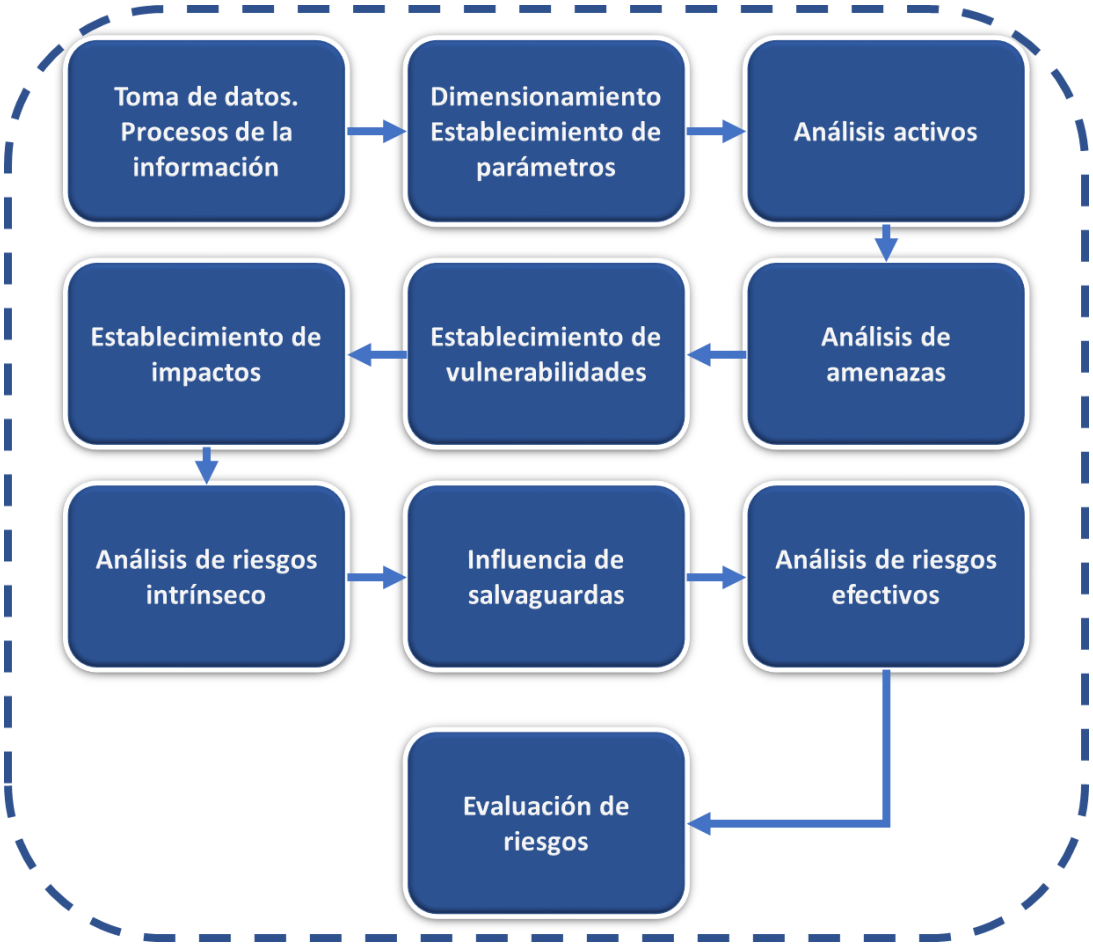
Anexo F – Metodología de análisis de riesgos.

Como se ha descrito en el documento principal, la metodología elegida para el análisis de riesgos de Ícaro S.A. es MAGERIT.

MAGERIT, sigue un proceso partido en fases destinado a llegar a la elaboración e identificación de todos los riesgos de una organización.

El en siguiente esquema se describen las fases y a continuación se hace una breve descripción de cada una de ellas.



1. Toma de datos y procesos de información

En esta primera fase, se definen el alcance que se ha de analizar y dependiendo del mismo, será más o menos costoso el análisis de riesgos.

Para Ícaro S.A. se analizarán los procesos que ejecuta la empresa para descubrir y estudiar los riesgos asociados a los mismos y discernir cuáles de ellos son críticos.

Cabe la posibilidad que existan amenazas que no pueden provocar interferencias en las actividades de la empresa y que no deban ser analizadas en fases posteriores puesto que no tiene sentido.

En esta fase también se determinará la granularidad que tendrá el análisis de riesgos y será determinada por el nivel de detalle al que se quiera llegar en la toma de datos.

2. Dimensionamiento y establecimiento de parámetros

Esta segunda fase es la más importante y es donde se establecen los parámetros que se usarán para ejecutar el análisis de riesgos.

Los parámetros que se deben identificar son:

2.1 Valor de los activos

Este parámetro sirve para asignar una valoración económica a todos los activos de la empresa necesarios para desempeñar su función.

Para la asignación económica no solo hay que tener en cuenta el valor de compra del activo, si no también su valor según la importancia que este tenga.

Para Ícaro S.A. se tendrá en cuenta:

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

Para realizar la valoración se establecen diferentes grupos de activos según su valor y a cada grupo se le asigna un valor económico estimado que se utilizará para todos los activos que pertenezcan a ese grupo. En la siguiente tabla se presenta los grupos de valoración para el análisis de riesgos de Ícaro S.A.

Valoración	Rango	Valor estimado
Muy Alta	Valor > 200K€	300K€
Alta	100K€ < Valor < 200K€	150K€
Media	50K€ < Valor < 100K€	75K€
Baja	10K€ < Valor < 50K€	30K€
Muy baja	Valor < 10K€	10K€

2.2 Vulnerabilidad

Para el método MAGERIT las vulnerabilidades se entienden como la frecuencia de ocurrencia de una amenaza; es decir, la frecuencia con que la organización puede sufrir una amenaza en concreto.

Esta frecuencia de ocurrencia también se plasma en una escala de valores que para Ícaro S.A. se representa en la siguiente tabla.

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

El valor numérico del rango de vulnerabilidad se extrae mediante estimaciones anuales basadas en días, es decir, asignando un número de veces por año:

Valor Vulnerabilidad = Frecuencia estimada en días al año/ 365 (Nº de días de un año).

2.3 Impactos

Para el método MAGERIT, se entiendo por impacto el tanto por ciento del valor de activo que se pierde en caso de que se produzca un incidente de seguridad sobre el mismo.

Como en los parámetros anteriores también se realiza una estimación por rangos de impactos, es decir, se establecen los distintos grupos que se quieren utilizar y a partir de los mismos asignar el porcentaje de valor que se estima que puede perderse en cada grupo.

A continuación, se presenta una tabla de grupos de porcentaje de impacto para Ícaro S.A.

Impacto	Valor
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy Bajo	5%

2.4 Efectividad del control de seguridad

Este parámetro consiste en ver la influencia que tendrá las medidas de protección adoptadas antes los riesgos detectados por el análisis, es decir, valorar como las medidas de seguridad que se implantarán van a minimizar los riesgos.

Respecto al hecho de minimizar un riesgo hay que tener en cuenta que las medidas de seguridad tienen dos formas de actuar; o bien reducen la vulnerabilidad o bien reducen el impacto que provoca la consecución del riesgo.

También para este parámetro se realiza una clasificación por grupos. A continuación, se presenta el utilizado para Ícaro S.A.

Valoración Efectividad	Valor
Muy Alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy Bajo	10%

3. Análisis de activos

Esta fase consiste en identificar cuáles son los activos que posee la organización y que necesita para su actividad, y está estrechamente relacionada con la primera fase del método ya que solo se deberían analizar los activos definidos en el alcance.

Respecto a los activos a analizar cabe destacar que estos deben clasificarse según los valores que se han establecido previamente. (Reposición, configuración, etc.)

Además, los propios activos a analizar estarán diferenciados en diferentes tipos:

- **Activos físicos:** Serían todos los activos de tipo hardware que se utilizan en la organización: ordenadores, servidores, portátiles, PDA, teléfonos móviles, impresoras, etc.

- **Activos lógicos:** Serían todos los elementos de software que se utilizan: sistemas operativos, aplicaciones propias, paquetes cerrados de mercado, procesos bach, etc.

- **Activos de personal:** Son las personas, desde el punto de vista de roles perfiles que intervienen en el desarrollo de las actividades de la organización: responsable de seguridad, administrador de la red, personal de administración, secretarios, usuarios, etc.

- **Activos de entorno e infraestructura:** Son todos los elementos que posee la organización y que necesita para que el resto pueda funcionar correctamente. Son, por ejemplo, los sistemas de aire acondicionado o el cableado de datos y de corriente eléctrica, etc.

- **Activos intangibles:** Son aquellos elementos que directamente no posee la organización pero que son importantes para ella, como pueden ser la imagen corporativa, la credibilidad, la confianza de los clientes, el know how, etc.

4. Análisis de amenazas

Para el análisis de amenazas MAGERIT las clasifica en cuatro grandes grupos:

- **Accidentes:** Se trata de situaciones provocadas involuntariamente y que la mayoría de veces no pueden evitarse, ya que pueden provocarse, por ejemplo, por efectos naturales.

- **Errores:** Se trata de situaciones cometidas de manera involuntaria por el propio desarrollo de las actividades diarias.

- **Amenazas intencionales presenciales:** Se trata de situaciones provocadas de manera voluntaria por el personal de la organización.

- **Amenazas intencionales remotas:** Se trata de situaciones provocadas voluntariamente por personas ajenas a la empresa.

5. Establecimiento de las vulnerabilidades

En el método MAGERIT no es necesario listar las vulnerabilidades que tiene la empresa en sus procesos o activos, pero si es necesario tenerlas en cuenta para estimar la frecuencia de ocurrencia de una amenaza sobre un proceso o activo.

La relación entre vulnerabilidad y amenaza es importante que quede clara en este documento a la hora de tener en cuenta el establecimiento de las vulnerabilidades, ya que sin vulnerabilidad no hay amenaza en tanto en cuanto es la vulnerabilidad la que permite que una amenaza pueda causar daño.

6. Valoración de impactos

Según MAGERIT a la hora de analizar y valorar los impactos que una amenaza pueda producir se deben tener en consideración los siguientes aspectos:

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

7. Análisis de riesgos intrínseco

Los riesgos intrínsecos son aquellos a los que la empresa está expuesta sin tener en cuenta las medidas de seguridad que podamos implantar.

Una vez obtenidos los parámetros anteriores y con los valores que hayamos identificado para cada situación ya se puede realizar el estudio de riesgos actuales (Previo a las salvaguardas) a los que está sometida la empresa.

Para este estudio es necesario aplicar la siguiente fórmula con las variables que ya conocemos:

Riesgo = Valor del activo x Valor del Impacto

8. Influencia de salvaguardas

Una vez analizados los riesgos intrínsecos a los que se encuentra expuesta la empresa, se entra en la fase de gestión de los riesgos o como escoger la mejor solución de seguridad que permita mitigarlos.

Las salvaguardas se pueden dividir en dos tipos fundamentales basados en cómo se pueden mitigar las amenazas:

- **Preventivas:** Son aquellas medidas de seguridad que reducen las vulnerabilidades.

  Nueva Vulnerabilidad = Vulnerabilidad x % disminución de vulnerabilidad

- **Correctivas:** Son aquellas medidas de seguridad que reducen el impacto de las amenazas.

  Nuevo impacto = Impacto x Porcentaje de disminución de impacto

9. Análisis de riesgos efectivos

Es el resultado de estudiar cómo se reducirían los riesgos con cada una de las medidas de protección que se identifiquen, es decir, calcular el riesgo definitivo teniendo en cuenta las salvaguardas implantadas.

Por tanto, el riesgo efectivo se calcula con:

Riesgo efectivo =Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto

=

Riesgo efectivo = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto)

=

Riesgo efectivo = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

10. Gestión de riesgos

Esta última fase del método MAGERIT consiste en tomar las decisiones por parte de la empresa acerca de las medidas de seguridad que debe escoger entre las distintas salvaguardas que reducen los riesgos.

En términos generales, la pretensión de la gestión de riesgos será la reducción que se de estos hasta situarlos por debajo del denominado “umbral de riesgos”.

Ahora bien, a la hora de gestionar los riesgos en la empresa existen tres decisiones que pueden tomarse:

- Reducirlos
- Transferirlos
- Aceptarlos

Para la gestión de estos riesgos debe elaborarse un plan de acción que contendrá la siguiente información:

- **Establecimiento de prioridades:** Consiste en designar aquellos riesgos que tendrán que ser reducidos en primer lugar debido a que son los más elevados para la organización.
- **Planteamiento del análisis de coste/beneficio:** Consiste en estudiar, para cada una de las medidas que se pueden implantar, qué coste le supondría a la organización y en qué porcentaje reduciría los riesgos detectados.
- **Selección de controles definitivos:** Una vez analizado el coste/beneficio de todos los controles, hay que seleccionar definitivamente los que tendrá que implantar la organización para reducir los riesgos hasta situarlos por debajo de su umbral de riesgo.
- **Asignación de responsabilidades:** Consiste en asignar los responsables dentro de la organización de llevar a cabo la implantación de los controles. Es importante tener identificadas a estas personas ya que, si no, existe el peligro de que las decisiones que se tomen acaben por no ser implantadas.
- **Implantación de controles:** Consiste en realizar la implantación de los controles de seguridad designados. Hay que tener en cuenta que no forzosamente los controles que se implanten han de ser técnicos, sino que podrían ser controles organizativos o procedimentales.