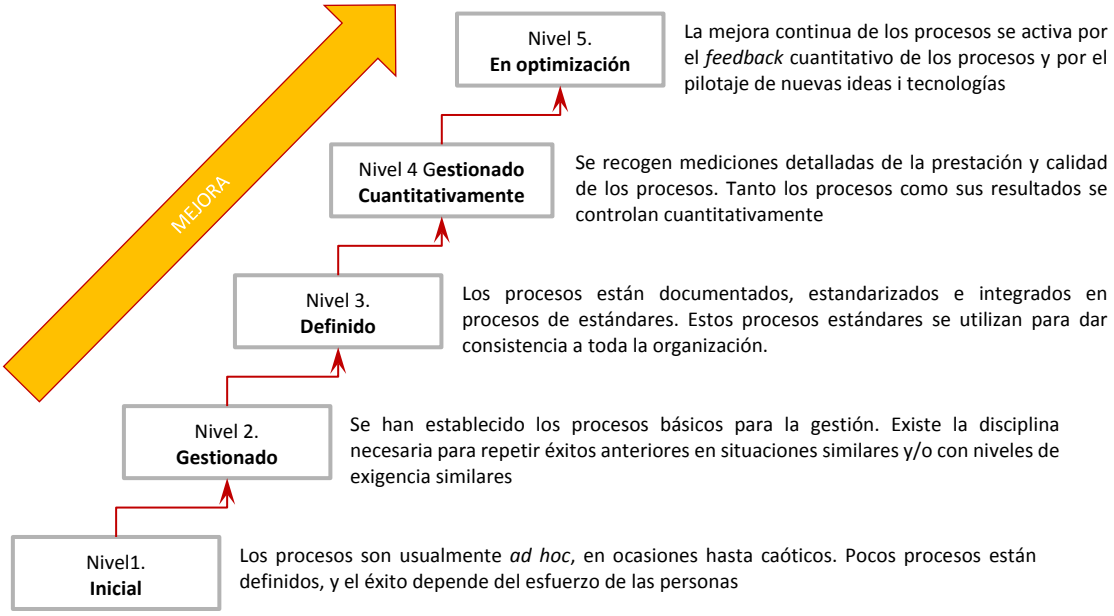


Figura 16: Niveles del CMMI

Asimismo, se detallan los distintos niveles de madurez expuestos anteriormente:

Nivel 1 – Inicial:

En el nivel de madurez 1, los procesos son generalmente *ad-hoc* y caóticos.

La organización generalmente no proporciona un entorno estable para dar soporte a los procesos.

El éxito en estas organizaciones depende de la competencia y heroicidad del personal de la organización y no del uso de procesos probados.

A pesar de este caos, las organizaciones de nivel de madurez 1 a menudo producen productos y servicios que funcionan; sin embargo, frecuentemente exceden sus presupuestos y no cumplen sus calendarios.

Las organizaciones de nivel de madurez 1 se caracterizan por una tendencia a comprometerse en exceso, a abandonar los procesos en tiempos de crisis y a una incapacidad para repetir sus éxitos.

Nivel 2 – Gestionado:

En el nivel de madurez 2, los proyectos de la organización han asegurado que los procesos se planifican y realizan de acuerdo a políticas; los proyectos emplean personal con habilidad que dispone de recursos adecuados para producir resultados controlados; involucran a las partes interesadas relevantes; se monitorizan, controlan y revisan; y se evalúan en cuanto a su adherencia a sus descripciones de proceso. La disciplina de proceso reflejada por el nivel de madurez 2 ayuda a asegurar que las prácticas existentes se mantienen durante tiempos de estrés. Cuando estas prácticas están en su lugar, los proyectos se realizan y gestionan de acuerdo a sus planes documentados.

En el nivel de madurez 2, el estado de los productos de trabajo y la entrega de los servicios son visibles a la dirección en puntos definidos (p.ej., en los hitos principales y al finalizar las tareas principales).

Se establecen compromisos entre las partes interesadas relevantes y se revisan, según sea necesario. Los productos de trabajo se controlan de forma apropiada. Los productos de trabajo y servicios satisfacen sus descripciones de proceso especificadas, estándares y procedimientos.

Nivel 3 – Definido:

En el nivel de madurez 3, los procesos son bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos. El conjunto de procesos estándar de la organización, que es la base del nivel de madurez 3, se establece y mejora a lo largo del tiempo.

Estos procesos estándar se usan para establecer la consistencia en toda la organización. Los proyectos establecen sus procesos definidos adaptando el conjunto de procesos estándar de la organización de acuerdo a las guías de adaptación (consultar el glosario para una definición de "conjunto de procesos estándar de la organización").

Una distinción crítica entre los niveles de madurez 2 y 3 es el alcance de los estándares, descripciones de proceso y procedimientos.

En el nivel 2, los estándares, descripciones de proceso y procedimientos pueden ser bastante diferentes en cada instancia específica de un proceso (p.ej., en un proyecto particular). En el nivel 3, los estándares, descripciones de proceso y procedimientos para un proyecto se adaptan para adecuarse a un proyecto particular o unidad organizativa a partir del conjunto de procesos estándar de la organización y, por tanto, son más consistentes, exceptuando las diferencias permitidas por las guías de adaptación.

Otra distinción crítica es que en el nivel 3, los procesos normalmente se describen más rigurosamente que en el nivel 2. Un proceso definido establece claramente el propósito, entradas, criterios de entrada, actividades, roles, medidas, etapas de verificación, salidas y criterios de salida. En el nivel 3, los procesos se gestionan más proactivamente utilizando una comprensión de las interrelaciones de las actividades del proceso y las medidas detalladas del proceso, sus productos de trabajo y sus servicios.

En el nivel 3, la organización debe madurar más las áreas de proceso de nivel 2. Para lograr el nivel de madurez 3, se aplican las prácticas genéricas asociadas con la meta genérica 3 que no fueron tratadas en el nivel 2.

Nivel 4: Gestionado cuantitativamente

En el nivel de madurez 4, la organización y los proyectos establecen objetivos cuantitativos en cuanto al rendimiento de calidad y del proceso, y los utilizan como criterios en la gestión de los procesos. Los objetivos cuantitativos se basan en las necesidades del cliente, usuarios finales, organización e implementadores del proceso. El rendimiento de calidad y del proceso se comprende en términos estadísticos y se gestiona durante la vida de los procesos.

Las medidas de rendimiento de calidad y del proceso se incorporan en el repositorio de medición de la organización para dar soporte a la toma de decisiones basada en hechos. Se identifican las causas especiales de variación y, donde sea apropiado, se corrigen las fuentes de las causas especiales para prevenir sus futuras ocurrencias.

Una distinción crítica entre los niveles de madurez 3 y 4 es la predictibilidad del rendimiento del proceso. En el nivel de madurez 4, el rendimiento de los procesos se controla utilizando técnicas estadísticas y otras técnicas cuantitativas, y es predecible cuantitativamente.

En el nivel de madurez 3, los procesos normalmente sólo son predecibles cualitativamente.

Nivel 5 – En optimización:

En el nivel de madurez 5, una organización mejora continuamente sus procesos basándose en una comprensión cuantitativa de las causas comunes de variación inherentes a los procesos.

El nivel de madurez 5 se centra en mejorar continuamente el rendimiento de procesos mediante mejoras incrementales e innovadoras de proceso y tecnológicas. Los objetivos cuantitativos de mejora de procesos para una organización se establecen, se revisan continuamente para reflejar el cambio a los objetivos del negocio, y se utilizan como criterios para gestionar la mejora de procesos. Los efectos de las mejoras de procesos desplegadas se miden y evalúan frente a los objetivos cuantitativos de mejora de procesos. Tanto los procesos definidos como el conjunto de procesos estándar de la organización son objeto de las actividades de mejora cuantitativa.

Una distinción crítica entre los niveles de madurez 4 y 5 es el tipo de variación del proceso tratado. En el nivel de madurez 4, la organización se preocupa por tratar las causas especiales de variación del proceso y por proporcionan predictibilidad estadística de los resultados.

Aunque los procesos pueden producir resultados predecibles, los resultados pueden ser insuficientes para alcanzar los objetivos establecidos.

En el nivel de madurez 5, la organización se interesa en tratar las causas comunes de variación del proceso y en cambiar el proceso (para cambiar la media de rendimiento del proceso o reducir la variación inherente del proceso experimentada) para mejorar el rendimiento del proceso y para alcanzar sus objetivos cuantitativos de mejora de procesos establecidos.

6.5.1 Diferencia de madurez entre los niveles

Dado que la madurez organizativa mejorada se asocia con la mejora en el rango de resultados esperados que pueden lograrse en una organización, es un modo de predecir los resultados generales del siguiente proyecto de la organización (por ejemplo, en el nivel de madurez 2, la organización se ha elevado desde ad hoc hasta disciplinada, estableciendo una gestión de proyectos sólida).

A medida que la organización logra las metas genéricas y específicas para el conjunto de áreas de proceso en un nivel de madurez, aumenta su madurez organizativa y recoge los beneficios de la mejora de procesos.

Dado que cada nivel de madurez forma una base necesaria para el siguiente nivel, tratar de saltar niveles de madurez suele ser contraproducente. En relación con lo anterior, se muestra una tabla comparativa sobre los niveles de madurez:

Nivel	Foco	Áreas de Procesos Clave	Resultados
5 – En optimización	Mejora continua de los procesos	- Análisis causal y resolución - Innovación y despliegue en la organización	Muy alta calidad / Muy bajo riesgo
4 – Gestionado cuantitativamente	Gestión cuantitativa de los procesos	- Rendimiento de los procesos de la organización - Gestión cuantitativa de proyectos	Alta calidad / Bajo riesgo
3 – Definido	Estandarización de procesos	- Desarrollo de requisitos - Solución técnica - Integración de producto - Verificación - Validación - Enfoque de procesos de la organización - Definición de procesos de la organización - Formación organizativa - Gestión integrada de proyectos - Gestión de riesgos - Análisis de decisiones y resolución	Calidad media / Riesgo medio
2 – Gestionado	Gestión básica de proyectos	- Gestión de requisitos - Planificación de proyectos - Seguimiento y control de proyectos - Gestión de acuerdos con proveedores - Medición y análisis - Aseguramiento de la calidad de proceso y de producto - Gestión de la configuración	Baja calidad / Alto riesgo
1 – Inicial	Proceso informal y ad hoc		Muy baja calidad / Muy alto riesgo

6.5.2 Modelo CMMI

Para facilitar la implementación del modelo, las áreas de proceso se agrupan en cuatro categorías que, a su vez, se focalizan en mayor o menor medida en los niveles de madurez. Dichas categorías son:

1. **Gestión de Procesos:**

Las áreas de proceso de Gestión de procesos contienen las actividades transversales a los proyectos relacionadas con la definición, planificación, despliegue, implementación, monitorización, control, evaluación, medición y mejora de los procesos.

Las áreas de proceso de Gestión de procesos de CMMI son las siguientes:

- Enfoque en procesos de la organización
- Definición de procesos de la organización
- Formación organizativa
- Rendimiento de procesos de la organización
- Innovación y despliegue en la organización

2. Gestión de Proyectos:

Las áreas de proceso de Gestión de proyectos cubren las actividades de gestión de proyectos relacionadas con la planificación, monitorización y control de proyectos.

Las áreas de proceso de Gestión de proyectos del CMMI son las siguientes:

- Planificación de proyecto.
- Monitorización y control de proyecto.
- Gestión de acuerdos con proveedores.
- Gestión integrada de proyecto.
- Gestión de riesgos.
- Gestión cuantitativa de proyecto.

3. Ingeniería (para el modelo CMMI-DEV):

Las áreas de proceso de Ingeniería cubren las actividades de desarrollo y de mantenimiento que se comparten entre las disciplinas de ingeniería.

Las áreas de proceso de Ingeniería de CMMI son las siguientes:

- Desarrollo de requerimientos.
- Gestión de requerimientos.
- Solución técnica.
- Integración de producto.
- Verificación.
- Validación.

4. Soporte:

Las áreas de proceso de Soporte cubren las actividades que dan soporte al desarrollo y al mantenimiento del producto. Las áreas de proceso de Soporte tratan los procesos que se usan en el contexto de la ejecución de otros procesos.

Las áreas de proceso de soporte de CMMI son las siguientes:

- Gestión de configuración.
- Aseguramiento de la calidad de proceso y de producto.
- Medición y análisis.
- Análisis de decisiones y resolución.
- Análisis causal y resolución.

A continuación se expone la relación entre las áreas de procesos, las categorías y los niveles de madurez de la organización:

	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Soporte	- Gestión de la configuración - Medición y análisis - Aseguramiento de la calidad del proceso y el producto	- Análisis de decisiones y resolución	-	- Análisis de causas y resolución
Gestión de Proyectos	- Seguimiento y control de proyectos - Planificación de proyectos - Gestión de requisitos - Gestión de acuerdos con proveedores	- Gestión integrada de proyectos - Gestión de riesgos	- Gestión cuantitativa de proyectos	-
Gestión de Procesos	-	- Definición organizativo de los procesos - Enfoque organizativo de los procesos - Formación organizativa	- Rendimiento organizativo de los procesos	- Gestión del rendimiento organizativo
Ingeniería	-	- Integración del producto - Desarrollo de requisitos - Solución técnica - Validación - Verificación		

Para conseguir un nivel de madurez elevado se detallan las fases del proceso de mejora a seguir según la Norma ISO 15504-4:

1. Examinar los objetivos de negocio de la organización.
2. Iniciar el ciclo del proceso de mejora.
3. Evaluar la capacidad actual.
4. Desarrollar un Plan de Acción.
5. Implementar las mejoras.
6. Confirmar las mejoras.
7. Sostener las mejoras.
8. Monitorizar el rendimiento.

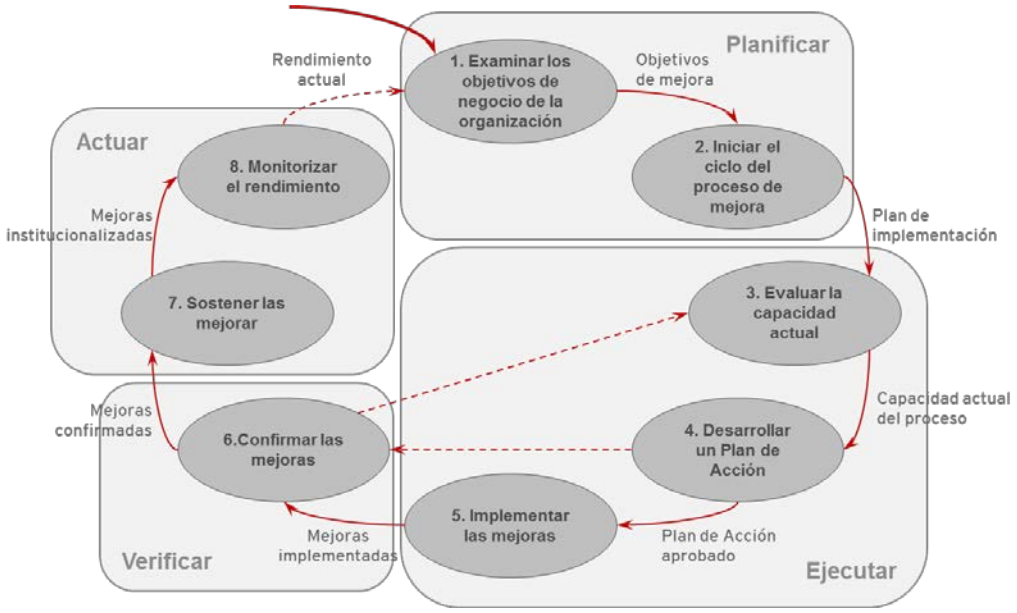


Figura 17: Fases del proceso de mejora CMMI

Adicionalmente al proceso de mejora, para poder determinar la capacidad, se siguen 7 fases según la Norma ISO 15504-4:

1. Iniciar la determinación de la capacidad del proceso.
2. Determinar la capacidad deseada (objetivo).
3. Evaluar la capacidad actual.
4. Determinar la capacidad propuesta.
5. Verificar la capacidad propuesta.
6. Analizar las diferencias.
7. Actuar sobre los resultados.

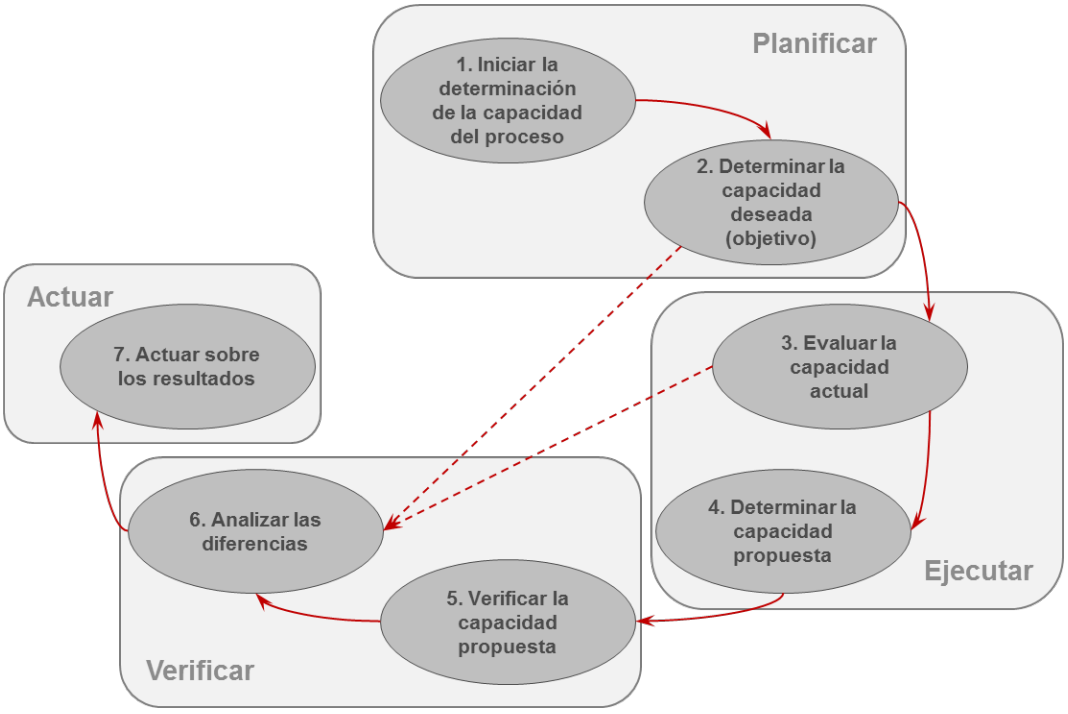


Figura 18: Fases del proceso de determinación de la capacidad

7 Metodología de análisis y gestión de riesgos

En el presente apartado, se detallará el proceso seguido en la empresa GUIMARUBI para realizar el análisis de riesgos y se explicará la metodología seguida para realizar dicho análisis de riesgos. El mapa conceptual seguido para la metodología se puede observar en la Figura 4: Relación de los conceptos teóricos de un AARR.

En base a la probabilidad y el impacto de que se materialice una amenaza aprovechando una vulnerabilidad existente en un activo se obtienen los posibles riesgos existentes.

La relación existente entre los diferentes elementos de un análisis de riesgos se expone en la Figura 5: Mapa conceptual de un AARR.

Las amenazas se aprovechan de las vulnerabilidades existentes y a su vez exponen a los activos de la compañía. Las vulnerabilidades, a su vez, incrementan los riesgos, cosa que hace que estos últimos incrementen las amenazas y generen unos requisitos de seguridad para generar controles de seguridad que protejan las vulnerabilidades.

El proceso seguido consta de 4 fases cíclicas para garantizar un proceso continuo de gestión del riesgo:

Figura 19: Fases para garantizar un proceso continuo de gestión del riesgo.

Dicho proceso tiene las características siguientes:

- Lenguaje claro y orientado a negocio.
- Mantenimiento ágil y rápido.
- Guías para la identificación de riesgos novedosos.
- Integrado con el universo de riesgos de negocio.
- Seguimiento continuo de la evolución de riesgos mediante indicadores.
- Metodología definida y repetible.
- Garantiza la trazabilidad de los resultados.
- No requiere herramientas complejas (MS Excel).

7.1 Identificación de Riesgos

En cuanto a la fase de Identificación de Riesgos, de acuerdo a la metodología, los riesgos de seguridad resultan de la combinación de un "*trigger*" (amenaza) y una "vulnerabilidad" asociados a los activos de información bajo análisis.

En esa línea, la metodología proporciona una guía de identificación de riesgos que ayuda a la identificación de riesgos de manera eficiente. Algunos de estos riesgos son:

- Fuga de Información.
- APT
- Seguridad en Servicios Externalizados.
- Redes Sociales.
- Movilidad.
- *Cloud*.
- *Big Data*.
- Usuarios Privilegiados.

Figura 20: Identificación de Riesgos

La metodología se mantiene actualizada año a año con amenazas (*triggers*) y riesgos novedosos, alineado con tendencias, nuevas amenazas y mejores prácticas del mercado.

Por otra parte, también se garantiza la identificación de riesgos "reales" y "relevantes" desde el punto de vista de la Organización.

En cuanto a lo que concierne a los activos, se clasificarán en función de la guía de clasificación de la información vigente[3] y teniendo en cuenta la criticidad de las siguientes dimensiones:

1. **Confidencialidad**: Garantizar la información, ya sea almacenada, transmitida o incluso ya eliminada. Impide la divulgación de información a personas o sistemas no autorizados.

[3] NOROS007 - Guía de Clasificación de la información

¿Se asegura que sólo quienes estén autorizados pueden acceder a la información?

0	**N/A**	•	Esta dimensión no es de aplicación.
1	**B –** BAJA	•	Información **pública** o de uso interno que no requiere de protección.
2	**M –** MEDIA	•	Información de ámbito **interno**.
3	**A –** ALTA	•	Información confidencial de uso restringido y **difusión limitada**.
4	**MA –** MUY ALTA	•	Información **confidencial** y estratégica para la compañía.

Figura 21: Niveles de confidencialidad

2. **Integridad**: Mantener los datos libres de modificaciones no autorizadas. Permite mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

¿Se garantiza la exactitud y no alteración de la información y de los métodos de procesamiento de la misma?

0	**N/A**	•	Esta dimensión no es de aplicación.
1	**B –** BAJA	•	No es un requisito aunque se realizan controles discrecionales.
2	**M –** MEDIA	•	Cualquier modificación ha de ser identificada.
3	**A –** ALTA	•	Cualquier modificación ha de ser identificada y validada en origen.
4	**MA –** MUY ALTA	•	Cualquier modificación ha de ser identificada y validada en origen y destino.

Figura 22: Niveles de Integridad

3. **Disponibilidad**: Garantizar el acceso a la información que debe encontrarse disponible para los procesos, aplicaciones o personas autorizadas en el momento que así lo requieran.

¿Se asegura que los usuarios autorizados disponen de acceso a la información cuando lo requieren?

0	**N/A**	•	Esta dimensión no es de aplicación.
1	**B –** BAJA	•	Indisponibilidad aceptable de más de 7 días.
2	**M –** MEDIA	•	Indisponibilidad aceptable de más de 1 día.
3	**A –** ALTA	•	El tiempo máximo de indisponibilidad no puede ser superior a 4 horas.
4	**MA –** MUY ALTA	•	El tiempo máximo de indisponibilidad no puede ser superior a 1 hora.

Figura 23: Niveles de Disponibilidad

Conceptualmente se considera una amenaza como la causa potencial de un incidente, el cual puede resultar en un daño sobre una organización o sistema. Asimismo, se exponen algunas de las amenazas existentes relacionadas con los ámbitos de Información, Suministro, Personal, Tecnología y Entorno:

Figura 24: Ejemplos de amenazas existentes

Las vulnerabilidades son consideradas en una Organización como deficiencias o debilidades en un activo que favorecen la materialización de la amenazas sobre los activos y se detallan algunas en la siguiente figura:

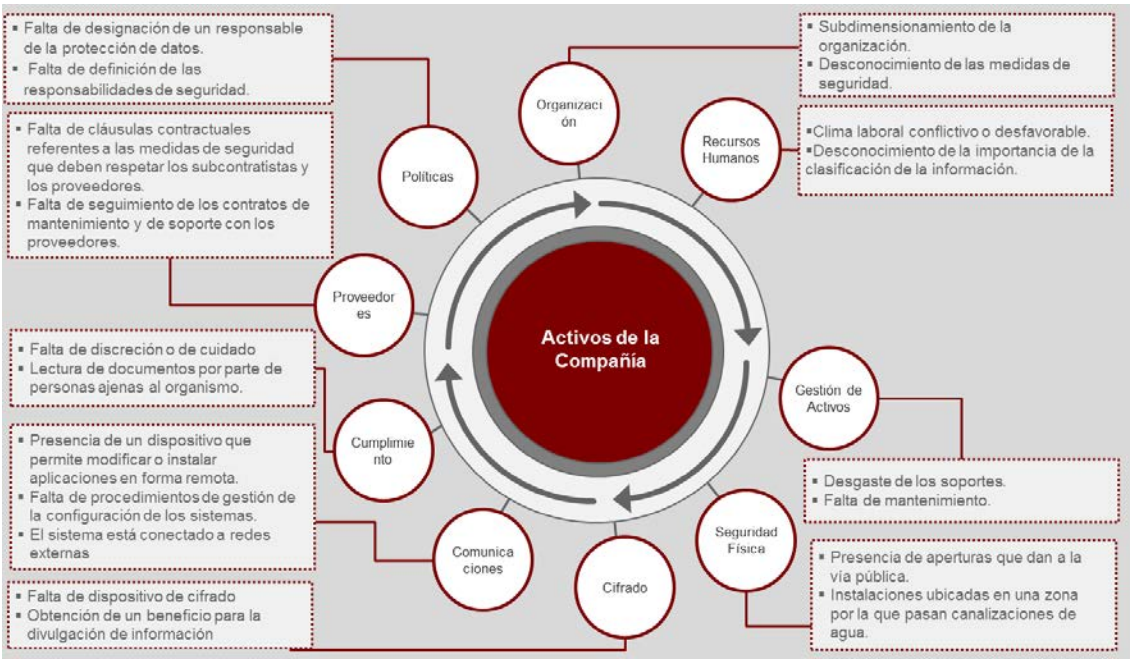


Figura 25: Ejemplos de vulnerabilidades existentes

7.2 Evaluación de Riesgos

La metodología evalúa la importancia del riesgo para la Organización, valorando los siguientes parámetros:

1. **Impacto económico**: Representa la pérdida de ingresos o coste asociado en caso de materializarse el riesgo.

¿Qué volumen de pérdidas se prevé en el peor de los casos de ocurrencias del riesgo (costes, costes indirectos, multas, pérdidas de ingresos, etc.)?		
0	**Menospreciable**	< 3.000 €
1	**B** – BAJO	3.000 € – 250.000 €
2	**M** – MEDIO	250.000 € - 1M €
3	**A** – ALTO	1M € – 10M €
4	**MA** – MUY ALTO	> 10M €

Figura 26: Niveles de impacto económico

2. **Impacto Imagen**: Evalúa el daño de imagen desde el punto de vista de Organización si el riesgo se materializase.

¿Qué daño de imagen implicaría para la organización si el riesgo se produjera (aparición en los medios, conocimiento público, etc.)?		
0	**Menospreciable**	Sin afectación.
1	**B** – BAJO	Crisis temporal.
2	**M** – MEDIO	Pérdida de confianza.
3	**A** – ALTO	Pérdida temporal de reputación.
4	**MA** – MUY ALTO	Pérdida de reputación.

Figura 27: Niveles de Impacto Imagen

3. **Probabilidad**: Periodicidad estimada con la que se puede materializar el riesgo.

Con la situación actual en la que existen vulnerabilidades y salvaguardas, ¿en que periodo se prevé la materialización del riesgo?		
0	**Menospreciable**	Más de 5 años.
1	**B** – BAJA	Entre 3 y 5 años.
2	**M** – MEDIA	Entre 2 y 3 años.
3	**A** – ALTA	Entre 1 y 2 años.
4	**MA** – MUY ALTA	Menos de 1 año.

Figura 28: Niveles de Probabilidad

El impacto final se calculará en base al impacto económico y el impacto imagen, aunque posteriormente se tendrán en cuenta las diferentes clasificaciones de los activos y por último se obtendría el riesgo sin tener en cuenta las medidas obtenidas, donde el riesgo sería:

$$Riesgo = [(ImpactoEconómico * ImpactoImagen) * Valor] * Probabilidad$$

			Impacto de Imagen				
			0	1	2	3	4
			Menospreciable	B – BAJO	M – MEDIO	A – ALTO	MA – MUY ALTO
Impacto Económico	4	MA – MUY ALTO	Alto	Alto	Muy alto	Muy alto	Muy alto
	3	A – ALTO	Medio	Alto	Alto	Muy alto	Muy alto
	2	M – MEDIO	Bajo	Medio	Medio	Alto	Muy alto
	1	B – BAJO	Bajo	Bajo	Medio	Alto	Alto
	0	Menospreciable	N/A	Bajo	Bajo	Medio	Alto

Figura 29: Impacto de Imagen vs. Impacto Económico

			Impacto (Imagen Vs. Económico)				
			0	1	2	3	4
			Menospreciable	B – BAJO	M – MEDIO	A – ALTO	MA – MUY ALTO
MAX(C, I, D)	4	MA – MUY ALTO	Medio	Medio	Alto	Alto	Muy alto
	3	A – ALTA	Bajo	Medio	Alto	Alto	Alto
	2	M – MEDIA	Bajo	Medio	Medio	Alto	Alto
	1	B – BAJA	N/A	Bajo	Medio	Medio	Medio
	0	N/A	N/A	N/A	Bajo	Bajo	Medio

Figura 30: Impacto vs. MAX(C, I, D)

		Cálculo del riesgo				
Impacto	Muy alto	Medio	Alto	Alto	Muy alto	Muy alto
	Alto	Bajo	Medio	Alto	Alto	Muy alto
	Medio	Bajo	Bajo	Medio	Alto	Alto
	Bajo	Muy bajo	Bajo	Bajo	Medio	Alto
	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo	Medio
		Muy bajo	Bajo	Medio	Alto	Muy alto
		Probabilidad				

Figura 31: Riesgo (Impacto vs. Probabilidad)

7.3 Identificación de medidas y controles

A partir de los riesgos identificados se definen medidas y controles asociados a uno o varios riesgos, valorando la Reducción del Riesgo con la implantación de la medida.

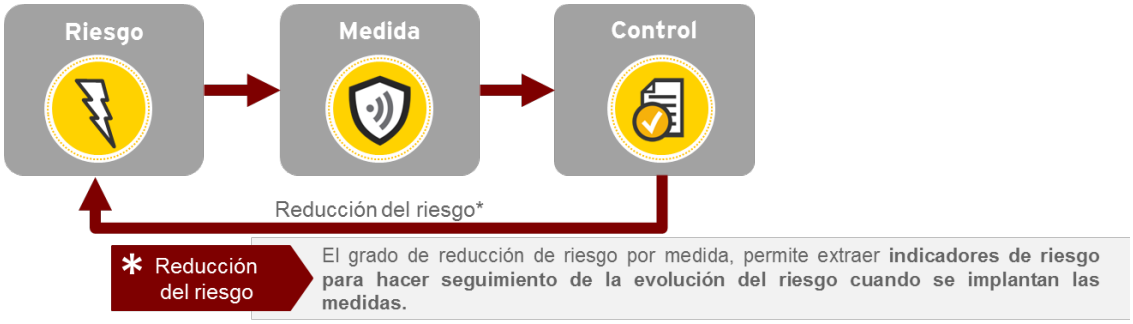


Figura 32: Proceso de reducción de riesgo

En función de las medidas correctivas implantadas se calculará el impacto residual:

		Cálculo del impacto residual				
Impacto	Muy alto	Muy bajo	Bajo	Medio	Alto	**Muy alto**
	Alto	Muy bajo	Muy bajo	Bajo	Medio	Alto
	Medio	Muy bajo	Muy bajo	Muy bajo	Bajo	Medio
	Bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo
	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo
		Cobertura total	Cobertura alta	Cobertura media	Cobertura baja	Cobertura nula
		Medidas correctivas				

Figura 33: Cálculo del impacto residual

Medidas correctivas implantadas	
0 Cobertura nula	Las medidas correctivas implantadas prácticamente no reducen el nivel de impacto sobre el funcionamiento del servicio.
1 Cobertura baja	Las medidas correctivas implantadas reducen en algún aspecto el nivel de impacto sobre el funcionamiento del servicio.
2 Cobertura media	Las medidas correctivas implantadas reducen parcialmente el nivel de impacto sobre el funcionamiento del servicio.
3 Cobertura alta	Las medidas correctivas implantadas reducen en gran parte el nivel de impacto sobre el funcionamiento del servicio.
4 Cobertura total	Las medidas correctivas implantadas reducen en su totalidad el nivel de impacto sobre el funcionamiento del servicio.

Figura 34: Niveles de medidas correctivas implantadas

De la misma manera se calculará la probabilidad residual después de aplicar las medidas correctivas:

		Cálculo de la probabilidad residual				
Probabilidad de materializarse una amenaza	Muy alta	Muy baja	Baja	Media	Alta	**Muy alta**
	Alta	Muy baja	Muy baja	Baja	Media	Alta
	Media	Muy baja	Muy baja	Muy baja	Baja	Media
	Baja	Muy baja	Muy baja	Muy baja	Muy baja	Baja
	Muy baja	Muy baja	Muy baja	Muy baja	Muy baja	Muy baja
		Cobertura total	Cobertura alta	Cobertura media	Cobertura baja	Cobertura nula
		Medidas preventivas				

Figura 35: Cálculo de la probabilidad residual

Medidas preventivas implantadas	
0 Cobertura nula	Las medidas preventivas implantadas prácticamente no reducen el nivel de probabilidad sobre el funcionamiento del servicio.
1 Cobertura baja	Las medidas preventivas implantadas reducen en algún aspecto el nivel de probabilidad sobre el funcionamiento del servicio.
2 Cobertura media	Las medidas preventivas implantadas reducen parcialmente el nivel de probabilidad sobre el funcionamiento del servicio.
3 Cobertura alta	Las medidas preventivas implantadas reducen en gran parte el nivel de probabilidad sobre el funcionamiento del servicio.
4 Cobertura total	Las medidas preventivas implantadas reducen en su totalidad el nivel de probabilidad sobre el funcionamiento del servicio.

Figura 36: Niveles de medidas preventivas implantadas

7.4 Gestión y seguimiento del Riesgo

Una vez obtenidos los resultados del Análisis de Riesgos, se decidirán las medidas a implantar y durante esta fase, la metodología y herramienta permiten:

- Simulación de escenarios de riesgo en función de las medidas que se implantan.
- Seguimiento de la evolución del riesgo real a medida avanza la implantación de medidas.
- Integración con el universo de riesgos de negocio de indicadores clave de riesgos de seguridad.

8 Trabajo realizado

En este apartado se detallarán las fases que compondrán el proyecto. Estas fases son el resultado de la adaptación y optimización de la metodología utilizada, para la realización de Planes Directores de Seguridad:

Figura 37: Fases de la metodología utilizada en el presente proyecto

En los futuros apartados se detallarán los objetivos y tareas realizadas a lo largo de estas fases.

8.1 Postura de seguridad Actual

8.1.1 Análisis de situación actual

8.1.1.1 Análisis de entorno y selección de activos críticos

Objetivos:

- Realizar un entendimiento de cuál es el estado de la organización de seguridad de la información actual y de los procesos de negocio, los activos relacionados (información, sistemas, infraestructura y personas).
- Identificar y revisar para los procesos de negocio de la corporación cuales son los activos más críticos en base a su valoración de acuerdo a los criterios de seguridad y su relación con los objetivos de negocio y de seguridad.

En esta fase se ha realizado un entendimiento de los procesos de negocio de la compañía. Se han realizado reuniones de entendimiento con los responsables del proyecto del Plan Director para entender los procesos de negocio, sus flujos de información, los sistemas de información que utilizan, la infraestructura que soporta a estos procesos y las personas relacionadas.

Se han identificado y entendido los objetivos de negocio. Se han identificado los responsables de proyecto y los responsables de las áreas de negocio para entender cuáles son los objetivos de negocio de la corporación y analizar la relación de dependencia entre los objetivos de negocio y los de seguridad.

Se ha identificado y recopilado la información relacionada con el actual Plan Director de Seguridad. Se han realizado entrevistas de entendimiento con los actuales responsables de la

seguridad de la información para conocer el grado de implantación de medidas en la compañía y el estado de los proyectos de seguridad en curso y realizados del Plan Director de Seguridad.

Se han revisado las valoraciones de los activos respecto a la clasificación de la información (Disponibilidad, Integridad, Confidencialidad) así como la exactitud y completitud de los recursos que contienen los diferentes activos de información.

Finalmente se han identificado y seleccionado los principales activos de información / recursos tecnológicos. Tras la realización de las entrevistas de entendimiento y con el actual inventario de activos de información del que dispone la corporación se han priorizado y seleccionado aquellos activos más críticos / recursos tecnológicos que guarden relación o que puedan tener mayor impacto sobre los objetivos de negocio y de seguridad anteriormente identificados.

Tras analizar el inventario de activos de GUIMARUBI, formado por 123 activos y clasificados con la colaboración de todos los responsables de negocio, se han identificado 13 categorías principales que agrupan todos los activos.

El nivel de criticidad de cada categoría está determinado por la sensibilidad la información incluida en los mismos. En este sentido, el nivel de criticidad de las agrupaciones realizadas es el máximo nivel de confidencialidad, integridad y disponibilidad de los activos que los componen. Adicionalmente, se ha determinado para cada agrupación de activos una ponderación, con el objetivo de tenerlos en mayor consideración a la hora de realizar el análisis de riesgos y reajustar valores de forma parcialmente subjetiva para asegurar que los resultados teóricos se ajustan mejor a la realidad de GUIMARUBI.[4]

ACTIVOS DE INFORMACIÓN		C	I	D	Ponderación media
Análisis del negocio		**4**	**4**	**4**	**12**
2	Balance	4	4	1	
35	*Dashboard* de cuenta de resultados	4	4	1	
28	*Dashboard* de logística	2	4	1	
32	*Dashboard* de pérdidas de CC	2	4	1	**0**
33	*Dashboard* de stock y coberturas	2	4	1	
36	*Dashboard* de ventas	4	4	1	
58	Datos de productividad	2	4	2	
114	Datos de resultados para comunicaciones	0	2	0	
91	Datos de ventas de empleados	2	4	0	
29	Informe de faltas	2	4	1	
31	Informe de logística	2	4	1	
30	Informe de productividad	2	4	1	
25	Informe de ventas	4	4	1	
39	Márgenes de venta	4	2	4	
112	Resultados de la compañía	1	1	0	
Auditoría		**4**	**4**	**1**	**9**
26	Informe de auditoría de delitos penales	4	4	0	
34	Informe de auditoría de procesos	2	4	0	
78	Informe de auditoría y analíticas	4	4	1	
47	Informe de auditoría y licencias	2	4	1	
27	Investigaciones de delitos	4	4	0	
Jurídico		**4**	**4**	**0**	**8**

[4] Clasificación basada en la normativa interna de Seguridad "NOROS007 - Guía de Clasificación de la información"

17	Contratos de servicios internos	2	4	0	
43	Contratos dept. técnico	2	4	0	
110	Demandas y sanciones	2	4	0	
77	Contratos	4	4	0	
107	Escrituras	0	4	0	
Gestión de clientes		**2**	**4**	**4**	**10**
3	Base de datos de clientes	2	4	4	
53	Datos de contacto de clientes	2	1	0	
103	Datos de gestión de clientes	2	1	0	
123	Datos fiscales	2	4	1	
92	Datos personales de clientes	2	4	0	**0**
63	Facturas de clientes	2	4	4	
55	Ficha de alta de cliente	2	4	0	
82	Gestión de derechos ARCO	2	4	1	
57	Histórico de consumo de clientes	2	1	1	
71	Informe de impagos	2	2	0	
64	Pedidos de clientes	2	4	4	
Gestión de instalaciones		**2**	**4**	**4**	**10**
113	Datos de centros	0	2	0	
44	Documentación de obras	2	4	1	
21	Documentación de suministro eléctrico	2	4	0	
50	Informe de reparaciones	2	1	0	
46	Inspecciones periódicas	2	4	1	
40	Libros de frío	2	4	4	
Gestión de productos		**4**	**4**	**4**	**12**
66	Base de datos de productos	2	4	4	**0**
52	Catálogo de ventas	0	2	0	
13	Condiciones comerciales COMPRAS	2	4	1	
41	Condiciones comerciales EXPORT	2	4	1	
67	Condiciones comerciales GUI	2	4	1	
65	Contrato de suministro	4	4	0	
9	Contratos comerciales	4	4	0	**0**
59	Contratos con proveedores de logística	2	4	0	
37	Contratos de exclusividad y distribución	4	4	0	
1	Contratos de franquicias y grandes cuentas	4	4	0	
54	Contratos de suministro	4	4	0	
74	Coste de productos (PMP)	2	4	4	
8	Coste neto neto	4	4	4	
56	Cotizaciones y precios de *food service*	2	2	1	
12	*Dashboards* de faltas	2	4	2	
14	Datos logísticos de artículos	2	4	1	
86	Documentación aduanera	2	4	1	
83	Gestión de logística	2	4	1	
60	Hojas de ruta	2	1	2	
72	Listado de precios de ofertas	0	4	1	
22	Ofertas de *GuiMarUbi*	2	1	0	
51	Precios de folletos	0	4	1	**0**
16	Precios de tarifa	2	4	1	
18	Solicitudes de modificación del maestro de artículos	2	2	1	
68	Tarifa de GC	2	4	1	
69	Tarifa de ofertas (GC)	2	4	1	
15	Tarifas de proveedores	2	4	1	

11	Variaciones de coste (Neto)	4	4	0	
	Gestión de proveedores	**2**	**4**	**4**	**10**
62	Base de datos de precios de proveedores	2	4	4	
48	Condiciones con industriales	2	1	1	
61	Cotizaciones de proveedores de transporte	2	1	0	
19	Datos de contacto de proveedores	2	1	0	
20	Datos de contacto y referencias de proveedores	2	1	0	
7	Facturas de proveedores	2	4	1	
6	Información de gestión de proveedores	2	2	0	
73	Presupuestos	2	4	0	
23	RFIs	2	1	0	
	Gestión de RRHH	**4**	**4**	**0**	**8**
104	Actas de comité de seguridad y salud	1	4	0	
117	Currículums	2	1	0	
101	Datos de contacto de empleados	2	1	0	
102	Datos de contacto de empleados, centros y clientes	2	1	0	**0**
93	Estudios de puestos y condiciones de trabajo	2	4	0	
116	Evaluación del desempeño de empleados	2	4	0	
94	Expediente de empleados	2	4	0	
81	Información sindical	4	2	0	
75	Informe médicos	4	4	0	
121	Nóminas	4	4	0	
97	Notificaciones de baja	2	4	0	
106	Ofertas salariales	2	1	0	
76	Partes de accidente	4	4	0	
98	Resultados de revisiones médicas	2	4	0	
105	Test psicotécnicos	2	2	0	
	Gestión del negocio	**4**	**4**	**2**	**10**
79	Actas del comité ejecutivo	4	4	0	
122	Datos del comité ejecutivo	4	4	2	
118	Normativas y procedimientos internos	1	4	0	
38	Plan estratégico desarrollo de negocio CC y *delivery*	4	4	0	
10	Política de precios	4	4	0	
95	Tickets de *helpdesk*	2	1	2	
	Marketing y comunicación	**2**	**4**	**1**	**7**
70	Acciones comerciales	2	2	0	
42	Cupones	2	4	1	
100	Datos de visitas promocionales	2	2	0	
45	Estudios de clientes	2	4	0	
119	Libro de actividad comercial	2	2	0	
49	Listado de clientes potenciales	2	1	0	
120	Miquel Informa	2	2	0	
24	Precios de venta de la competencia	0	1	0	
	Seguridad alimentaria	**2**	**4**	**1**	**7**
109	Certificaciones	1	1	0	
108	Fichas técnicas de productos	0	4	1	
89	Protocolos de analíticas	2	4	1	
	Seguridad corporativa	**2**	**4**	**2**	**8**
115	Alerta de delincuentes	0	1	0	
99	Datos de presencia	2	2	0	
90	Datos de PRL de externos	2	4	0	
96	Datos de visitas de externos	2	2	1	

111	Gestión de paquetería y correo	1	1	0	
80	Imágenes VV	2	4	2	
87	Informe de incidentes de seguridad	2	4	1	
88	Inspecciones de policía	2	4	1	
84	Listado de empleados con acceso a alarmas	2	4	1	
85	Listado de empleados de transporte de fondos	2	4	1	
Tesorería		**2**	**4**	**1**	**7**
4	Fichero de cobros	2	4	1	
5	Fichero de pagos	2	4	1	

123 TOTAL de Activos de información

A modo resumen, las 13 categorías resultantes de agrupar dichos activos han quedado de la siguiente manera:

ACTIVOS DE INFORMACIÓN	C	I	D	Ponderación media
Análisis del negocio	4	4	4	12
Auditoría	4	4	1	9
Jurídico	4	4	0	8
Gestión de clientes	2	4	4	10
Gestión de instalaciones	2	4	4	10
Gestión de productos	4	4	4	12
Gestión de proveedores	2	4	4	10
Gestión de RRHH	4	4	0	8
Gestión del negocio	4	4	2	10
Marketing y comunicación	2	4	1	7
Seguridad alimentaria	2	4	1	7
Seguridad corporativa	2	4	2	8
Tesorería	2	4	1	7

123 TOTAL de Activos de información

8.1.1.2 Análisis normativo ISO27002

Objetivos:

- En esta etapa el principal objetivo es revisar el estado de los controles ISO 27001/27002:2013, evaluando el nivel de madurez de los mismos.
- Identificar debilidades importantes por falta de algún control que supongan un riesgo elevado para la Organización y que requieran acciones urgentes.
- En caso de interés, el estado de madurez actual de la organización respecto la ISO 27001/2 en relación a compañías similares y los diferentes dominios de seguridad.

Durante esta fase se han realizado reuniones con los principales interlocutores de los diferentes departamentos de la corporación con el objetivo de analizar las actividades de seguridad realizadas con cada en cada uno de los departamentos.

Se han solicitado los procedimientos existentes en materia de seguridad, a continuación se enumeran algunos de ellos:

a) Política Seguridad Información de la Información.
b) Roles y funciones en materia seguridad información.
c) Análisis de riegos, PCN

d) Procedimiento de gestión de accesos a las instalaciones.
e) Procedimiento de ABM de usuarios (Altas, Bajas y Modificaciones).
f) Clasificación de la información.
g) Normas básicas de seguridad en el uso de recursos informáticos.
h) Clausulados en la selección y contratación del Personal.
i) Guías de Bastionado.
j) Detección de vulnerabilidades.
k) Segregación de Redes.
l) Guías de desarrollo seguro
m) Gestión de Cambios.
n) Políticas de actualización y parcheado de los SI
o) Gestión de incidentes de seguridad.
p) Protección contra el malware.

Se han revisado y analizado los procedimientos de seguridad obtenidos. Para los procedimientos obtenidos, y en generales para los procesos existentes se han realizado peticiones de evidencias para verificar la adecuada implantación de las medidas y el seguimiento de los procedimientos definidos.

Finalmente se ha evaluado el grado de implantación de los controles de la ISO 27002 en base al modelo estándar CMMI y se ha realizado un benchmarking del estado actual de la compañía respecto a la norma ISO27001/27002:2013 respecto a organizaciones similares por sectores y volumen de negocio.

8.1.1.3 Revisión de organización y procesos de seguridad

Objetivos:

- Asegurar que la organización, modelo de relación, procesos, tecnología y personas están alineadas para dar respuesta a las necesidades de la compañía, tanto en procesos operativos, tácticos como estratégicos.
- Garantizar que los procesos de seguridad son adecuados y maduros para prevenir, detectar y responder ante incidentes o brechas de seguridad.

Durante esta fase se ha realizado un análisis de la organización, las responsabilidades y las actividades que se realizan como parte de los procesos de seguridad existentes. Algunos ejemplos ilustrativos son los siguientes:

- Bastionado y Parcheado de Sistemas con Tiempos de Respuesta (SLA).
- Gestión de Eventos de Seguridad e incidentes de seguridad.
- Gestión de Vulnerabilidades.
- Gestión de Equipos de Protección (IPS/IDS).
- Participación de Seguridad en Proyectos (S-SDLC).

Se ha hecho una revisión y análisis de los procesos de seguridad. Se han analizado los procesos existentes mediante la técnica de *walk-through* (caminar por el proceso), identificando la adecuada implantación de las medidas y el seguimiento de los procedimientos definidos.

Se ha revisado y analizado la función de seguridad en otros procesos de IT o de negocio. Mediante entrevistas con los recursos que han participado en estos procesos, se ha realizado un análisis de la integración de actividades de seguridad en otros procesos de negocio (por ej. Mantenimiento TIC, Explotación, Desarrollo).

Se ha analizado la alineación de la organización, responsabilidad, procesos y plataformas tecnológicas que lo soportan para el entendimiento real de funcionamiento del proceso e identificación de *gaps*.

Finalmente, se ha hecho un análisis global del modelo organizativo, de relación y dimensionamiento de la función de seguridad y sus procesos anteriormente revisada y comparativa con organizaciones similares. Durante esta tarea se ha evaluado la alineación y relación con el gobierno y otros procesos IT.

8.1.1.4 Análisis de nuevas amenazas

Objetivos:

- Identificar nuevas amenazas y riesgos novedosos, de acuerdo a la evolución tecnológica en la organización.
- Analizar la afectación de estas amenazas a la organización, identificando posibles vulnerabilidades que puedan ser utilizar para materializarse riesgos.

A partir de una reunión inicial con el equipo de trabajo, se han determinado los ámbitos de nuevas amenazas y riesgos novedosos a profundizar durante la identificación (por ejemplo, seguridad activos industriales, cibercrimen, movilidad, *cloud computing*, etc.). La determinación del ámbito ha permitido seleccionar mejor las personas a involucrar durante este análisis.

Las acciones realizadas con el equipo de trabajo y expertos para analizar nuevas amenazas han sido:

i. Identificación, por ámbito (por ej. *Big Data*, Redes Sociales, Movilidad, *Cloud Computing*) amenazas y riesgos asociados.
ii. Análisis de debilidades existentes que pueden incrementar la probabilidad de materialización de los riesgos.
iii. Identificación y diseño de alto nivel, conjuntamente con la organización, de potenciales soluciones de acuerdo a tendencias y mejores prácticas de otros clientes.

Consolidación de las amenazas y riesgos identificados, incluyendo de manera clara la situación en relación al riesgo, el potencial impacto para la organización y posibles soluciones existentes. Esta información se incluirá y desarrollará dentro de la posterior fase de Análisis de Riesgos

8.1.1.5 Análisis DAFO

Objetivos:

- El objetivo de esta fase es poner en común los resultados de las diferentes actividades de análisis y evaluación realizadas para poder ofrecer una visión unificada del estado actual de la compañía.
- Identificación de las prioridades, preocupaciones y necesidades de las áreas de negocio en términos de seguridad de la información.
- Realizar un análisis de visión estratégica y organizativa DAFO para un mejor entendimiento de la situación

Durante esta fase se han identificado las preocupaciones, necesidades y prioridades del negocio en el ámbito de la seguridad. Se han realizado una serie de reuniones con las áreas de negocio significativas para entender e identificar sus necesidades y preocupaciones en términos de seguridad de la información.

Se ha realizado un análisis Interno de seguridad, cuyas actividades incluyen las siguientes:

- Alineación de la seguridad con las prioridades y necesidades de las áreas de negocio.

- Valoración de la Organización de la seguridad Actual, modelo de relación y procesos de seguridad.
- Requerimientos de seguridad desde la perspectiva de negocio.
- Situación respecto a nuevas amenazas y la externalización de servicios.
- Diagnóstico normativo y regulatorio respecto a PCI-DSS, LOPD, ISO 27000, NIST 800-53, LPIC.

Se ha realizado un análisis Externo, cuyas actividades incluyen las siguientes:

- Análisis de tendencias y posicionamiento de la empresa en Seguridad.
- Inclusión de nuevas amenazas que suponen nuevos riesgos para la empresa:
- Retos futuros como organización.
- Comparativa de situación con otras compañías similares.

Finalmente se ha realizado un análisis DAFO concluyendo en Fortalezas y Debilidades, junto con las Amenazas y Oportunidades en el ámbito de la seguridad.

8.1.2 Evaluación de seguridad técnica

En esta fase se han realizado tres actividades, las cuales no están en el alcance del trabajo realizado de este proyecto pero ello no implica su no realización. Por ese motivo únicamente se han explicado los objetivos de dichas actividades:

8.1.2.1 Análisis de seguridad interno

Objetivos:

- Identificar debilidades de la red interna de los sistemas, elementos de red, comunicaciones y telefonía que soportan los procesos de negocio de la compañía.
- Evaluar el nivel de accesibilidad y visibilidad de los sistemas y de las diferentes redes (o contextos de seguridad) y enrutamientos entre las mismas.
- Presentar y validar los resultados de las diferentes pruebas tanto al personal técnico responsable de corregirlas, como a la dirección, permitiendo así la toma de decisiones en función en función del impacto y riesgo asociado.

8.1.2.2 Análisis de seguridad WIFI

Objetivos:

- Análisis de la cobertura de señal inalámbrica en los entornos corporativos indicados en el alcance. Para las pruebas se utilizarán elementos hardware que permitan ampliar el nivel de señal (tarjetas, antenas direccionales, amplificadores de señal,..)
- Identificación de las redes inalámbricas vulnerables que puedan ser utilizadas por parte de terceros para comprometer la infraestructura informática.
- Usar técnicas para suplantar la señal de puntos de acceso usados por GUIMARUBI que permita el acceso a las aplicaciones corporativas.
- Realizar pruebas de intrusión para evidenciar la posibilidad de acceso a redes internas a través de la infraestructura inalámbrica.

8.1.2.3 Test de intrusión Externo

Objetivos:

- Identificar debilidades de la red externa de los sistemas, elementos de red, comunicaciones y telefonía que soportan los procesos de negocio de la compañía.

- Presentar y validar los resultados de las diferentes pruebas tanto al personal técnico responsable de corregirlas, como a la dirección, permitiendo así la toma de decisiones en función en función del impacto y riesgo asociado.

8.2 Modelo objetivo y gestión del riesgo

8.2.1 Análisis de riesgos

8.2.1.1 Identificación y evaluación de riesgos

Objetivo:

- Evaluar los riesgos de seguridad resultantes de las debilidades y vulnerabilidades identificadas en fases anteriores. Esta evaluación se realizará a partir de un perfil de amenaza específico de GUIMARUBI y a partir de la clasificación de los activos de información.
- Inventariar y documentar los riesgos en un lenguaje de negocio, identificando claramente las amenazas y las posibles vulnerabilidades asociadas.
- De los riesgos identificados, determinar su importancia desde la perspectiva de negocio en caso de materializarse.

Para la identificación y evaluación de riesgos combinación de un "*trigger*" (amenaza) y una "vulnerabilidad" por activo de información, se han realizado talleres conjuntos con el equipo de proyecto GUIMARUBI. Las actividades realizadas han sido:

- Integración de los riesgos resultado del análisis de nuevas amenazas y riesgos novedosos así como todas las vulnerabilidades resultantes por falta de control ISO 27002.
- Utilizando la guía Identificación de riesgos, se han identificado vulnerabilidades que puedan permitir la materialización de amenazas (por ej. Fuga de Información, Ataque Persistente, Servicios Externalizados, *Cloud*…). Adicionalmente se han personalizado los riesgos a la organización, personalizando las vulnerabilidades seleccionadas del catálogo y las amenazas.
- Se ha valorado la importancia de los riesgos en términos de negocio, tanto en un concepto de probabilidad pueda entender como en términos de impacto asociados al daño de imagen y a la pérdida de ingresos o costes.
- Se han consolidado y documentado los riesgos. Garantizando la trazabilidad de la información utilizada para llegar a los riesgos (por ej. Vulnerabilidades, amenazas, criterio de valoración de impacto). Mediante la herramienta se representarán los mapas de riesgos y otros gráficos como se verá en futuros apartados.

En base a las amenazas definidas en los apartados anteriores mediante las reuniones con los diferentes responsables de las áreas, se ha obtenido un catálogo de 18 amenazas aplicables:

1. Filtración de información sensible de la organización.
2. Publicación de información confidencial.
3. Pérdida total o parcial de comunicaciones.
4. Fallo técnico o humano.
5. Robo de activos físicos o información.
6. Explotación de vulnerabilidades técnicas.
7. Utilización de los sistemas de la red corporativa con fines ilícitos.
8. Distribución de malware (p.ej.: virus).
9. Ataques de ingeniería social (p.ej.: *phishing*)
10. Acceso no autorizado a sistemas corporativos.

11. Incumplimiento de la política de seguridad interna, las normas, procedimientos y legislación aplicable.
12. Desconocimiento de la política de seguridad interna, normas, procedimientos y legislación aplicable.
13. Daños o destrucción de equipos, material o información.
14. Dependencia total o parcial de proveedores o terceras partes.
15. Manipulación de las instalaciones imposibilitando el acceso
16. Concentraciones en el perímetro de las instalaciones.
17. DoS.
18. *Hackeo* de páginas web modificando el contenido (*defacement*).

Después de la determinación de un catálogo de amenazas basado en el catálogo establecido por el CNPIC y las mejores prácticas. Las amenazas afectan al medio de tratamiento que soporta los activos de información, no a la propia información en sí. Por lo que para cada amenaza, se ha definido el impacto que supondría su materialización para cada grupo de activos de información.

El impacto de dichas amenazas ha sido analizado teniendo en consideración las dimensiones de seguridad sobre la que tiene una mayor afectación. Por consiguiente, el valor asignado al impacto de cada amenaza viene determinado por la valoración de dicha dimensión sobre cada activo de información.

La probabilidad/frecuencia de dichas amenazas se ha definido en base a la probabilidad de que ésta se materializara sobre cada grupo de activos, teniendo en consideración lo siguiente:

1. Vulnerabilidades existentes (organizativas y técnicas).
2. Medio de tratamiento que soporta cada agrupación de activos (Sistemas informáticos/ofimáticos y papel).
3. Ubicación física de los datos (en instalaciones de GUIMARUBI o de terceros).
4. Encargados de tratamiento (medios de transferencia y controles establecidos).

Asimismo, se mostrará una tabla del estado de riesgo actual por cada activo de información en función de las amenazas:

ID	Categoría de activo	A1. Manipulación de las instalaciones imposibilitando el acceso			A2. Pérdida total o parcial de comunicaciones.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	1 - Bajo	Bajo	2 - Media	4 - Muy Alto	Alto
2	Auditoría	1 - Baja	1 - Bajo	Bajo	2 - Media	3 - Alto	Alto
3	Jurídico	1 - Baja	1 - Bajo	Bajo	2 - Media	3 - Alto	Alto
4	Gestión de clientes	1 - Baja	1 - Bajo	Bajo	2 - Media	4 - Muy Alto	Alto
5	Gestión de instalaciones	1 - Baja	1 - Bajo	Bajo	2 - Media	4 - Muy Alto	Alto
6	Gestión de productos	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
7	Gestión de proveedores	1 - Baja	1 - Bajo	Bajo	2 - Media	4 - Muy Alto	Alto
8	Gestión de RRHH	1 - Baja	1 - Bajo	Bajo	2 - Media	1 - Bajo	Bajo
9	Gestión del negocio	1 - Baja	1 - Bajo	Bajo	2 - Media	2 - Medio	Medio
10	Marketing y comunicación	1 - Baja	1 - Bajo	Bajo	2 - Media	1 - Bajo	Bajo
11	Seguridad alimentaria	1 - Baja	1 - Bajo	Bajo	2 - Media	1 - Bajo	Bajo
12	Seguridad corporativa	1 - Baja	3 - Alto	Medio	2 - Media	2 - Medio	Medio
13	Tesorería	1 - Baja	1 - Bajo	Bajo	2 - Media	1 - Bajo	Bajo
	PROMEDIOS	1 - Baja	1 - Bajo	1 - Bajo	2 - Media	3 - Alto	2 - Medio

Consideraciones respecto a las amenazas:

Afectación:	Afectación a procesos que requieren de acción presencial. Debido al entorno virtualizado, los procesos que no requieren ser ejecutados de forma presencial, se pueden llevar a cabo de forma remota.	Principalmente a la disponibilidad.
Probabilidad:	Por lo general, la probabilidad de que se materialice la amenaza es baja dado que la mayor parte de la información es digital y por tanto la afectación de esta amenaza. Sin embargo, se considera un poco más elevada para aquellos activos que tengan mayor soporte en papel o no se tenga clara la afectación a la operativa de una amenza de este tipo.	Se considera de forma general que la probabilidad es baja, pero se incrementa un nivel dado que no se disponen de controles y procesos de continuidad al 100%.
Impacto:	Por lo general, se baja el impacto dado que la mayor parte de la información está digitalizada y se dispone de copias de seguridad. Sin embargo, se mantiene como medio en aquellos activos que tengan mayor soporte en papel o no se tenga clara la afectación a la operativa de una amenza de este tipo.	Se fija el valor máximo de la dimensión de Disponibilidad.

ID	Categoría de activo	A3. Robo de activos físicos o información.			A4. Distribución de malware (p.ej.: virus).		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
2	Auditoría	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
3	Jurídico	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
4	Gestión de clientes	2 - Media	2 - Medio	Medio	1 - Baja	4 - Muy Alto	Medio
5	Gestión de instalaciones	1 - Baja	2 - Medio	Bajo	1 - Baja	4 - Muy Alto	Medio
6	Gestión de productos	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
7	Gestión de proveedores	1 - Baja	2 - Medio	Bajo	1 - Baja	4 - Muy Alto	Medio
8	Gestión de RRHH	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
9	Gestión del negocio	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
10	Marketing y comunicación	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
11	Seguridad alimentaria	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
12	Seguridad corporativa	2 - Media	2 - Medio	Medio	1 - Baja	2 - Medio	Bajo
13	Tesorería	2 - Media	2 - Medio	Medio	1 - Baja	2 - Medio	Bajo
	PROMEDIOS	2 - Media	3 - Alto	2 - Medio	1 - Baja	3 - Alto	2 - Medio

Consideraciones respecto a las amenazas:

Afectación:	Principalmente a la confidencialidad y a la reputación. No tenemos en cuenta afectación a la disponibilidad.	Igualmente a la Confidencialidad y Disponibilidad.
Probabilidad:	Se ajusta probabilidad en función de los datos que se consideran que pueden ser más susceptibles de ser robados por personal interno, proveedores o terceros.	La probabilidad de afectación por malware en general según buenas prácticas.
Impacto:	Se fija el valor máximo de la dimensión de Confidencialidad.	Se fija el valor máximo de la dimensión Disponibilidad o Confidencialidad

ID	Categoría de activo	A5. Daños o destrucción de equipos, material o información.			A6. Ataque de denegación de servicio (DoS).		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	4 - Muy Alto	Medio	1 - Baja	1 - Bajo	Bajo
2	Auditoría	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
3	Jurídico	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
4	Gestión de clientes	1 - Baja	4 - Muy Alto	Medio	1 - Baja	3 - Alto	Medio
5	Gestión de instalaciones	1 - Baja	4 - Muy Alto	Medio	1 - Baja	1 - Bajo	Bajo
6	Gestión de productos	1 - Baja	4 - Muy Alto	Medio	1 - Baja	3 - Alto	Medio
7	Gestión de proveedores	1 - Baja	4 - Muy Alto	Medio	1 - Baja	1 - Bajo	Bajo
8	Gestión de RRHH	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
9	Gestión del negocio	1 - Baja	2 - Medio	Bajo	1 - Baja	1 - Bajo	Bajo
10	Marketing y comunicación	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
11	Seguridad alimentaria	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
12	Seguridad corporativa	1 - Baja	2 - Medio	Bajo	1 - Baja	1 - Bajo	Bajo
13	Tesorería	1 - Baja	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
	PROMEDIOS	1 - Baja	2 - Medio	1 - Bajo	1 - Baja	1 - Bajo	1 - Bajo

Consideraciones respecto a las amenazas:

Afectación:	Principalmente a la disponibilidad de la información.	Principalmente a la disponibilidad de la información.
Probabilidad:	Comentar, ya que depende de las medidas de los cpd's, así como las locales para la información que sea susceptible de ser tratada en local. No tiene que haber nada en local.	Depende mucho de la visibilidad del activo. Por ello, el impacto es mayor a la información contenida en las webs por el daño a la imagen.
Impacto:	Se fija el valor máximo de la dimensión de Disponibilidad.	Depende mucho de la visibilidad del activo. Por ello se conserva el máximo valor de la dimensión de Disponibilidad, excepto para la información pública donde se eleva un nivel el riesgo por el tipo de información que puede incluir el portal privado.

ID	Categoría de activo	A7. Explotación de vulnerabilidades técnicas.			A8. Ataques de ingeniería social (p.ej.: *phishing*).		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
2	Auditoría	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
3	Jurídico	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
4	Gestión de clientes	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
5	Gestión de instalaciones	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
6	Gestión de productos	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
7	Gestión de proveedores	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
8	Gestión de RRHH	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
9	Gestión del negocio	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
10	Marketing y comunicación	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
11	Seguridad alimentaria	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
12	Seguridad corporativa	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
13	Tesorería	1 - Baja	4 - Muy Alto	Medio	1 - Baja	2 - Medio	Bajo
	PROMEDIOS	1 - Baja	4 - Muy Alto	2 - Medio	1 - Baja	3 - Alto	1 - Bajo

Consideraciones respecto a las amenazas:

Afectación:	Igualmente a Confidencialidad, Disponibilidad e Integridad. El máximo valor para todas, en función de su nivel de sensibilidad.	Principalmente a la confidencialidad.
Probabilidad:	A raíz de las revisiones técnicas realizadas y auditorías internas, se concluye que la mayoría de sistemas tienen vulnerabilidades medias-bajas.	Alta en general dado que afectaría a los archivos ofimáticos, y a todos aquellos con SSO, excepto documentos oficiales donde predomina el papel.
Impacto:	Al ser una vulnerabilidad general, se aplica el máximo nivel de sensibilidad marcado en alguna de las dimensiones del inventario de clasificación de la información, excepto en información pública que se sube por el tipo de información que puede incluir el portal privado.	Se fija el valor máximo de la dimensión de Confidencialidad.

ID	Categoría de activo	A9. Acceso no autorizado a sistemas corporativos.			A10. Filtración de información sensible de la organización.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
2	Auditoría	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
3	Jurídico	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
4	Gestión de clientes	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
5	Gestión de instalaciones	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
6	Gestión de productos	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
7	Gestión de proveedores	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
8	Gestión de RRHH	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
9	Gestión del negocio	1 - Baja	4 - Muy Alto	Medio	2 - Media	4 - Muy Alto	Alto
10	Marketing y comunicación	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
11	Seguridad alimentaria	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
12	Seguridad corporativa	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
13	Tesorería	1 - Baja	2 - Medio	Bajo	2 - Media	2 - Medio	Medio
	PROMEDIOS	1 - Baja	3 - Alto	1 - Bajo	2 - Media	3 - Alto	2 - Medio

Consideraciones respecto a las amenazas:

Afectación:	Principalmente a la confidencialidad.	Principalmente a la confidencialidad.
Probabilidad:	La probabilidad tendrá en cuenta el medio en el que se encuentra (papel más probable) y las políticas de los sistemas de información involucrados pero como amenaza es la que tiene que tener una probabilidad más alta. Hay buenas políticas de contraseñas, pero hay que mejorar los procesos de gestión de identidades (cambios depart...) ni segundos factores), riesgo ssoo.	La probabilidad en general es Media.
Impacto:	Se fija el valor máximo de la dimensión de Confidencialidad.	Se fija el valor máximo de la dimensión de Confidencialidad.

ID	Categoría de activo	A11. Utilización de los sistemas de la red corporativa con fines ilícitos.			A12. Concentraciones en el perímetro de las instalaciones.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	2 - Media	3 - Alto	Alto	1 - Baja	1 - Bajo	Bajo
2	Auditoría	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
3	Jurídico	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
4	Gestión de clientes	2 - Media	3 - Alto	Alto	1 - Baja	1 - Bajo	Bajo
5	Gestión de instalaciones	2 - Media	3 - Alto	Alto	1 - Baja	1 - Bajo	Bajo
6	Gestión de productos	2 - Media	3 - Alto	Alto	1 - Baja	4 - Muy Alto	Medio
7	Gestión de proveedores	2 - Media	3 - Alto	Alto	1 - Baja	1 - Bajo	Bajo
8	Gestión de RRHH	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
9	Gestión del negocio	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
10	Marketing y comunicación	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
11	Seguridad alimentaria	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
12	Seguridad corporativa	2 - Media	1 - Bajo	Bajo	1 - Baja	3 - Alto	Medio
13	Tesorería	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
	PROMEDIOS	2 - Media	2 - Medio	2 - Medio	1 - Baja	1 - Bajo	1 - Bajo

Consideraciones respecto a las amenazas:

Afectación:	Principalmente a disponibilidad.	Principalmente a disponibilidad.
Probabilidad:	Se considera que la probabilidad de materialización es media para todos los sistemas, dado que se ha observado en las auditorías que es posible utilizar herramientas de hacking.	La probabilidad por norma general de este tipo de acciones es baja.
Impacto:	Esta amenaza no afecta directamente a los activos de información ya que podría suponer un daño a la imagen de GUIMARUBI en caso de publicarse alguna noticia vinculado a dicho mal uso (descarga de contenido no adecuado…) si bien podría afectar al rendimiento de los activos. Bajamos nivel de disponibilidad 1 punto a todos los activos excepto para "información pública" que se mantiene por el tipo de información que puede incluir el portal privado.	Impacto muy leve porque la afectación sería sobre aquella información no accesible remotamente.

ID	Categoría de activo	A13. Hackeo de páginas web modificando el contenido (defacement).			A14. Publicación de información confidencial.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
2	Auditoría	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
3	Jurídico	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
4	Gestión de clientes	1 - Baja	3 - Alto	Medio	2 - Media	2 - Medio	Medio
5	Gestión de instalaciones	1 - Baja	0 - No aplica	No aplica	2 - Media	2 - Medio	Medio
6	Gestión de productos	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
7	Gestión de proveedores	1 - Baja	0 - No aplica	No aplica	2 - Media	2 - Medio	Medio
8	Gestión de RRHH	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
9	Gestión del negocio	1 - Baja	0 - No aplica	No aplica	2 - Media	4 - Muy Alto	Alto
10	Marketing y comunicación	1 - Baja	3 - Alto	Medio	2 - Media	2 - Medio	Medio
11	Seguridad alimentaria	1 - Baja	0 - No aplica	No aplica	2 - Media	2 - Medio	Medio
12	Seguridad corporativa	1 - Baja	0 - No aplica	No aplica	2 - Media	2 - Medio	Medio
13	Tesorería	1 - Baja	0 - No aplica	No aplica	2 - Media	2 - Medio	Medio
	PROMEDIOS	1 - Baja	1 - Bajo	1 - Bajo	2 - Media	3 - Alto	2 - Medio

Consideraciones respecto a las amenazas:

Afectación:	Principalmente a la integridad de las webs (1 activo).	Principalmente a la confidencialidad.
Probabilidad:	La probabilidad siempre existe aunque sea baja. Por ello se mantiene con valor BAJO para todos los activos excepto para la información pública. Para ésta, se fija un valor ALTO, dado que es muy probable que se dé (es fácil de realizar sin conocimientos expertos y adicionalmente cada vez es más frecuente el ataque a recursos públicos en Internet).	Probabilidad media de forma global
Impacto:	Por lo general, impacto con valor BAJO para todos los activos excepto para la información pública por el tipo de información que puede incluir el portal privado.	Se fija el valor máximo de la dimensión de Confidencialidad, a excepción de la información pública que por tanto no es confidencial.

ID	Categoría de activo	A15. Fallo técnico o humano.			A16. Dependencia total o parcial de proveedores o terceras partes.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
2	Auditoría	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
3	Jurídico	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
4	Gestión de clientes	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
5	Gestión de instalaciones	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
6	Gestión de productos	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
7	Gestión de proveedores	2 - Media	4 - Muy Alto	Alto	1 - Baja	4 - Muy Alto	Medio
8	Gestión de RRHH	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
9	Gestión del negocio	2 - Media	2 - Medio	Medio	1 - Baja	2 - Medio	Bajo
10	Marketing y comunicación	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
11	Seguridad alimentaria	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
12	Seguridad corporativa	2 - Media	2 - Medio	Medio	1 - Baja	2 - Medio	Bajo
13	Tesorería	2 - Media	1 - Bajo	Bajo	1 - Baja	1 - Bajo	Bajo
	PROMEDIOS	2 - Media	2 - Medio	2 - Medio	1 - Baja	2 - Medio	1 - Bajo

Consideraciones respecto a las amenazas:

Afectación:	Igualmente a Confidencialidad, Disponibilidad e Integridad. El máximo valor para todas.	Igualmente a Confidencialidad, Disponibilidad e Integridad. El máximo valor para todas.
Probabilidad:	Probabilidad media de forma global	Todos los activos dependen de proveedores
Impacto:	Depende mucho de la visibilidad del activo. Por ello se conserva el máximo valor de la dimensión de Disponibilidad.	Depende mucho de la visibilidad del activo. Por ello se conserva el máximo valor de la dimensión de Disponibilidad

ID	Categoría de activo	A17. Incumplimiento de la política de seguridad interna, las normas, procedimientos y legislación aplicable.			A18. Desconocimiento de la política de seguridad interna, normas, procedimientos y legislación aplicable.		
		PROBABILIDAD	IMPACTO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO
1	Análisis del negocio	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
2	Auditoría	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
3	Jurídico	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
4	Gestión de clientes	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
5	Gestión de instalaciones	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
6	Gestión de productos	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
7	Gestión de proveedores	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
8	Gestión de RRHH	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
9	Gestión del negocio	1 - Baja	4 - Muy Alto	Medio	1 - Baja	4 - Muy Alto	Medio
10	Marketing y comunicación	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
11	Seguridad alimentaria	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
12	Seguridad corporativa	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
13	Tesorería	1 - Baja	2 - Medio	Bajo	1 - Baja	2 - Medio	Bajo
	PROMEDIOS	1 - Baja	3 - Alto	1 - Bajo	1 - Baja	3 - Alto	1 - Bajo

Consideraciones respecto a las amenazas:

Afectación:	El no cumplimiento de las políticas no debería suponer un impacto muy elevado ya que deben establecerse los mecanismos que minimicen la dependencia de los mismos de los usuarios. Aun así, hay información que es muy susceptible de que tenga pérdidas de confidencialidad en función de los sistemas empleados. Por ello, lo vinculamos a confidencialidad.	Ídem que la anterior.
Probabilidad:	Baja	Ídem que la anterior, la diferencia de riesgo la determinará la probabilidad. Ídem que anterior.
Impacto:	Se fija el valor máximo de la dimensión de Disponibilidad	Ídem que la anterior.

Se incluye el resumen de las tablas anteriores de "Estado de riesgo", donde se han agrupado finalmente algunas de las amenazas inicialmente definidas y se ha identificado el nivel de riesgo final para cada categoría de activos.

Listado de amenazas (ordenadas de mayor a menor riesgo):

ID	AMENAZAS	RIESGO	PROBABILIDAD	IMPACTO
A10	Filtración de información sensible de la organización.	**5,8**	2,0	2,9
A14	Publicación de información confidencial.	**5,8**	2,0	2,9
A02	Pérdida total o parcial de comunicaciones.	**5,2**	2,0	2,6
A15	Fallo técnico o humano.	**4,6**	2,0	2,3
A03	Robo de activos físicos o información.	**4,4**	1,5	2,9
A07	Explotación de vulnerabilidades técnicas.	**4,0**	1,0	4,0
A11	Utilización de los sistemas de la red corporativa con fines ilícitos.	**3,6**	2,0	1,8
A04	Distribución de malware (p.ej.: virus).	**3,4**	1,0	3,4
A08	Ataques de ingeniería social (p.ej.: *phishing*)	**2,9**	1,0	2,9
A09	Acceso no autorizado a sistemas corporativos.	**2,9**	1,0	2,9
A17	Incumplimiento de la política de seguridad interna, las normas, procedimientos y legislación aplicable.	**2,9**	1,0	2,9
A18	Desconocimiento de la política de seguridad interna, normas, procedimientos y legislación aplicable.	**2,9**	1,0	2,9
A05	Daños o destrucción de equipos, material o información.	**2,3**	1,0	2,3
A16	Dependencia total o parcial de proveedores o terceras partes.	**2,3**	1,0	2,3
A01	Manipulación de las instalaciones imposibilitando el acceso	**1,4**	1,0	1,4
A12	Concentraciones en el perímetro de las instalaciones.	**1,4**	1,0	1,4
A06	Ataque de denegación de servicio (DoS).	**1,3**	1,0	1,3
A13	*Hackeo* de páginas web modificando el contenido (*defacement*).	**0,5**	1,0	0,5

Listado de activos (ordenados de mayor a menor riesgo promedio):

ID	ACTIVOS	RIESGO PROMEDIO
6	**Gestión de productos**	5
1	**Análisis del negocio**	4
4	**Gestión de clientes**	3
9	**Gestión del negocio**	3
2	**Auditoría**	3
3	**Jurídico**	3
5	**Gestión de instalaciones**	3
7	**Gestión de proveedores**	3
8	**Gestión de RRHH**	3
12	**Seguridad corporativa**	2
10	**Marketing y comunicación**	2
13	**Tesorería**	2
11	**Seguridad alimentaria**	2

A modo resumen, se puede ver de una manera más visual el análisis expuesto anteriormente en este apartado:

Figura 38: Resultado del AARR en función de las amenazas y activos

El mapa de riesgos resultante el análisis realizado sería el siguiente:

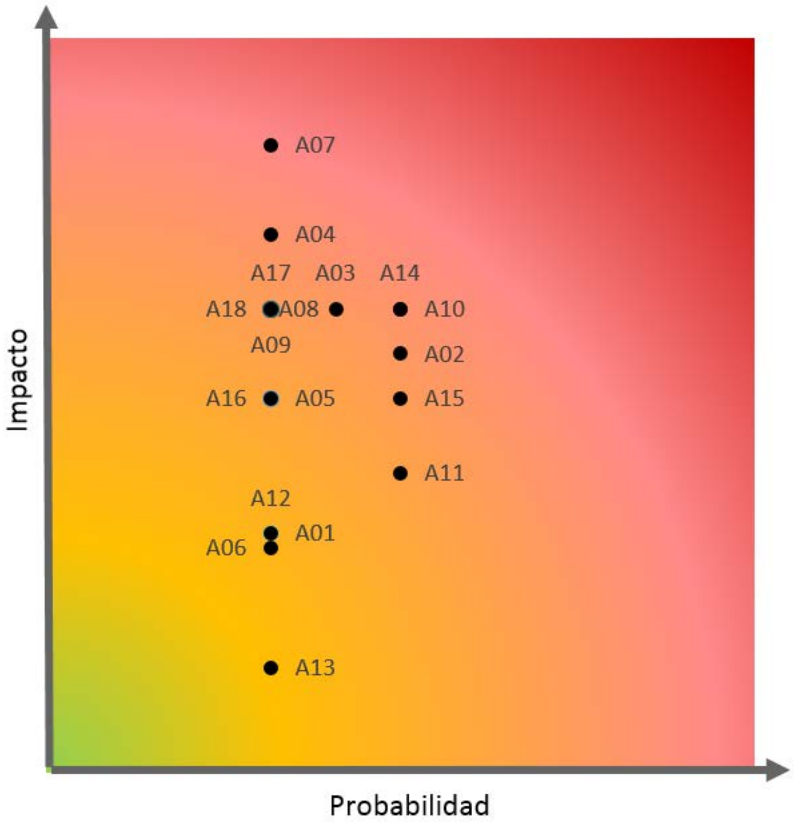


Figura 39: Resultado del AARR en un mapa de calor

8.2.1.2 Medidas y controles

Objetivo:

- A partir de los riesgos identificados, identificar medidas y controles que permitan reducir dichos riesgos cubriendo de manera total o parcial las vulnerabilidades relacionadas.
- Identificar la contribución a la reducción del riesgo de cada una de las medidas y controles propuestos.
- Realizar una estimación de costes de cada una de las medidas, obteniendo una priorización de medidas en base al criterio coste vs reducción riesgo.

A partir de los riesgos identificados, se ha realizado un inventario de medidas para cubrir estos riesgos y las vulnerabilidades que potencialmente pueden ser utilizadas por las amenazas.

Mediante la realización de talleres con el equipo de proyecto mixto, y la participación de expertos en el ámbito que se requiera, se han analizado y seleccionado las medidas y controles más adecuadas para cada uno de los riesgos, evitando medidas solapadas e identificando sinergias entre riesgos de diferentes activos de información.

Se ha determinado, de manera cualitativa, en qué grado cada medida o control contribuye a la reducción del riesgo y actuando sobre alguna de sus vulnerabilidades. De esta manera se obtendrá un valor cualitativo global por medida.

Siguiendo el criterio de proporcionalidad coste vs reducción del riesgo (beneficio), se ha obtenido un parámetro de prioridad por medida que permitirá ordenar las medidas en términos de importancia teniendo en cuenta el coste asociado.

8.2.1.3 Gestión del riesgo e indicadores

Objetivo:

- Asesoramiento en el entendimiento y toma de decisiones para el tratamiento de los riesgos. De acuerdo a criterios de proporcionalidad, decidir umbrales de riesgos y desarrollar la estrategia para el tratamiento y gestión de riesgos obtenidos, identificando acciones correctivas necesarias para su tratamiento.
- Identificación de indicadores por medidas y riesgos para realizar el seguimiento del estado del riesgo y su evolución en función de la implantación de proyectos.

Durante esta fase se ha establecido el Nivel de Riesgo Aceptable resultante del equilibrio entre el coste de seguridad (coste de las medidas de medidas de Seguridad de la Información) y el coste del riesgo (coste o impacto que tendría si el riesgo se hiciera realidad).

Se han clasificado los niveles de riesgos identificados de acuerdo a niveles o requerimientos legislativos/normativos. A partir de los resultados de la Evaluación de Riesgos de Seguridad de la Información y teniendo en cuenta el Nivel de Riesgo Aceptable establecido, se ha decidido el tratamiento o gestión que se realizará de los riesgos.

Adicionalmente se han identificado indicadores para los diferentes riesgos para evaluar la reducción real del riesgo mediante la implementación de las medidas identificadas. En el caso de riesgos aceptados, indicadores de riesgo para monitorizar que los riesgos se mantienen en niveles aceptables.

Finalmente se han simulado los niveles de riesgo con la situación futura de implementación de medidas, así como la utilización de los indicadores para realizar un seguimiento continuo de la evolución de los riesgos de acuerdo a la implantación de las medidas.

8.2.2 Definición situación objetivo

8.2.2.1 Modelo organizativo de seguridad y objetivos

Objetivos:

- Realizar una propuesta de modelo organizativo, de relación y dimensionamiento para dar cobertura a las necesidades identificadas en fases anteriores de manera sostenible.
- Establecer los objetivos de seguridad de la organización, de acuerdo al resultado del análisis y gestión del riesgo cubriendo los diferentes niveles organizativos (estratégico, táctico y operativo).

Durante el transcurso de esta fase, a partir de las revisiones organizativas y técnicas se ha definido un modelo organizativo de seguridad recogiendo:

- Una propuesta de funciones y estructura jerárquica en materia de seguridad de la información, teniendo en cuenta, que la seguridad de la Información es una responsabilidad organizativa que deberá ser compartida por todos los miembros.
- Se han dimensionado de los diferentes miembros y recursos necesarios para realizar las funciones y procesos de seguridad así como se han definido las responsabilidades en relación a la planificación, implantación y monitorización de las medidas de seguridad como respuesta a una estrategia de gestión de riesgos.
- Se han hecho recomendaciones acerca de la estructura de comités de seguridad de la información como parte del proceso de gestión y gobierno de la seguridad garantizando que los riesgos se tratan adecuadamente.
- Se ha definido el modelo de relación de la función de seguridad con otras áreas internas y entidades externas.

Se han definido los objetivos de seguridad de acuerdo a la gestión de riesgos de seguridad y cumplimiento normativo y regulatorio. Identificando la viabilidad de los objetivos, de acuerdo al coste de inversión, así como establecer períodos de consecución progresiva de objetivos (objetivos a corto, medio y largo plazo).

Se ha establecido la relación entre los objetivos definidos y los indicadores de riesgo identificados en la fase anterior así como la relación de las medidas definidas con los objetivos de la Organización, agrupándolos en los distintos períodos (corto, medio, largo) y por ámbito estratégico, táctico y operativo, incluyendo, de manera ilustrativa:

- Aspectos normativos y de organización de la seguridad.
- Procesos operativos de seguridad tecnológica.
- Soluciones técnicas y arquitectura de seguridad.
- Seguridad funcional en el desarrollo de nuevos sistemas.
- Funciones de seguimiento, control y monitorización de la seguridad.
- Estrategia, comunicación y reporting.

8.2.2.2 Arquitectura técnica de seguridad:

Objetivos:

- Ubicar y conceptualizar las medidas de seguridad en respuesta a la gestión de los riesgos en la arquitectura técnica actual de la Organización.
- Revisar y proponer mejoras de diseño de la arquitectura técnica de seguridad que responda a los objetivos y modelo de seguridad, así como a la eficiencia y la viabilidad con el entorno actual de la compañía.

Durante esta fase se han identificado las medidas a incorporar en la arquitectura técnica actual teniendo en cuenta las diferentes fases de despliegue.

Se ha diseñado la arquitectura técnica futura teniendo en cuenta:

- Identificación de sinergias entre diferentes recursos tecnológicos.
- Identificación de problemas o retos de integración de medidas en la arquitectura y establecimiento de planes alternativos. En caso necesario, reanalizar la viabilidad de la medida y redefinir el plan de gestión del riesgo de fases anteriores.
- Ubicar en la arquitectura aquellos elementos que formen parte de la seguridad perimetral e interna de la red (por ej. IDS, FWs) así como soluciones / servicios que proporcionen servicios de seguridad (por ej. Soluciones DLP, E-DRM...).
- En la medida de lo posible, también se representaran los controles de carácter normativo que tengan implicaciones en la arquitectura técnica (por ej. “Limitación a 2 saltos” implica la restricción o migración de ciertas zonas de seguridad).

8.2.2.3 Validación y alineación con la estrategia del negocio

Objetivos:

- Determinar los criterios para alinear los riesgos de seguridad con negocio e incorporar los riesgos clasificados como parte del universo de riesgos de negocio.
- Definir y establecer indicadores de riesgos que puedan ser útiles para la gestión de riesgos de negocio.
- Determinar los criterios para determinar de manera clara aquellos riesgos relevantes para la Dirección desde el punto de vista de negocio.

Durante esta fase se han identificado los riesgos que suponen una relevancia elevada para negocio y deban ser escalados a la dirección, como por ejemplo:

i. Riesgos con valores muy elevados.
ii. Riesgos con impactos muy relevantes para negocio desde el punto de vista económico.
iii. Riesgos con impacto de imagen severo.
iv. Riesgos que en caso de materializarse, relevancia Penal Alta involucrando a la dirección.
v. Riesgos que en caso de materializarse, impactará en los mercados.

De acuerdo a los riesgos o grupo de riesgos integrados con negocio, se han definido indicadores de riesgo así como los mecanismos para que puedan ser medidos y comunicados al área encargada de la gestión de los riesgos de negocio

Se han realizado sesiones específicas de trabajo con el personal encargado de la gestión de riesgos de negocio para alinear criterios y metodologías de trabajo.

8.2.2.4 GAP e identificación de iniciativas

Objetivos:

- A partir del modelo de seguridad objetivo, y considerando la arquitectura técnica objetivo, identificar las iniciativas necesarias para alcanzar dichos modelos respecto la situación actual de la Organización en los plazos establecidos.
- Disponer las iniciativas en agrupaciones de proyectos, aprovechando sinergias que se puedan identificar.
- Simular los diferentes escenarios de riesgo de acuerdo al despliegue de las iniciativas.

Durante esta fase se ha hecho una representación comparativa (GAP) entre la situación actual de la organización respecto el modelo de seguridad objetivo, la arquitectura técnica y el cumplimiento normativo y regulatorio.

Mediante la realización de talleres con los equipos de proyecto, se han identificado iniciativas que permitan desplegar las medidas y controles de seguridad para cubrir el GAP entre la situación actual y la objetivo en los plazos establecidos en el modelo de seguridad.

Se han relacionado las diferentes iniciativas identificadas con los riesgos de la Organización así como con los indicadores de riesgo previamente definidos.

Se han definido diferentes escenarios de implantación de iniciativas identificadas, realizando simulaciones de evolución del riesgo respecto a la situación actual. Mediante estas simulaciones se ha revisado el cumplimiento del modelo objetivo y los objetivos de seguridad.

Por lo que concierne al análisis GAP realizado, se exponen los hechos detectados más significativos.

1. **En el análisis de seguridad de los websites corporativos:**

- Se ha conseguido acceso (lectura, modificación y eliminación) a la base datos de clientes reales de GUIMARUBI CASH
- Se han obtenido todos los usuarios y sus contraseñas de los portales web.
- Se ha detectado el uso de protocolos de comunicación que no garantizan la confidencialidad

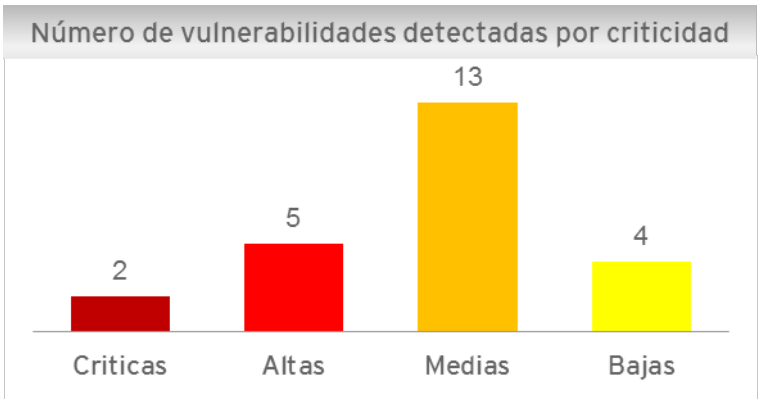


Figura 40: Número de vulnerabilidades detectadas.

Las principales causas raíz de las debilidades identificadas son las siguientes:

i. Falta de actualización y parcheado de los sistemas de información.
ii. No homogeneización del nivel de seguridad de los sistemas de información (p.e. externalizados).
iii. Ausencia de controles que garanticen la seguridad de las aplicaciones web desarrolladas.
iv. Uso de canales de comunicación no seguros (sin cifrar).

2. Análisis de seguridad de la red interna

Hechos detectados más significativos:

- Se ha conseguido el acceso y control de múltiples dispositivos de video vigilancia.
- Desde un CASH, se ha podido acceder a los servidores alojados en los *Data Center* corporativos.
- Se ha identificado software obsoleto, actualmente sin soporte del fabricante.
- Se ha detectado el uso de protocolos de comunicación que no garantizan la confidencialidad.
- Mediante ingeniería social, se ha conseguido obtener múltiples usuarios y contraseñas de empleados.
- Se ha obtenido la mayoría de usuarios y sus contraseñas, y por tanto el control total de la red interna de la Compañía.

Principales causas raíz de las debilidades identificadas:

i. Falta de actualización y parcheado de los sistemas de información.
ii. No homogeneización del nivel de seguridad de los sistemas de información.
iii. Ausencia de controles que garanticen segregación interna de la red (oficinas-CASH).
iv. Falta de integración de la seguridad en la homologación de software y hardware.
v. Falta de concienciación en la seguridad de la información.

3. Análisis de seguridad del entorno SAP

Hechos detectados más significativos:

- Se han detectado 17 usuarios con máximos permisos de acceso (SAP_ALL) y otros 118 con elevados permisos de acceso (ZSAP_ALL y ZSAP_ALL_NEW).
- Se han detectado debilidades en la política de contraseñas (no se obliga al cambio periódico y permite contraseñas poco complejas).

- Se han identificado 74 usuarios que no acceden en los últimos 6 meses.
- El 90% de los usuarios existentes tienen conflictos de acceso en cuanto a la segregación de funciones.
- El 30% de los roles definidos tienen conflictos de acceso en cuanto a la segregación de funciones.

Principales causas raíz de las debilidades identificadas:

i. Ausencia de controles que garanticen el cumplimiento de la normativa existente relativa Alta / Baja / C.
ii. Falta procedimientos para la revisión periódica de usuarios y permisos asignados.
iii. Debilidades en la configuración de seguridad de la plataforma SAP.
iv. Inadecuada gestión de permisos de accesos a usuarios y roles, que no garantiza una correcta segregación de funciones (potenciales riesgos para el negocio).

4. Análisis GAP ISO/IEC 27002

En la siguiente figura se detalla el estado de cumplimiento actual en función de los dominios de control de la ISO/IEC 27002:2013, conjuntamente con los niveles de madurez estipulados según el CMMI y las características de los controles de seguridad.

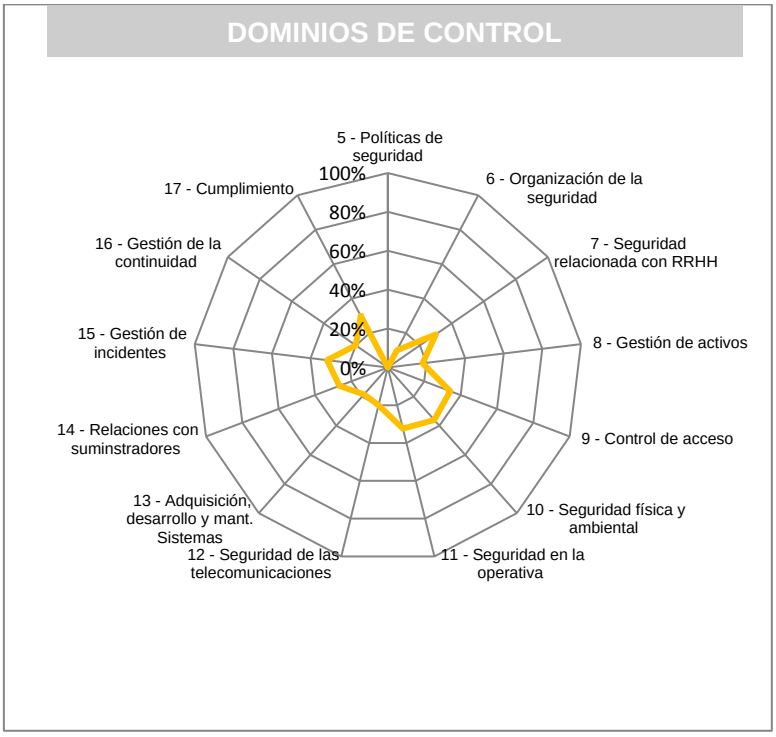


Figura 41: Situación actual de cumplimiento

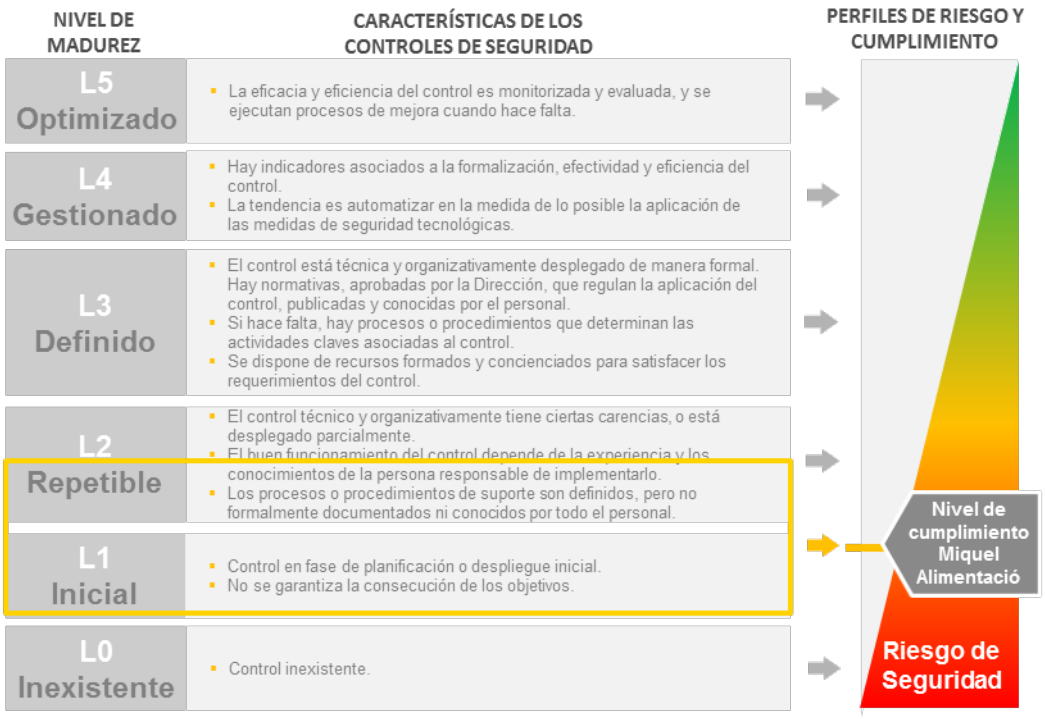


Figura 42: Nivel de amdurez actual

Las principales debilidades adicionales identificadas a las comentadas anteriormente son las siguientes:

i. Faltan políticas, normativas y procedimientos que regulen la mayor parte de los dominios de la ISO.
ii. No se ha definido un marco de control homogéneo para el control y la supervisión de los proveedores.
iii. Ausencia de controles para una adecuada monitorización, gestión e identificación de incidentes de seguridad.

No obstante a las debilidades identificadas, a continuación se exponen las fortalezas más significativas encontradas:

1. *La* infraestructura tecnológica, que da soporte a la operativa diaria del negocio, dispone de alta disponibilidad, para minimizar impactos en caso de contingencia o desastre.
2. Todas las conexiones de los usuarios con las aplicaciones informáticas que soportan los procesos de negocio, se realizan por canales de comunicación seguros (CITRIX).
3. Se dispone de una estructura organizativa y procedimientos que permiten gestionar de una forma adecuada la gestión de incidencias (*SAI+Service Desk + Help Desk*)
4. Se han definido y asignado algunas responsabilidades en materia de seguridad de la información: Comité LOPD/RGPD e IT *Security* (dentro del área de Sistemas de Información).
5. Existen múltiples controles de seguridad física que dificultan el acceso no autorizado tanto a los Data Centers corporativo como a las propias instalaciones de trabajo.

8.3 Plan Director de la Seguridad de la Información

8.3.1 Estudio de viabilidad

Objetivos:

- Identificar las necesidades para alcanzar el modelo objetivo de la seguridad de la información y analizar la viabilidad de su implantación.
- Obtener un estudio de viabilidad de las iniciativas que componen el Plan de Necesidades, tanto a nivel individual como en conjunto, permitiendo agrupación definición y priorización de las incitativas en diferentes proyectos.

Teniendo en cuenta la situación actual y el análisis de riesgos realizado en las fases anteriores, en base a la situación objetivo a la que se quiere dirigirse la corporación, se elaborará el Plan de necesidades y el estudio de viabilidad de las mismas, para ello se han realizado las siguientes actividades:

1. Estudio de viabilidad de cada una de las iniciativas o grupos de iniciativas identificadas, se han analizado exhaustivamente – como mínimo – los siguientes aspectos:
    - **Efectos sobre el riesgo:** reducción del impacto o probabilidad de las amenazas según el caso, vulnerabilidades, posibles impactos, etc).
    - **Tiempos y plazos de ejecución estimada:** estimación de la implementación y despliegue de las medidas identificadas.
    - **Recursos humanos:** Valorar en FTEs los recursos necesarios para la implementación de las medidas.
    - **Modelo de costes:** lo más exacto posible, ya sea esté por gasto y/o inversión.
    - **Dependencias con otras iniciativas y o grupos de iniciativas inidentificadas.**
    - **Indicadores de seguimiento.**
2. Aprobación por parte del comité de seguridad y por la dirección del proyecto del Estudio de Viabilidad, en base a los efectos sobre la mitigación de los riesgos, requerimientos de negocio y tecnológico a corto, medio y largo plazo y las expectativas de a seguridad.

8.3.2 Plan de Proyectos

Objetivos:

- Definir el plan de proyectos de seguridad, no sólo de manera individual sino de manera conjunta, definiendo la hoja de ruta que permita implantar de forma ordenada las acciones e incitativas identificadas, estableciendo las dependencias con otras acciones o proyectos.
- Definir detalladamente las acciones a realizar en cada uno de los proyectos, así como la planificación, recursos, riegos, dependencias y presupuesto de ejecución e implementación.

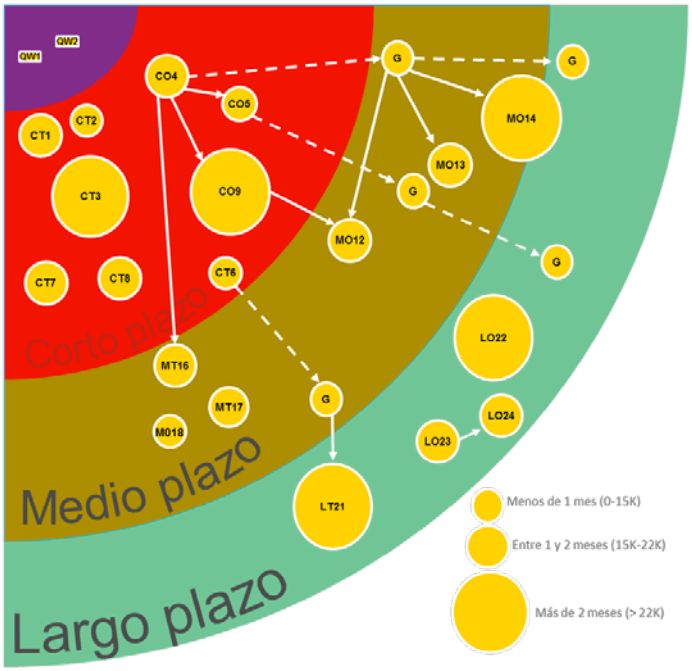
Durante esta fase se ha definido la hoja de ruta para la implantación de los proyectos, estableciendo las precedencias y dependencias entre proyectos.

Se ha hecho una priorización de los proyectos a corto, medio y largo plazo, teniendo en cuenta las dependencias identificas entre el resto de proyectos que componen el Plan Director de Seguridad de la Información.

Se ha definido detalladamente cada uno de los proyectos teniendo en cuenta los siguientes aspectos:

- Antecedentes y objetivos.
- Alcance con una descripción detallada de la tarea.
- Estimación de tiempos y plazos de implementación y ejecución.
- Modelo de costes, lo más exacto posible, teniendo en cuenta los gastos y/o inversión, ya sean o no recurrentes, incluyendo:
  - Costes estimados del proyecto tecnológico y perfil de los proveedores que lo podrán realizar.
  - Costes estimados de la colaboración externa para implantar la acción y perfil de los proveedores que podrían prestar esta colaboración.
  - Costes internos estimados (en horas).
- Análisis coste beneficio indicando su efecto sobre los riesgos identificados.
- Dependencias de otros proyectos.
- Requisitos de implementación.
- Indicadores que se estiman que mejoraran una vez implementada la acción.

La siguiente figura muestra el Plan de proyectos realizado para GUIMARUBI, teniendo en cuenta el trabajo realizado en las fases anteriores, que se ha incorporado en el siguiente plan, el cual incluye los dominios y controles de la ISO extraídos del análisis GAP y el coste estimado (tanto temporal como económico).



QW1	Definición de la política de seguridad corporativa	2.6K
QW2	Definición y divulgación de la organización de la seguridad.	2.6K
CT1	Resolución de las vulnerabilidades más significativas identificadas durante el PDS	20.8K
CT2	Securizar entornos web	27.5K
CT3	Securizar entornos CASH (52 centros)	262K
CO4	*(G). Desarrollo de normativa y procedimientos de seguridad*	*20.8K*
CO5	*(G). Programa de concienciación de seguridad de la información*	*10.4K*
CT6	*(G). Auditorías técnicas de seguridad*	*10.4K*
CT7	Implementación arquitectura doble capa (firewall entre perimetral e interna)	20.8K
CT8	Revisión y mejora del proceso de parcheado.	20.8K
CO9	Rediseño de roles para una segregación de funciones en SAP	70K
MO12	Definición de los procesos de gestión de identidades	20.8K
MO13	Diseño del marco de control relativo a servicios IT externalizados.	20.8K
MO14	Inventariado de activos y clasificación de la información.	31.2K
MT16	Definición de guías de bastionado de sistemas de información	20.8K
MT17	Integrar la seguridad en la homologación de soft/hard.	20.8K
MO18	Gestión de cuentas privilegiadas	10.4K
LT21	Despliegue de un servicio de seguridad gestionada (SIEM / SOC)	31.2K
LO22	Plan de continuidad de negocio	41.6K
LO23	Cuadro de mandos de seguridad	20.8K
LO24	Sistema de gestión de la seguridad de la información	20.8K

Figura 43: Plan de proyectos

Este Plan de proyectos se ha separado en 5 partes, aquellos proyectos que pueden realizarse de manera inmediata (*QuickWins*), de manera gradual, a corto plazo, a medio plazo y a largo plazo. El Plan de Proyectos puede verse en el apartado 13 Anexos.

9 Planificación, tiempo y coste

El proyecto se asignó a EY a principios de Diciembre de 2017 pero no se inició hasta principios de Enero de 2018. El presente proyecto se ha realizado en horario laboral, empleando de media 40 horas semanales aproximadamente, no obstante, algunas semanas se han realizado horas extras. Cabe destacar que durante semana santa no se realizaron actividades algunas debido a que eran vacaciones.

La duración del proyecto ha tomado 24 semanas reales, a una media de 40h por semana, sin tener en cuenta la Semana Santa ni la fase de Evaluación de Seguridad Técnica (que como se ha comentado anteriormente ha sido realizada por otro equipo) se han empleado un **total de 800h**.

El detalle de las semanas empleadas para la realización de este proyecto se puede ver reflejado en el siguiente cronograma (separado en dos en semana santa –columna gris-):

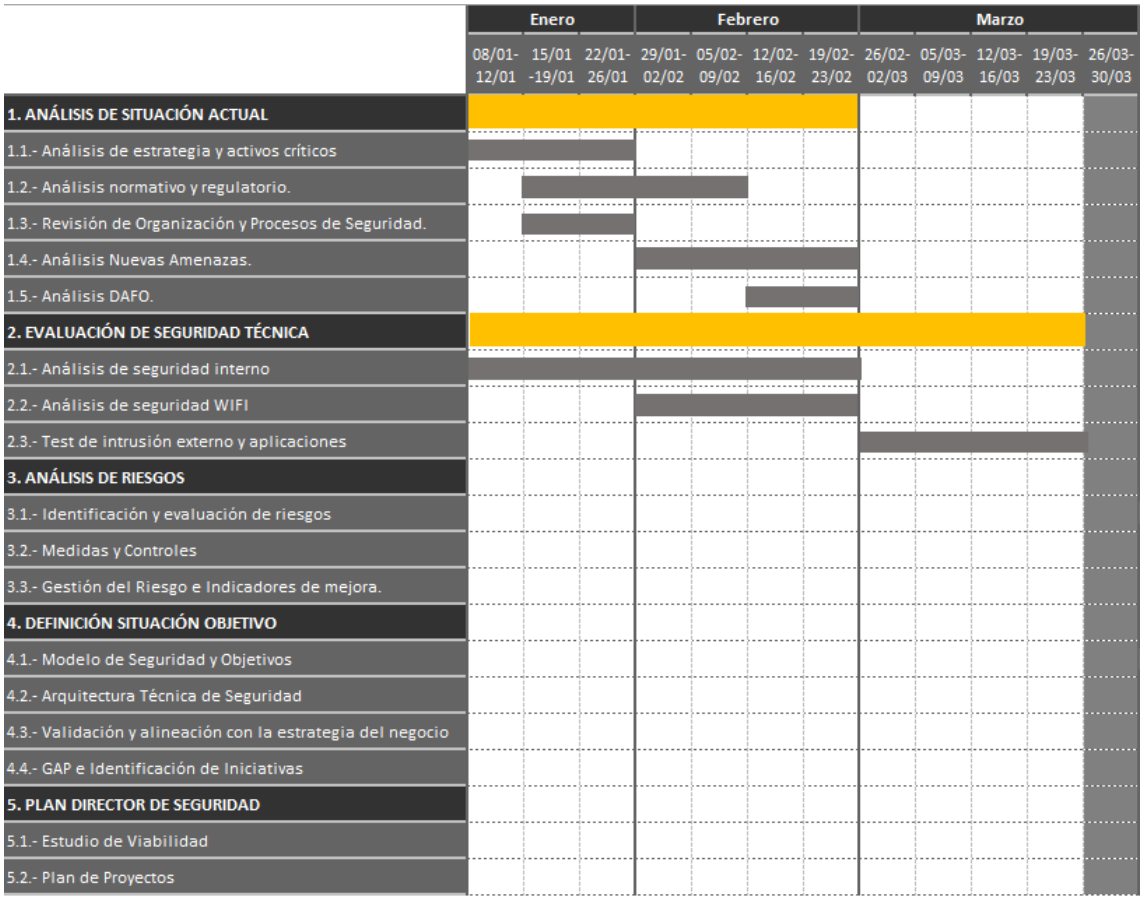


Figura 44: Estimación del coste en horas Enero-Marzo

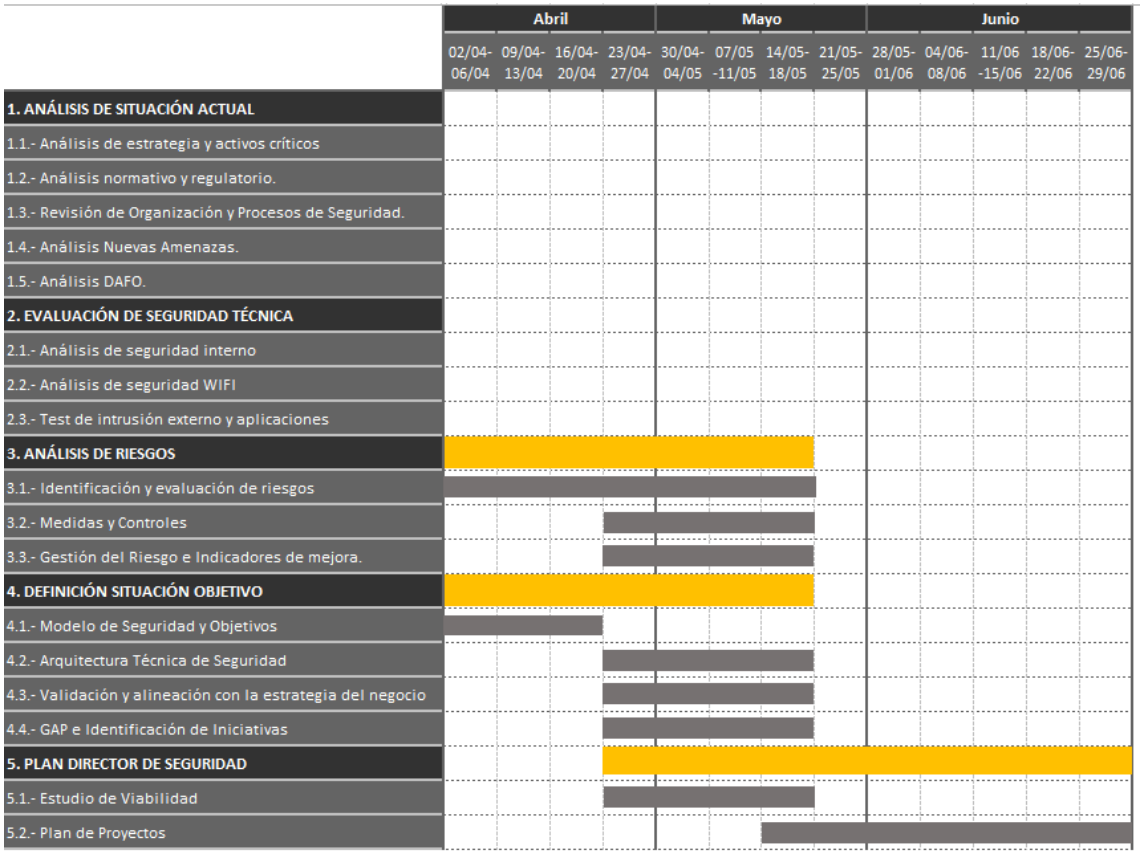


Figura 45: Estimación del coste en horas Abril-Junio

10 Conclusiones

El trabajo realizado ha servido para definir un Plan Director de Seguridad alineado con la estrategia de la compañía y con las mejores prácticas de seguridad. A día de hoy la compañía cuenta con un plan de futuro (a 3 años vista) definido, que ha permitido observar los proyectos de mejora posibles en cada una de las áreas implicadas y de esta manera prever los gastos necesarios para los próximos años. La compañía ha agregado este plan como parte de su plan estratégico y de sistemas.

El propósito principal de la realización de este proyecto ha sido el análisis de riesgos para poder identificar todos aquellos *gaps* que la compañía tenía en comparación con las mejores prácticas de seguridad para posteriormente solucionar las carencias que tiene la empresa.

Previamente al análisis de riesgos, se realizó un inventario de activos críticos en términos de seguridad, el cual ha permitido a la organización tener una visión global de aquellos activos que son más críticos para su negocio y poder actualizar su plan estratégico en función de éstos.

Por otra parte, el análisis de riesgo ha permitido a la compañía tener una consciencia sobre las posibles vulnerabilidades y amenazas existentes y el grado de riesgo que éstas conllevan en caso de materializarse en los activos más críticos. De esta manera la organización tiene una foto clara de los riesgos más significativos a los que se enfrenta. No obstante, el análisis del presente documento expone los riesgos objetivos identificados pero, es la compañía quién, al final, selecciona aquellos riesgos que desea asumir y cuales desea mitigar, valorando de manera subjetiva los costes asociados a cada riesgo.

Adicionalmente, el plan de mitigación de los riesgos hallados (Plan Director de Seguridad), incluye todos aquellos proyectos que han resultado alineados con el plan estratégico de la compañía. Cabe destacar que no se prevé realizar algunos proyectos ya que la compañía pretende asumir algunos riesgos sobre ciertos activos y por ende, se prevé realizar aquellos proyectos indicados en el apartado 9.2.

Además del censo de proyectos a realizar, el presente trabajo ha permitido dar una visión integrada de los procesos de seguridad de la compañía, tanto a nivel tecnológico como a nivel organizativo. Es habitual que los departamentos estén segmentados por cada una de las áreas de responsabilidad de cada uno pero, con este proyecto, se ha conseguido unificar a todos los departamentos implicados para trazar un Plan Director de Seguridad para los próximos años.

A día de hoy, la compañía ha iniciado la implementación de alguno de los proyectos detallados en capítulos anteriores y se está manteniendo la planificación detallada en el apartado 9.2.

11 Líneas de futuro

Existen dos líneas de futuro significativamente definidas, una de ellas, en relación con el nuevo Reglamento Europeo de Protección de Datos 2016/679 (10) y otra con la implementación de los proyectos definidos en el Plan Director de Seguridad.

11.1 RGPD

La nueva norma de privacidad del parlamento europeo que entró en vigor el pasado 25 de mayo de 2018, tiene una implicación muy elevada a nivel de protección de datos a nivel técnico, por esta razón, es importante alinear el Plan Director de Seguridad con dicha norma y asegurarse que se cumplen todos los requisitos, tanto legales como técnicos, teniendo en cuenta los diferentes proyectos tecnológicos que pueden surgir del proceso de adecuación a la RGPD, para con ello, incorporarlos al Plan Director de Seguridad.

Asimismo, se deberá realizar un análisis de riesgos como el ejecutado en el presente documento pero enfocado a los requerimientos del RGPD, enfocado a privacidad, teniendo en cuenta tanto controles tecnológicos como los vistos en este proyecto como controles legales y de privacidad.

11.2 Ejecución de proyectos identificados

Los proyectos incluidos en el alcance son aquellos definidos en el Plan de proyectos anterior que no han sido abordados a día de hoy y que la compañía pretende abordar. Dichos proyectos, de entre todos los enumerados anteriormente son los siguientes:

QUICKWINS Acciones inmediatas	CORTO PLAZO 0 meses – 12 meses	MEDIO PLAZO 12 meses – 24 meses	LARGO PLAZO 24 meses – 36 meses
QW1. Definición de la política de seguridad corporativa	CT1. Resolución de las vulnerabilidades más significativas identificadas durante el PDS	*MO10 (G). Programa de concienciación de seguridad de la información*	*LO19 (G). Programa de concienciación de seguridad de la información*
	CT2. Securizar entornos web	*MO11 (G). Desarrollo de normativa y procedimientos de seguridad*	*LO20 (G). Desarrollo de normativa y procedimientos de seguridad*
	CT3. Securizar entornos CASH (52 centros)	MO12. Definición de los procesos de gestión de identidades	LT21. Despliegue de un servicio de seguridad gestionada (SIEM / SOC)
	CO4 (G). Desarrollo de normativa y procedimientos de seguridad	MO13. Diseño del marco de control relativo a servicios IT externalizados.	
	CO5 (G). Programa de concienciación de seguridad de la información	MO14. Inventariado de activos y clasificación de la información.	LO22. Plan de continuidad de negocio
	CT6 (G). Auditorias técnicas de seguridad	*MT15 (G). Auditorias técnicas de seguridad*	
	CT7. Implementación arquitectura doble capa (firewall entre perimetral e interna)	MT16. Definición de guías de bastionado de sistemas de información	
QW2. Definición y divulgación de la organización de la seguridad.	CT8. Revisión y mejora del proceso de parcheado.	MO17. Integrar la seguridad en la homologación de soft/hard.	LO23. Cuadro de mandos de seguridad
	CO9. Rediseño de roles para una segregación de funciones en SAP	MO18. Gestión de cuentas privilegiadas (PET - portátiles)	LO24. Sistema de gestión de la seguridad de la información

G: Proyecto gradual Cx: Proyecto a corto plazo Mx: Proyecto a medio plazo Lx: Proyecto a largo plazo xO: Operacional xT: Técnico

Figura 46: Proyectos a realizar

Los proyectos que se han acordado realizar junto con la compañía se detallan en las siguientes figuras:

CO5 MO10 Programa de concienciación.

Descripción y objetivos

El presente proyecto tiene por objeto proporcionar a la dirección y usuarios de los sistemas de información una **concienciación adecuada en materia de seguridad de la información.**

La formación y concienciación de los empleados de GUIMARUBI en el buen uso de los sistemas y recursos de IT constituye una pieza fundamental dentro del ámbito de la seguridad de la información. Dicha formación y concienciación debe ser renovada periódicamente y debe adaptarse a los cambios que GUIMARUBI vaya implementando en sus sistemas.

Impacto ISO 27002

- **DOMINIO 7:** Seguridad ligada a los RRHH

Actividades y consideraciones

Elaboración del plan de concienciación + Ejecución de iniciativas

- Elaborar y validar el plan de concienciación así como los colectivos de usuarios objetivos a los que irá dirigido.
- EY propone la ejecución de las siguientes iniciativas –dentro de este plan de concienciación:
  - ✓ 1 simulación de phising.
  - ✓ 1 simulación de "usb perdido" (donde almacenaremos un malware controlado, para visualizar el impacto de cuantos empleados cogen esos usb y los conectan a sus equipos corporativos).
  - ✓ 1 simulación de un "wifi acces point abierto y gratuito".
  - ✓ 1 charla de concienciación general al Comité Ejecutivo (1h).
  - ✓ 1 charla de concienciación general a los Directores y Managers (2h).
  - ✓ 4 comunicados/newsletters de concienciación para todos los usuarios (sept-dic), donde se podrán incorporar resultados de algunas de las iniciativas de concienciación llevadas a cabo (usb, access point…)
  - ✓ 1 formación técnica para los equipos de desarrollo sobre el desarrollo seguro (4hs).

Entregables

- Material de formación y concienciación relativo a:
  - ✓ Iniciativas prácticas.
  - ✓ Charlas de concienciación.
  - ✓ Formación.
  - ✓ Comunicados o newsletters.

Dedicación estimada por parte de GUIMARUBI: Muy baja

CT6 Auditorias técnicas de seguridad.

Descripción y objetivos

- Revisiones técnicas (hacking ético) para **evaluar el nivel de seguridad de aquellos activos tecnológicos nuevos o no revisados hasta el momento** (p.e. redes OT o sistemas SCADA).
- Del mismo modo, con estas auditorias también se pretende **verificar que las vulnerabilidades críticas y altas detectadas durante la definición del plan director de seguridad, ya han sido solventadas** (p.e. entornos web expuestos).

Impacto ISO 27002

- **DOMINIO 18:** Cumplimiento.

Actividades y consideraciones

Ejecución de auditorias + Soporte para la resolución de las vulnerabilidades detectadas

- Para cada una de las auditorias se realizarán las siguientes actividades:
  - ✓ Preparación de los programas de trabajo / plan de pruebas específicos.
  - ✓ Tramitación de requisitos para realizar las auditorias (por ej. accesos, ventanas de actuación, usuarios…).
  - ✓ Planificación y sesión de lanzamiento con interlocutores.
  - ✓ Ejecución de las auditorias de manera coordinada con los equipos.
  - ✓ Elaboración de informes detallados del trabajo realizado y conclusiones obtenidas.
  - ✓ Plan de remediación para corregir las debilidades / vulnerabilidades identificadas.
  - ✓ Presentaciones ejecutivas de resultados.
- *Para el desarrollo de las auditorias, EY utilizará tanto herramientas comerciales como especificas desarrolladas internamente (p.e. Nmap, Gping, Nessus, Nitko, Getacct, crack, nipper…).*

Entregables

- Informes de resultados, que incluirán –como mínimo:
  - ✓ Listado de vulnerabilidades detectadas, clasificadas por criticidad (basado en la exposición al riesgo).
  - ✓ Propuestas con el detalle para remediar las vulnerabilidades detectadas.

Dedicación estimada por parte de GUIMARUBI: Muy baja

CT8 Revisión y mejora del proceso de parcheado.

Descripción y objetivos

- El objetivo del presente proyecto es la **mejora del proceso de gestión de parcheado de los sistemas de información**, para mejorar el control de versiones de software / firmware instalado, así como optimizar la automatización en el despliegue de actualizaciones de seguridad.

Impacto ISO 27002

- **DOMINIO 12:** Gestión de operaciones.

Actividades y consideraciones

Análisis del proceso + Elaboración de procedimiento + Propuesta de herramientas

- Analizar y evaluar el proceso actual relativo a la gestión y despliegue de parches de seguridad – teniendo en cuenta roles encargados, sistemas afectados, procedimientos existentes y grado de automatización de las tareas asociadas.
- Elaboración o actualización del procedimiento relativo a la gestión del proceso de parcheado; para ello, se realizarán las siguientes actividades:
  - ✓ Identificación de tecnologías y versiones actuales de los sistemas de información.
  - ✓ Documentar las actividades llevadas a acabo para la identificación de vulnerabilidades.
  - ✓ Definir un método de clasificación de vulnerabilidades.
  - ✓ Definir políticas de parcheo de sistemas teniendo en cuenta las recomendaciones de cada fabricante y las características particulares de GUIMARUBI (recursos, sistemas…etc).
  - ✓ Identificar y documentar excepciones en el procedimiento, y protocolo de escalado.
  - ✓ Identificar protocolos de actuación para el despliegue y pruebas previas a realizar.
- Para la automatización de actividades del procedimiento desarrollado, EY dará asesoramiento especializado para identificar posibles herramientas que permitan dar soporte al proceso de gestión de parcheado.

Entregables

- Informe de situación (AS IS)
- Procedimiento relativo a la gestión de parches de seguridad , que incluirá – como mínimo:
  - ✓ Clasificación de vulnerabilidades.
  - ✓ Políticas de parcheado.
  - ✓ Excepciones y escalado.
  - ✓ Protocolos de actuación para el despliegue.
- Propuesta de herramientas para automatizar actividades del procedimiento realizado.

Dedicación estimada por parte de GUIMARUBI: Baja (análisis y diseño); Media (Implementación)

MO11 Desarrollo de normativa de seguridad y actualización de la política de uso de medios tecnológicos

Descripción y objetivos

- La definición y la aprobación de un cuerpo normativo de seguridad permite proporcionar el marco regulatorio para el cumplimiento de la Política de Seguridad. Este cuerpo normativo se tiene que configurar como el conjunto de reglas generales de obligado cumplimiento.
- El objetivo principal de este proyecto es la **elaboración del cuerpo normativo**, tomando como base el cumplimiento con los diferentes controles del estándar de Seguridad ISO.
- Adicionalmente, se contempla la **actualización de la política existente relativa al uso de medios tecnológicos**.

Impacto ISO 27002

- **TODOS LOS DOMINIOS**

Actividades y consideraciones

Elaboración normativa + Actualización de la política de uso + Mejora de la normativa existente

- Desarrollo del cuerpo normativo relativo a los siguientes ámbitos:
  - ✓ Redes sociales
  - ✓ Clasificación y tratamiento de la información.
  - ✓ Conservación de la información.
  - ✓ Gestión de identidades y accesos.
  - ✓ Adquisición, desarrollo y mantenimiento de sistemas.
  - ✓ Seguridad de la información en los procesos de gestión de personal.
  - ✓ Seguridad física y medioambiental.
- Revisión y actualización de la política existente relativa al uso de medios tecnológicos.
- Revisión y actualización del cuerpo normativo existente (correspondiente a la fase 1 del PDS): monitorización de la seguridad, operación de sistemas de información, contratación de servicios, protección de datos personales, intercambio de información, gestión de riesgos y seguridad en las comunicaciones.
- Definición de los procesos formales de revisión y evaluación periódica de este cuerpo normativo, con el objetivo de garantizar su adecuación y vigencia en el tiempo.
- Integrar dentro de los mecanismos existentes la publicación y divulgación del cuerpo normativo de seguridad.

Entregables

- Normativas de seguridad de la información
- Política de uso de medios tecnológicos actualizada.
- Propuestas de mejora sobre la normativa de seguridad existente (correspondiente a la fase 1 del PDS).

Dedicación estimada por parte de GUIMARUBI: Muy baja

MO14 Inventario y clasificación de la Información.

Descripción y objetivos

La clasificación de la información, así como de los activos que la tratan, es uno de los pilares básicos sobre la que se asienta la seguridad de la información. Esta determinará en gran medida las salvaguardas que deben ser implantadas para proteger la información de la compañía.

Por ello, el presente proyecto tiene por objeto realizar un **inventario y clasificación de los activos de información de GUIMARUBI, determinando las medidas de seguridad aplicables a cada tipo de información** en función de su criticidad para la compañía.

Impacto ISO 27002

- **DOMINIO 8**: Gest. de activos

Actividades y consideraciones

Definición guía de clasificación + Inventario + Clasificación

- Definición del concepto de activo de información para GUIMARUBI.
- Definición de una Guía de Clasificación de la Información que determine los controles de seguridad a aplicar a la información en función de su nivel de criticidad para la organización. Para ello, se definirán las dimensiones de seguridad aplicables (Confidencialidad, Disponibilidad, Integridad y Trazabilidad)
- Realización del inventario de activos de información y clasificación de los mismos en función de la Guía establecida.
- Determinación de los activos tecnológicos que soportan la información inventariada así como los medios de tratamiento aplicables (automatizados, papel, mixto).
- Identificación de la ubicación de los datos, y de la existencia de externos que traten dichos activos de información.

Entregables

- Guía de clasificación de la información.
- Inventario de activos de información, incluyendo como mínimo:
  - ✓Clasificación de los activos.
  - ✓Activos tecnológicos asociados a cada activo de información.
  - ✓Propietario
  - ✓Terceras partes con acceso.

Dedicación estimada por parte de GUIMARUBI: Media

MT15 Auditorias técnicas de seguridad (maquetas de terminales de usuario)

Descripción y objetivos

- **Revisión técnica de seguridad de las maquetas existentes** para desplegar en terminales de usuarios.
- Adicionalmente, **se propondrán mejoras** destinadas a aumentar el nivel de seguridad, y **se dará soporte y asesoramiento para su correcta implantación**.

Impacto ISO 27002

- **DOMINIO 18**: Cumplimiento.

Actividades y consideraciones

Ejecución de auditorias + Asesoramiento para la configuración segura de las maquetas

- Respecto a los terminales de usuario, se contempla la revisión técnica de la seguridad de las maquetas existentes para PC y portátiles.
- Con los resultados obtenidos de la auditoría técnica, se dará soporte y asesoramiento para:
  - ✓ La configuración segura de las maquetas revisadas.
  - ✓ Su correcta implantación y despliegue.
- Del mismo modo, también se contempla la revisión técnica de la seguridad de un móvil y una tablet corporativa. En este caso, y dado que para una gestión eficiente de su seguridad es necesario la implantación de herramientas MDM (actualmente no implantada en la Compañía), el resultado de esta parte específica del trabajo será el desarrollo de un documento de "buenas prácticas" en el uso de estos dispositivos (que podrá ser entregado conjuntamente con el dispositivo).

Entregables

- Guía de bastionado asociada a las maquetas de los terminales de usuario.
- Buenas prácticas en el uso de los dispositivos móviles (móvil y tablets).

Dedicación estimada por parte de GUIMARUBI: Baja (análisis y diseño); Media (Implementación)

MT16 Definición de guías de bastionado de sistemas de información

Descripción y objetivos

- **Elaboración de guías de bastionado** concretas que garanticen las securización de los principales entornos y sistemas que tratan la información de GUIMARUBI.

Impacto ISO 27002

- **DOMINIO 12:** Gestión de operaciones.
- **DOMINIO 18:** Cumplimiento.

Actividades y consideraciones

Elaboración de guías + soporte para su implementación + propuesta de herramientas

- Elaboración de las guías de bastionado para garantizar la securización homogénea de los requerimientos de seguridad aplicables a la totalidad de las tecnologías existentes. Se contemplan el desarrollo de las siguientes guías asociadas los principales sistemas y versiones de GUIMARUBI:
  - ✓ Servidores Windows (2008 y 2012).
  - ✓ Servidores Oracle 12.
  - ✓ Servidores SQL (2008 y 2012)
  - ✓ Servidores Linux (Red Hat y SUSE)
  - ✓ Servidores Aix 7.9
  - ✓ *Terminales de usuario Windows (7, 7 embedded, 10)* ***Alcance ya incluido para proyecto MT15.***
- Asesoramiento y soporte para la correcta implementación de las guías de bastionado definidas.
- Para la automatización de las actividades de verificación de cumplimiento de las guías de bastionado, EY dará asesoramiento especializado para identificar posibles herramientas que permitan cubrir este aspecto.

Entregables

- Guía de bastionado para servidores.
- Propuestas de herramientas para automatizar las tareas de seguimiento del cumplimiento de las guías.

Dedicación estimada por parte de GUIMARUBI: Baja (análisis y diseño); Alta (Implementación)

MO17 Definición del proceso de homologación de software corporativo

Descripción y objetivos

- El objetivo del presente proyecto es la **definición del proceso para la homologación de software**, con el fin de garantizar que la seguridad de la información se integra en todos los procesos de adquisición y mantenimiento de sistemas de información.
- De esta forma se pretende ampliar el catálogo de pruebas a realizar para cualquier homologación, no limitándose únicamente a valoraciones de afectación de rendimiento, operativa o licenciamiento.

Impacto ISO 27002

- **DOMINIO 12:** Gestión de operaciones.

Actividades y consideraciones

Diseño del proceso + Elaboración del procedimiento + listado de software homologado

- Análisis y revisión de las actividades actualmente llevadas a cabo para "homologar" el software.
- Diseño del proceso de homologación de software corporativo, para integrar la seguridad de la información en los procesos relativos a la adquisición y mantenimiento de software.
- Elaboración del procedimiento asociado al proceso de homologación de software corporativo; este contendrá –como mínimo- los siguientes apartados:
  - ✓ Funciones y responsabilidades.
  - ✓ Clasificación de software y requerimientos de seguridad asociados.
  - ✓ Catálogo de pruebas a realizar.
  - ✓ Protocolo de escalado para tratar las excepciones.
  - ✓ Actividades de revisión y mantenimiento del inventario de software homologado o corporativo.
  - ✓ Actividades de seguimiento del cumplimiento del procedimiento.
- Inventario de software homologado. Para su creación inicial, se utilizará tanto la información disponible actualmente por el área IT como información adicional que pueda ser obtenida de forma transparente por el usuario por herramientas automáticas de autodescubrimiento.

Entregables

- Informe de situación (AS IS)
- Procedimiento relativo a la homologación de software, que incluirá –como mínimo:
  - ✓ Requerimientos de seguridad en base a la tipología y funcionalidad del software.
  - ✓ Catálogo de pruebas potenciales.
  - ✓ Protocolo de escalado para excepciones.
- Listado de software corporativo (homologado).
- Procedimiento de revisión y mantenimiento del listado.

Dedicación estimada por parte de GUIMARUBI: Baja (análisis y diseño); Media (Implementación)

MO18	Gestión de cuentas privilegiadas.

Descripción y objetivos

- El objetivo del presente proyecto es **garantizar la correcta gestión y monitorización de las cuentas privilegiadas** de IT, **especialmente en aquellos casos en los que las cuentas pertenezcan a personal externo** a la organización.

Impacto ISO 27002

- **DOMINIO 9**: Control de acceso

Actividades y consideraciones

Diseño del proceso + Elaboración del procedimiento + propuesta de herramientas

- Análisis y revisión de las actividades actualmente llevadas a cabo para la gestión y supervisión las cuentas privilegiadas asociadas a personal externo.
- Diseño del proceso de gestión de cuentas privilegiadas: a nivel de sistemas operativo tanto en servidores como en terminales de usuario.
- Elaboración del procedimiento asociado a la gestión de cuentas privilegiadas; este contendrá –como mínimo- los siguientes apartados:
  - ✓ Proceso de solicitud de cuentas privilegiadas.
  - ✓ Información mínima de los registros.
  - ✓ Determinación de los registros de auditoría necesarios.
  - ✓ Procedimiento de revisión de los registros definidos.
- Para automatizar la supervisión de estas cuentas en los terminales de usuario, EY pone a disposición de GUIMARUBI -sin coste adicional- la implantación de su herramienta EY PET (Privilege Elevation Tool).
- Para servidores, EY identificará y asesorará a GUIMARUBI en las posibles herramientas que existen en mercado y que más se adapten a las necesidades propias.

Entregables

- Informe de situación (AS IS)
- Procedimiento para la gestión de cuentas privilegiadas.
- PET: herramienta de EY para la gestión de cuentas privilegiadas en terminales de usuario.
- Propuesta de herramientas para la gestión de cuentas privilegiadas en servidores.

Dedicación estimada por parte de GUIMARUBI: Baja (análisis y diseño); Media (Implementación)

Tras el diagnóstico de la situación actual del Grupo, se fijó un estado objetivo en el ámbito de la seguridad de la información (basado en la norma ISO/IEC 27002). El desarrollo de los proyectos definidos permitirá ir alcanzando paulatinamente el objetivo propuesto. A continuación, se presenta la evolución de madurez esperada tras la implantación de los proyectos definidos en cada uno de los periodos.

Fase 1 (corto plazo): Evolución de la madurez de los controles ISO/IEC 27002:

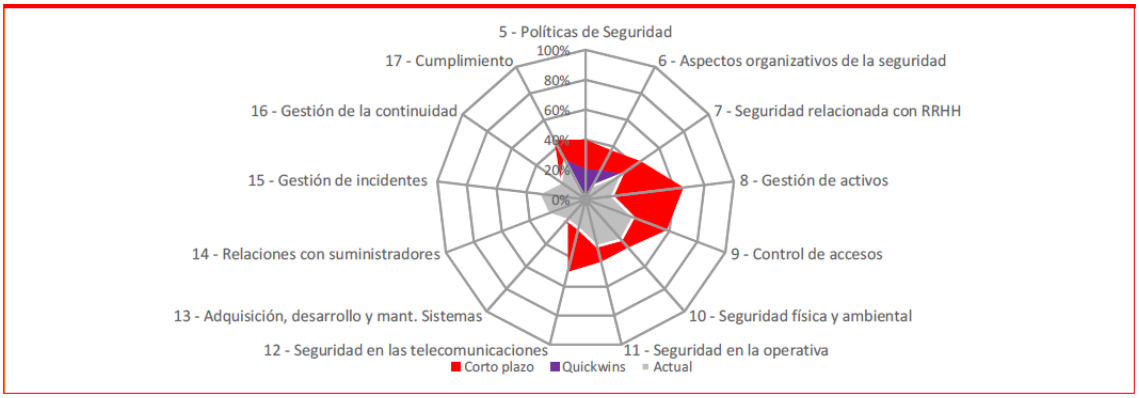


Figura 47: Evolución de la madurez de los controles ISO/IEC 27002 Fase 1

Fase 2 (medio plazo): evolución de la madurez de los controles ISO/IEC 27002:

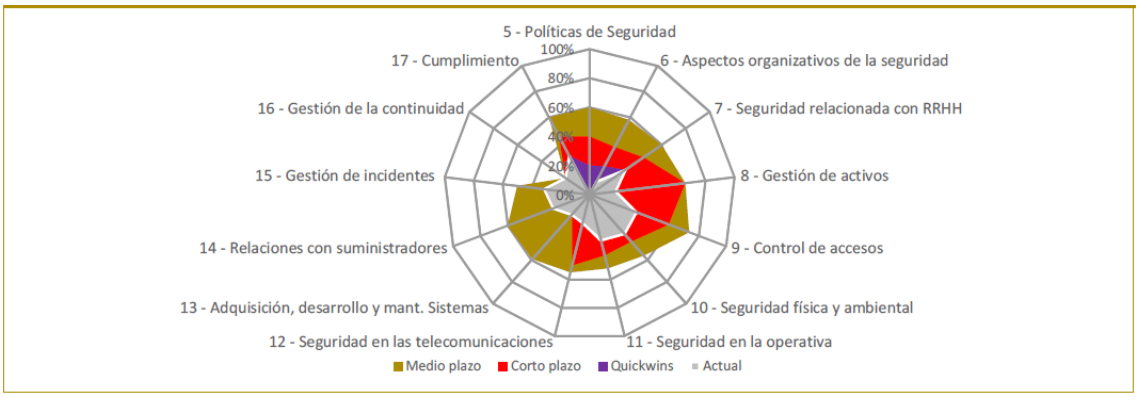


Figura 48: Evolución de la madurez de los controles ISO/IEC 27002 Fase 2

Fase 3 (largo plazo): evolución de la madurez de los controles ISO/IEC 27002:

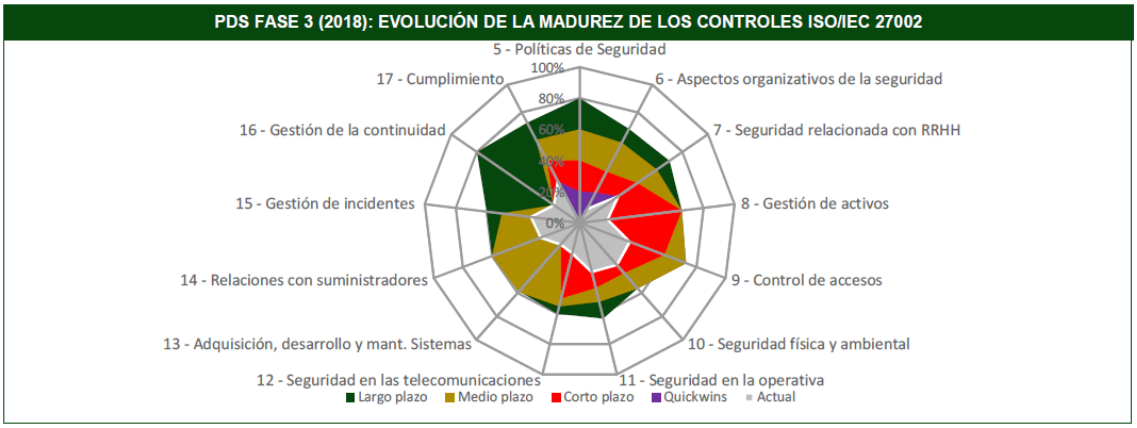


Figura 49: Evolución de la madurez de los controles ISO/IEC 27002 Fase 3

Finalmente se detalla el tiempo estimado para la realización de dichos proyectos:

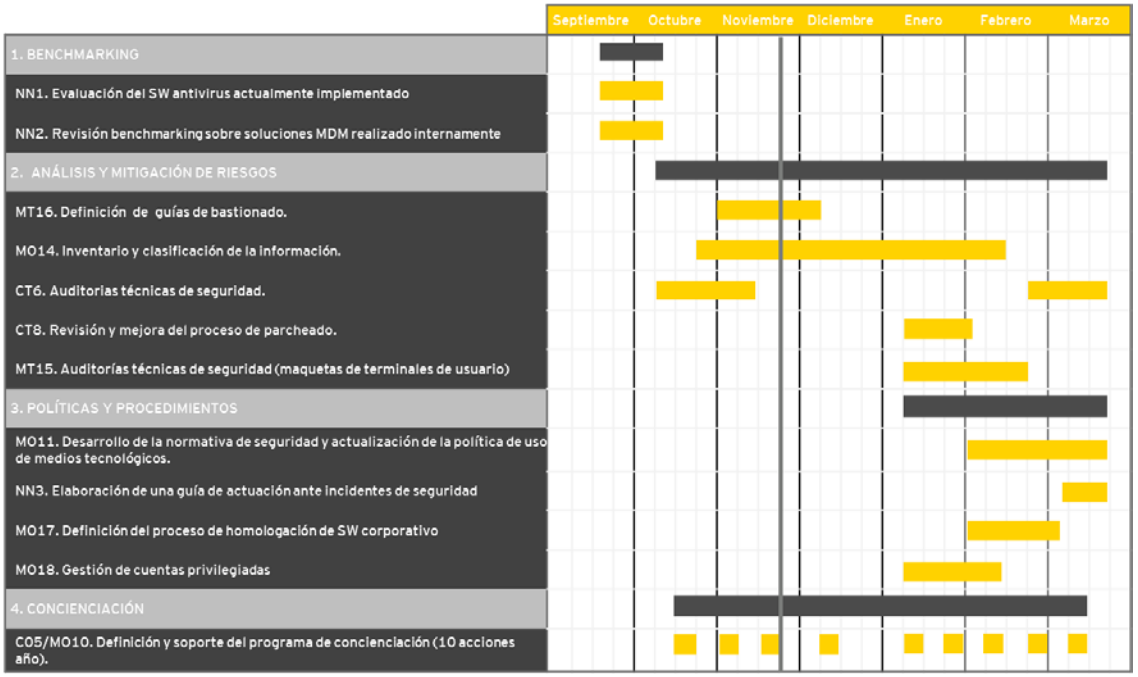


Figura 50: Planificación estimada de ejecución de los proyectos identificados

12 Referencias

1. *What is Computer security?* **Bishop, Matt.** s.l. : IEE Security and Privacy mMagazine, 2003, págs. 67-69.

2. **International Organization for Standardization.** *ISO/IEC 27001:2013.* 2013.

3. —. *ISO/IEC 27002:2013.*

4. **Mellon, Carnegie.** *OCTAVE Model.* 2002.

5. **ENS.** *Libro I - MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : 2012.

6. —. *Libro II - MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : 2012.

7. —. *Libro III - MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid : 2012.

8. **NIST.** *SP 800-30 Rev. 1 Guide for Conducting Risk Assessments.* 2012.

9. **Wikipedia. [En línea] [Citado el: 24 de 09 de 2018.] https://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration.**

10. Europea, Unión. ***REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.*** **2016.**

11. International Organization for Standardization. ***ISO 31000:2018.***

12. Wikipedia. [En línea] [Citado el: 24 de 09 de 2018.] https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico.

13 Anexos

13.1 Proyectos Inmediatos (*QuickWins*)

Organizativo / Técnico	ID	Título	Descripción	Dependencia con otros proyectos	Dominio Controles ISO	Objetivos de control ISO	Esfuerzo estimado
Organizativo	QW1	Definición de la política de seguridad corporativa	Elaborar, aprobar y divulgar la política de seguridad de la información de la Compañía.		5. Políticas de seguridad de la información 7. Seguridad ligada a los recursos humanos	5.1.1 Políticas de seguridad de la información 7.2.1 Responsabilidades de la Dirección	1 semana
Organizativo	QW2	Definición y divulgación de la organización de la seguridad.	Identificar y establecer nuevas figuras y responsabilidades de Seguridad para cubrir las tareas y responsabilidades en GUIMARUBI así como divulgar dicha organización para el conocimiento de los empleados.		6. Organización de la seguridad de la información	6.1.1 Roles y responsabilidades relativas a la seguridad de la información 6.1.2 Separación de tareas 6.1.3 Contacto con las autoridades 6.1.4 Contacto con grupos de especial interés 6.1.5 Seguridad de la información en la gestión de proyectos	1 semana
Técnico	QW3	Eliminación VNC	Esta herramienta supone un riesgo importante para el acceso a máquinas remotas, puesto que el *password* es conocido		9. Control de acceso 13. Seguridad de las comunicaciones	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 13.1.2 Seguridad de los servicios de red	1 mes

13.2 Proyectos Graduales

Organizativo / Técnico	ID	Título	Descripción	Dependencia con otros proyectos	Dominio Controles ISO	Objetivos de control ISO	Esfuerzo estimado
Organizativo	*CO4*	*(G). Desarrollo de normativa y procedimientos de seguridad*	El presente proyecto tiene por objetivo desarrollar la Normativa de Seguridad de GUIMARUBI. Las normas vienen a desarrollar las directrices marcadas en la Política de Seguridad y constituyen la base para el desarrollo e implantación de medidas de seguridad específicas, que se concretarán mediante su formalización en procedimientos o documentos operativos derivados. Así mismo se debe reflejar también las consecuencias disciplinarias en caso de infracción. El objetivo es desarrollar gradualmente toda la normativa necesaria para la correcta implantación de controles y medidas de seguridad. Para ello, y durante el primer año de implantación del PDS, la normativa que se propone elaborar sería la siguiente: a) Monitorización de seguridad de la información b) Seguridad en la operación de sistemas de información c) Seguridad de la información en la contratación de servicios d) Protección de datos personales e) Intercambio y compartición de información f) Gestión de riesgos de Seguridad de la información g) Seguridad en las comunicaciones	Necesario para soportar la realización de la mayor parte de los proyectos de corto plazo	5. Políticas de seguridad de la información 6. Organización de la seguridad de la información 7. Seguridad ligada a los recursos humanos 9. Control de acceso 12. Gestión de operaciones 13. Seguridad de las comunicaciones 15. Relaciones con proveedores 16. Gestión de incidentes 18. Cumplimiento	Todos los controles asociados a los dominios afectados	2 meses

Organizativo	*CO5*	*(G). Programa de concienciación de seguridad de la información*	Este proyecto es un proyecto gradual a lo largo de las tres fases definidas a corto, medio y largo plazo que propone el despliegue del plan de Formación y Concienciación en materia de Seguridad de la Información a los empleados de GUIMARUBI. Dicha formación y concienciación debe ser renovada periódicamente y debe adaptarse a los cambios que GUIMARUBI vaya implementando en sus sistemas. A continuación se indican algunos ejemplos de formación propuestos: 1) Píldoras mensuales de concienciación a todos los empleados. 2) Píldoras específicas a proveedores. 3) Demostraciones o simulaciones de ataques (p.e. *Phising* o USB "perdido"). 4) Jornadas de formación con contenidos interactivos como vídeos de seguridad o trípticos.		7. Seguridad ligada a los recursos humanos	7.2.2 Concienciación, formación y capacitación en seguridad de la información	1 mes
Técnico	*CT6*	*(G). Auditorias técnicas de seguridad*	Las auditorías son una herramienta que permite evaluar la seguridad de la compañía y detectar incumplimientos, desviaciones y mejoras con la finalidad de desencadenar la puesta en marcha de acciones para corregir las deficiencias o incumplimientos (acciones correctivas), acciones para prevenir nuevas deficiencias (acciones preventivas) y oportunidades de mejora. El objetivo de este proyecto es revisar periódicamente (es un proyecto gradual), desde el punto de vista de la Seguridad, todos aquellos aspectos que implican los Sistemas de Información de la empresa. En estas auditorías se llevan a cabo revisiones técnicas exhaustivas de los sistemas, convirtiendo este análisis en un estudio integral a todos los niveles de los Sistemas de Información. A continuación se exponen algunos ejemplos de auditorías propuestas: 1) Testeos de penetración en entornos web (hacking). 2) Auditoría técnica a las redes internas asociadas a los CASH. 3) Revisiones de accesos remotos por parte de los proveedores. 4) Auditoría técnica de las redes Wifi. 5) Auditoría de backups.	Necesario para hacer LT21	9. Control de acceso 12 Gestión de operaciones 14. Adquisición, desarrollo y mantenimiento de los sistemas 18. Cumplimiento	9.1.2. Acceso a redes y servicios en red 9.2.5. Revisión de derechos de acceso de usuario 9.2.6 Terminación o revisión de los privilegios de acceso 9.4.4 Uso de los recursos del sistema con privilegios especiales 9.4.5. Control de acceso al código fuente de los programas 12.6.1 Control de las vulnerabilidades técnicas 12.7.1 Controles de auditoría de los sistemas de información	1 mes

						14.2.8 Pruebas de seguridad del sistema 14.2.9 Pruebas de aceptación del sistema 18.2.1 Revisión independiente de la seguridad de la información 18.2.2 Cumplimiento de las políticas y normas de seguridad 18.2.3 Comprobación del cumplimiento técnico	

13.3 Proyectos a Corto Plazo

Organizativo / Técnico	ID	Título	Descripción	Dependencia con otros proyectos	Dominio Controles ISO	Objetivos de control ISO	Esfuerzo estimado
Técnico	QW4	Entorno SAP: Caducidad de contraseñas	La contraseña tiene una periodicidad excesiva y no cumple lo establecido en las políticas de seguridad estándar de la compañía.		9.4. Control de acceso al sistema y a las aplicaciones	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 13.1.2 Seguridad de los servicios de red	2 meses
Técnico	QW5	Accesos desde Back Office requieren permisos elevados en R/3	Los usuarios de *Back Office* requieren que el usuario de comunicación creado en R3 tenga permisos Z:SAP_ALL para que no haya problemas en la ejecución de acciones. El riesgo está en aquellos usuarios que también acceden a SAP GUI con el mismo usuario de Back Office		9.4. Control de acceso al sistema y a las aplicaciones	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 13.1.2 Seguridad de los servicios de red	1 mes

Técnico	QW6	Detectadas reglas permisivas del firewall	Revisión de las reglas vigentes del FW y sustituirlas por otras con carácter menos permisivo Se está realizando la revisión de las reglas actuales en los firewalls del CPD. Se buscará apoyo en el equipo que participe en la migración del CPD		13.1. Gestión de la seguridad de las redes	13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red	6 meses
Técnico	QW7	Salida a Internet directa portátiles	La navegación a través de la conexión de intranet se ha controlado a través del firewall, sin embargo, otros perfiles sí pueden acceder (directivos)		13.1. Gestión de la seguridad de las redes	13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red	
Técnico	QW8	Borrar usuarios locales de las máquinas Windows	Esta tarea se ejecutará tras la adjudicación del tender del lote 2	Migración CPD	9. Control de acceso	9.2 Gestión del acceso de usuario 9.4 Control de acceso al sistema y a las aplicaciones	2 meses

Técnico	CT1	Resolución de las vulnerabilidades más significativas identificadas durante el PDS	El proyecto propone solucionar aquellas vulnerabilidades técnicas más críticas detectadas durante el análisis de seguridad de la red interna, que se pueden solucionar de una manera más rápida y que no requiere de un gran esfuerzo para evitar y reducir gran parte de los riesgos detectados. Para ello, las principales actividades a realizar, serían: 1) Actualización de los sistemas (parcheado). 2) Configuración para el uso de protocolos de comunicación seguros. 3) Securización de los sistemas críticos o con más vulnerabilidades (cambio de contraseñas por defecto, limitación de servicios abiertos, limitación de uso de administradores).	Migración CPD	9. Control de acceso 13. Seguridad de las comunicaciones	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 13.1.2 Seguridad de los servicios de red	2 meses
Técnico	CT2	Securizar entornos web	Durante el análisis de seguridad de las *websites* externas se han detectado vulnerabilidades que permitirían el acceso a intrusiones no deseadas y a información sensible del Grupo. Este proyecto tiene como objetivo securizar estos entornos web públicos y privados de la compañía que contienen datos de la organización para evitar la posible materialización de los riesgos encontrados. Para ello, las principales actividades a realizar serían: 1) Actualización de los sistemas (parcheado) 2) Procedimientos para la validación de parámetros de entrada en los aplicativos web. 3) Segregación de entornos entre los diferentes websites. 4) Mejora de las políticas de contraseñas.	Contratación nuevo proveedor mantenimiento webs	9. Control de acceso 13. Seguridad de las comunicaciones 14. Adquisición, desarrollo y mantenimiento de los sistemas	9.1.2 Acceso a redes y servicios en red 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red 13.1.3 Segregación de redes 14.1.1 Análisis y especificación de los requisitos de seguridad 14.1.2 Aseguramiento de servicios y aplicaciones en redes públicas 14.1.3 Protección de las transacciones	2,5 meses

Técnico	CT3	Securizar entornos CASH (51 centros)	Durante el análisis de la seguridad de la red interna asociada a los entornos CASH, se evaluaron tanto un entorno migrado con la nueva arquitectura/infraestructura como uno antiguo no migrado. Todas las mejoras detectadas son únicamente aplicables al entorno antiguo. Por ello, este proyecto intenta cubrir el proceso de actualización o migración de los CASH aún no migrados a la arquitectura/infraestructura considerada segura. Para ello, las principales actividades a realizar serían las siguientes para 51 centros CASH: 1) Cambiar protocolos de comunicación wifi. 2) Segregar la red interna asociada a los CASH 3) Securización de los sistemas (mejora de la política de contraseñas, mejora de la gestión usuarios y accesos, limitación de servicios). Este proyecto requiere una inversión asociada a la adquisición de infraestructura.		9. Control de acceso 13. Seguridad de las comunicaciones 14. Adquisición, desarrollo y mantenimiento de los sistemas	9.1.2 Acceso a redes y servicios en red 13.1.1 Controles de red 13.1.2 Seguridad de los servicios de red 13.1.3 Segregación de redes 14.1.1 Análisis y especificación de los requisitos de seguridad 14.1.2 Aseguramiento de servicios y aplicaciones en redes públicas 14.1.3 Protección de las transacciones	4 meses
Técnico	CT7	Implementación arquitectura doble capa (*firewall* entre perimetral e interna)	El objetivo de este proyecto es la implementación de una nueva arquitectura para segregar correctamente la red interna y la red perimetral. Para ello, las actividades principales a realizar serían las siguientes: 1) Identificar los entornos necesarios a segregar. 2) Diseñar la arquitectura para una correcta segregación de redes. 3) Actualizar y configurar las reglas del firewall para implementar el diseño de la nueva arquitectura.	Tender de CPD	9. Control de acceso 13. Seguridad de las comunicaciones	9.1.2 Acceso a redes y servicios en red 9.4.1 Restricción de acceso a la información 9.4.4 Uso de los recursos del sistema con privilegios especiales 13.1.2 Seguridad de los servicios de red 13.1.3 Segregación de redes	2 meses

Técnico	CT8	Revisión y mejora del proceso de parcheado.	Implantar un proceso de gestión de parcheado para los equipos que permita mejorar el control sobre las versiones de SW/firmware instaladas en los sistemas, automatización del despliegue de actualizaciones de seguridad. 1) Identificar las tecnologías y versiones actuales de los sistemas de información (servidores, SSOO, BBDD y aplicativos). 2) Identificar, clasificar y valorar las actualizaciones necesarias a desplegar para los sistemas identificados. 3) Definir las políticas actualización de los sistemas teniendo en cuenta las recomendaciones de cada uno de los fabricantes. 4) Elaborar un procedimiento de gestión del ciclo de vida de actualizaciones por tecnología. 5) Definir un plan de migración de los sistemas afectados a nuevas versiones	Tender de CPD	12. Gestión de operaciones	12.1.2 Gestión de cambios 12.4.1 Registro de eventos 12.5.1 Instalación de software en sistemas operacionales 12.6.1 Control de las vulnerabilidades técnicas 12.6.2 Restricciones a la instalación de software	2 meses

Organizativo	CO9	Rediseño de roles para una segregación de funciones en SAP	La asignación y el uso de privilegios para perfiles en la aplicación SAP tiene que ser restringido y controlado a través de un estricto proceso de autorización y asignación. El objetivo de este proyecto es garantizar que los usuarios de SAP únicamente tengan acceso a las transacciones y recursos según las tareas que tengan asignadas y garantizando una adecuada segregación de funciones. Para ello, las principales actividades a realizar serían las siguientes: 1) Validar y aprobar la matriz de incompatibilidades. 2) Analizar las incompatibilidades: según la matriz de incompatibilidad y con la información del análisis se determinarán las incompatibilidades existentes así como las acciones necesarias para corregir la situación. 3) Redefinición y nueva asignación de roles. 4) Una vez realizado el análisis se definirá un procedimiento de revisión para garantizar la adecuada segregación de funciones en todo momento. 5) Adicionalmente, se revisará la configuración de seguridad de los parámetros establecidos en RSPARAM.	Necesario para MO12	9. Control de acceso	9.2.1 Altas y bajas de usuarios 9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.2.6 Terminación o revisión de los privilegios de acceso 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario	4 meses

13.4 Proyectos a Medio Plazo

Organizativo / Técnico	ID	Título	Descripción	Dependencia con otros proyectos	Dominio Controles ISO	Objetivos de control ISO	Esfuerzo estimado
Organizativo	M11	*(G). Desarrollo de normativa y procedimientos de seguridad*	El presente proyecto tiene por objetivo desarrollar la Normativa de Seguridad de GUIMARUBI. Las normas vienen a desarrollar las directrices marcadas en la Política de Seguridad y constituyen la base para el desarrollo e implantación de medidas de seguridad específicas, que se concretarán mediante su formalización en procedimientos o documentos operativos derivados. Así mismo se debe reflejar también las consecuencias disciplinarias en caso de infracción. El objetivo es desarrollar gradualmente toda la normativa necesaria para la correcta implantación de controles y medidas de seguridad. Para ello, y durante el primer año de implantación del PDS, la normativa que se propone elaborar sería la siguiente: a) Clasificación y tratamiento de la información b) Conservación de la información c) Gestión de identidades y accesos d) Adquisición, desarrollo y mantenimiento de sistemas e) Seguridad de la información en los procesos de gestión de personal f) Seguridad física y medioambiental	Necesario para soportar la realización de la mayor parte de los proyectos de medio plazo	5. Políticas de seguridad de la información 7. Seguridad ligada a los recursos humanos 9. Control de acceso 11. Seguridad física y del entorno 18. Cumplimiento	Todos los controles asociados a los dominios afectados	1 mes

Organizativo	MO12	Definición de los procesos de gestión de identidades	Para cada una de las aplicaciones de la compañía, los usuarios deben tener acceso a cada una de las aplicaciones acorde con sus responsabilidades y roles en la compañía. La correcta definición de la identidad digital y asignación de permisos garantizará una adecuada segregación de funciones. La definición de los procesos de gestión de identidades tiene como objetivo garantizar el adecuado acceso de los usuarios basado en sus necesidades de negocio. Para ello, las principales actividades a realizar serían las siguientes: 1) Definir una base de datos con las funciones de los empleados dentro de la compañía. 2) Identificar todas las aplicaciones que se utilizan en la compañía. 3) Definir un catálogo de roles con todos los roles de las aplicaciones documentados y todos los permisos asociados a cada rol. 4) Definir una matriz de accesos. 5) Implantar y concienciar a los empleados de este proceso de gestión.	Requiere CO9	9. Control de acceso	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.2.6 Terminación o revisión de los privilegios de acceso 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario	2 meses

Organizativo	MO13	Diseño del marco de control relativo a servicios IT externalizados.	El presente proyecto tiene como objetivo establecer un proceso adecuado de gestión de proveedores que permita reducir los riesgos de dependencia de proveedores sobre la gestión de servicios IT externalizados, y garantizar unos niveles de seguridad acordes a los implantados internamente por la Compañía. Para ello, las principales actividades a realizar serían las siguientes: 1) Identificar y clasificar los servicios IT externalizados o potencialmente a externalizar. 2) Definir los requerimientos de seguridad por tipología de servicio a externalizar. 3) Identificar responsabilidades de la implantación de los requerimientos de seguridad. Para aquellos, cuya responsabilidad de implantación sea de GUIMARUBI, incluir en el plan de auditorías periódicas la verificación de esos controles. Cuando la responsabilidad de implantación sea del proveedor, podrá ser cubierta por contrato o solicitando evidencias de su correcta efectividad.		15. Relaciones con proveedores 18. Cumplimiento	15.1.1 Política de seguridad de la información en las relaciones con proveedores 15.1.2 Tratamiento de la seguridad en contratos con proveedores 15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones 15.2.1 Supervisión y revisión de los servicios prestados por terceros 15.2.2 Gestión del cambio en los servicios prestados por terceros Todos los controles definidos en el 18.1 Cumplimiento de los requisitos legales y contractuales 18.2.2 Cumplimiento de políticas y normas de seguridad 18.2.3 Comprobación del cumplimiento técnico	2 meses

Organizativo	MO14	Inventariado de activos y clasificación de la información.	El presente proyecto tiene por objeto realizar una identificación y clasificación de la información y activos de GUIMARUBI definiendo las medidas de seguridad aplicables a cada tipo de información. Para ello, las principales actividades a realizar serían las siguientes: 1) Realizar entrevistas con los distintos interlocutores para identificar los activos tipo información. Inventariar la información de la organización. 2) Definir los niveles de clasificación de la información. 3) Identificar las medidas de seguridad asociadas a cada nivel. 4) Identificar los activos software que tratan cada información clasificada. 5) Actualizar o crear una base de datos centralizada con toda la información anterior (CMDB). 6) Definir los procedimientos necesarios para el correcto mantenimiento de la CMDB. 7) Definir un plan de acción para implementar las medidas de seguridad necesarias para cumplir con los requerimientos asociados a la clasificación de la información.		8. Gestión de activos 9. Control de acceso 12. Gestión de operaciones	8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.2.1 Clasificación de la información 8.2.2 Marcado de la información 8.2.3 Manejo de activos 9.2.4 Gestión de la información secreta de autenticación de usuarios 9.3.1 Uso de la información secreta de autenticación 12.1.2 Gestión de cambios 12.4.1 Registro de eventos	3 meses

Técnico	MT16	Definición de guías de bastionado de sistemas de información	El objetivo de este proyecto es definir unas guías de bastionado para los principales sistemas de la Compañía, que garanticen un nivel de seguridad homogéneo. Para ello, las principales actividades a realizar serían las siguientes: 1) Identificar las tecnologías y versiones actuales de los sistemas de información (servidores, SSOO, BBDD y aplicativos). 2) Para aquellos que por volumen o por criticidad se considere críticos, desarrollar guías de bastionado para garantizar los mismos requerimientos de seguridad. 3) Definir procedimientos de revisión periódica de estas guías, en base a las recomendaciones de los fabricantes o las buenas prácticas de mercado. 4) Integrar el uso de las guías con los procesos de homologación de software.	Necesario para MT17	9. Control de acceso 12. Gestión de operaciones 13. Seguridad de las comunicaciones 14. Adquisición, desarrollo y mantenimiento de los sistemas	9.2.2 Gestión de derechos de acceso de los usuarios 9.2.3 Gestión de derechos de acceso especiales 9.2.5 Revisión de derechos de acceso de usuario 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de las contraseñas de usuario 12.1.1 Dcoumentación de los procedimientos de operación 12.2.1 Contro contral código malicioso Todos los controles relativos al objetivo de control 12.4 Registro y monitorización 13.2.1 Políticas y procedimientos de transferencia de información 14.1.1 Análisis y especificación de los requisitos de seguridad	2 meses

Técnico	MT17	Integrar la seguridad en la homologación de SW / HW	El objetivo de este proyecto es garantizar que la seguridad de la información se integra dentro las actividades IT que implican una gestión de cambio. Para ello, se pretende definir un proceso de homologación no limitado únicamente a valoraciones de afectación de rendimiento, operativa o licenciamiento. Este procedimiento debería contemplar los siguientes aspectos: a) Comunicar al área de seguridad cualquier nueva adquisición (*soft/hard*) o desarrollo de software. b) "Pasar" las guías de bastionado definidas. b) Disponer de entornos diferenciados para el desarrollo de software. c) Testear el nuevo software antes de su paso a producción (aplicaciones web). d) Información que almacenará o tratará, para identificar los requisitos de seguridad asociados a la clasificación de la información. e) Verificar los riesgos asociados a los servicios necesarios para su puesta en producción o su integración con otros sistemas o aplicaciones.	Requiere MT16	6. Organización de la seguridad de la información 8. Gestión de activos 11. Seguridad física y del entorno 12. Gestión de operaciones 14. Adquisición, desarrollo y mantenimiento de los sistemas	6.1.5 Seguridad de la información en la gestión de proyectos 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.2.3 Manejo de activos 11.2.1 Emplazamiento y protección de equipos 12.1.1 Documentación de los procedimientos de operación 12.1.2 Gestión de cambios 12.1.3 Gestión de capacidades 12.1.4 Separación de entornos de desarrollo 12.5.1 Instalación de software en sistemas operaciones 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma 14.2.4 Restricciones a los cambios en los paquetes de software 14.2.5 Principios para la ingeniería de sistemas seguros	2 meses

						14.2.6 Entorno de desarrollo seguro 14.2.9 Pruebas de aceptación del sistema	
Organizativo	MO18	Gestión de cuentas privilegiadas	El objetivo de este proyecto es garantizar una adecuada gestión de las cuentas privilegiadas, especialmente en aquellos casos en los que las cuentas pertenezcan a personal externo a la organización. Para ello, las principales actividades a realizar serían las siguientes: Opción A: 1) Establecer un procedimiento de gestión y administración de las cuentas privilegiadas. 2) Instalar herramienta PET en los terminales de usuario desarrollada por EY para hacer una gestión sencilla de elevación temporal de privilegios. Opción B:	Requiere MO12	7. Seguridad ligada a los recursos humanos 9. Control de acceso	7.3.1 Terminación o cambio de responsabilidades laborales 9.2.1 Altas y bajas de usuarios 9.2.6 Terminación o revisión de los privilegios de acceso 9.4.1 Restricción del acceso a la información 9.4.4 Uso de los recursos del sistema con privilegios especiales	1 mes (OP A) 3 meses (OP B)

			1) Implantar una herramienta que permita la monitorización y control sobre la utilización de la cuentas privilegiadas de IT que garantice la seguridad en la asignación, administración y monitorización de las mismas.				

13.5 Proyectos a Largo Plazo

Organizativo / Técnico	ID	Título	Descripción	Dependencia con otros proyectos	Dominio Controles ISO	Objetivos de control ISO	Esfuerzo estimado
Organizativo	L20	*(G). Desarrollo de normativa y procedimientos de seguridad*	El presente proyecto tiene por objetivo desarrollar la Normativa de Seguridad de GUIMARUBI. Las normas vienen a desarrollar las directrices marcadas en la Política de Seguridad y constituyen la base para el desarrollo e implantación de medidas de seguridad específicas, que se concretarán mediante su formalización en procedimientos o documentos operativos derivados. Así mismo se debe reflejar también las consecuencias disciplinarias en caso de infracción. El objetivo es desarrollar gradualmente toda la normativa necesaria para la correcta implantación de controles y medidas de seguridad. Para ello, y durante el primer año de implantación del PDS, la normativa que se propone elaborar sería la siguiente: a) Seguridad para la continuidad de negocio b) Seguridad en la movilidad c) Seguridad de la información en servicios de Cloud Computing	Necesario para soportar la realización de la mayor parte de los proyectos de largo plazo	5. Políticas de seguridad de la información 7. Seguridad ligada a los recursos humanos 9. Control de acceso 11. Seguridad física y del entorno 18. Cumplimiento	Todos los controles asociados a los dominios afectados	1 mes
Técnico	LT21	Despliegue de un servicio de seguridad gestionada (SIEM / SOC)	Este proyecto se basa en el despliegue de una herramienta para la automatización de la monitorización, gestión y correlación de eventos de seguridad. Para ello, las principales actividades a realizar serían las siguientes: 1) Identificar y analizar las necesidades de operación de seguridad actuales. 2) Evaluar las tendencias, tecnologías y servicios existentes en el mercado. 3) Seleccionar la tecnología y servicio que mejor se adecua a los requisitos del Grupo. 4) Desplegar las herramientas necesarias para la operación y parametrización del servicio.	Requiere CT6	12. Gestión de operaciones 16. Gestión de incidentes de seguridad de la información	12.1.1 Documentación de los procedimientos de operación 12.4.1 Registro de eventos 12.4.2 Protección de la información de los registros 12.4.3 Registros de administración y operación 12.4.4 Sincronización del reloj 12.6.1 Control de las	3 meses

			5) Definir las métricas del servicio para la mejora continua. 6) Definir el procedimiento de mejora de las reglas de correlación de eventos			vulnerabilidades técnicas Todos los controles del dominio 16	
Organizativo	LO22	Plan de continuidad de negocio	El objetivo principal del proyecto es minimizar el impacto causado por la materialización de amenazas sobre la continuidad del negocio de la Compañía. Para ello, las principales actividades a realizar serían las siguientes: 1) Revisar y actualizar el BIA existente. 2) Analizar y revisar las estrategias de continuidad definidas para los escenarios de desastre. 3) Asegurar que esas estrategias de continuidad cubren con los requisitos identificados en el BIA; en caso contrario, identificar nuevas estrategias para alcanzar con las necesidades de continuidad identificadas por negocio en el BIA. 4) Definir los documentos soporte para una adecuada implantación del modelo de continuidad de la Compañía (Roles y Responsabilidades en el ámbito de la continuidad, plan de gestión de incidentes, plan de comunicación). 5) Realizar formación a los interlocutores involucrados en la gestión de la continuidad de la Compañía. 6) Definir planes soporte adicionales (plan de pruebas y mantenimiento).		17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Todos los controles asociados al dominio afectado	4 meses

Organizativo	LO23	Cuadro de mandos de seguridad	El objetivo de este proyecto es la definición e implantanción de un cuadro de mandos para el control y seguimiento del estado de la seguridad. Para ello, las principales actividades a realizar serían las siguientes: 1) Identificar los principales aspectos de la seguridad de la información que quieren medirse o evaluarse y que conformarán el modelo de seguridad de la Compañía. 2) Descripción detallada de los indicadores y métricas incluyendo como mínimo: formula de cálculo de los indicadores, fuentes de información para realizar la medición, periodicidad para la realización de la medida, responsables de la medida del indicador, límites aceptables o umbrales del indicador, evidencias o registros de cada uno de los indicadores y el método analítico de resultados. La implantación del cuadro de mandos puede ir acompañada de una herramienta soporte. El alcance del proyecto no contempla ni la selección ni la customización de una herramienta específica.	Requiere de todos los anteriores	18. Cumplimiento	18.2.2 Cumplimiento de las políticas y normas de seguridad	2 meses

Organizativo	*LO24*	Sistema de gestión de la seguridad de la información	El objetivo de este proyecto, es la definición de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la ISO 27001. Para la definición del sistema de gestión se incorporarán todos los controles, medidas y procedimientos resultantes de la implantación de todos los proyectos incluidos en el Plan Director de Seguridad. Para ello, las principales actividades a realizar serían las siguientes: 1) Definir formalmente el alcance del SGSI y objetivos a cubrir. 2) Desarrollar la declaración de aplicabilidad (controles que deberán formar parte del SGSI). 3) Definir una metodología soporte para la evaluación y tratamiento de riesgos. 4) Elaborar los procedimientos y mecanismos de control que soportan el propio SGSI. 5) Definir las responsabilidades aplicables en cuanto a operación, monitorización, revisión y mantenimiento del SGSI. 6) Generación, almacenamiento y custodia de los registros asociados al SGSI, como evidencia de conformidad con lo estipulado en el SGSI.	Requiere todos los anteriores	Todos los dominios	Todos los controles establecidos por la Compañía	2 meses