# GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005:2011 ADAPTANDO LA *METODOLOGÍA MEHARI* PARA EL CASO DE ESTUDIO: PROCEDIMIENTO DE DESARROLLO Y MANTENIMIENTO DE APLICACIONES DE LA DIVISIÓN TIC DE LA UNIVERSIDAD DEL CAUCA

Diego Fernando Calero Velasco
Jesús Eduardo Flores Quinayás

*Universidad del Cauca*
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistema
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Junio de 2016

# GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005:2011 ADAPTANDO LA *METODOLOGÍA MEHARI* PARA EL CASO DE ESTUDIO: PROCEDIMIENTO DE DESARROLLO Y MANTENIMIENTO DE APLICACIONES DE LA DIVISIÓN TIC DE LA UNIVERSIDAD DEL CAUCA


Trabajo de Grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones

Diego Fernando Calero Velasco
Jesús Eduardo Flores Quinayás

Director: Ing. Esp. Siler Amador Donado

*Universidad del Cauca*
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistema
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Junio de 2016

# AGRADECIMIENTOS

Primero que todo, un especial agradecimiento a Dios por ser el dueño de la vida, Él fue quien permitió que se culminara satisfactoriamente esta etapa. Agradecemos al Ing. Siler Amador Donado por la orientación en el desarrollo de este proyecto de grado. Al Phd. Francisco Pino por sus observaciones y recomendaciones durante todo el desarrollo de este proyecto. Al Ing. Juan Carlos Oidor y a todo el equipo del Procedimiento de Desarrollo y Mantenimiento de Aplicaciones por la disposición y el acceso a la información para sacar adelante este proyecto.

Damos un especial agradecimiento al Sr. Jean-Louis Roule miembro de CLUSIF quien facilito la última versión actualizada y gratuita de la base de datos de reconocimiento de MEHARI para la ejecución de este proyecto.

Por otra parte queremos agradecer a nuestros familiares que son nuestro apoyo constante, sin ellos nada de esto hubiera sido posible.

# TABLA DE CONTENIDO

# LISTA DE ILUSTRACIONES

# LISTA DE TABLAS

# LISTA DE ACRÓNIMOS

| | |
|---|---|
| **CID** | Confidencialidad, Integridad y Disponibilidad |
| **CLUSIF** | Club de la Sécurité de l'Information Français, Club de los Francés de la Seguridad de la Información |
| **CNI** | Centro Nacional de Inteligencia |
| **COBIT** | Control Objectives for Information and Related Technology, Objetivos de Control para Información y Tecnologías Relacionadas |
| **CONPES** | Consejo Nacional de Política Económica y Social |
| **CRAMM** | CCTA Risk Analysis and Management Method, Análisis de Riesgo de la CCTA y Método de Gestión |
| **DARCA** | División de Admisiones, Registro y Control Académico |
| **DIV** | División |
| **DNS** | Domain Name System, Sistemas de Nombres de Dominio |
| **EBIOS** | Expression des Besoins et Identification des Objetifs de Sécurité, Expresión de Necesidad e Identificación de Objetivos de Seguridad |
| **EDGI** | Índice de Desarrollo Gobierno Electrónico |
| **GIT** | Grupo de Tecnologías de la Información |
| **IEC** | International Electro-Technical Commission, Comisión Electrónica Internacional |
| **ISMS** | Information Security Management System, Sistema de Gestión de la Seguridad de la Información |
| **ISO** | International Organization for Standardization, Organización Internacional de Estandarización |
| **MAGERIT** | Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información |
| **MEHARI** | Method for Harmonized Analysis of Risk, Metodología de Análisis de Riesgo Armonizado |

| | |
|---|---|
| **NIST SP** | National Institute of Standards and Technology Special Publications, Publicación Especial del Instituto Nacional de Estándares y Tecnologías |
| **OCTAVE** | Operationally critical Threat, Asset and Vulnerability Evaluation, Amenaza y Evaluación de Vulnerabilidad Operacional Crítica |
| **PDCA** | Plan, Do, Check and Act, Planificar, Ejecutar, Verificar y Actuar |
| **RTP** | Risk Treatment Plan, Plan de Tratamiento de Riesgo |
| **SGSI** | Sistema de Gestión de la Seguridad de la Información |
| **SI** | Seguridad de la Información |
| **SIC** | Superintendencia de Industria y Comercio |
| **SIMCA** | Sistema Integrado de Matricula y Control Académico. |
| **SOA** | Statement of Applicability, Declaración de Aplicabilidad |
| **TIC** | Tecnologías de la Información y de las Comunicaciones |
| **USD** | United States Dollar, Dólar de Estados Unidos |

# GLOSARIOS DE TÉRMINOS

**Amenaza:** Descripción de todos los factores principales de la ocurrencia del riesgo, incluyendo los eventos iniciales y si es voluntario o accidental y las circunstancias en las cuales el evento ocurre.

**Cuestiones de Seguridad:** Las consecuencias de un incidente de seguridad en los objetivos de la organización.

**Escenario de riesgo:** Descripción de todas las características del riesgo, incluyendo el activo involucrado, la vulnerabilidad intrínseca del activo afectado, y las amenazas principales de la ocurrencia del riesgo.

**Impacto intrínseco:** las consecuencias en lo que concierne a la organización si el riesgo en cuestión ocurre en ausencia de cualquier medida de seguridad.

**Impacto:** las consecuencias en lo que concierne a la organización, si el riesgo en cuestión ocurre.

**Probabilidad del riesgo:** la probabilidad de que el riesgo pueda ocurrir en lo que concierne al contexto de la organización.

**Probabilidad intrínseca:** la probabilidad de que el riesgo pueda ocurrir en lo que concierne al contexto de la organización en ausencia de cualquier medida de seguridad.

**Servicio de seguridad:** Descripción de una función de seguridad que satisface una necesidad.

**Vulnerabilidad Contextual:** El defecto o falla en un mecanismo de seguridad que pueda ser explotado desde una amenaza hasta una huelga apuntando al sistema o activo.

**Vulnerabilidad Intrínseca:** Las características intrínsecas del sistema, objetos o activos que puedan ser susceptibles a una amenaza.

# 1 PLANTEAMIENTO DEL PROBLEMA

La ciberdelincuencia crece aceleradamente año tras año, el denominado cibercrimen se ha convertido en una de las principales amenazas de cualquier organización, *"se calcula que el impacto económico de esta actividad es de unos 3 trillones (USD) a nivel mundial cifra muy superior a la del narcotráfico (1 trillón USD). Así lo afirma el experto en delitos informáticos de la firma internacional Digiware Andrés Galindo"* quien además afirma que los hackers trabajan para grandes organizaciones dedicadas al cibercrimen lo que hace aún más preocupante el panorama para las organizaciones *[1]*.

Lamentablemente Colombia en Seguridad de la Información ha sido deficiente, en el año 2010 The Economist Intelligence Unit publicó un informe en el cual afirma que Colombia se encuentra entre los "peores países", este informe destacó a Colombia en fraude electrónico. También se afirma que la quinta parte de los negocios virtuales están siendo víctimas de ataques, en dicho estudio, de 17 países latinoamericanos evaluados Colombia ocupó el número 15 solo superior a Guatemala y República Dominicana *[2]*.

En el 2015 según Intel Security el cibercrimen dejo pérdidas en Colombia del orden de los 600 millones de dólares (USD), así mismo la unidad de delitos informáticos recibió alrededor de 7118 denuncias debido al cibercrimen. Uno de los problemas que deriva de no estar bien protegidos en la Seguridad de la Información es el bajo presupuesto que se destina para la Seguridad de la Información que muchas veces ni siquiera supera el 10 por ciento.

Pasando al ámbito institucional, la Universidad del Cauca no es ajena a este tipo de amenazas, la institución es una organización la cual genera, maneja y administra información muy importante, personal y confidencial de estudiantes, profesores y administrativos, a través de sus plataformas SIMCA[1], SRF Plus[2], Finanzas Plus[3],

[1] Sistema Integrado de Matricula y Control Académico.
[2] Sistema de Recursos Financieros.
[3] Sistema de Información Financiero.

QUERYS SRH[4], SIVRI[5], Smart Access Control[6], Unicornio[7], Apolo[8], los cuales son sistemas de información vitales para la institución.

Infortunadamente, la institución no cuenta actualmente con un SGSI que permita gestionar los riesgos en la Seguridad de la Información, lo cual pone de manifiesto una problemática que podría tener grandes consecuencias, en caso de que un incidente de seguridad ocurriera afectando el normal desarrollo de las actividades institucionales. No obstante y acordes con el cambio tecnológico, la Universidad del Cauca ha tomado medidas para iniciar la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo como recomendación la norma ISO/IEC 27001:2013 que da las pautas para la correcta ejecución de un SGSI.

Siempre que se va a implementar un SGSI en una organización, en la fase inicial, se debe seleccionar una metodología de gestión de los riesgos apropiada para la organización de acuerdo a su tamaño, propósito, alcance del SGSI, etc. En la actualidad, existen muchas metodologías de gestión del riesgo que se pueden seleccionar para llevar a cabo esta tarea, pero la institución con el objetivo de encontrar la metodología que mejor se adapte a sus propósitos, ha probado con diferentes metodologías de gestión de riesgo tales como Octave-S, NIST-SP-800-53 y Cobit-5. En este trabajo de grado se evaluará y adaptará la metodología MEHARI para la gestión del riesgo en el caso de estudio propuesto, con el fin de que Jefe de TIC's de la Universidad del Cauca en compañía del Director de este trabajo de grado, analicen entre las metodologías ya probadas y la metodología MEHARI cual es más benéfica para la institución. Se parte del hecho de que se selecciona la metodología MEHARI, ya que el objetivo es ejecutarla y evaluarla en el procedimiento de estudio seleccionado.

Según lo expuesto, surge el siguiente interrogante para el proyecto:

[4] Sistemas Recursos Humanos.
[5] Sistema de Información Vicerrectoría de Investigaciones.
[6] Sistema Control de Acceso.
[7] Sistema de Información Bibliográfica.
[8] Sistema de Información para Hemeroteca.

¿Es la metodología MEHARI adecuada y adaptable para el desarrollo de la fase de planeación de un SGSI para gestionar el riesgo de la Seguridad de la Información según la norma ISO/IEC 27001:2013 para el caso de estudio propuesto?

## 1.1 JUSTIFICACIÓN DEL PROYECTO

Para la Universidad del Cauca es fundamental la Seguridad de la Información, debido a que la mayor parte de la información de la universidad tanto financiera como académica es manejada por sistemas de información que la misma universidad administra. El Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca es un procedimiento crítico, por tal motivo es necesario tomarlo en cuenta dentro del alcance de un SGSI. El diagrama de flujo del procedimiento está consignado en el anexo A.8.

El tema de la Seguridad de la Información para la universidad es muy importante y toma relevancia, esto lo demuestra la resolución R-005 de 2015 *[3]*, en la cual la institución manifiesta la necesidad de la implantación de un sistema de gestión de Seguridad de la Información. Además, la universidad emitió la resolución R-785 de 2015 en donde se especifican las políticas generales de seguridad que guiarán a la institución en este tema de Seguridad de la Información *[4]*. Esto evidencia el interés que tiene la universidad en realizar la implantación de este sistema para proteger sus activos de información y el buen nombre con el que siempre se ha destacado.

Por otro lado, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia está invitando a todas las entidades públicas locales, regionales y nacionales a adelantar el programa de Gobierno en Línea a través de la *"Estrategia Gel" [5]*. El programa de Gobierno en Línea tiene seis componentes: "Elementos Transversales", "Información en Línea", "Interacción en Línea", "Transacción en Línea", "Transformación" y "Democracia en Línea". Cada uno de estos componentes se materializa en actividades para cumplir con cada objetivo. En el primer componente "Elementos Transversales" se tienen cuatro actividades: Institucionalizar la estrategia de Gobierno en Línea, centrar la atención en el usuario, implementar un sistema de gestión TI y por ultimo implementar un SGSI *[6].* Esto quiere decir, que para implementar la estrategia que el manual de Gobierno en

Línea propone, se debe establecer un SGSI como actividad importante en este componente inicial[9].

Por otra parte el Estado Colombiano aprobó una nueva política nacional de seguridad digital el 11 de abril de 2016 conocido como conpes 3854 que obliga a las entidades públicas y privadas del país a mitigar los riesgos informáticos a través de la valoración y gestión del riesgo.

Acorde con la ley vigente, con la necesidad institucional de proteger la información y de encontrar la metodología de gestión del riesgo más conveniente para la institución, se propone el presente trabajo de grado para ser ejecutado en el caso de estudio Procedimiento Desarrollo y Mantenimiento de Aplicaciones de la Universidad del Cauca.

## 1.2 CASO DE ESTUDIO

Se utilizará el caso de estudio según el protocolo descrito por Yin (1984), con el fin de analizar en profundidad y en contexto a la organización, Robert Yin especifica las fases para poder desarrollar un caso de estudio. Se decide usar el caso de estudio como estrategia para conocer la problemática de la organización, responder algunas cuestiones necesarias para la adaptación de la metodología y recolectar la información para el análisis.

La *ilustración 1-1* muestra el protocolo de estudio según Robert Yin, cada una de estas fase serán descritas teniendo en cuenta de no afectar la confidencialidad de la organización en cuanto al tratamiento y divulgación de los datos.

[9] Ver anexos A.4 y A.5

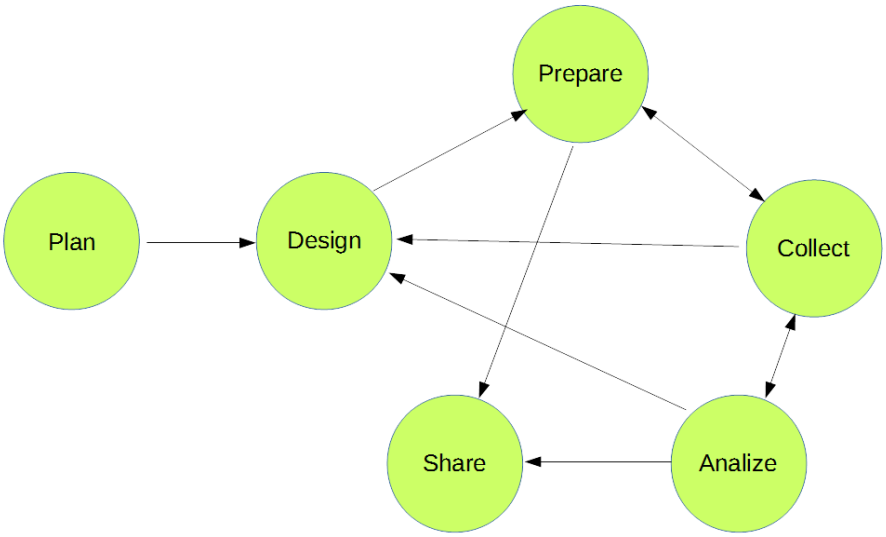



***Ilustración 1-1.*** *Protocolo de caso de estudio Robert Yin.*

## 1.2.1 Diseño del caso de estudio

*1. Pregunta de estudio*

En esta fase se identifica la pregunta del caso de estudio que se quiere resolver, teniendo en cuenta que se va a trabajar en la División de Tecnologías de la Información y las Comunicaciones es necesario en este apartado conocer los antecedentes de la organización con respecto al tema que se va a tratar en este caso en Seguridad de la Información y las ventajas que tiene un SGSI.

Un SGSI es muy importante para todo tipo de organizaciones cualquiera sea su propósito, la Universidad del Cauca y específicamente el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones no ha iniciado trabajos relacionados con la Seguridad de la Información ni se encuentran trabajos anteriores que aporten en cuanto a este tema. La pregunta de caso de estudio que se plantea es: ¿cómo se pude adaptar la metodología MEHARI en el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca?

*2. Unidad de análisis*

La unidad de análisis es el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la Universidad del Cauca, por lo tanto el diseño de caso de estudio es holístico simple. Este procedimiento se encuentra completamente descrito con sus respectivas actividades en el anexo A.8.

### 1.2.2 Preparación para la recolección de datos

Se obtienen copias de los documentos de la organización, al igual que se elabora un plan de clasificación, consulta y almacenamiento de la información, en el capítulo 4 de este documento se muestra la recopilación de toda la información con el personal encargado del área.

### 1.2.3 Recopilación de datos en el campo

La recopilación de los datos en el campo, es decir, en el caso de estudio se realiza a través de múltiples entrevistas, grabaciones y encuestas.

La recopilación de algunos de los datos para este caso de estudio específico se realizó a través de entrevistas individuales al personal de desarrollo y mantenimiento de las aplicaciones, así como también por medio de las grabaciones y por medio de la observación directa. En la identificación de los requisitos de la organización se muestran la información recolectada del caso de estudio ver capítulo 4.

Esta fase de igual manera permitió la identificación de los activos de información a cargo de cada miembro del equipo de desarrollo, la recopilación de la información de los activos de información se encuentra en el anexo B.7 requisitos de seguridad.

### 1.2.4 Evaluación y análisis de los datos

El análisis y la evaluación de los datos se describen en el capítulo 4 sección 4.4 no sin antes mencionar que por motivos de confidencialidad algunos detalles se omiten.

## 1.3 INVESTIGACIÓN-ACCIÓN

El principal objetivo de la investigación-Acción es la generación de conocimiento a partir de la práctica *[7]*. La adaptación de la metodología MEHARI al caso de estudio se realizó mediante la ejecución de la metodología MEHARI al procedimiento y siguiendo como filosofía la Investigacion-Accion. El proceso que se siguió en para la adaptación de la metodología MEHARI al caso de estudio se muestra en la *ilustración 1-2.*

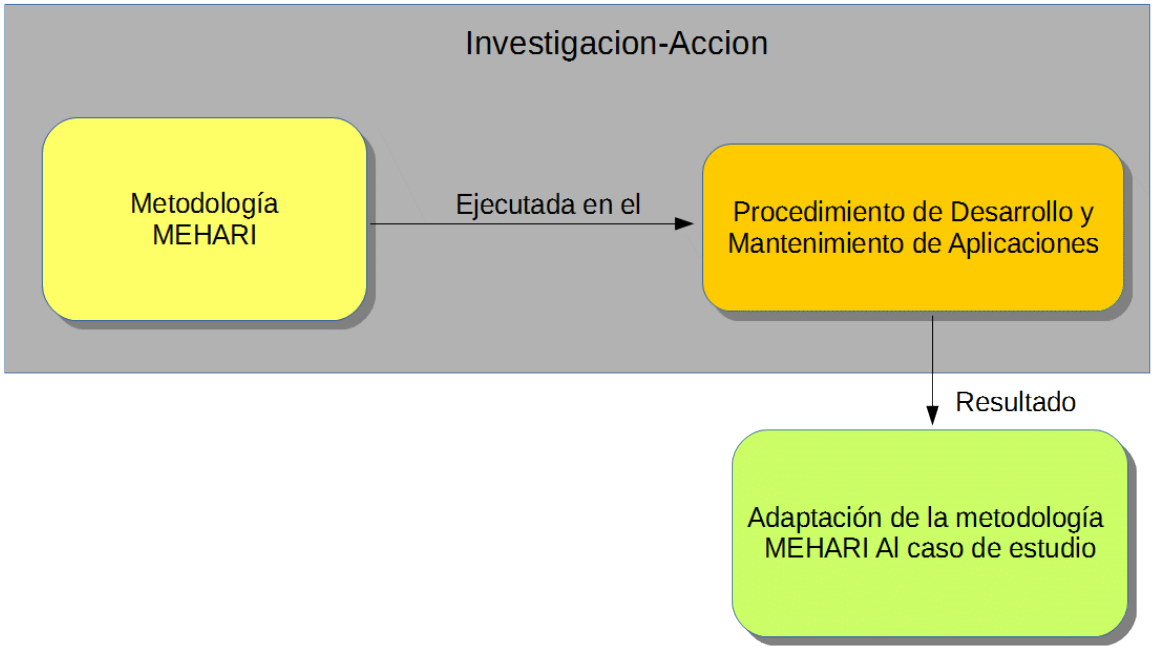



***Ilustración 1-2.*** *Filosofía de Investigación-Acción*

## 1.4 OBJETIVOS

### 1.4.1 Objetivo general

Ejecutar la fase de planeación de un SGSI para gestionar el riesgo de la Seguridad de la Información según la norma ISO/IEC 27001:2013 adaptando la *metodología MEHARI* para el caso de estudio: Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca.

### 1.4.2 Objetivo especifico

- Definir el alcance y los límites del SGSI para el caso de estudio.
- Definir las políticas que se apoyarán dentro del marco de la política general SGSI de la Universidad del Cauca.
- Analizar los requisitos de Seguridad de la Información relacionados al caso de estudio de acuerdo al alcance del SGSI definido.
- Valorar el riesgo y planificar el tratamiento de riesgos según la metodología MEHARI.

# 2 MARCO TEÓRICO

## 2.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI es la abreviatura que se utiliza para nombrar un Sistema de Gestión de la Seguridad de la Información[10] *[8].* El objetivo de un SGSI es establecer directrices, políticas, procedimientos y controles de seguridad con el fin de mantener lo más seguro posible el activo más importante que es la información, dejando en un nivel mínimo la exposición frente a riesgos y amenazas, que son inherentes a las organizaciones que hacen uso de las tecnologías de la información y las comunicaciones (TIC).

Un SGSI es un sistema que consta de una serie de actividades que deben realizarse mediante procesos, documentos y procedimientos en una organización. El propósito de este sistema no es exactamente garantizar seguridad en un 100%, se da por establecido que no existe la forma de garantizar que un sistema sea completamente seguro. En su lugar, el SGSI se implementa para garantizar que los riesgos de la Seguridad de la Información sean gestionados, asumidos, conocidos y en lo posible minimizados *[9].*

Según el documento en *[9]* la norma ISO/IEC 27001, requiere los siguientes documentos bases para la implantación de un SGSI:

1. Alcance del SGSI
2. Política y objetivos de seguridad
3. Estándares, procedimientos, y guías que soportan SGSI
4. Metodología de evaluación de riesgo
5. Informe de evaluación de riesgo
6. Plan de tratamiento de riesgos
7. Registros
8. Declaración de aplicabilidad
9. Control de la documentación

[10] o ISMS, Information Security Management System por sus siglas en inglés.

## 2.2 ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Antes de abordar el tema de gestión de Seguridad de la Información se debe tener claro el término Seguridad de la Información, la Seguridad de la Información es la preservación de tres principios básicos: confidencialidad, disponibilidad e integridad *[9]*.

Cuando se habla de Gestión de la Seguridad de la Información necesariamente se recurre a los organismos más importantes de estandarización, la familia de normas ISO/IEC 27000 contienen las mejores prácticas recomendadas en Seguridad de la Información y regulan los SGSI dentro de las organizaciones. La norma más importante de la serie es la ISO/IEC 27001[11], esta norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI *[10]*.

La ISO/IEC 27002[12] contiene la guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a la Seguridad de la Información. La ISO/IEC 27003[13] se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo a la norma ISO/IEC 27001:2013. La ISO/IEC 27004 es una guía para el desarrollo y la utilización de métricas y técnicas de medida aplicable para determinar la eficacia de un SGSI y de los controles o grupo de controles implementados según la ISO/IEC 27001:2013 *[11]*.

La norma que se ocupa de la gestión de los riesgos de la Seguridad de la Información es la ISO/IEC 27005, esta norma da las pautas para la gestión del riesgo en cualquier organización, apoyando los requisitos establecidos del SGSI definidos en la ISO/IEC 27001. Las principales normas de la serie ISO/IEC 27000 son las que se describen a continuación:

- ISO/IEC 27000: Términos y definiciones.

[11] Véase anexo A.1.
[12] Véase anexo A.2.
[13] Véase anexo A.3.

- ISO/IEC 27002: Objetivos de control y controles.
- ISO/IEC 27003: Guía de implementación de un SGSI.
- ISO/IEC 27004: Métricas y técnicas de medidas de la efectividad de un SGSI
- ISO/IEC 27005:Guía para la gestión del riesgo de Seguridad de la Información

La relación entre las normas ISO/IEC mencionadas anteriormente se detalla en la *ilustración 2-1.*


***Ilustración 2-1.*** *Relación entre las normas ISO en el marco de un SGSI*

La única norma que es certificable de toda la serie es la ISO/IEC 27001 que a la fecha de la realización de este trabajo de grado, la versión más reciente de la norma es la ISO/IEC 27001: 2013.

La diferencia de la ISO/IEC 27001: 2013.con respecto a su versión antecesora es que los controles especificados en el anexo A de la norma eran obligatorios, pero a partir de la nueva versión esos anexos se hicieron opcionales, dándole la oportunidad a la organización de que ella mismas implante los controles de seguridad que requieran la organización de acuerdo a sus necesidades *[12]*.

## 2.3 IMPLANTACIÓN DE UN SGSI

La implementación de un sistema de gestión de Seguridad de la Información (SGSI) es una decisión estratégica que debe involucrar a toda la organización y debe ser apoyada y dirigida desde la dirección, ya que fundamentalmente es la dirección quien decidirá invertir o no en los diferentes mecanismos de seguridad, es por este hecho que el SGSI debe ser guiado y apoyado por la alta dirección. Véase anexo A.6.

### 2.3.1 Ciclo Deming

El ciclo Deming conocido así por su creador Edward Deming en 1950 *[13]*, es una herramienta que se ha hecho muy popular y ha sido aplicada en muchas organizaciones con el fin de alcanzar la mejora continua de sus procesos, la ISO/IEC 27001:2013 adopta este modelo.

Este modelo está debidamente estructurado y tiene cuatro fases bien definidas las cuales son[14]: *planear, ejecutar, verificar y actuar.* Es un ciclo constante de modo que al terminar la fase *Actuación* el ciclo vuelve a comenzar con la fase inicial.

La ISO/27001 recomienda seguir este modelo para su proceso de mejora continua en el sistema de gestión de Seguridad de la Información (SGSI). La *ilustración 2-2* muestra los cuatro ciclos del modelo PDCA.

[14] O PDCA por sus siglas en inglés: Plan, Do, Check and Act

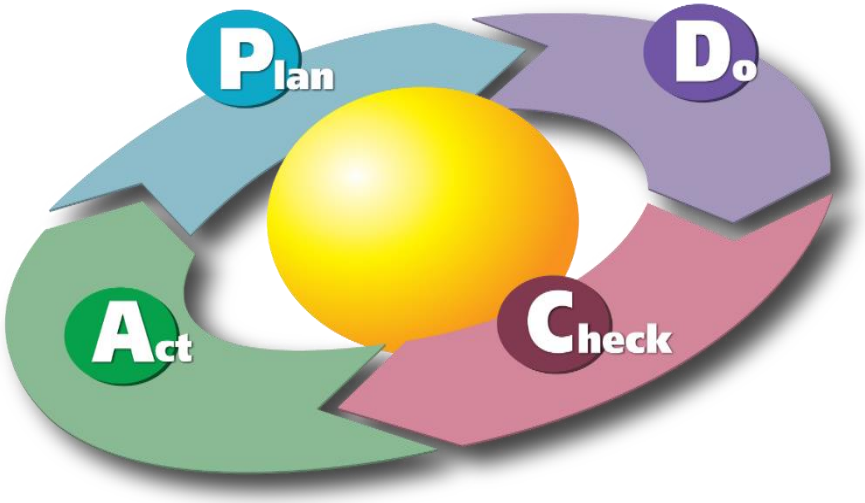



***Ilustración 2-2.*** *Modelo PDCA*

## 2.3.2 Fase de planeación

En la fase *planeación* se define el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión, además se definen la políticas de seguridad que incluya el marco general y los objetivos de Seguridad de la Información de la organización, se establecen los criterios para la evaluación de los riegos, esta debe estar aprobada por la dirección, además se define una metodología de evaluación de riesgos apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y uso criterios de aceptación de los mismos. En la *ilustración 2-3* se muestra la fase de planeación conforme a la norma ISO/IEC 27001

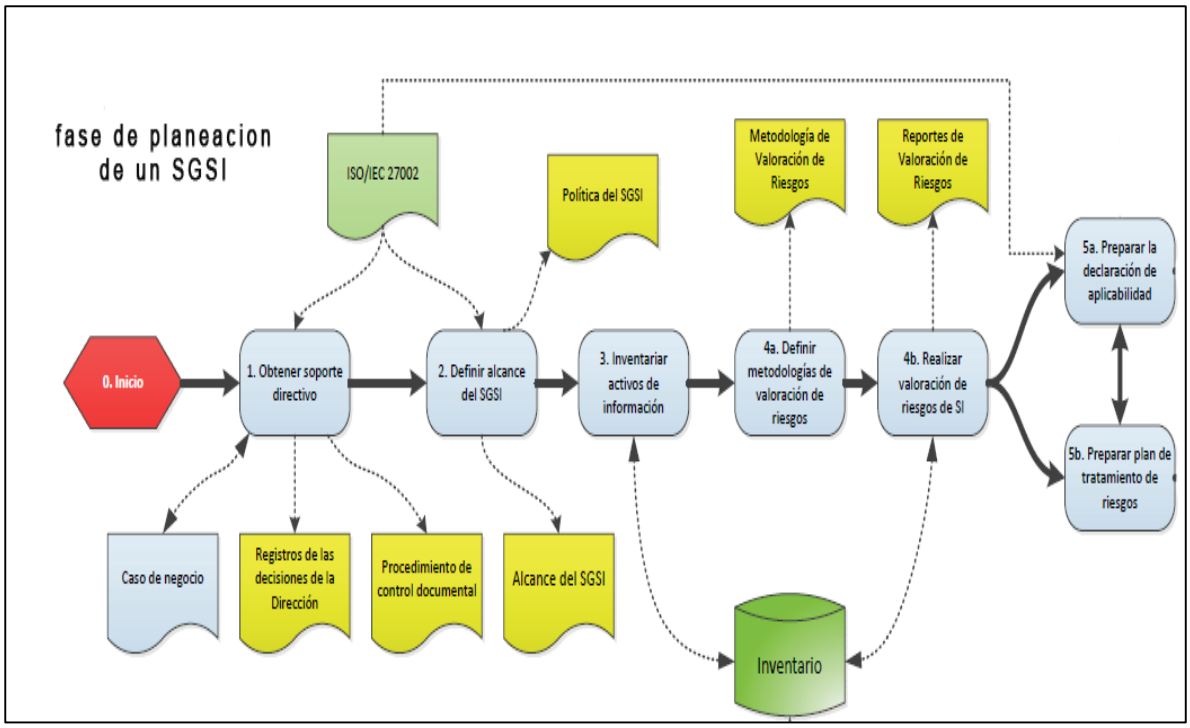



***Ilustración 2-3.*** *Fase de planeación de un SGSI según la norma ISO/IEC 27001*

Las diferentes tareas de la fase de plan de un SGSI se describen a continuación *[14]*:

1. *Obtener gestión de soporte*

El obtener la gestión de soporte es muy importante. La administración debe apoyar activamente la Seguridad de la Información, hacia una dirección clara, que demuestre el compromiso de la organización. La administración debe aprobar la política de Seguridad de la Información, debe asignar los recursos, funciones de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización, el apoyo a la gestión abierta hace que la seguridad de información sea más eficaz en toda la organización.

2. *Definir alcance del SGSI*

El alcance de la SGSI debe ser definido en términos de la naturaleza de la empresa. Toda exclusión de la aplicación dentro de la SGSI debe ser justificada y documentada. Si los controles comunes se consideran no aplicable, esto debe ser argumentado y documentado en la declaración de aplicabilidad Statement of

Applicability (SOA). Los auditores de la certificación comprobarán la documentación exigida por la norma correspondiente.

*3. Inventariar activos de información*

Se debe realizar un inventario de todos los activos de información importantes, estos deben ser desarrollados y mantenidos, registrando detalles como:

- ✓ Formato
- ✓ Localización.
- ✓ Copia de seguridad.
- ✓ Información de licencia.
- ✓ Valor empresarial.

*4. Realizar valoración de riesgo de Seguridad de la Información*

Las evaluaciones de riegos deben identificar, cuantificar y priorizar los riesgos de la seguridad de información en contra de los criterios definidos para la aceptación del riesgo y los objetivos relevantes para la organización.

Los resultados deben guiar y determinar la apropiada acción de gestión del riesgo de la Seguridad de la Información y de la aplicación de los controles seleccionados para la protección contra riesgos. Valoración de riesgos y controles de selección pueden necesitarse en varias ocasiones a través de diferentes partes de los sistemas de la organización. La evaluación de los riesgos de seguridad de información debe tener un ámbito claramente definido y complementar las evaluaciones de riesgos en otros aspectos de la empresa.

*5a. Preparar la declaración de aplicabilidad*

La declaración de aplicabilidad (SOA) es un documento clave de una SGSI, lista los objetivos de control y controles de seguridad que la organización adoptará. La declaración de aplicabilidad se deriva de los resultados de la evaluación de riesgos, donde:

- ✓ Los requisitos legales y reglamentos pertinentes han sido identificados
- ✓ Las obligaciones contractuales se entienden completamente
- ✓ Una revisión propia de necesidades y requerimientos de negocio de la organización se ha llevado acabo.

*5b. Preparar plan de tratamiento del riesgo*

La organización debe formular un plan de tratamiento del riesgo, Risk Treatment Plan (RTP), la identificación de las acciones de gestión adecuadas, recursos, responsabilidades y prioridades para hacer frente a los riesgos de Seguridad de la Información. El plan de tratamiento del riesgo se debe establecer en el contexto de la Política de Seguridad de la Información de la organización y debe identificar claramente el enfoque al riesgo y los criterios de aceptación de riesgo.

### 2.3.3 Fase de ejecución

En la fase de *ejecución* se lleva a cabo la implantación de los controles de seguridad seleccionados en la fase anterior, estos controles se refieren a los controles más técnicos, así como la documentación necesaria. En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, también se formula y se implementa un plan de riesgo.

### 2.3.4 Fase de verificación y actuación

La tercera fase del ciclo Deming es la fase de *seguimiento* en ella se evalúa la eficacia y el éxito de los controles implantados, el modelo PDCA se completa con la fase de *mejora* durante la que se llevará a cabo las labores de mantenimiento del sistema. Todo el proceso de implementación de un SGSI con sus cuatro fases correspondientes descritas según las ISO/IEC 27001 se muestra en los anexos A.6 cada uno de los entregables que son obligatorios para la correcta implementación del SGSI están ilustrados, así como también se ilustra el ciclo Deming en cada una de sus etapas.

## 2.4 GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA ISO/IEC 27005

La norma encargada de proveer lo requerimientos de la gestion del riesgo es la ISO/IEC 27005, esta norma da soporte a los requerimientos de la ISO/IEC 27001:2013. La ISO 27005 no especifica cómo realizar el proceso de evaluación y análisis del riesgo específicamente, sino que se centra en aspectos teóricos muy generales que deben ser considerados, de ahí que existen muchas metodologías para la valoración y análisis de riesgo para llenar este vacío que deja la norma. El proceso de gestión del riesgo descrito por ISO/IEC 27005 comprende el establecimiento del contexto, valoración de riesgos, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, monitoreo y revisión del riesgo tal como se muestra en el *ilustración 2-4*.

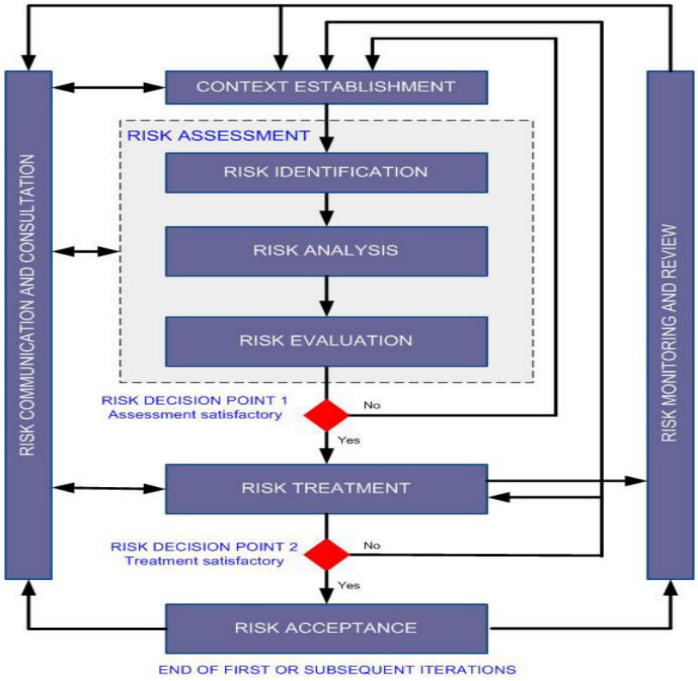



***Ilustración 2-4.*** *Diagrama funcional de la norma ISO/IEC 27005*

# 3 GESTIÓN DE RIESGOS CON LA METODOLOGIA MEHARI

## 3.1 CONCEPTOS GENERALES DE LA METODOLOGIA MEHARI

El principal objetivo de MEHARI es proporcionar una metodología para la evaluación y gestión del riesgo en el dominio de la Seguridad de la Información conforme los requerimientos de la norma ISO/IEC 27005 *[15]*. La metodología de valoración de riesgos MEHARI fue desarrollada por una organización de seguridad sin ánimo de lucro, CLUSIF[15] *[16]*.

MEHARI es una metodología de gestión del riesgo notable por el hecho de que realiza un análisis de los riesgos de manera directa e individual *[17]*, en contraste con otro tipo de metodologías de análisis de riesgos que lo hacen de una manera general lo que provee menos diferenciación entre los riesgos. Existen dos enfoques para la gestión de los riesgos, el primer tipo de gestión del riesgo consiste en identificar todos los tipos de riesgos y analizar cada situación de riesgo identificando y tomando las decisiones específicas para cada una, con una fuerte intervención del profesional a cargo de la Seguridad de la Información la *ilustración 3-1* muestra el proceso de identificación de los riesgos, análisis y evaluación siguiendo el enfoque directo e individual.

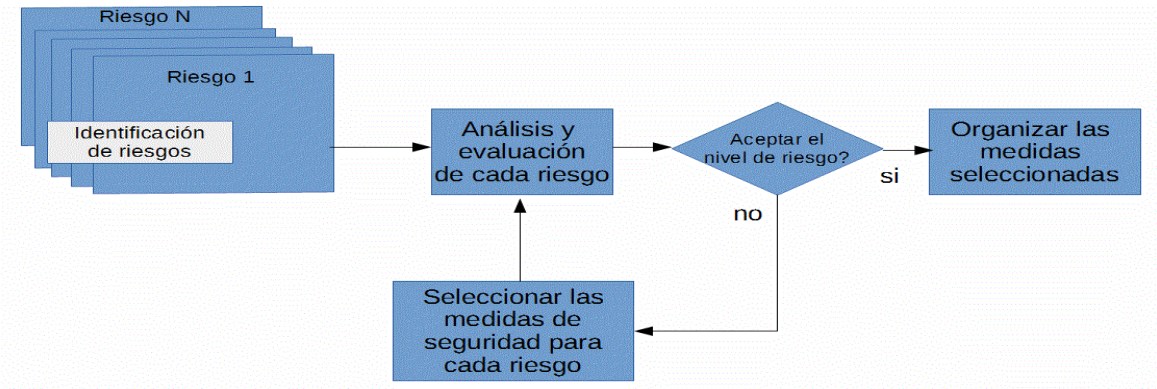



***Ilustración 3-1.*** *Enfoque individual para la gestión del riesgo*

[15] Club de la Security Français por sus siglas en Francés en 1996

El segundo tipo de gestión del riesgo en contraste hace un análisis mucho más general que identifica los objetivos de seguridad y regulaciones específicas para una reducción global del riesgo, sin un profundo análisis y sin una gestión del riesgo directa o individual y probablemente con menor intervención del profesional en Seguridad de la Información.

La *ilustración 3-2* muestra el proceso que sigue un enfoque metodológico general de análisis de riesgos.

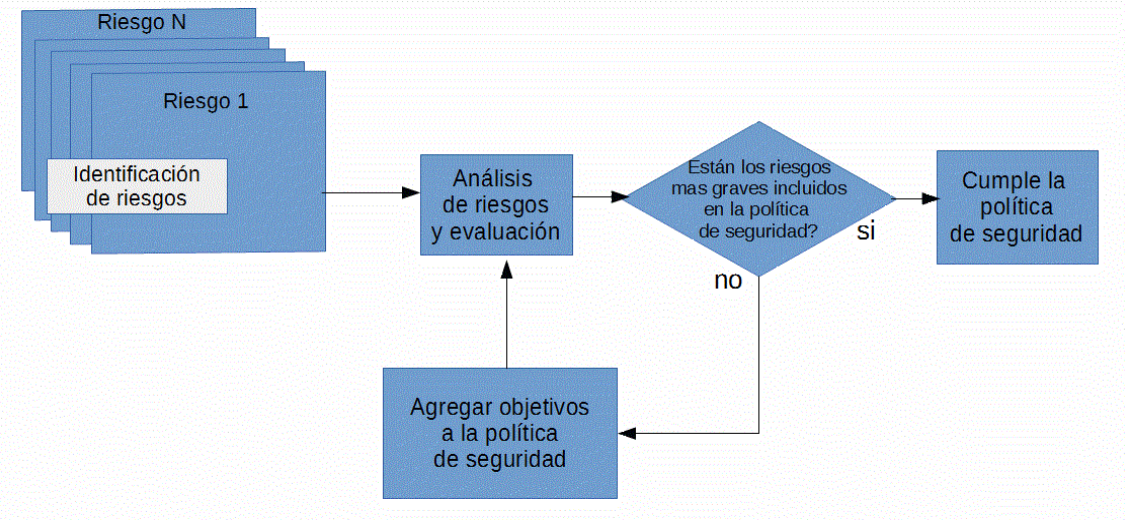



***Ilustración 3-2.*** *Enfoque general de gestión del riesgo*

Cada uno de estos enfoques para el análisis de riesgos tiene sus ventajas y desventajas. La *tabla 3-1* muestra una comparativa entre los dos enfoques *[18]*.

| | **Directa e individual gestión del riesgo** | **Global e indirecta gestión del riesgo** |
|---|---|---|
| **Ventajas** | • Identificación y análisis de todas las situaciones de riesgos.<br>• Evaluación precisa del nivel de riesgo por cada situación de riesgo.<br>• Precisa evaluación de los efectos de las medidas de seguridad sobre el nivel de riesgo por cada situación de riesgo. | • Presentación simple del riesgo.<br>• Fácil de entender el concepto.<br>• Fácil comunicación de los riesgos.<br>• Facilidad de vincular el riesgo a la medida para el control. |
| **Desventajas** | • Requiere un completo modelo de la presentación de todos los riesgos.<br>• Requiere que cada situación de riesgo sea presentada en toda su complejidad. | • Abierto para ignorar graves situaciones de riesgo.<br>• Carencia de valoración de la gravedad del nivel del riesgo.<br>• Sobrecosto o sub-evaluación en el tratamiento del riesgo. |

***Tabla 3-1.*** *Ventajas y desventajas de tipos de enfoque para la gestión del riesgo*

La metodología MEHARI adopta un enfoque para un análisis directo e individual de cada situación de riesgo, en ese sentido cada riesgo debe ser identificado y descrito por escenarios que contienen cierto número de elementos precisos y muy específicos. Cada escenario de riesgo puede ser evaluado cuantitativamente (es decir que el riesgo puede ser medido) y esta evaluación tiene en cuenta:

- El impacto intrínseco del escenario de riesgo que refleja el nivel de consecuencia de la ocurrencia del escenario, en ausencia de cualquier medida de seguridad.

- La probabilidad intrínseca del escenario (o exposición natural del escenario) que refleja la probabilidad de ocurrencia del escenario, en ausencia de cualquier mecanismo de seguridad.

- Los factores de reducción de riesgo basados en las medidas de seguridad, categorizados por el tipo de efecto que ellos tienen sobre el impacto o la probabilidad de las medidas de riesgo y de la calidad de esas medidas.

El proceso para la evaluación de cada escenario permite seleccionar medidas de seguridad, con objetivos cualitativos por cada medida para que el riesgo pueda ser mantenido por debajo de un nivel aceptable por la organización.

La estructura de gestión del riesgo de MEHARI se muestra en la *ilustración 3-3.* El objetivo de MEHARI es ser detallado en cada fase *[19]*.

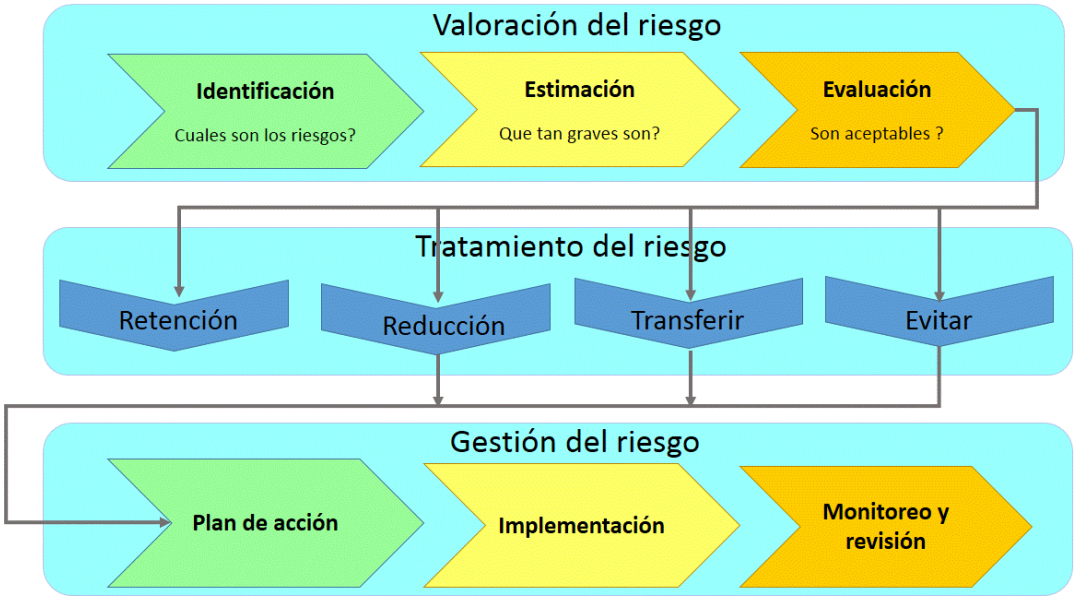



***Ilustración 3-3.*** *Proceso de valoración, tratamiento y gestión del riesgo según MEHARI*

## 3.2 VALORACION DEL RIESGO SEGÚN MEHARI

La valoración del riesgo consiste en un análisis tan exhaustivo como sea posible de todas la situaciones de riesgo a los que está expuesta una organización y evaluar si cada riesgo será aceptado o no. Cada paso en este proceso debe ser desarrollado asegurando una precisa evaluación de la gravedad de cada riesgo de acuerdo con

el contexto y especialmente con las medidas de seguridad existentes. Los tres pasos que constituyen todo el proceso de valoración del riesgo son:

1. *Identificación del riesgo*
2. *Estimación del riesgo*
3. *Evaluación del riesgo*

### 3.2.1 Identificación del riesgo

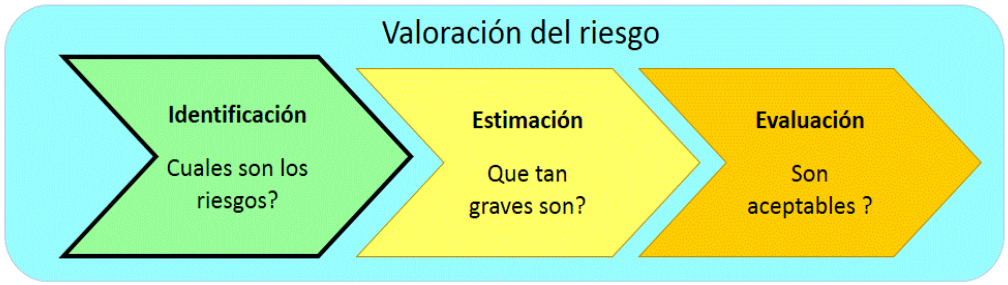



***Ilustración 3-4.*** *Proceso de identificación del riesgo*

El objetivo de la identificación del riesgo no es solamente la identificación de las situaciones de riesgo, sino que también la caracterización de cada riesgo en detalle, esto es, sus diferentes factores que hacen que el riesgo exista con el fin de ver cuán grave es cada riesgo. Los elementos que deben ser descritos para cada riesgo son: el activo, la vulnerabilidad intrínseca del activo afectado por el riesgo, el activo afectado y todos los factores que conllevan a la ocurrencia del riego.

Mehari realiza una descripción de los activos de información y los clasifica de acuerdo a tres categorías principales las cuales son: servicios, datos necesarios para la función de los servicios y gestión de procesos, estos activos son los denominados por MEHARI como activos de información primarios.

Los activos de información tienen vulnerabilidades y la explotación de esas vulnerabilidades es lo que causa el riesgo. Para encontrar estas vulnerabilidades en MEHARI es crucial distinguir lo siguiente por cada activo primario:

- Las diferentes formas que el activo puede tomar.
- Las diferentes contingencias sobre los cuales el activo puede depender.

Las formas y contingencias pueden ser agrupadas bajo el nombre de activos de soporte o activos secundarios. MEHARI está en conformidad con la ISO/IEC 27005 en cuanto a este requisito los activos primarios corresponden a las necesidades funcionales, mientras que los activos secundarios corresponden a un nivel físico y concreto que son los medios requeridos para reunir las necesidades funcionales (activos primarios).

Para cumplir con los objetivos de una gestión del riesgo de manera directa e individual cada riesgo identificado debe incluir una descripción del activo en cuestión esta descripción deben tener en cuenta tanto el activo primario como el activo secundario involucrado.

El riesgo surge del hecho de que un activo de información tiene uno o varias vulnerabilidades, las vulnerabilidades intrínsecas dependen del tipo de activos secundarios, cada riesgo identificado debe incluir una descripción de la vulnerabilidad intrínseca asociada además cada riesgo debe especificar el tipo de daño al activo, cada riesgo identificado debe incluir una descripción de activo en cuestión esta descripción debería especificar tanto el activo primario como el activo secundario, MEHARI y su base de datos de conocimiento cumplen con estas especificaciones.

El último paso en la identificación es la descripción de las causas de la ocurrencia de las amenazas, se deben identificar los eventos que originaron la amenaza o las amenazas, los actores que producen la amenaza y la circunstancias en las cuales la amenaza o amenazas ocurren, si el evento es voluntario o es accidental, el actor y la circunstancias en que el evento ocurre, cada uno de estos elementos claramente tienen una influencia en la probabilidad de ocurrencias del riesgo.

En la *ilustración 3-5* se muestra el proceso de la definición de activos, la identificación de las vulnerabilidades por cada uno de los activos y los eventos que originan las amenazas. La descripción de cada uno de los riesgos y sus vulnerabilidades asociadas ayudan a la creación de los escenarios de riesgos para la valoración. Cada riesgo debe estar debidamente detallado de forma individual este es el enfoque que le da la metodología MEHARI.

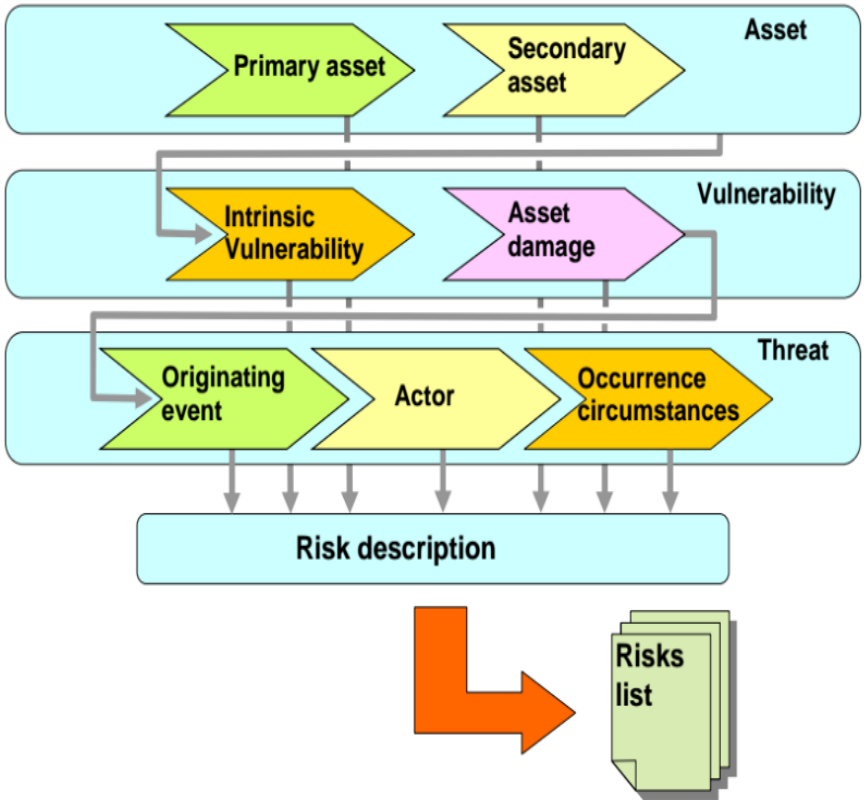



***Ilustración 3-5.*** *Proceso de listado de los riesgos siguiendo el enfoque individual*

### 3.2.2 Estimación del riesgo


***Ilustración 3-6**. Proceso de estimación del riesgo*

El objetivo de la estimación del riesgo es identificar qué tan grave es cada uno de los riesgos identificados previamente, teniendo en cuenta las diferentes medidas de seguridad implementadas.

Frecuentemente el riesgo se mide basado en dos parámetros conocidos como el impacto, que significa el nivel de gravedad de las consecuencias y la probabilidad de ocurrencia del riesgo. Una valoración global y directa de estos dos parámetros es generalmente difícil, es preferible usar un enfoque más analítico que desglose estos parámetros en múltiples niveles y evaluarlos individualmente:

- El impacto intrínseco excluyendo todas las medidas de seguridad.
- La probabilidad intrínseca excluyendo todas las medidas de seguridad.
- El efecto de las medidas de seguridad sobre estos dos parámetros.

El impacto intrínseco de un riesgo es definido por el nivel máximo de consecuencia en que la organización pueda incurrir, en ausencia de cualquier medida de seguridad diseñada específicamente para reducir estas consecuencias. Esto se deberá hacer referenciando el tipo de activo primario o secundario y el tipo de consecuencias. La probabilidad intrínseca es la máxima probabilidad de que el riesgo pueda ocurrir sin tomar en cuenta ninguna medida de seguridad específicamente para mitigar esta probabilidad.

Algunos factores permiten la reducción tanto del impacto y de la probabilidad de ocurrencia de los riesgos estas medidas se conocen en MEHARI como efectos de medidas de seguridad[16].
Los factores de reducción del riesgo de la probabilidad se conocen como medidas disuasivas y medidas preventivas, los factores de reducción del impacto son denominados confinamiento y paliación.

Cada escenario de riesgo es valorado en múltiples fases, cada una de las cuales contribuye independientemente a evaluar la probabilidad y el impacto de cada escenario de riesgo como se muestra en la *ilustración 3-7*.

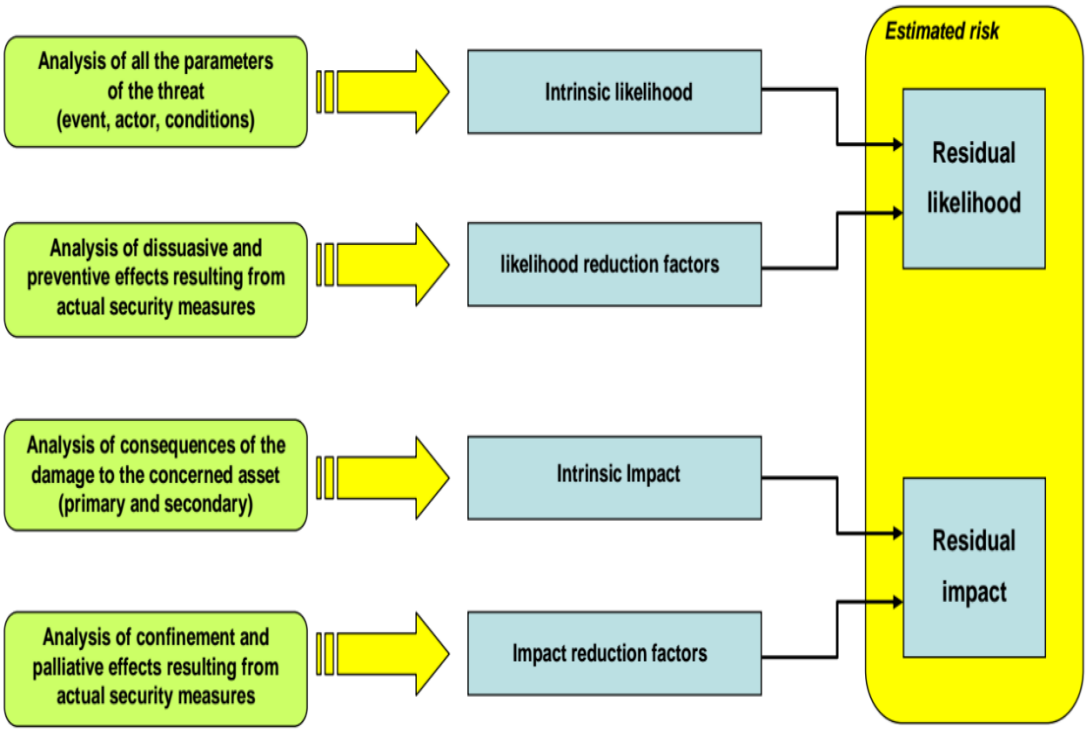



***Ilustración 3-7.*** *Estimación del riesgo teniendo en cuenta los parámetros de MEHARI*

[16] Factores de Reducción de Riesgos

### 3.2.3 Evaluación del riesgo


***Ilustración 3-8.*** *Proceso de evaluación del riesgo*

La gravedad de cada escenario de riesgo es función tanto de la probabilidad residual, como del impacto residual, en este paso de la evaluación se decide si la situación de riesgo es aceptable por la organización o no. Las tres categorías en las que el riesgo puede ser definido es:

Riesgo intolerable: el cual requiere medidas urgentes, fuera del normal ciclo de balance o análisis de riesgos.

Riesgo inadmisible: que puede ser reducido o eliminado en algún momento en el tiempo este debe ser integrado al ciclo de planeación (plan de seguridad)

Riesgo aceptable: no requiere medidas urgentes

En la *ilustración 3-9* se muestra manera de medir la gravedad global que propone MEHARI, esta ilustración depende de dos factores el impacto y la probabilidad anteriormente descritos.

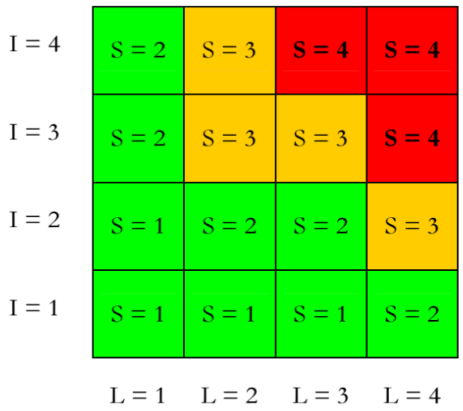



***Ilustración 3-9.*** *Evaluación de la gravedad global del riesgo*

## 3.3 TRATAMIENTO DEL RIESGO

Diferentes opciones están disponibles para tratar los riesgos una vez han sido identificados, listados y evaluados como se muestra en la *ilustración 3-10*. A continuación se describen las opciones para tratar el riesgo según la norma ISO/IEC 27005 y la metodología MEHARI.

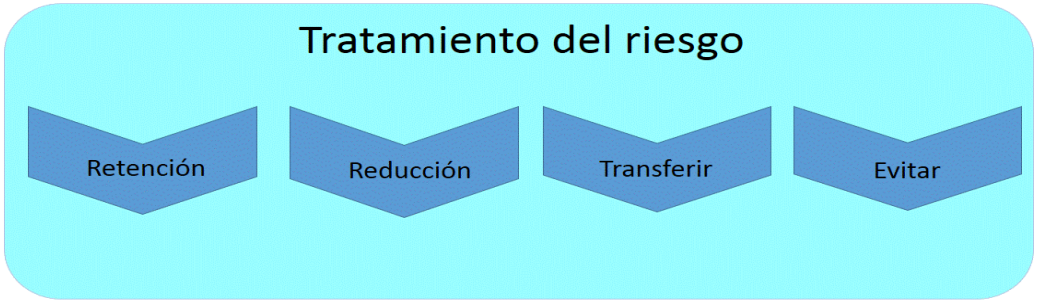



***Ilustración 3-10.*** *Tratamiento del Riesgo según MEHARI*

*1. Retener (aceptar) el riesgo*

Retener un riesgo significa aceptar la situación de riesgo que se describe en el escenario de riesgo.

2. *Reducir el riesgo*

Reducir significa minimizar uno de los dos parámetros característicos del riesgo, probabilidad o impacto, o en ocasiones ambos usando acciones específicas tales soluciones son determinadas por los riesgos identificados como no aceptables.

3. *Transferir el riesgo*

Significa, en términos prácticos, transferir el riesgo a un tercero.

4. *Evitar el riesgo*

Evitar el riesgo es similar a reducir un riesgo a través de medidas estructurales. La diferencia está en el hecho de que el riesgo no exista más, en otras palabras destruir el riesgo.

## 3.4 GESTION DEL RIESGO

La gestión del riesgo contempla todo el proceso que facilita la implementación de las decisiones previas hechas concernientes al tratamiento del riesgo, monitoreando los efectos de esas decisiones y mejorándolos si es necesario. La *ilustración 3-11* muestra el proceso de gestión del riesgo según la metodología MEHARI.

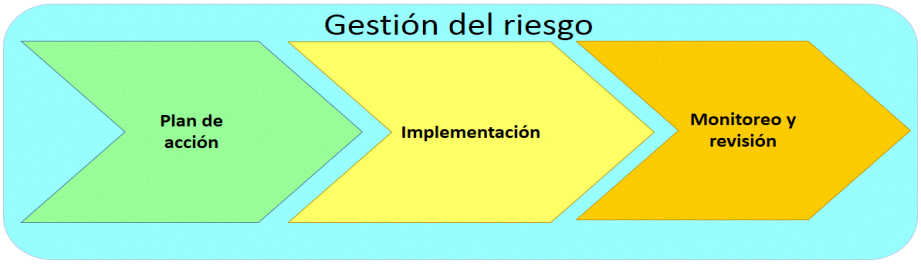



***Ilustración 3-11.*** *Gestión del Riesgo de MEHARI*

*1. Plan de acción*

Después de analizar el riesgo y tomar decisiones sobre cómo tratarlos, la organización decide cómo proseguir con un cierto número de acciones de acuerdo al tipo de tratamiento elegido.

2. *Implementación del plan de acción*
Implementar el plan de acción puede tener dificultades de aplicación, básicamente, la implementación es a juicio de la organización y los auditores.

*3. Monitoreo y revisión*
Numerosas verificaciones deben ser llevadas a cabo para dirigir la gestión del riesgo.

## 3.5 PROCESO GENERAL DE LA METODOLOGÍA MEHARI

La *ilustración 3-12* muestra las fases de la metodología MEHARI con todas sus fases, en donde no solo tiene en cuenta la gestión del riesgo, sino también la fase preparatoria de acuerdo a los lineamientos seguidos por la norma ISO/IEC 27003.


***Ilustración 3-12.*** *Fases de la metodología MEHARI*

### 3.5.1 Fase preparatoria

En esta fase se realiza todo lo relacionado con el establecimiento del contexto de la organización, los parámetros técnicos y las tablas de aceptabilidad.

*1. Evaluación del contexto*
El objetivo es establecer puntos que deben ser claros y tomados en cuenta para el análisis y tratamiento del riesgo. Recolectar y establecer datos e información técnica que pueda ser necesaria para el análisis y tratamiento del riesgo. Recolectar y establecer datos e información de la estructura de la organización que pueda ser utilizada para el análisis y tratamiento del riesgo.

*2. Determinar el alcance y límites*
El objetivo es formalizar el alcance técnico para iniciar la operación de análisis y tratamiento del riesgo. Formalmente establecer el alcance organizacional para el análisis y tratamiento del riesgo. Establecer una relación para la vigilancia entre el análisis y tratamiento del riesgo y la dirección.

*3. Establecer parámetros de riesgos principales*
El objetivo es establecer tablas de aceptabilidad, para ser usadas posteriormente con el fin de determinar si un escenario en riesgo es tolerable o no. Formalmente se establece la tabla de exposición natural o tabla intrínseca de probabilidad usada más adelante para establecer el potencial de riesgo de los escenarios. Formalmente se establecen tablas que permitan evaluar amenazas residuales.

### 3.5.2 Fase operacional – Análisis del riesgo

El análisis de amenazas es un paso fundamental para cualquier proceso de gestión de riesgos. El análisis de amenazas de acuerdo con la metodología MEHARI muestra dos tipos de resultados los cuales son:

- La escala de valores de malfuncionamiento
- La valoración o clasificación de activo relacionados con la información.

De estos dos conjuntos de resultados es posible deducir la tabla de impacto intrínseco, usado para valorar los escenarios de riesgos que provee MEHARI.

El proceso que se sigue para el análisis de amenazas se muestra en la *ilustración 3-13*. El enfoque de la metodología MEHARI consiste en analizar las actividades de la organización y por lo tanto sus procedimientos administrativos que tienen que ver con la información para deducir que mal funciones podrían ocurrir y evaluar que tan graves estas mal funciones podrían ser, una vez hecho esto, es posible valorar los activos relacionados con la información.

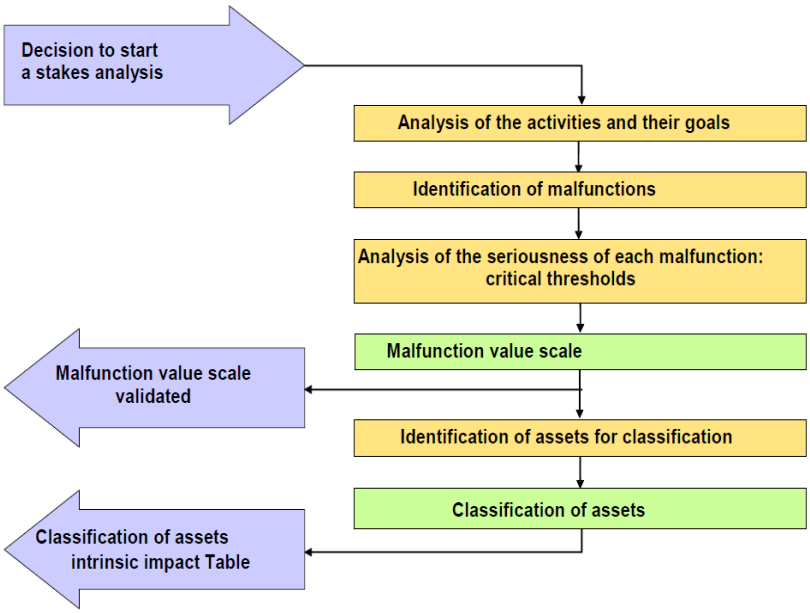



***Ilustración 3-13.*** *Identificación de las malfunciones de las actividades y selección de activos*

En este punto, se debe recopilar toda la información pertinente a la organización sus activos, su ubicación, sus locales, etc. En este punto se debe tener el contexto y el inventario de activo. Estos activos son clasificados en tres categorías sugeridas por la metodología, clasificación de datos, clasificación de servicios y clasificación del cumplimiento (efectos contractuales y regulaciones). En esta sub fase se obtienen tablas de impacto intrínseco y tabla de exposiciones naturales, esta última representa eventos que MEHARI caracteriza como casos fortuitos.

La metodología MEHARI dentro de su base de datos de reconocimiento provee una lista de activos denominados activos primarios, que están agrupados en tres grandes categorías las cuales son activos en la categoría de servicios, activos en la categoría de datos y activos en la categoría de proceso de administración.

Una vez se ha realizado la clasificación de los activos de la información y su respectiva agrupación se realiza la valoración en cuanto a confidencialidad, integridad y disponibilidad teniendo en cuenta los criterios de la gravedad de las malfunciones.

Este punto es importante para organizaciones que tengan servicios de seguridad. Estos servicios se traducen en preguntas de auditoria que tiene MEHARI, este inciso tiene cientos de preguntas de auditoria que tiene la metodología, esto con el fin de evidenciar que los controles de la norma ISO 27002 estén correctamente implantados y sean operacionales. Una vez, estas preguntas de auditoria son diligenciadas (solo las que apliquen dependiendo del contexto de la organización), la herramienta arroja los puntajes respecto a cómo está la organización en cuanto a los controles de seguridad.

*1. Evaluación del riesgo*

La evaluación del riesgo comprende los activos y las tres clasificaciones que sugiere MEHARI. Estos activos y sus clasificaciones son puestas en numerosos escenarios (más de 800) donde se prueban valores como la confidencialidad, disponibilidad, integridad y eficiencia. Lo primera medida se debe establecer qué escenarios son aplicables a la organización, una vez determinados se procede a evaluar el riesgo, con la probabilidad e impacto. La probabilidad que ocurra el evento (bajo qué circunstancias) y el impacto, que tan grave puede ser si ese escenario sucede. Existe una probabilidad e impacto que trae esta evaluación basada en los datos que se ingresan en la *"clasificación de activos y análisis de cuestiones"*, ya es a consideración de la organización si se dejan esos valores o si se determinan valores diferentes. Aquí está el primer filtro de tratamiento, en el cual se puede *"aceptar el riesgo"* o se puede *"transferir el riesgo"*.

### 3.5.3 Fase de tratamiento del riesgo y planificación

Esta fase debe realizarse después de tener los resultados de la valoración de riesgo, en este punto, la organización determinaría cuales son las formas más adecuadas de tratar los riesgos, en beneficio de la organización. Se tiene el plan de tratamiento como media vital para el tratamiento del riesgo, donde MEHARI determina por si misma basada en las tres clasificaciones que sugiera *[18]*. Dependiendo de qué parámetro se desea reducir (en caso que se decida como opción de tratamiento el "reducir el riesgo") si es probabilidad o impacto, la metodología recomienda ciertos planes *[20]*. Estos planes son de: "disuasión, prevención, confinación o paliación". Dependiendo de qué parámetro se desea reducir en *[20]* se encuentra la recomendación del plan que se debe adoptar.

*1. Planificación de medidas inmediatas*

El objetivo es priorizar que escenarios en riesgo se deben tratar con mayor urgencia, estos son los escenarios en riesgo que tienen el nivel más elevado.

*2. Planificación de medidas en contextos específicos*

El objetivo es escoger entre las posibles estrategias de tratamiento y seleccionar el criterio para establecer las prioridades, teniendo en cuenta que por lo general no es posible tratar todos los riesgos al mismo tiempo.

*3. Vigilancia de la implantación del tratamiento de riesgo.*

En realidad se trata del monitoreo de la implantación del tratamiento de riesgo. Vigilar que se estén tomando en cuenta las medidas decididas por la organización y que se implementen los controles establecidos.

| Metodología MEHARI | | |
|---|---|---|
| **Fases** | **Sub fase** | **Actividades** |
| Fase preparatoria | Evaluación del contexto | Contexto estratégico |
| | | Contexto técnico |
| | | Contexto estructural |
| | Determinar el alcance y sus limites | Perímetros técnicos |
| | | Perímetros organizacionales |
| | | Estructura de pilotaje |
| | Establecer parámetros de riesgos principales | Tabla de aceptabilidad de riesgo |
| | | Tabla de exposición natural |
| | | Tabla de evaluación del riesgo |
| Fase operacional | Clasificación de activos y análisis de cuestiones | Escala de valores de malfuncionamiento |
| | | Clasificación de activos |
| | | Tabla de impacto intrínseco |
| | Evaluando la calidad del servicio de seguridad | Establecimiento de un esquema de auditoria |
| | | Evaluar la calidad de los servicios de seguridad |
| | Evaluación del riesgo | Seleccionando los escenarios parar el análisis |
| | | Evaluando los escenarios de riesgo |
| Fase de tratamiento | Medidas de planificación inmediata | Selección de riesgo parar tratamiento inmediato |
| | | Selección de medidas parar la implementación inmediata |
| | Planificación de medidas en contextos específicos | Estrategia prioritaria y de tratamiento |
| | | Selección de medidas y planes |
| | Vigilancia de la implantación del tratamiento de riesgo | Vigilancia de planificación |
| | | Selección de indicadores, dashboards y gráficos |

***Tabla 3-2.*** *Tabla de Fases, Sub fases y Actividades de la metodología MEHARI*

# 4 DESARROLLO DE LA FASE DE PLANEACIÓN DE UN SGSI Y APLICACIÓN DE LA METODOLOGÍA MEHARI

Este capítulo aborda el desarrollo de la fase de planeación de un SGSI en el caso de estudio propuesto *[21]*. Toda la información a continuación ha sido obtenida por parte de los autores de este trabajo de grado en múltiples reuniones que se llevaron a cabo en el área de Desarrollo y Mantenimiento de Aplicaciones. Los valores aquí consignados fueron alterados intencionalmente para proteger el principio de la confidencialidad de la información.

El trabajo y los resultados obtenidos presentados en este capítulo están protegidos por un acta de confidencialidad firmada entre los autores de este trabajo de grado y la Universidad del Cauca. Esta medida se toma, debido a que la mayoría de la información recolectada es clasificada por la universidad como sensible y privada.

Todo el desarrollo del proyecto, se realiza con las últimas versiones vigentes de las normas ISO/IEC y con la última versión de la metodología MEHARI[17]. Los datos recolectados están justificados y fundamentados en actas firmadas por los desarrolladores del trabajo y el encargado del Procedimiento de Desarrollo y Mantenimiento de Aplicaciones.

Este trabajo desarrolla la fase de planeación de un SGSI cumpliendo con la norma ISO/IEC 27001, siguiendo la ISO/IEC 27003 ("*guía para la implementación de un SGSI*"). Esta fase de planeación se desarrolla en los puntos cinco, seis, siete y ocho. Ver *ilustración 2-3.* La fase 9 no entra en consideración dentro del alcance de este proyecto.

[17] Esta última versión de la metodología MEHARI no está disponible en el sitio web de la metodología, esta versión fue proporcionada por el sr Jean-Louis Roule colaborador en la creación de esta herramienta.


***Ilustración 4-1.*** *Fase de planeación de un SGSI según la norma ISO/IEC 27003*

## 4.1 OBTENER APROBACIÓN DE LA DIRECCIÓN PARA INICIAR UN PROYECTO DE SGSI

Conforme a la ISO/IEC 27003 la fase 5 tiene como objetivo obtener el soporte directivo para la implementación de un SGSI como se muestra en la *ilustración 4-2*,


***Ilustración 4-2.*** *Fase 5 de la fase de planeación de un SGSI*

Esta fase tiene muchas actividades que deben ser ejecutadas, al finalizar la fase 5 se debe presentar un caso de negocio a la alta dirección para que motive a aprobar el SGSI en la organización y se destinen los recursos necesarios. Las actividades de la fase 5 se describen en a continuación.

### 4.1.1 Objetivos, prioridades de la Seguridad de la Información y requisitos organizacionales

El Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca es un procedimiento que se deriva del sub proceso Gestión de Recursos Tecnológicos que a su vez se deriva del proceso Gestión Administrativa de la Universidad del Cauca.

Este procedimiento se encarga del desarrollo y mantenimiento de algunas de las plataformas existentes actualmente de la Universidad del Cauca. Como objetivo, el procedimiento debe implementar y mantener sistemas de informaciones fiables y con buen desempeño para que sean usados por toda la comunidad universitaria. Esta procedimiento recibe solicitudes de las diferentes dependencias universitarias para modificación de información en bases de datos, requerimientos para el desarrollo aplicaciones y requerimientos para corrección de alguna inconsistencia dentro del uso de las aplicaciones.

Actualmente no se cuenta con ningún tipo de Seguridad de la Información y no se está siguiendo ningún tipo de metodología de tratamiento de riesgo, debido a que no se cuenta actualmente con un SGSI. En el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca se manejan bases de datos que contienen información confidencial y aplicaciones que tienen manejo de información que es considerada como crítica, es necesaria la implantación de un SGSI. En cuanto a los requisitos organizacionales para la implementación de un SGSI, se deben seguir las políticas existentes de la Universidad del Cauca en cuanto a la Seguridad de la Información, estos son considerados requisitos organizacionales.

### 4.1.2 Requisitos reglamentarios y contractuales.

Todos los requisitos reglamentarios que debe cumplir el procedimiento y la institución son requisitos que motivan la implementación de un SGSI, existen

muchas leyes a nivel nacional como las que demanda el estado y que son descritas en el anexo B.8.

### 4.1.3 Característica del negocio

Las características del negocio del Procedimiento de Desarrollo y Mantenimiento de Aplicaciones de la División TIC de la Universidad del Cauca se detallan en el anexo B.1

### 4.1.4 Alcance preliminar del SGSI

El alcance preliminar del SGSI está detallado en el anexo B.2.

### 4.1.5 Caso de negocio y propuesta de proyecto

Es muy importante realizar el caso de negocio para ser presentado a la alta dirección para que apruebe la realización de un SGSI en la organización. El caso de negocio y la propuesta están descritos en detalle en el anexo B.3.

### 4.1.6 Importancia y beneficios del proyecto

Es importante dejar documentado los beneficios y la importancia que tiene el implementar un SGSI en la organización, además este debe ser socializado para motivar su realización. El contenido, importancia y beneficios del proyecto para el procedimiento en estudio se describen en los anexos B.4.

## 4.2 DEFINICIÓN DEL ALCANCE DEL SGSI, SUS LÍMITES Y LA POLÍTICA DE SGSI


***Ilustración 4-3.*** *Fase 6 de la fase de planeación de un SGSI*

Para definir esta fase, se tienen en cuenta varias fuentes, como la información recolectada en el numeral 4.2, el libro "*Diseño de un sistema de gestión de seguridad de información*" *[22]* y las políticas generales establecidas por la Universidad del Cauca *[4].*

### 4.2.1 Definición del alcance y los límites de la organización

Siempre que se decide implantar un SGSI dentro de la organización se debe tener en cuenta qué áreas de la organización son las más críticas para que se incluyan dentro del alcance estas áreas deben ser las de mayor importancia para la organización.

El Procedimiento de Desarrollo y Mantenimiento de Aplicaciones es un procedimiento crítico ya que hace uso extensivo de las TIC, además atiende solicitudes de desarrollo de aplicaciones por parte de todas las dependencias institucionales, por tal motivo es considerado dentro del alcance del SGSI, una vez se ha definido este procedimiento es importante considerar el alcance y los límites de la organización, el alcance y los límites de las tecnologías de la información y las comunicaciones y el alcance y los límites físicos tal como lo sugiere la ISO/IEC 27003.

- ✓ **Alcance y límites de la organización**

El procedimiento y mantenimiento de aplicaciones de la Universidad del Cauca cuenta actualmente con 6 personas más la vinculación de monitores que se hace cada semestre. De las 6 persona encargadas del áreas 4 son contratistas y 2 son contratados directamente por la Universidad del Cauca.

En el procedimiento no existe una jerarquía de mando, todo el personal toma decisiones por igual para el desarrollo y mantenimiento, sin embargo el procedimiento pertenece al proceso gestión de recursos tecnológicos y este proceso está a cargo del Jefe de la División TIC. Se identifican que entre los involucrados en el procedimiento hay intercambio de información tanto documentada del desarrollo de una determinada aplicación como del código fuente de las aplicaciones.

El proceso de definir el alcance y límites de la organización debe estar claro y debidamente documentado.

- ✓ **Alcance y límite de las TIC**

El procedimiento de desarrollo y mantenimiento está dedicado a la creación de aplicaciones para las diferentes dependencias de la Universidad del Cauca, mas no tiene a cargo ninguna responsabilidad en cuanto a la infraestructura de la Universidad, esto quiere decir que el área encargada de garantizar conexión y solucionar problemas de red está a cargo del área de infraestructura de red. El procedimiento es el encargado de desarrollar y mantener las aplicaciones teniendo total responsabilidad del software que brindan a la comunidad universitaria. Algunas veces la administración del software se hace de forma compartida con otras dependencias como DARCA[18] y vicerrectoría académica. Muchas de las aplicaciones realizadas son ejecutadas en los servidores de la Universidad del Cauca, donde se alojan servicios importantes de la universidad como SIMCA[19].

[18] División de Admisiones, Registro y Control Académico
[19] Sistema Integrado de Matricula y Control Académico.

El hardware y el software necesario para la producción de las aplicaciones están relacionados con equipos de cómputo, software de licencia libre y algunas otras herramientas de desarrollo con licencias propias de la universidad. No existe una responsabilidad por el software ni por el hardware, el cual se utiliza para desarrollar las aplicaciones en el procedimiento, esta responsabilidad está en los trabajadores del procedimiento, pero no existen responsabilidades asignadas explícitamente.

- ✓ **Alcance y límites físicos**

El área de Desarrollo y Mantenimiento de Aplicaciones en su labor y cumplimiento de obligaciones no cuenta con oficinas remotas que hagan parte del procedimiento y que colaboren con su desarrollo. El procedimiento está ubicado en el edificio de la división de las TIC de la Universidad del Cauca con sede en Tulcán, con única sede para el cumplimento de sus obligaciones, todo el desarrollo y el mantenimiento se realiza dentro de las instalaciones. No existe actualmente control sobre las instalaciones físicas por parte de Desarrollo y Mantenimiento de Aplicaciones, estas instalaciones son compartidas por personal de servidores y con personal de otros procedimientos. Este documento igual que los anteriores deben estar claramente documentado y justificar cualquier inclusión o exclusión dentro del alcance del SGSI.

### 4.2.2 Metodología de las elipses parar definir el alcance y los límites de la organización

La metodología de las elipses es un buen método para definir el alcance y los límites de una organización de manera gráfica *[22]*, este método consiste en ubicar en una elipse central los procedimientos de una misma área, luego en una elipse intermedia se deben ubicar los procedimientos que hacen parte de la organización y finalmente en una elipse externa se deben ubicar las dependencias que ya no hacen parte de la organización, pero que por algún motivo se comunican con los procedimientos de la elipse central.

La tabla del anexo B.5, muestra los procedimientos que pertenecen al sub proceso gestión de recursos tecnológicos, y especifica cuáles de ellos se relacionan directa o indirectamente con el caso de estudio.

La metodología de las elipses se llevó a cabo en reuniones reiteradas con el personal del Procedimiento de Desarrollo y Mantenimiento de Aplicaciones que identificaron todas las interrelaciones con otros procedimientos, la *ilustración 4-4* muestra el diagrama de las elipses construido para el procedimiento en estudio.

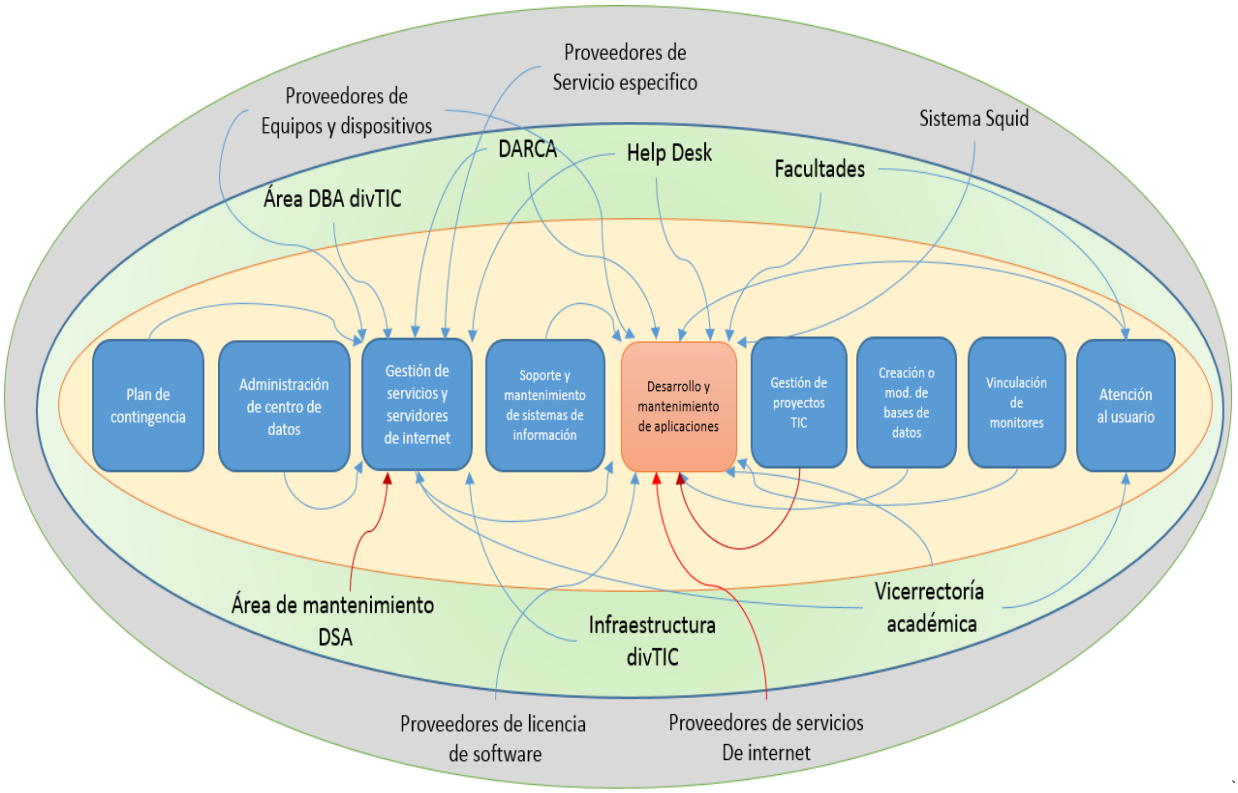



***Ilustración 4-4.*** *Modelo de las elipses del caso de estudio*

## 4.2.3 Políticas de Seguridad de la Información del SGSI

Como punto crucial en la fase de planeación es la definición de la política de seguridad, esta política debe seguir los lineamientos de los requisitos reglamentarios y satisfacer todos los efectos contractuales que el procedimiento tenga. Para lo anterior se tuvo en cuenta la política general vigente para toda la universidad *[4]* y se tuvo en cuenta los requisitos reglamentarios. Esta política está disponible en el anexo B.6.

## 4.3 REALIZAR EL ANÁLISIS DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN


***Ilustración 4-5.*** *Fase 7 de la fase de planeación de un SGSI*

### 4.3.1 Requisitos de la Seguridad de la Información

La definición de los requisitos de Seguridad de la Información hace referencia a las necesidades de la organización para la implementación de un SGSI, también deben considerarse las medidas reglamentarias que demanda la institución y el gobierno nacional en cuanto a la protección de los datos. Las vulnerabilidades de los sistemas de información y algún incidente de seguridad que se haya presentado son consideradas requisito de la seguridad para ser tenido en cuenta en el SGSI.

Existen requisitos de la Seguridad de la Información como la ley del Habeas Data que protege la información de las personas, donde se estipula que la información no se puede divulgar sin el consentimiento del usuario. Si algún incidente de seguridad ocurriera dentro de la organización esto podría ser muy grave que podría involucrar información personal.

Por otra parte las aplicaciones desarrolladas se ejecutan y mantienen en los servidores de la Universidad del Cauca lo cual hace que esta actividad sea crítica, si bien el procedimiento de servidores no es considerado dentro del alcance se

deben ejercer actividades que permitan validar el código fuente de las aplicaciones antes de poder ponerlas en funcionamiento en el servidor. El procedimiento cuenta actualmente con monitoreo de cámaras de seguridad que permiten controlar el acceso a personal no involucrado en el área, además de control de acceso biométrico a personal ajeno a la división TIC.

La identificación de las necesidades anteriormente descritas son importantes para ser tenidas en cuanta dentro del SGSI, esta actividad debe ser documentada.

### 4.3.2 Activos de la información

Es necesario identificar los activos de la información dentro del alcance. Los activos de información y el resultado de la valoración de la seguridad se encuentran en el anexo B.7. Esta clasificación y valoración se hizo en conformidad con la normativa emitida por el Ministerio de Tecnología de la Información y las Comunicaciones en cuanto a la clasificación de activos en el documento *[23]*.

## 4.4 REALIZAR LA VALORACIÓN DEL RIESGO Y PLANIFICAR EL TRATAMIENTO DEL RIESGO


***Ilustración 4-6.*** *Fase 8 de la fase de planeación de un SGSI*

Esta fase 8 de la norma ISO/IEC 27003 debe realizarse con una metodología de gestión de riesgos y debe cumplir los requisitos que establece la norma ISO/IEC 27005. El tema principal en esta fase 8 es la adaptación de la metodología MEHARI al caso de estudio como se muestra en la *ilustración 4-7*.


***Ilustración 4-7.*** *Inclusión MEHARI al caso de estudio*

La metodología MEHARI se adaptara al caso de estudio en la fase 8 de la ISO/IEC 27003, cada una de las fases de la metodología MEHARI que se presentan en la *ilustración 4-8* será analizada en detalle para ser incluidas o excluidas.

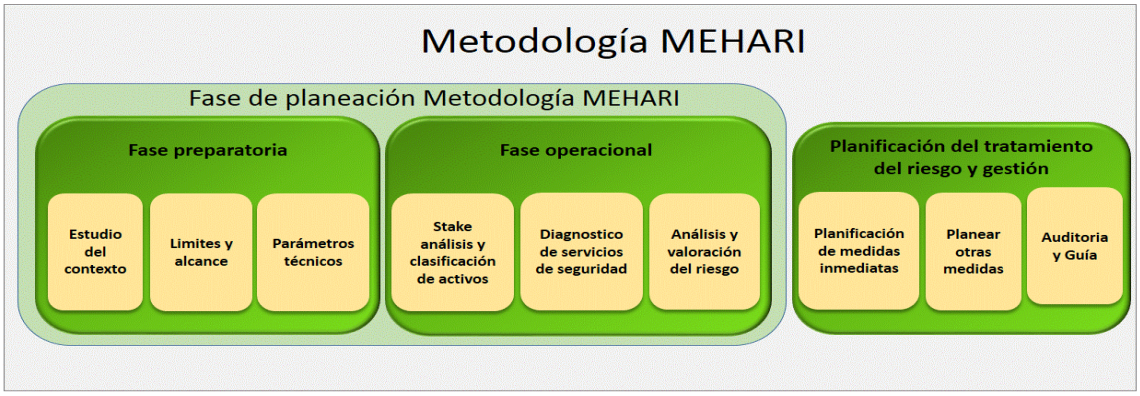



***Ilustración 4-8.*** *Metodología MEHARI en fases*

### 4.4.1 Fase preparatoria

✓ **Estudio del contexto**

La evaluación del contexto de acuerdo a la metodología MEHARI es todo lo que se debe conocer de la organización. Esta definición fue realizada en la sección 4.2 de este documento. Todos los productos obtenidos por la norma ISO/IEC 27003 en su fase 5, satisfacen estos apartados los cuales son:

1. *Contexto estratégico.*
2. *Contexto técnico.*
3. *Contexto estructural.*

Después de realizar comparaciones entre la ISO/IEC 27003 en su fase 5, y la evaluación del contexto en la fase preparatoria de MEHARI, se determina que estos tienen objetivos similares, por lo tanto, con el fin de evitar iteraciones se omite realizar el estudio del contexto de MEHARI. Véase el desarrollo en el anexo C.1.1.

✓ **Determinar el alcance y los limites**

De acuerdo a la metodología MEHARI esta fase considera:

1. *Perímetros técnicos*
2. *Perímetros organizacionales*
3. *Estructura de pilotaje*

La norma ISO/IEC 27003 en su fase 6 requiere la definición del alcance del SGSI, sus límites y políticas. La metodología MEHARI tiene un objetivo similar, al analizar el contenido de la fase 6 de la ISO/IEC 27003 se puede determinar que el alcance y los límites definidos son del SGSI, es decir, estos límites y alcance se utilizan no solamente en esta etapa de planeación sino que este mismo alcance y limite se toman en las otras tres etapas restantes (ejecución, verificación y actuación). Por otro lado, MEHARI requiere este alcance para ser realizado únicamente dentro del proceso de valoración del riesgo y únicamente con este objetivo, de este modo,

debido a que el SGSI contiene la fase de valoración del riesgo[20], se da por establecido que los límites y alcance del SGSI que solicita la norma ISO/IEC 27003 en su fase de planeación es mucho más completo, que el que plantea la metodología MEHARI. Véase desarrollo en el anexo C.1.2.

Con el fin de soportar los dos puntos anteriores se remite al numeral 7 de la norma ISO/IEC 27005 "*Nota: La norma NTC-ISO/IEC 27001 no utiliza el termino contexto. Sin embargo, todo el numeral 7 de esta norma se relaciona con los requisitos de definir el alcance y los límites del SGSI, definir la política de un SGSI y definir el enfoque para la valoración del riesgo que se especifica en la norma NTC-ISO/IEC 27001*" *[24]*.

✓ **Establecer parámetros de riesgos principales**

Como punto de partida es importante determinar que se acepta y que no, a pesar que la escala de 1 a 4 utilizada para medir los diferentes parámetros de seguridad (1 muy bajo y 4 muy alto) es la misma para toda la metodología, en algunos casos esos valores tienen significados diferentes. En el anexo A.7 se detallan algunas escalas utilizadas por la metodología MEHARI y su significado.

*1. Tabla de aceptabilidad de riesgo*

En el documento *[18]* se encuentra la aceptabilidad del riesgo. MEHARI tiene una clasificación de aceptabilidad del riesgo y es aquella en el cual se determina cuando un riesgo es aceptado por la organización. La metodología MEHARI establece los valores 1 y 2 como aceptables, 3 y 4 como no aceptables. Esta misma notación se utilizará en este proyecto.

En este trabajo de grado se trabajará con las mismas tablas de aceptabilidad que sugiere MEHARI, esto se determinó así, debido a que se analizó la aceptación del riesgo para MEHARI y se encontró que es mínima, y que el reconocimiento que tiene esta metodología en cuanto a la valoración de riesgo es realmente muy alta, por lo tanto se utiliza las mismas tablas de aceptabilidad del riesgo de MEHARI.

[20] La valoración de riesgo y tratamiento de riesgo es simplemente la fase 8 de la norma ISO/IEC 27003

| NIVEL | SIGNIFICADO |
|---|---|
| **4** | Intolerable |
| **3** | Inadmisible |
| **2** | Aceptable |
| **1** | Bajo |

***Tabla 4-1.*** *Escala de valoración MEHARI*

*2. Tabla de exposición natural*

En los documentos *[18]* y *[19]* se encuentra la tabla de exposición sugerida por MEHARI, la cual es la misma que se utilizará, con la diferencia de que los valores que se darán son acorde al riesgo. La tabla de exposición natural se encuentra en el anexo C.1.3 inciso 2.

*3. Tabla de evaluación del riesgo*

En *[18]* y *[19]*, se encuentra lo relacionado con esta tabla, que al igual que el anterior se utilizará el sugerido por MEHARI. Estas tablas están almacenadas en el anexo C.1.3 inciso 3. En la *ilustración 4-9* muestra cómo se va adaptando la metodología MEHARI en la fase preparatoria al caso de estudio.

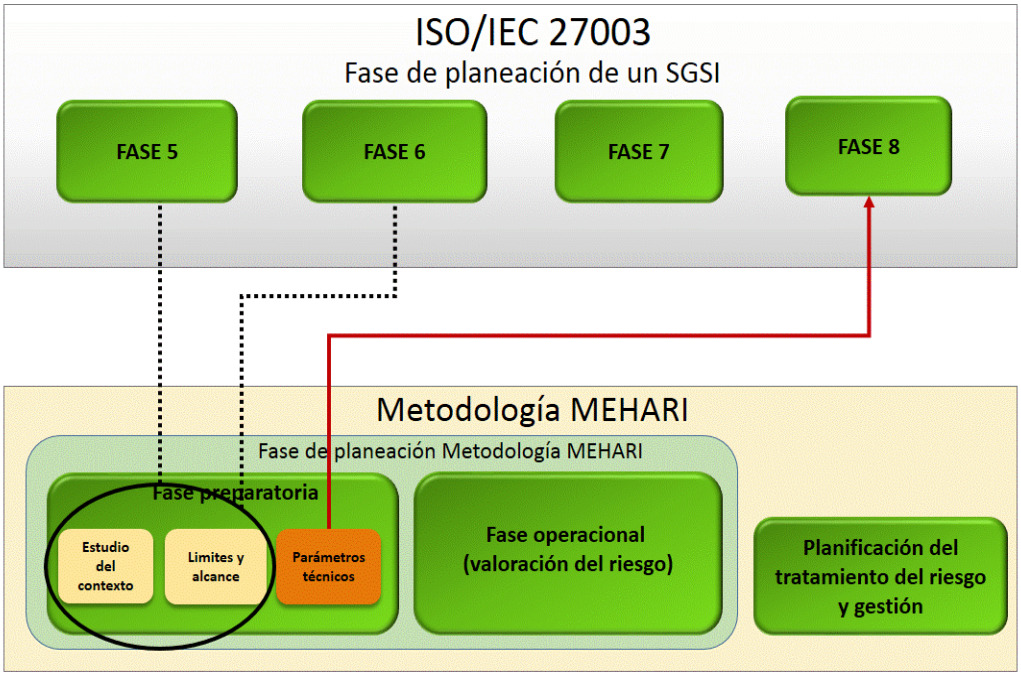



***Ilustración 4-9.*** *Iteraciones detectadas entre norma ISO/IEC 27003 y Metodología MEHARI*

### 4.4.2 Fase operacional – Análisis del Riesgo

✓ **Clasificación de activos y análisis de cuestiones**

La clasificación de activos y análisis de cuestiones se desarrolla en el anexo C.2.1.

*1. Escala de valores de malfuncionamiento*

Según el documento *[17]* un mal funcionamiento es aquello que puede fallar en un activo y puede generar un riesgo a la organización. En el anexo C.2.1 inciso 1 se encuentra la valoración de los activos que se realizó al caso de estudio, de los resultados de esta valoración preliminar se obtienen los datos para la *"clasificación de activos"*.

*2. Clasificación de activos*

La clasificación de activos es el proceso inicial en la herramienta, en el documento *[16]* se dice de qué manera se puede obtener los activos iniciales. Posteriormente en el documento *[17]*, basado en la escala de valores de malfuncionamiento se asignan valores a los activos de información. Estos activos se introducen en la tabla T1, T2 y T3 de la herramienta *[25]*.

Esta clasificación de activos es la base de todo el proceso de valoración de riesgo para su posterior tratamiento. Aquí se organizaron todos los activos y actividades del caso de estudio, y según su mal funcionamiento se determinó un valor según el criterio del personal del caso del estudio. Estos activos y actividades tienen en MEHARI una nomenclatura según el tipo de activo (D01, D02, D03, etc.). En el anexo C.2.1 inciso 2 se encuentran las tablas de clasificación de activos ("*clasificación de datos*", "*clasificación de servicios*", "*clasificación del cumplimiento*" y "*exposición natural*") y escalas de niveles.

*3. Tabla de impacto intrínseco*

Esta tabla muestra los resultados después de clasificar los activos y su mal funcionamiento. Los resultados de esta tabla se verán reflejados en más de 800 escenarios que tiene por defecto la metodología MEHARI, en la tabla 4-2 se muestra la tabla de impacto intrínseco para los activos seleccionados en el procedimiento en estudio.

| Tabla de Impacto Intrínseco | | | | | Selección de Activos |
|---|---|---|---|---|---|
| **Activos de datos y de información** | | **A** | **I** | **C** | |
| ***Datos e información*** | | | | | |
| D01 | Archivos de datos y bases de datos que se acceden por aplicaciones | 4 | 4 | 4 | 1 |
| D02 | Archivos y datos compartidos en la oficina | 4 | 4 | 4 | 1 |
| D03 | Archivos de oficina personales (en estaciones de trabajo de usuarios y equipos) | 4 | 4 | 4 | 1 |
| D04 | Información escrita o impresa y datos almacenado por usuarios y los archivos personales | 4 | | 3 | 1 |
| D05 | Documentos impresos o listados | | | | 0 |
| D06 | Intercambio de mensajes, vistas de pantalla, datos individuales sensibles | 4 | 4 | 4 | 1 |
| D07 | Correo Electrónico | 3 | 3 | 3 | 1 |
| D08 | (Postal) Correos postales y faxes | 2 | 2 | 2 | 1 |
| D09 | Archivos patrimoniales y documentos utilizados como pruebas | 2 | | 1 | 1 |
| D10 | Archivos relacionados con TI | | | | 0 |
| D11 | Datos e información publicada en sitios públicos o internos | | | | 0 |
| **Activos de servicio** | | **A** | **I** | **C** | |
| ***Servicios generales*** | | | | | |
| G01 | Espacio de trabajo del usuario y el ambiente | 3 | | | 1 |
| G02 | Servicios de telecomunicaciones (voz, fax, audio y video conferencias, etc.) | 3 | 3 | | 1 |
| ***Servicios de redes y TI*** | | | | | |
| R01 | Servicios de redes extendidas | 3 | 3 | | 1 |
| R02 | Servicios de redes de área local | 4 | 4 | | 1 |
| S01 | Servicios prestados por las aplicaciones | 4 | 4 | 4 | 1 |
| S02 | Servicios compartidos de oficina (servidores, gestión de documentos, impresoras compartidas, etc.) | 4 | 4 | | 1 |
| S03 | Disposición de equipos de usuarios (estaciones de trabajo, impresoras locales, periféricos, interfaces específicas, etc.) **Nota : Aplica a un pérdida masiva de esos servicios, no para uno ni pocos usuarios** | 4 | 3 | | 1 |
| S04 | Servicios comunes, ambiente de trabajo: mensajería, archivos, impresiones, edición, etc. | 3 | 3 | | 1 |
| S05 | Servicio de edición de Web (interna o pública) | | | | 0 |
| **Proceso de gestión de tipo de activos** | | **E** | | | |
| ***Procesos de gestión para el cumplimiento de las leyes o reglamentaciones*** | | | | | |
| C01 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de datos personales. | 4 | | | 1 |
| C02 | Cumplimiento a las leyes o regulaciones relacionadas a la comunicación financiera. | | | | 0 |
| C03 | Cumplimiento a las leyes o regulaciones relacionadas al control contable digital. | 3 | | | 1 |
| C04 | Cumplimiento a las leyes o regulaciones relacionadas a la propiedad intelectual. | 3 | | | 1 |
| C05 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de sistemas de información. | 4 | | | 1 |
| C06 | Cumplimiento a las leyes o regulaciones relacionadas a la seguridad de las personas y protección del ambiente. | 3 | | | 1 |

***Tabla 4-2.*** *Tabla intrínseca de datos ingresados a MEHARI*

### ✓ Evaluando la calidad del servicio de seguridad

MEHARI es una herramienta de valoración de riesgo y como herramienta debe ser completa en el sentido que debe poderse ejecutar tanto en organizaciones con un SGSI implantando como para las que no. La metodología parte del hecho de que las organizaciones que desean realizar una valoración del riesgo son organizaciones que tienen algún tipo de control o medida de seguridad que MEHARI lo denomina "*servicio de seguridad*" se debe tener presente que el caso de estudio en consideración actualmente no cuenta con un SGSI implantado.

El objetivo de esta sub fase es valorar los controles de seguridad (implantados) a través de preguntas de auditoria, una vez realizadas las preguntas la herramienta puede detectar si ciertos controles de la norma ISO/IEC 27002 está implantado o no, teniendo en cuenta que el caso de estudio no tiene un SGSI implantado este no tiene controles relacionados con la norma ISO/IEC 27002 y tampoco tiene controles propios estipulados se considera por consiguiente que no tiene sentido realizar la evaluación de servicios de seguridad, porque no habría controles ni medidas de seguridad que valorar.

Esta sub fase considerados puntos los siguientes puntos:

1. *Establecimiento de un esquema de auditoria.*
2. *Evaluación de la calidad de los servicios de seguridad.*

Sin embargo, una vez existan controles implantados es recomendable que se regrese inmediatamente a esta sub fase para realizar la valoración de los activos con los servicios de seguridad establecidos. Se debe recordar, que MEHARI es comparado con un ciclo continuo de mejora (ciclo Deming). Por lo tanto esta valoración de riesgo debería realizarse periódicamente. Véase el anexo C.2.2.

### ✓ Evaluación del riesgo

Después de haber identificado los activos y las clasificaciones con sus respectivos mal funcionamientos. Se llega a este punto de evaluación del riesgo. Esta evaluación toma como entrada la información anterior y la pone en más de 800 escenarios *[16]*.

*1. Seleccionando los escenarios para el análisis*

Con el criterio del personal del procedimiento se eligieron los escenarios, MEHARI cuenta con más de 800 escenarios de riesgo, de los cuales se eligieron 617 escenarios a criterio del personal del área y los autores de este trabajo de grado. El criterio para la elección se basa en las características del área y a que tan posible es que alguno de estos escenarios puede ocurrir.

*2. Evaluando los escenarios de riesgo*

Una vez se identifican los escenarios de riesgo se procede a realizar la valoración, esta valoración considera la información proporcionada en "*Clasificación de Activos y Análisis de Cuestiones* y en *Evaluación de la calidad del servicio de seguridad.* En el documento" *[26]* se explica detalladamente las casillas de la base de datos de reconocimiento (herramienta que suministra MEHARI) la cual evalúa los escenarios de riesgo *[25]*.

La tabla 4-3 muestra un resumen de la valoración de los escenarios de riesgo. La evaluación completa de los escenarios de riesgo se detalla en la base de datos de reconocimiento de MEHARI.

| | | Disponibilidad | | | | Integridad | | | | Confidencialidad | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Activos de datos y de información** | | **N. 1** | **N. 2** | **N. 3** | **N. 4** | **N. 1** | **N. 2** | **N. 3** | **N. 4** | **N. 1** | **N. 2** | **N. 3** | **N. 4** |
| ***Datos e información*** | | | | | | | | | | | | | |
| D01 | Archivos de datos y bases de datos que se acceden por aplicaciones | 0 | 3 | **31** | 0 | 0 | 0 | **15** | 0 | 0 | 0 | **20** | 0 |
| D02 | Archivos y datos compartidos en la oficina | 0 | 1 | **20** | 0 | 0 | 0 | **9** | 0 | 0 | 0 | **18** | 0 |
| D03 | Archivos de oficina personales (en estaciones de trabajo de usuarios y equipos) | 0 | 3 | **21** | 0 | 0 | 0 | **7** | 0 | 0 | 1 | **16** | 0 |
| D04 | Información escrita o impresa y datos almacenado por usuarios y los archivos personales | 0 | 0 | **4** | 0 | | | | | 0 | 0 | **12** | 0 |
| D05 | Documentos impresos o listados | | | | | | | | | 0 | 0 | 0 | 0 |
| D06 | Intercambio de mensajes, vistas de pantalla, datos individuales sensibles | 0 | 0 | **5** | 0 | 0 | 0 | **14** | 0 | 0 | 0 | **13** | 0 |
| D07 | Correo Electrónico | 0 | 0 | **8** | 0 | 0 | 0 | **3** | 0 | 0 | 0 | **4** | 0 |
| D08 | (Postal) Correos postales y faxes | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 7 | 0 | 0 |
| D09 | Archivos patrimoniales y documentos utilizados como pruebas | 0 | 0 | 0 | 0 | | | | | 4 | 0 | 0 | 0 |
| D10 | Archivos relacionados con TI | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D11 | Datos e información publicada en sitios públicos o internos | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| | | | | | | | | | | | | | |
| **Activos de servicio** | | | | | | | | | | | | | |
| ***Servicios generales*** | | | | | | | | | | | | | |
| G01 | Espacio de trabajo del usuario y el ambiente | 0 | 0 | **3** | 0 | | | | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G02 | Servicios de telecomunicaciones (voz, fax, audio y video conferencias, etc.) | 0 | 2 | **13** | 0 | 0 | 0 | **6** | 0 | | | | |
| | ***Servicios de redes y TI*** | | | | | | | | | | | | |
| R01 | Servicios de redes extendidas | 0 | 3 | **21** | 0 | 0 | 0 | **5** | 0 | | | | |
| R02 | Servicios de redes de área local | 0 | 3 | **21** | 0 | 0 | 0 | **5** | 0 | | | | |
| S01 | Servicios prestados por las aplicaciones | 0 | 6 | **49** | 0 | 0 | 0 | **18** | 0 | 0 | 0 | **16** | 0 |
| S02 | Servicios compartidos de oficina (servidores, gestión de documentos, impresoras compartidas, etc.) | 0 | 5 | **47** | 0 | 0 | 0 | **9** | 0 | | | | |
| S03 | Disposición de equipos de usuarios (estaciones de trabajo, impresoras locales, periféricos, interfaces específicas, etc.) Nota : Aplica a un pérdida masiva de esos servicios, no para uno ni pocos usuarios | 0 | 0 | **10** | 0 | | | | | | | | |
| S04 | Servicios comunes, ambiente de trabajo: mensajería, archivos, impresiones, edición, etc. | 0 | 6 | **47** | 0 | 0 | 0 | **9** | 0 | | | | |
| S05 | Servicio de edición de Web (interna o pública) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| | **Proceso de gestión de tipo de activos** | **Eficiencia** | | | | | | | | | | | |
| | ***Procesos de gestión para el cumplimiento de las leyes o reglamentaciones*** | | | | | | | | | | | | |
| C01 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de datos personales. | 0 | 4 | 0 | 0 | | | | | | | | |
| C02 | Cumplimiento a las leyes o regulaciones relacionadas a la comunicación financiera. | 0 | 0 | 0 | 0 | | | | | | | | |
| C03 | Cumplimiento a las leyes o regulaciones relacionadas al control contable digital. | 0 | 4 | 0 | 0 | | | | | | | | |
| C04 | Cumplimiento a las leyes o regulaciones relacionadas a la propiedad intelectual. | 0 | 4 | 0 | 0 | | | | | | | | |
| C05 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de sistemas de información. | 0 | 4 | 0 | 0 | | | | | | | | |
| C06 | Cumplimiento a las leyes o regulaciones relacionadas a la seguridad de las personas y protección del ambiente. | 0 | 4 | 0 | 0 | | | | | | | | |
| | **Número de escenarios D, I, C:** | 0 | 34 | **30 0** | 0 | 0 | 1 | **10 0** | 0 | 4 | 8 | **99** | 0 |
| | **Eficiencia:** | 0 | 20 | 0 | 0 | | | | | | | | |

***Tabla 4-3.*** *Valoración de los escenarios del procedimiento por MEHARI*

Esta es una de las tablas más importantes debido a que es el resultado de la valoración que se obtuvo de los escenarios seleccionados en el caso de estudio. Es importante mencionar que los valores fueron muy altos demostrando que se tienen muchos activos en riesgo, esto era un resultado que se esperaba debido a que el procedimiento no cuenta con ningún tipo de control de Seguridad de la Información. Adicional a esto en el anexo C.2.3 inciso 2 se tiene el resumen de la valoración de

eventos naturales que pueden causar algún tipo de efecto adverso en la Seguridad de la Información para el procedimiento.

Los resultados de la valoración en términos prácticos fueron:

a. Escenarios de malfuncionamientos en disponibilidad total 334.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 300 |
| 2 | 34 |
| 1 | 0 |

***Tabla 4-4.*** *Valoración malfuncionamiento disponibilidad*

b. Escenarios de malfuncionamientos en integridad total 101.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 100 |
| 2 | 1 |
| 1 | 0 |

***Tabla 4-5.*** *Valoración malfuncionamiento integridad.*

c. Escenarios de malfuncionamientos en confidencialidad total 101.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 89 |
| 2 | 8 |
| 1 | 4 |

***Tabla 4-6.*** *Valoración malfuncionamiento confidencialidad.*

d. Escenarios de malfuncionamientos en eficiencia total 20.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 0 |
| 2 | 20 |
| 1 | 0 |

***Tabla 4-7.*** *Valoración malfuncionamiento eficiencia.*

Finalmente los artefactos que se tomaron de la fase operacional de la metodología MEHARI para el procedimiento en estudio se muestran en la *ilustración 4-10.*

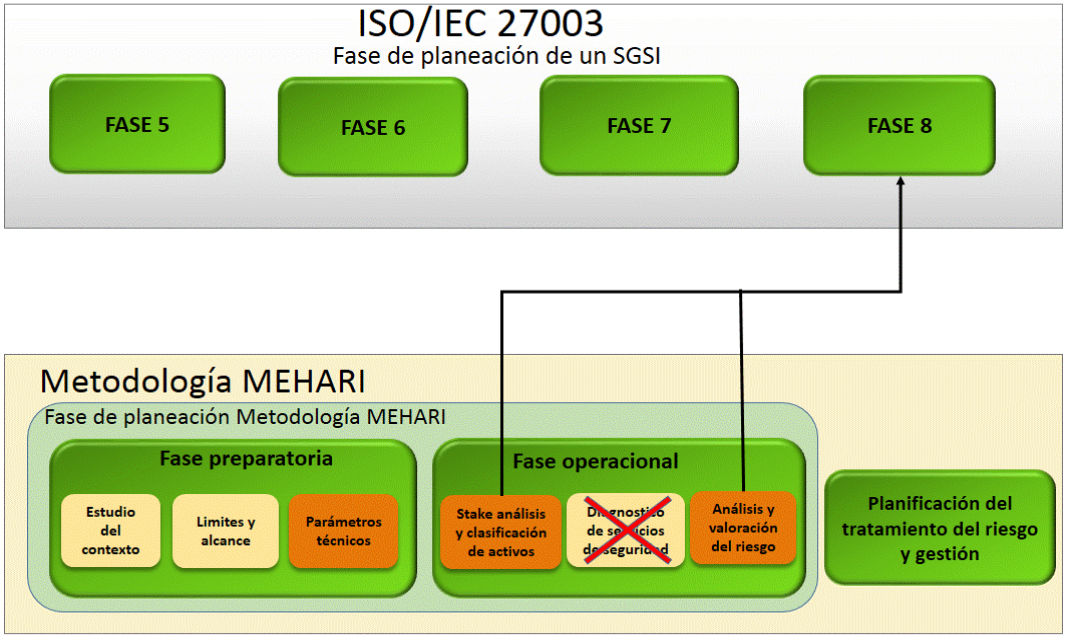



***Ilustración 4-10.*** *Artefactos tomados de la fase operacional de la metodología MEHARI*

### 4.4.3 Fase planificación del tratamiento del riesgo y gestión

Después de haber realizado la valoración de riesgo es necesario planificar de qué manera se van a mitigar aquellos escenarios con valores altos o no aceptables, luego se debe realizar un plan de tratamiento del riesgo, para realizar esta fase se utilizará el documento *[18]*.

Según el alcance de este trabajo el cual solo considera la fase de planeación de un SGSI, esta fase de tratamiento solo debe proponer un plan para tratar el riesgo y amenazas encontrados en la "*evaluación del riesgo*" mas no tratarlos. Se aclara que esta fase corresponde a las etapas siguientes del ciclo Deming en la implementación de un SGSI. Sin embargo MEHARI provee la herramienta para

simular la implementación del plan y ver qué tan efectivas son las medidas seleccionadas.

✓ **Medidas de planificación inmediatas**

Las medidas de planificación inmediatas son aquellas que tienen una ponderación de 4, considerada la más alta, por lo tanto estos escenarios que en última instancia se traducen en activos, son los primeros que deben ser tratados y deben tener una planificación inmediata. Véase el anexo C.3.1.

*1. Selección de riegos para tratamiento inmediato*

La selección de aquellos riesgos que están en una calificación de 4 según lo establecido en la metodología necesita un tratamiento inmediato. En el caso de la valoración para el caso de estudio como se observa en la *tabla 4-2*, no se tiene ningún escenario con una valoración de 4, por lo que no se requiere una actuación inmediata, no obstante, esto no es un indicador de que la situación de seguridad en la organización no sea grave.

*2. Selección de medidas para la implementación inmediata*

En este punto, el objetivo no es necesariamente tener que reducir los riesgos en 4 hasta 1 o 2. Para cumplir el objetivo de este punto basta con reducir de 4 a 3 el riesgo de los escenarios en peligro, esto debido a que en la planificación de medidas específicas se tratará aquellos riesgos en nivel 3. En el caso de estudio, ningún escenario dio una ponderación de 4.

✓ **Selección de controles de seguridad (ISO/IEC 27002) para reducir el riesgo**

Después de realizar varios análisis con metodología se determinó que este artefacto incluirse. Esto debido a que la forma en la cual los riesgos se van a disminuir es a través de los controles.

| ISO 27002 : 2013 Controles | | | | ISO 27001 2013 SGSI |
|---|---|---|---|---|
| | | | | SGSI |
| 5 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN. | | | | |
| | 5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información. | | | |
| | | 5.1.1 | Políticas para la Seguridad de la Información. | |
| | | 5.1.2 | Revisión de las Políticas para seguridad de la información. | |
| 6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. | | | | |
| | 6.1 Organización Interna. | | | |
| | | 6.1.1 | Seguridad de la Información Roles y Responsabilidades. | 1 |
| | | 6.1.2 | Separación de deberes. | 1 |
| | | 6.1.3 | Contacto con las autoridades. | |
| | | 6.1.4 | Contacto con grupos de interés especial. | |
| | | 6.1.5 | Seguridad de la información en Gestión de Proyectos. | |
| | 6.2 Dispositivos Móviles y Teletrabajo. | | | |
| | | 6.2.1 | Política para dispositivos móviles. | 1 |
| | | 6.2.2 | Teletrabajo. | |
| 7 SEGURIDAD DE LOS RECURSOS HUMANOS. | | | | |
| | 7.1 Antes de asumir el empleo. | | | |
| | | 7.1.1 | Selección. | |
| | | 7.1.2 | Términos y condiciones del empleo. | |

***Tabla 4-8.*** *Preselección de controles de la norma ISO/IEC 27002*

De los 114 controles disponibles en el anexo A de la norma ISO/IEC 27002 se deben implementar 55. Estos controles se seleccionaron según el análisis y la valoración de riesgos. Este artefacto surge debido a que la metodología MEHARI es una metodología de alto nivel, y ella no selecciona directamente controles de la norma sino que los llama servicios de seguridad. Dado que la mayoría de metodología de valoración y gestión del riesgo son muy simplistas y utilizan los controles inmediatamente, se consideró incluir este artefacto para que auditores y Jefes de Seguridad que estén utilizando esta metodología MEHARI comprendan a grandes rasgos cuales son los controles a mejorar.

- ✓ **Planificación de medidas en contextos específicos**

Es necesario planificar las medidas específicas para los contextos, con el fin de realizar un correcto y eficiente plan de tratamiento.

*1. Estrategia prioritaria y de tratamiento*

Aquí se determinar qué estrategia se utiliza para los riesgos, antes de ir a las estrategias directamente, se debe tomar una decisión respecto a costo y eficiencia en una organización sobre la viabilidad de implementar algún plan de tratamiento. En lo posible se debe determinar que, en términos económico, el tratamiento de un riesgo determinado no resulte ser mayor al valor que representa el activo al que alude el riesgo dentro de la organización.

Para el caso de estudio se utilizan todas las estrategias sugeridas por MEHARI para tratar el riesgo, estas contemplan los planes expuestos en la siguiente tabla en "*Selección de medidas y planes".*

*2. Selección de medidas y planes*

Se deben determinar cuáles son los planes para desarrollar, teniendo en cuenta lo estipulado en los puntos anteriores. En el anexo C.3.2 inciso 1 se evidencia los planes seleccionados para los activos en riesgo

En total se utilizarán 37 decisiones para mitigar el riesgo de los activos de los 617 escenarios, este plan contempla el tratamiento de 566 el cual es un excelente número.

- ✓ **Vigilancia de la implantación del tratamiento de riesgo.**

Algo muy importante en el proceso de implementación de un SGSI es revisar que el plan de tratamiento elegido sea implementado y que cumpla con lo requerido por la organización, características y condiciones.

La vigilancia del tratamiento del riesgo no se considera debido a que no es el alcance de este proyecto.

Con el objetivo ver el efecto de implementar los controles de seguridad se "simulará" con ayuda de la base de datos de reconocimiento de MEHARI los controles seleccionados, con el propósito de visualizar como disminuirían los riesgos y las amenazas en caso de que se implementara el plan que se sugiere con los controles seleccionados.

*1. Vigilancia de planificación*

Las preguntas de auditorías con las que cuenta MEHARI tienen como propósito evidenciar que los controles están implantados, por lo tanto, si se afirma que los controles están implementados en la simulación, estas preguntas deberían contestarse afirmativamente. Esto quiere decir que en la herramienta y en los controles que se seleccionan el plan de tratamiento (con sus 37 decisiones) y servicios de seguridad relacionados deben contestarse como si existieran dentro del caso de estudio.

*2. Selección de indicadores, dashboards y gráficos*

Después de haber culminado las fases anteriores, se procede a verificar como cambian las tablas de resultado con controles "implantados"[21]. Los resultados son los siguientes:

.

| | | Disponible | | | | Integridad | | | | Confidencialidad | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Activos de datos y de información** | | **N. 1** | **N. 2** | **N. 3** | **N. 4** | **N. 1** | **N. 2** | **N. 3** | **N. 4** | **N. 1** | **N. 2** | **N. 3** | **N. 4** |
| ***Datos e información*** | | | | | | | | | | | | | |
| D01 | Archivos de datos y bases de datos que se acceden por aplicaciones | 33 | 1 | 0 | 0 | 15 | 0 | 0 | 0 | 0 | 20 | 0 | 0 |
| D02 | Archivos y datos compartidos en la oficina | 20 | 1 | 0 | 0 | 0 | 9 | 0 | 0 | 0 | 17 | 1 | 0 |
| D03 | Archivos de oficina personales (en estaciones de trabajo de usuarios y equipos) | 24 | 0 | 0 | 0 | 0 | 7 | 0 | 0 | 0 | 17 | 0 | 0 |
| D04 | Información escrita o impresa y datos almacenado por usuarios y los archivos personales | 0 | 2 | 2 | 0 | | | | | 0 | 12 | 0 | 0 |
| D05 | Documentos impresos o listados | | | | | | | | | 0 | 0 | 0 | 0 |
| D06 | Intercambio de mensajes, vistas de pantalla, datos individuales sensibles | 5 | 0 | 0 | 0 | 13 | 1 | 0 | 0 | 0 | 13 | 0 | 0 |
| D07 | Correo Electrónico | 8 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 4 | 0 | 0 |
| D08 | (Postal) Correos postales y faxes | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 7 | 0 | 0 |
| D09 | Archivos patrimoniales y documentos utilizados como pruebas | 0 | 0 | 0 | 0 | | | | | 4 | 0 | 0 | 0 |
| D10 | Archivos relacionados con TI | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| D11 | Datos e información publicada en sitios públicos o internos | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| | | | | | | | | | | | | | |
| **Activos de servicio** | | | | | | | | | | | | | |
| ***Servicios generales*** | | | | | | | | | | | | | |
| G01 | Espacio de trabajo del usuario y el ambiente | 3 | 0 | 0 | 0 | | | | | | | | |
| G02 | Servicios de telecomunicaciones (voz, fax, audio y video conferencias, etc.) | 14 | 1 | 0 | 0 | 0 | 4 | 2 | 0 | | | | |
| ***Servicios de redes y TI*** | | | | | | | | | | | | | |

[21] Esta implementación es producto de la simulación que se realiza para verificar como se reducirían los riesgos en caso tal se implemente el plan y los controles que se dijeron.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R01 | Servicios de redes extendidas | 13 | 11 | 0 | 0 | 0 | 5 | 0 | 0 | | | | | |
| R02 | Servicios de redes de área local | 22 | 2 | 0 | 0 | 0 | 5 | 0 | 0 | | | | | |
| S01 | Servicios prestados por las aplicaciones | 52 | 3 | 0 | 0 | 8 | 10 | 0 | 0 | 0 | 16 | 0 | 0 | |
| S02 | Servicios compartidos de oficina (servidores, gestión de documentos, impresoras compartidas, etc.) | 50 | 3 | 0 | 0 | 0 | 9 | 0 | 0 | | | | | |
| S03 | Disposición de equipos de usuarios (estaciones de trabajo, impresoras locales, periféricos, interfaces específicas, etc.) Nota : Aplica a un pérdida masiva de esos servicios, no para uno ni pocos usuarios | 9 | 0 | **1** | 0 | | | | | | | | | |
| S04 | Servicios comunes, ambiente de trabajo: mensajería, archivos, impresiones, edición, etc. | 50 | 3 | 0 | 0 | 0 | 9 | 0 | 0 | | | | | |
| S05 | Servicio de edición de Web (interna o pública) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | |
| | | | | | | | | | | | | | | |
| **Proceso de gestión de tipo de activos** | | **Eficiencia** | | | | | | | | | | | | |
| ***Procesos de gestión para el cumplimiento de las leyes o reglamentaciones*** | | | | | | | | | | | | | | |
| C01 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de datos personales. | 0 | 4 | 0 | 0 | | | | | | | | | |
| C02 | Cumplimiento a las leyes o regulaciones relacionadas a la comunicación financiera. | 0 | 0 | 0 | 0 | | | | | | | | | |
| C03 | Cumplimiento a las leyes o regulaciones relacionadas al control contable digital. | 0 | 4 | 0 | 0 | | | | | | | | | |
| C04 | Cumplimiento a las leyes o regulaciones relacionadas a la propiedad intelectual. | 0 | 4 | 0 | 0 | | | | | | | | | |
| C05 | Cumplimiento a las leyes o regulaciones relacionadas a la protección de sistemas de información. | 0 | 4 | 0 | 0 | | | | | | | | | |
| C06 | Cumplimiento a las leyes o regulaciones relacionadas a la seguridad de las personas y protección del ambiente. | 0 | 4 | 0 | 0 | | | | | | | | | |
| | | | | | | | | | | | | | | |
| **Número de escenarios D, I, C:** | | 303 | 28 | **3** | 0 | 36 | 63 | **2** | 0 | 4 | 106 | **1** | 0 | |
| **Eficiencia:** | | 0 | 20 | 0 | 0 | | | | | | | | | |
| | | | | | | | | | | | | | | |

***Tabla 4-9.*** *Valoración del procedimiento después de controles y plan de tratamiento*

La *tabla 4-9* es muy importante, muestra la valoración que se tendría en caso de que se realizara la implantación de los controles seleccionados. El resultado de la valoración para eventos naturales se detalla en el anexo C.3.3 inciso 1.

Los resultados de la valoración del riesgo en el caso de estudio son los mostrados en las *tablas 4-9, 4-10,4-11 y 4-12.*

a. Escenarios de malfuncionamientos en disponibilidad total 333.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 3 |
| 2 | 28 |
| 1 | 303 |

***Tabla 4-10.*** *Valoración en simulación malfuncionamiento disponibilidad*

b. Escenarios de malfuncionamientos en integridad total 101.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 2 |
| 2 | 63 |
| 1 | 36 |

***Tabla 4-11.*** *Valoración en simulación malfuncionamiento integridad.*

c. Escenarios de malfuncionamientos en confidencialidad total 101.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 1 |
| 2 | 106 |
| 1 | 4 |

***Tabla 4-12.*** *Valoración en simulación malfuncionamiento confidencialidad.*

d. Escenarios de malfuncionamientos en eficiencia total 20.

| Valoración | Numero Escenarios |
|---|---|
| 4 | 0 |
| 3 | 0 |
| 2 | 20 |
| 1 | 0 |

***Tabla 4-13. V****aloración en simulación malfuncionamiento eficiencia.*

Finalmente en la *ilustración 4-11* se muestran los artefactos que se tomaron de la metodología MEHARI para el procedimiento de estudio en la fase 8.

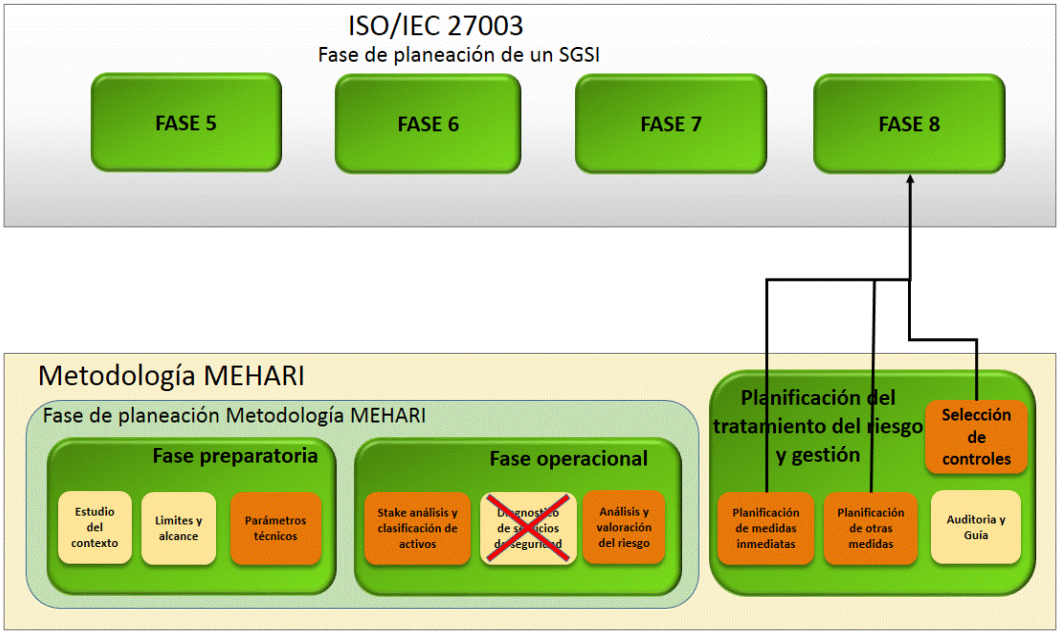



***Ilustración 4-11.*** *Inclusión de artefacto de la fase de planificación de MEHARI*

## 4.5 RESULTADOS OBTENIDOS

Una vez realizada la fase de planeación de un SGSI, se deben tener como entregables dos documentos de vital importancia en la implementación de un SGSI en su fase de planeación por una parte la declaración de Aplicabilidad y el plan de tratamiento determinado por la metodología.

### 4.5.1 Declaración de aplicabilidad

La declaración de aplicabilidad es un documento donde se consignan los controles seleccionados de la norma ISO/IEC 27002:2013 en su anexo A. Esta sección de anexos está dividida en 14 dominios de seguridad, 35 objetivos de control y 114

controles. La declaración de aplicabilidad considera los 114 controles recomendados por la norma[22].

La versión más reciente[23] de la ISO/IEC 27002 considera que se deben seleccionar solo los controles de seguridad que correspondan a la organización. Los controles que se elijan deben quedar documentados y bien definidos justificando cualquier exclusión.

Anteriormente en las auditorías para la certificación cuando los auditores internos realizaban las inspecciones se debía verificar que todos los controles estuvieran implantados en la organización, si alguno no estaba, se le daba un tiempo prudente a la organización para implantarlo, si después de ese tiempo no se cumplía, no se otorgaba la certificación, hoy con la nueva versión, los auditores internos, no se dirigen a todos los controles, en vez de eso se verifica cuáles son los controles seleccionados en la declaración de aplicabilidad de acuerdo al análisis y valoración realizado con la metodología seleccionada. La declaración de aplicabilidad para el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones se detalla en el anexo D.1.

### 4.5.2 Plan de tratamiento del riesgo

Cuando se tiene la “declaración de aplicabilidad”, la organización debe conocer la manera en que los controles elegidos se van a implementar. Esto se puede determinar con la norma ISO/IEC 27005, pero siempre es recomendable realizarla con una metodología de gestión de riesgo. Por lo tanto, el plan de tratamiento será el que haya estipulado la metodología. Para ver el plan de tratamiento del caso de estudio véase el anexo D.2.

La “simulación” realizada en 4.5.3 contempló los controles dados en la “declaración de aplicabilidad” y el plan de tratamiento del riesgo que aquí se expone, el resultado que se obtuvo de la simulación fue el producto de estos dos documentos. Según los

[22] En la versión anterior (versión 2005) se tenían 133 controles y era obligatoria que cualquier organización buscando la certificación ISO/IEC 27001 tuviera todos los controles implantados.
[23] Versión 2013 es la más reciente.

resultados obtenidos se puede determinar que los controles seleccionados y plan de tratamiento fueron acertados.

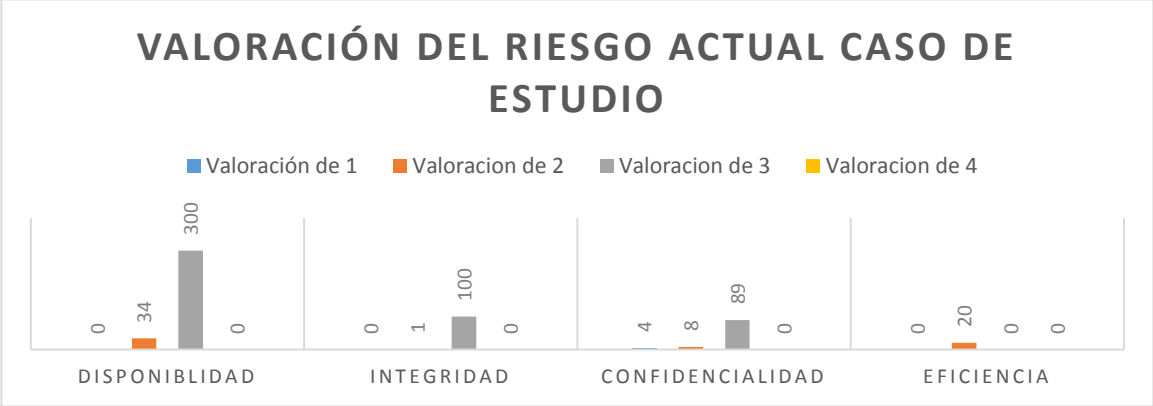



***Tabla 4-14.*** *Tabla general de la valoración del riesgo actual*

Después de realizar la "simulación" para determinar cómo estaría el riesgo después de haber implementado los controles y plan de tratamiento, se muestra la *tabla 4-14.*

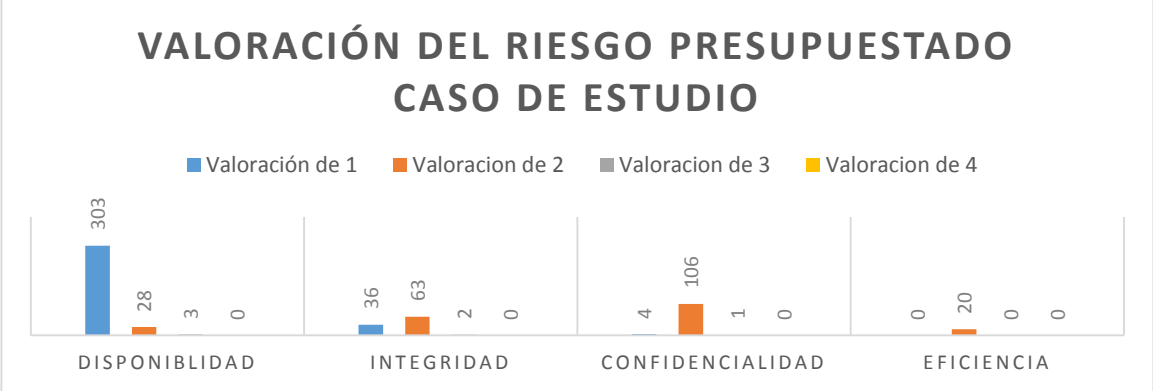



***Tabla 4-15.*** *Tabla general de la valoración del riesgo presupuestada*

# 5 DISCUSION DE LA ADAPTACIÓN DE LA METODOLOGIA MEHARI AL CASO DE ESTUDIO

La metodología MEHARI está en conformidad con la ISO/IEC 27005 ya que cumple con todas sus directrices.

En la tabla se presenta la adaptación de la metodología al procedimiento en estudio según la experiencia que se obtuvo durante el desarrollo del proyecto.

| **Adaptación de la metodología MEHARI** | | |
|---|---|---|
| **Fases** | **Sub fase** | **Actividades** |
| Fase preparatoria | Evaluación del contexto | *Ninguno (ISO/IEC 27003 paso 5)* |
| | | *Ninguno (ISO/IEC 27003 paso 5)* |
| | | *Ninguno (ISO/IEC 27003 paso 5)* |
| | Determinar el alcance y sus limites | *Ninguno (ISO/IEC 27003 paso 6)* |
| | | *Ninguno (ISO/IEC 27003 paso 6)* |
| | | *Ninguno (ISO/IEC 27003 paso 6)* |
| | Establecer parámetros de riesgos principales | Tabla de aceptabilidad de riesgo |
| | | Tabla de exposición natural |
| | | Tabla de evaluación del riesgo |
| Fase operacional | Clasificación de activos y análisis de cuestiones | Escala de valores de malfuncionamiento |
| | | Clasificación de activos |
| | | Tabla de impacto intrínseco |
| | Evaluando la calidad del servicio de seguridad | *Ninguno (No tiene controles)* |
| | | *Ninguno (No tiene controles)* |
| | Evaluación del riesgo | Seleccionando los escenarios parar el análisis |
| | | Evaluando los escenarios de riesgo |
| Fase de tratamiento | Medidas de planificación inmediata | Selección de riesgo parar tratamiento inmediato |
| | | Selección de medidas parar la implementación inmediata |
| | | *Nueva (Selección de controles de seguridad ISO/IEC 27002)* |
| | Planificación de medidas en contextos específicos | Estrategia prioritaria y de tratamiento |
| | | Selección de medidas y planes |
| | Vigilancia de la implantación del tratamiento de riesgo | *Vigilancia de planificación (Modificada)* |
| | | Selección de indicadores, dashboards y gráficos |

***Tabla 5-1.*** *Metodología MEHARI adaptada al caso de estudio.*

Se hace necesaria la adaptación de la metodología MEHARI al caso de estudio, para cumplir con los requerimientos de la organización.

Basado en la experiencia en la aplicación de la metodología MEHARI, se propone que quienes inicien un SGSI con el soporte de la metodología MEHARI ejecute la adaptación que se ha mostrado en este trabajo.

Se tiene que contar con escenarios similares al aquí planteado. La característica principal del caso de estudio es que no tiene implantado un SGSI, otro factor importante es que solo se está llevando a cabo la fase de planeación del SGSI y que para cumplir este propósito se sigue la normativa ISO/IEC 27003:2010. Además, este caso de estudio es solo un solo procedimiento de una organización muy amplia.

La adaptación de la metodología MEHARI al caso de estudio específico es propuesta con base a la experiencia y la retroalimentación obtenida a lo largo del uso que se le dio a la metodología en el caso de estudio. Esta adaptación es útil para tenerse en cuenta a la hora de desarrollar proyectos similares para valoración y tratamiento del riesgo con el soporte de la metodología MEHARI.

A continuación se retomaran las partes más importantes en la adaptación de la metodología MEHARI al caso de estudio.

- ✓ **Fase preparatoria**

Esta fase fue adaptada, debido a que mucho de las sub fases requeridas aquí, ya han sido abordadas durante el desarrollo de la norma ISO/IEC 27003:2010.

*1. Evaluación del contexto*

Se omite. Esta fase es equivalente a la fase 5 de la norma ISO 27003:2010 la cual se denomina *"Obtener Aprobación de la dirección para iniciar un proyecto de SGSI" [27]*. Al pasar por esta fase de la norma, se deben tener una lista de documentos, dentro de los cuales se determina el contexto estratégico, técnico y estructural de la organización. Se realiza un caso de estudio una propuesta de proyecto, un resumen de las características del negocio, etc. Esta fase contempla todo lo que exige la metodología MEHARI.

*2. Determinar el alcance y límites*

Se omite. Es equivalente a la norma ISO/IEC 27003:2010 fase 6 la cual se denomina *"Definir el alcance del SGSI, sus límites y la política de SGSI" [27]*.

*3. Establecer parámetros de riesgos principales*

No se altera. Debido a que se deben tener tablas de referencia para determinar cuándo un riesgo es tolerable o no, estos parámetros con propios de la metodología.

La *ilustración 5-1* muestra este proceso.

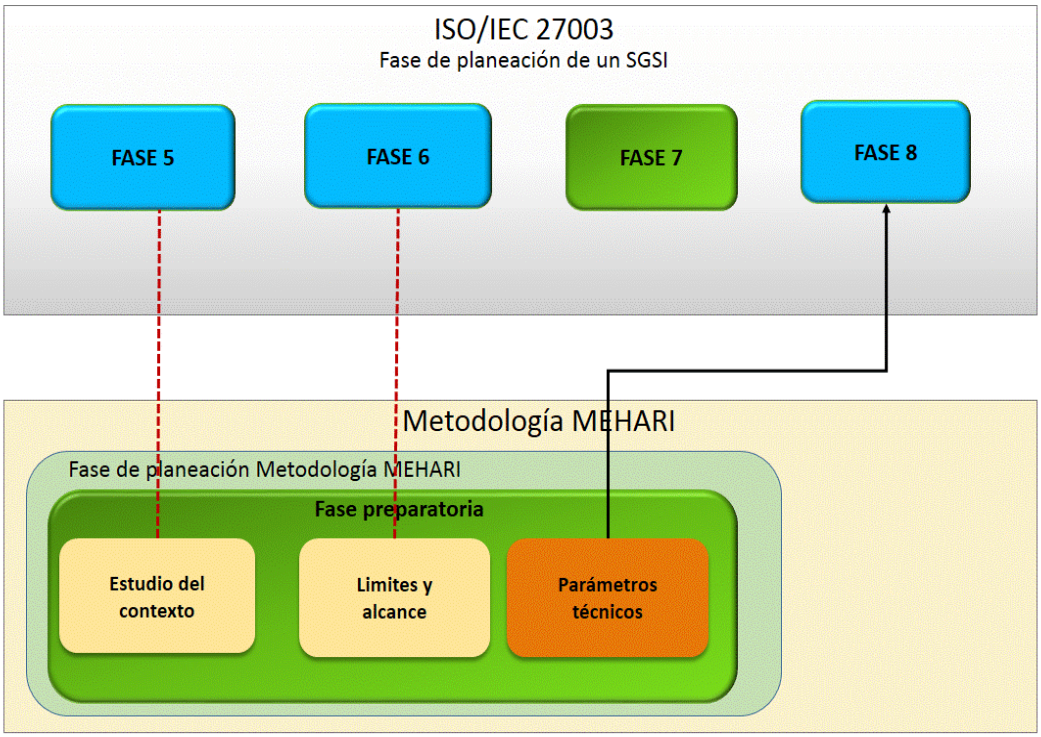



***Ilustración 5-1.*** *Fase preparatoria adaptada de la metodología MEHARI al caso de estudio*

✓ **Fase operacional – Análisis del riesgo**

*1. Clasificación de activos y análisis de cuestiones*

No se altera. Debido a que es necesario recopilar toda la información de la organización, en cuanto a activos, su ubicación, locales, categorías propuestas por MEHARI, etc.

*2. Diagnóstico de servicios de seguridad*

Se omite. Debido a que se considera innecesario realizar preguntas de auditoria o evidenciar controles, cuando a la organización que se realiza la valoración no tiene ningún tipo de control de seguridad referente a Seguridad de la Información. No existen datos para evaluar la calidad del servicio de seguridad, porque no hay servicio implantando.

*3. Análisis y valoración de riesgo*

No se altera. Debido a que es necesario valorar los activos en varios escenarios para tener en cuenta que es lo más riesgoso que tiene la organización y cuáles son los puntajes más elevados de gravedad del riesgo. Según los escenarios que apliquen. La *ilustración 5-2* muestra todo el proceso que se siguió.

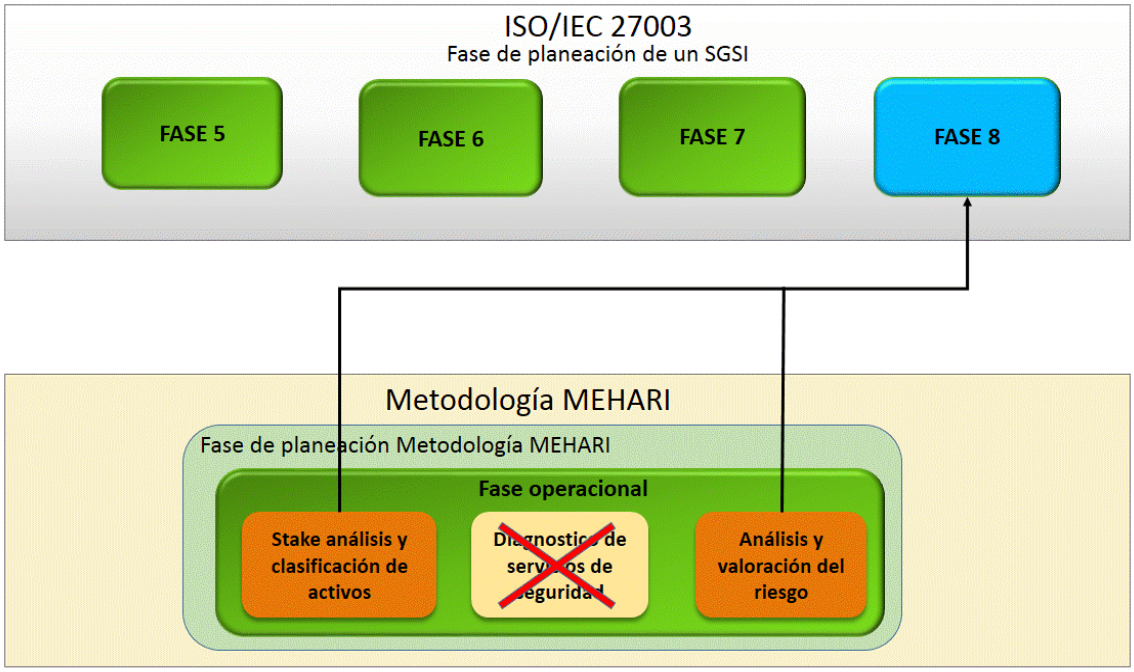



***Ilustración 5-2.*** *Fase operacional adaptada de la metodología MEHARI al caso de estudio*

✓ **Fase de tratamiento del riesgo y planificación**

*1. Medidas de planificación inmediatas*

Esta fase completa no se altera. Pero se le agrega a la sub fase "*Planificación de medidas inmediatas*" una actividad denominada *"selección de controles de*

*seguridad (ISO/IEC 27002) para reducir el riesgo".* Esta actividad está implícita en el plan de acción, pero se consideró que esta actividad es de mucha importancia para la reducción del riesgo, por lo tanto se eligió la fase de acciones inmediatas, para mitigar los riesgos, con el fin de reducirlos, con la implantación de controles de seguridad de la norma ISO/IEC 27002 en su anexo A directamente, y no implícitamente (a través de servicios de seguridad) *[26].*

2. *Planificación de otras medidas.*

No se altera. Se debe seleccionar la forma de realizar la planificación del tratamiento.

3. *Selección de controles*

Se agrega este artefacto, debido a que es necesario que el auditor conozca los controles que posiblemente pueda seleccionar, esto para darle una idea al auditor sobre qué servicios se deben mejorar. Esta pre selección se compara con los servicios de seguridad para determinar el SOA definitivo.

4. *Auditoria y Guía*

No es considerado ya que no está dentro del alcance de este proyecto.

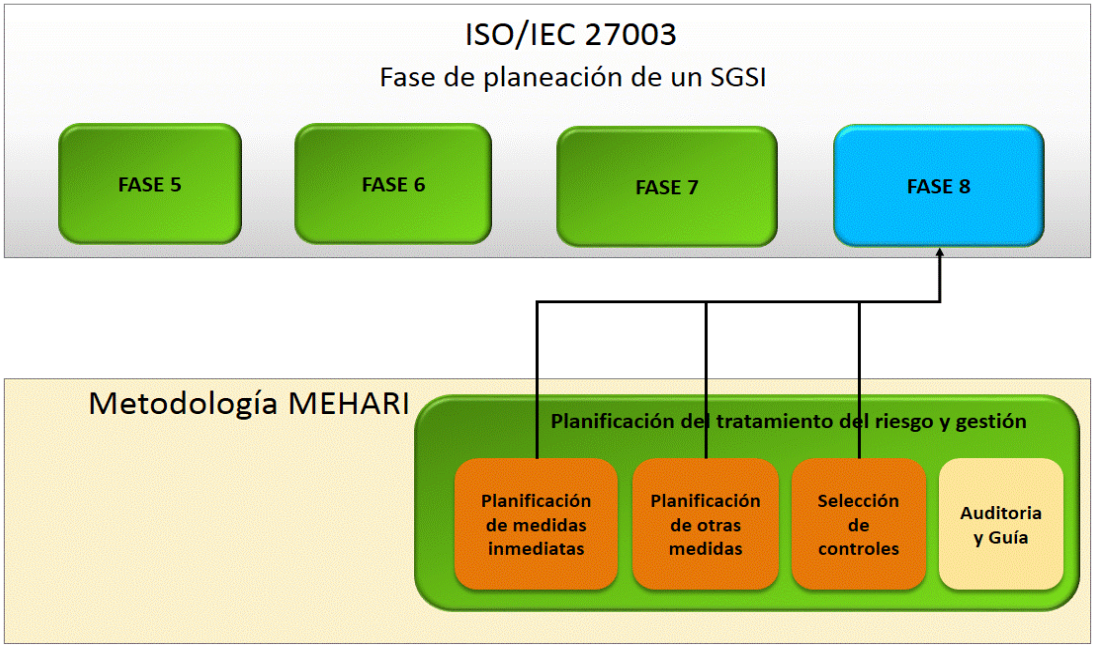



***Ilustración 5-3.*** *Fase de planificación adaptada de la metodología MEHARI al caso de estudio*

Finalmente en la *ilustración 5-4* se muestra la metodología MEHARI en todas sus fase y después en la *ilustración 5-5* la metodología MEHARI adaptada al caso de estudio.

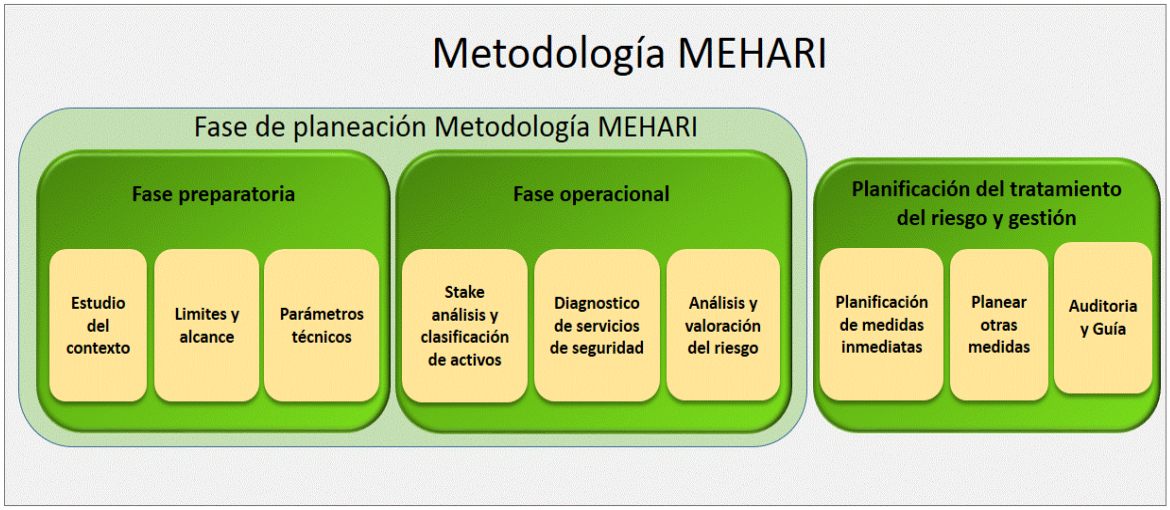



***Ilustración 5-4.*** *Metodología MEHARI completa fase a fase*

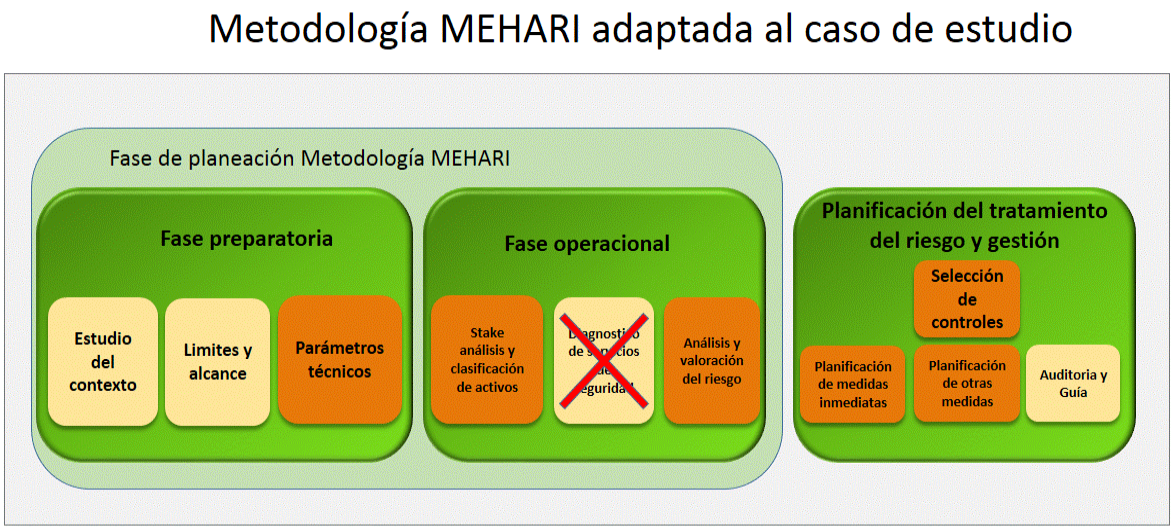
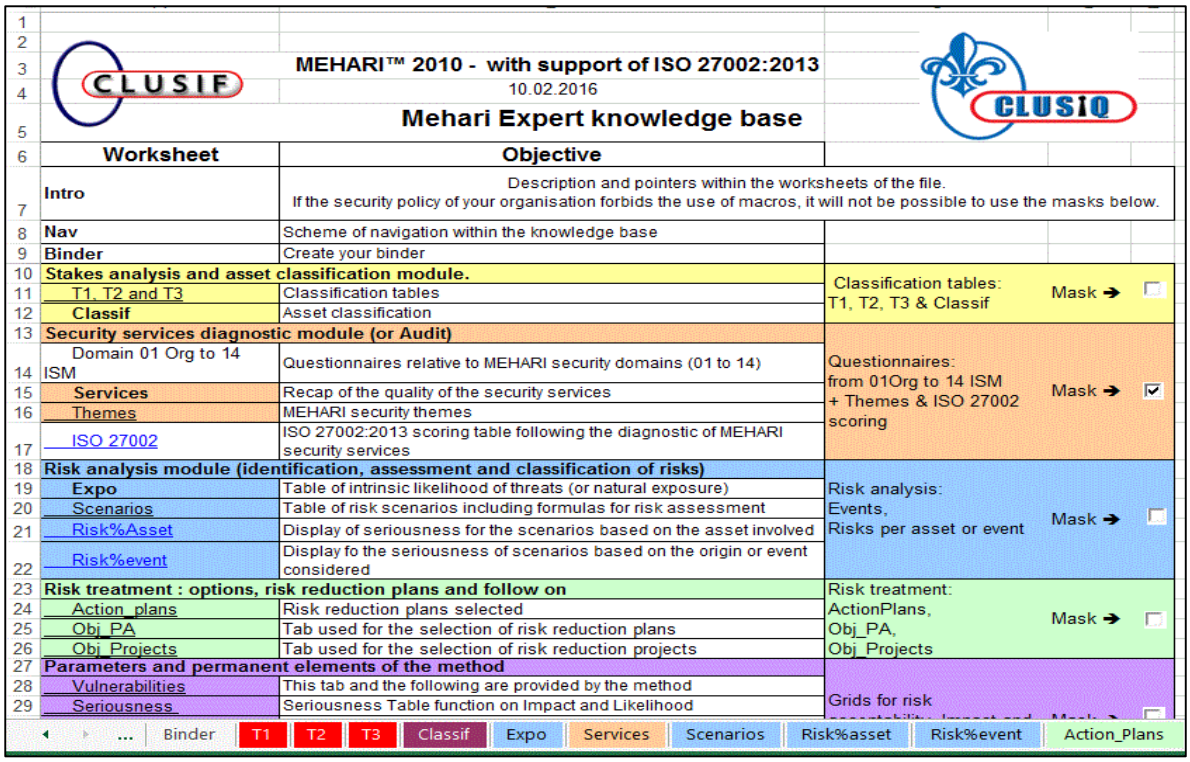



***Ilustración 5-5.*** *Metodología MEHAR adaptada al caso de estudio*

# 6 GUÍA PARA IMPLEMENTACIÓN DE LA METODOLOGÍA MEHARI

La metodología MEHARI es una metodología de gestión de riesgos que cumple con las directrices establecidas por la ISO/IEC 27005. La metodología MEHARI proporciona una extensa herramienta conocida como "Base de Reconocimiento" disponible en formato de Microsoft Excel mostrada en la *ilustración 6-1*, esta puede ser descargada del sitio web de CLUSIF de forma gratuita bajo la licencia de Open Source y permite realizar de forma completa el análisis y la valoración de los riesgos en cualquier organización. Sin embargo la herramienta proporcionada por la metodología MEHARI y la documentación no es clara y deja muchos vacíos a la hora de su ejecución en la práctica, la documentación original está disponible en Francés, existen algunas traducciones de la documentación al Inglés pero no está disponible de forma completa, debido a esto cuando cualquier encargado de la seguridad de la información inicia la implementación de un SGSI con el soporte de la metodología MEHARI sin ninguna experiencia, esta resulta ser muy compleja.

El objetivo de este capítulo es proporcionar una guía para la implementación de la metodología MEHARI. Se detallarán las actividades que se deben realizar para su correcta ejecución para que auditores, personal de Seguridad de la Información, jefes de Seguridad y en general cualquier persona que busque utilizar la metodología MEHARI para gestionar el riesgo en la seguridad de la información, lo hagan con el soporte de esta guía.



MEHARI™ 2010 - with support of ISO 27002:2013

10.02.2016

Mehari Expert knowledge base

| Worksheet | Objective | | |
|---|---|---|---|
| Intro | Description and pointers within the worksheets of the file. If the security policy of your organisation forbids the use of macros, it will not be possible to use the masks below. | | |
| Nav | Scheme of navigation within the knowledge base | | |
| Binder | Create your binder | | |
| **Stakes analysis and asset classification module.** | | Classification tables: T1, T2, T3 & Classif | Mask ➔ ☐ |
| T1, T2 and T3 | Classification tables | | |
| Classif | Asset classification | | |
| **Security services diagnostic module (or Audit)** | | Questionnaires: from 01Org to 14 ISM + Themes & ISO 27002 scoring | Mask ➔ ☑ |
| Domain 01 Org to 14 ISM | Questionnaires relative to MEHARI security domains (01 to 14) | | |
| Services | Recap of the quality of the security services | | |
| Themes | MEHARI security themes | | |
| ISO 27002 | ISO 27002:2013 scoring table following the diagnostic of MEHARI security services | | |
| **Risk analysis module (identification, assessment and classification of risks)** | | Risk analysis: Events, Risks per asset or event | Mask ➔ ☐ |
| Expo | Table of intrinsic likelihood of threats (or natural exposure) | | |
| Scenarios | Table of risk scenarios including formulas for risk assessment | | |
| Risk%Asset | Display of seriousness for the scenarios based on the asset involved | | |
| Risk%event | Display fo the seriousness of scenarios based on the origin or event considered | | |
| **Risk treatment : options, risk reduction plans and follow on** | | Risk treatment: ActionPlans, Obj_PA, Obj_Projects | Mask ➔ ☐ |
| Action_plans | Risk reduction plans selected | | |
| Obj_PA | Tab used for the selection of risk reduction plans | | |
| Obj_Projects | Tab used for the selection of risk reduction projects | | |
| **Parameters and permanent elements of the method** | | Grids for risk | |
| Vulnerabilities | This tab and the following are provided by the method | | |
| Seriousness | Seriousness Table function on Impact and Likelihood | | |

Binder | T1 | T2 | T3 | Classif | Expo | Services | Scenarios | Risk%asset | Risk%event | Action_Plans

***Ilustración 6-1.*** *Introducción a la Base de Reconocimiento de MEHARI*

## 6.1 GUÍA DE IMPLEMENTACIÓN

La guía de implementación de la metodología MEHARI se muestra en la *ilustración 6-2*. La metodología MEHARI sigue un completo proceso que puede ser comparado con la ISO/IEC 27003, esto quiere decir, que es una metodología que permite el mejoramiento constante cumpliendo así con los requerimientos de la norma ISO/IEC 27001. A continuación, se presenta la guía de implementación fase a fase de la metodología MEHARI.

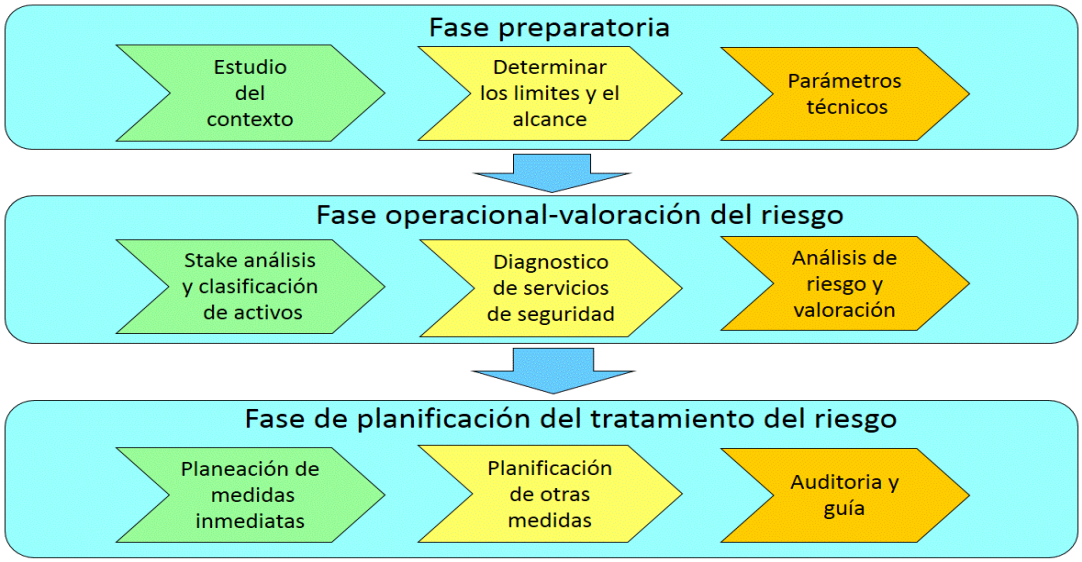



***Ilustración 6-2.*** *Guía de implementación de la Metodología MEHARI*

## 6.1.1 Fase Preparatoria

La fase preparatoria es la fase inicial, esta fase cuenta con tres sub fases: Estudio del Contexto, Límites y Alcance y Parámetros Técnicos, estas fases son similares a las establecidas por la ISO/IEC 27003 en el numeral 5 y 6 en donde también se realiza el estudio del contexto y además se determinan los límites y el alcance de la organización.

### 1. Estudio del Contexto

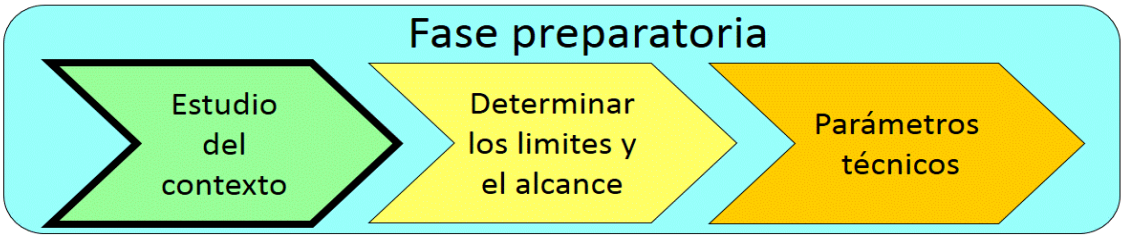



***Ilustración 6-3.*** *Fase preparatoria "Estudio del Contexto" de la Metodología MEHARI*

El objetivo de esta sub fase es conocer la organización con respecto a la Seguridad de la Información, durante esta sub fase se deben determinar 3 actividades principales.

### 1.1. Estudio del Contexto Estratégico

Para realizar esta actividad se debe tener en cuenta lo siguiente:

*Estructura del Contexto*
- ✓ Posicionamiento en el mercado de la organización.
- ✓ Actividades de naturaleza competitiva.
- ✓ Servicios críticos de la organización.
- ✓ Incidentes y malfuncionamiento que han ocurrido en la organización.

*Restricciones sobre las operaciones y la estructura de la entidad*
- ✓ Restricciones legales.
- ✓ Restricciones de regulaciones.
- ✓ Reglamento que debe seguirse.

*Información de la política de seguridad (Si existe)*
- ✓ Objetivos de seguridad.
- ✓ Roles en la valoración y tratamiento del riesgo.
- ✓ Gestión de apoyo.

Toda esta información debe ser documentada para ser presentada a la alta dirección para la aprobación de un SGSI en la organización.

Con el fin de recolectar toda la información necesaria para el SGSI, se deben realizar entrevistas, encuestas, reuniones, actas, grabaciones etc. Se deben planear reuniones con el Jefe de Información, con los directivos, con los departamentos y jefes de la organización. Al finalizar todas las reuniones se debe obtener lo siguiente debidamente documentado:

- ➢ Recolección de elementos disponibles referentes a la Seguridad de la Información.
- ➢ Generación de un resumen de información recolectada.

- Aprobación de la alta dirección para ejecutar un SGSI.

### 1.2. Estudio del Contexto Técnico

Para realizar esta actividad se debe determinar lo siguiente:

*Estructuras de los Sistemas de Información*
- ✓ Arquitectura de la red.
- ✓ Arquitectura del sistema.
- ✓ Arquitectura de aplicaciones.
- ✓ Cartografía general.

*Planes para la evaluación tecnológica a corto, mediano y largo plazo*
- ✓ Plan de desarrollo.
- ✓ Soluciones de durabilidad operacional.

*Proveedores críticos externos*
- ✓ Proveedores de servicios críticos.
- ✓ Proveedores de software.
- ✓ Proveedores de servicios ocasiones.

Para determinar los requisitos anteriores, se debe consultar con el Jefe de Información y con el administrador de la Red y de los sistemas. Se debe realizar los siguientes documentos obligatorios:

- Recolección de elementos técnicos disponibles.
- Generación de resumen de información recolectada.
- Aprobación por parte de del Jefe de Información de que la información recolectada sea la correcta.

### 1.3. Estudio del Contexto Organizacional

Para realizar esta actividad se debe determinar lo siguiente:

*Esquema organizacional*
- ✓ Relaciones hereditarias.

- ✓ Funciones de enlaces y relaciones.

*Distribución de responsabilidades de cuestiones de seguridad*

- ✓ Descripción de trabajos y asociaciones.
- ✓ División de responsabilidades.

*Estructura de Supervisión*

- ✓ Procesos existentes para aprobar planes de acción.
- ✓ Configuración y operaciones de estructura de supervisión.

Para determinar lo anterior se deben realizar entrevistas y reuniones con: Gerente de Recursos Humanos, Gerente Administrativo y Financiero y Jefe de Información. Se debe obtener los siguientes documentos obligatorios:

- ➢ Recolección de elementos organizacionales disponibles.
- ➢ Generación de resumen de información recolectada.
- ➢ Aprobación por parte del Gerente General para verificar que la información recolectada sea la correcta.

## 2. Determinar límites y Alcance

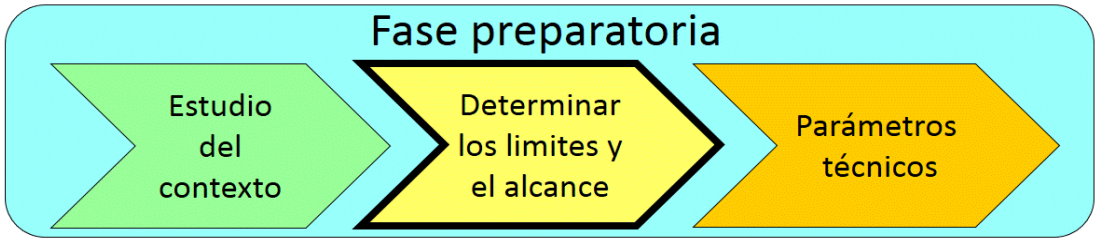



***Ilustración 6-4.*** *Fase preparatoria "Determinar los límites y alcance" de la Metodología MEHARI*

Esta sub fase cuenta con tres actividades principales que a su vez se derivan en otras actividades para dar cumplimiento a esta sub fase.

### 2.1. Perímetro técnico

Para realizar esta actividad se deben determinar las siguientes actividades:

*Perímetros geográficos*

- ✓ Sitios y ubicaciones.

*Sistemas de información*

- ✓ Sistemas de información generales.
- ✓ Exclusión (o no) de gestión de procesos industriales
- ✓ Exclusión (o no) de diseño de sistemas.
- ✓ Cualquier otro relacionado con sistemas de información.

*Información digital*

- ✓ Información digital.
- ✓ Documentos físicos o escritos digitalizados.
- ✓ Grabaciones o videos.

Para poder determinar los requisitos anteriores, se deben realizar entrevistas con el Jefe de Información y Gerente General. Una vez se ha terminado de recolectar la información anterior se debe realizar los siguientes documentos.

- ➢ Recolección de elementos importantes de clientes y de la organización.
- ➢ Generación de resumen de la información recolectada.
- ➢ Aprobación por parte de la Gerencia General que la información recolectada es la correcta.

## 2.2. Perímetro Organizacional

Para realizar esta actividad se deben determinar las siguientes actividades:

*Actividades de perímetros*

- ✓ Actividades concernientes.
- ✓ Unidades de servicio (si aplican).

*Tipos de riesgo incluidos en la operación*

- ✓ Toda la información relacionada a los riesgos.
- ✓ Limitación a una o varios tipos de riesgo.

Para determinar lo anterior, se debe realizar entrevistas con los clientes de la organización, Gerencia General y Jefe de Información. Al terminar estas actividades se deben realizar los siguientes documentos:

- Encuesta para el personal y clientes de la organización.
- Generación de resumen de información recolectada.
- Aprobación por parte de la Gerencia General de que la información recolectada es la correcta.

### 2.3. Supervisión

Para realizar esta actividad se deben determinar las siguientes actividades:

*Estructura de operaciones*

- ✓ Participantes
- ✓ Cronograma de reuniones

Para determinar los requisitos anteriores, se debe realizar entrevistas con los clientes de la organización, Gerencia General y Jefe de Información. Al terminar estas actividades se deben realizar los siguientes documentos:

- Encuesta para el personal y clientes de la organización.
- Generación de resumen de información recolectada.
- Aprobación por parte de la Gerencia General que la información recolectada es la correcta.

## 3. Parámetros técnicos

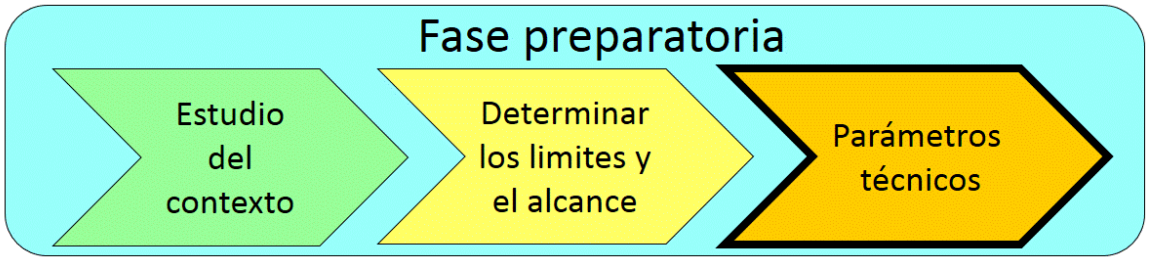



***Ilustración 6-5.*** *Fase preparatoria "Parámetros técnicos" de la Metodología MEHARI*

Los parámetros técnicos representan la escala de valores que se determina para analizar si un riesgo es aceptado o no, esta escala debe ser tenida en cuenta para la construcción de la tabla de impacto intrínseco, la tabla de eventos, la escala de mal funcionamientos y la tabla general de escenarios. MEHARI tiene su propia escala de valores de riesgo, la cual es numerada de 1 a 4, donde 1 y 2 son riesgo aceptables, 3 y 4 son riesgos no aceptables tal y como se muestra en la *ilustración 6-6*. Sin embargo, MEHARI da la opción al Auditor o Jefe de Seguridad de realizar su propia escala para dichas tablas.

Por sugerencia de los autores del trabajo de grado, se recomienda utilizar las mismas escalas y valoraciones que proporciona la metodología.

| Impacto | | | | | Gravedad del Riesgo |
|---|---|---|---|---|---|
| 4 | 2 | 3 | 4 | 4 | Convención de Color |
| 3 | 2 | 3 | 3 | 4 | 4 = Intolerable |
| 2 | 1 | 2 | 2 | 3 | 3 = Inadmisible |
| 1 | 1 | 1 | 1 | 2 | 2 = Aceptable |
| | 1 | 2 | 3 | 4 | 1 = Bajo |
| | Probabilidad | | | | |

***Ilustración 6-6.*** *Tabla impacto y probabilidad*

## 6.1.2 Fase operacional

Esta fase de la metodología MEHARI es la más importante ya que la metodología proporciona una herramienta muy completa para llevar a cabo esta tarea. Hasta el momento solo se ha realizado el estudio del contexto de la organización así como también la definición de los límites y el alcance. En esta fase operacional es donde se lleva a cabo la clasificación de activos, identificación de amenazas y valoración de riesgos. A continuación se detalla cada sub fase.

## 1. Análisis de cuestiones y clasificación de activos


***Ilustración 6-7**. Fase operacional "Stake análisis y clasificación de activos" de la Metodología MEHARI*

Todas las actividades que deben realizarse en el "Stake análisis y clasificación de activos" se muestran en la *ilustración 6-8*.

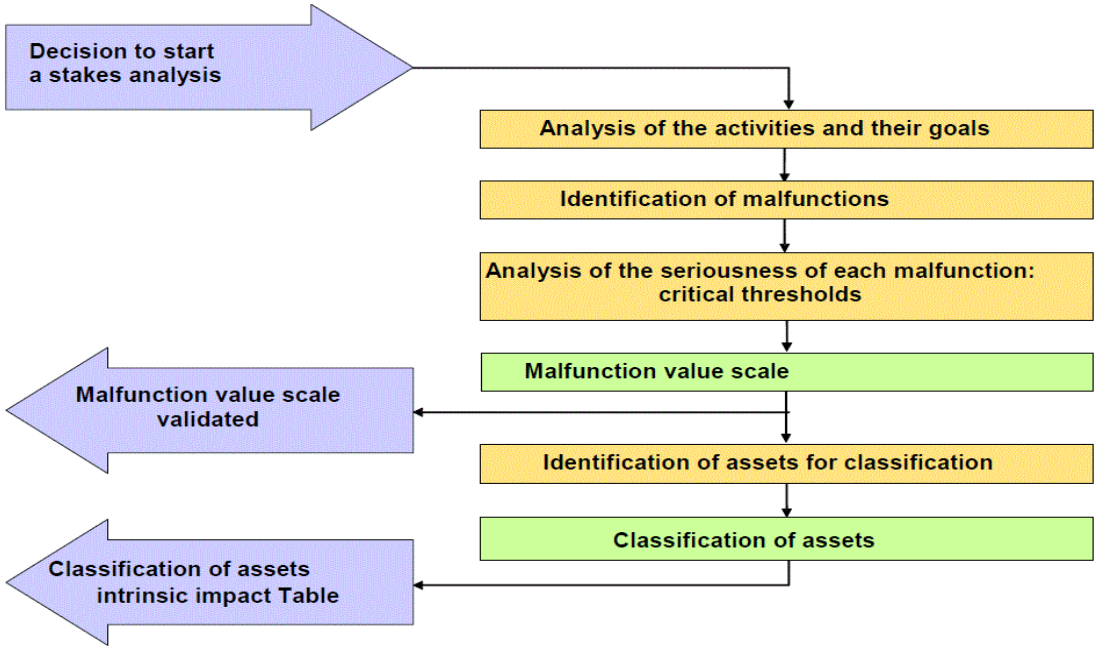



***Ilustración 6-8.** Identificación de malfunciones y clasificación de activos*

Primero que todo se debe identificar las actividades de la organización y sus objetivos, estas actividades deben estar descritas como funciones y se debe identificar los objetivos y los resultados esperados de la realización de dicha actividad, un ejemplo de la realización de la tabla de actividades se muestra en las

*tablas 6-1 y 6-2*, de igual manera de debe realizar la tabla completa con todas las actividades de la organización.

| Función | Objetivos y resultados esperados |
|---|---|
| Realizar, diseñar y construir la arquitectura del aplicativo de acuerdo a las especificaciones del usuario. | Diseñar la solución como resultado final se tiene el diseño de la aplicación. |

***Tabla 6-1.*** *Identificación de las actividades de la organización y sus respectivos objetivos*

| Función | Objetivos y resultados esperados |
|---|---|
| Realizar las pruebas internas colocando el sistema en marcha. Verificar: Corrección de errores descubiertos. Mejoras de implementación, Identificar nuevos requisitos. | Realización de pruebas internas con el fin de detectar fallos en el software como resultado de esta actividad se tienen recomendaciones de mejoras. |

***Tabla 6-2****. Identificación de las actividades de la organización y sus respectivos objetivos*

Una vez se han identificado las actividades, se deben identificar las respectivas malfunciones, es decir lo que podría llegar a suceder si la actividad en consideración no se realizara o fallara en cuanto a confidencialidad, disponibilidad e integridad. Las *tablas 6-3 y 6-4* muestran la identificación de las malfunciones por cada actividad y las consecuencias de esas malfunciones.

| **1. REALIZAR, DISEÑAR Y CONSTRUIR LA ARQUITECTURA DEL APLICATIVO DE ACUERDO A LAS ESPECIFICACIONES DEL USUARIO.** | |
|---|---|
| **Malfunción** | **consecuencias** |
| Divulgación del sistema o arquitectura | La divulgación del sistema o la arquitectura de la aplicación tendrían consecuencia en cuanto a la confidencialidad. |

*Tabla 6-3. Identificación de las malfunciones por actividad y sus consecuencias*

| **1. IMPLEMENTAR LA SOLUCIÓN PARA ADAPTARSE A LAS NECESIDADES DEL USUARIO.** | |
|---|---|
| **Malfunción** | **consecuencias** |
| Herramientas de desarrollo no disponibles (software y hardware) | La indisponibilidad de las herramientas y equipos de desarrollo no permitirían la realización de las actividades |
| Personal de desarrollo no disponible | Si el personal de desarrollo no está disponible la respuesta a las solicitudes de desarrollo no se puede llevar a cabo, esto sería muy crítico para la organización. |
| Indisponibilidad de la red interna | La indisponibilidad de la red interna no permite accede a el almacenamiento en los repositorios internos y la comunicación interna. |

| | |
|---|---|
| Fallas en el suministro energético | Las fallas en el suministro eléctrico no permiten que las actividades se lleven a cabo. |
| Errores o bugs en el código fuente | Una mala codificación de las aplicaciones podría ocasionar fallas en los sistemas que podrían ser explotadas por una amenaza, cuando sean ejecutados por los servidores |
| Indisponibilidad de internet | La indisponibilidad de la red para el acceso a internet no permite llevar a cabo las tareas de forma eficiente, debido a que no se permite la búsqueda de información ni acceder a los repositorios en línea. |
| Perdida de archivos almacenados a nivel interno | El almacenamiento no seguro pude ocasionar la perdida de la información(confidencialidad e integridad) |

***Tabla 6-4.*** *Identificación de las malfunciones por actividad y sus consecuencias*

La última tarea en la identificación de las malfunciones es describir que tan grave es la respectiva malfunción para la continuidad de la organización, para llevar a cabo esto, la metodología MEHARI utiliza una tabla predeterminada con valores de 1 a 4 con el respectivo significado como se muestra en la *tabla 6-5*.

| **Escala estándar del nivel de impacto** | |
|---|---|
| **Nivel 4 vital** | A este nivel el impacto es muy serio incluso para la continuidad de la organización (o al menos una de sus principales actividades) está en peligro, estaría la organización acarreando con un malfuncionamiento, esto sería grave y las consecuencias muy críticas. |
| **Nivel 3 muy serio** | A este nivel el impacto es considerado muy serio para la entidad, pero en un futuro no sería un riesgo, en términos económicos esto tendría un impacto negativo sobre las ganancias por un periodo de tiempo, aunque no sería una enorme pérdida para los socios. |
| **Nivel 2 serio** | Las malfunciones a este nivel tendrían un claro impacto sobre las operaciones de la entidad, resultados o imagen, pero es globalmente manejable |
| **Nivel1 insignificante** | A este nivel cualquier resultado dañino no tendría un impacto significativo sobre los resultados o imagen de la organización. |

***Tabla 6-5.*** *Escala estándar del nivel de impacto*

Una vez se ha definido la escala, se realiza la evaluación del impacto de cada malfunción para las actividades de la organización como se muestra en la *tabla 6-6 y 6-7*, valorándola en una escala de 1 a 4.

| **1. REALIZAR, DISEÑAR Y CONSTRUIR LA ARQUITECTURA DEL APLICATIVO DE ACUERDO A LAS ESPECIFICACIONES DEL USUARIO.** | | | | |
|---|---|---|---|---|
| **Malfunción** | **Nivel 1 insignificante** | **Nivel 2 serio** | **Nivel 3 muy serio** | **Nivel 4 vital** |
| Divulgación del sistema o arquitectura, almacenamiento en línea de la información. | La información es accedida y divulgada por personal dentro de la institución | | | La información es accedida y divulgada por fuera de la institución |

***Tabla 6-6.*** *Valoración del impacto de las malfunciones*

| **1. IMPLEMENTAR LA SOLUCIÓN PARA ADAPTARSE A LAS NECESIDADES DEL USUARIO.** | | | | |
|---|---|---|---|---|
| **Malfunción** | **Nivel 1 insignificante** | **Nivel 2 serio** | **Nivel 3 muy serio** | **Nivel 4 vital** |
| Herramientas de desarrollo no disponibles (software y hardware) | Las herramientas no están disponibles por más de una hora | Las herramientas no están disponibles por más de 3 horas | Las herramientas no están disponibles por un día | Las herramientas no están disponibles por una semana |
| Personal de desarrollo no disponible | | | Falta de un personal de desarrollo | Falta de todo el personal de desarrollo |
| Indisponibilidad de la red interna | Indisponibilidad de la red interna por más de una hora | Indisponibilidad de la red por más de dos horas | Indisponibilidad de la red interna por más de 6 oras | Indisponibilidad de la red interna por más de un día |
| Fallas en el suministro energético | Falla por una hora | Falla por más de una hora | Falla por más de 6 horas | Fala por más de un día |
| Errores o bugs en el código fuente | Involucra solo un modulo | | Involucra todos los módulos | Involucra todo el sistema |
| Indisponibilidad de internet | | Indisponibilidad por una hora | Indisponibilidad por más de 6 horas | Indisponibilidad por más de un día |

***Tabla 6-7.*** *Valoración del impacto de las malfunciones*

Se debe construir esta tabla para cada una de las actividades de la organización, al final se tendrá la escala de valores de malfuncionamiento por cada actividad, esta debe ser presentada a la alta dirección para su respectiva aprobación.

## 2. Identificación de Activos para la Clasificación

Se deben determinar los activos que tiene la organización. Un activo es todo aquello que represente valor para la empresa, un activo puede ser el personal, un computador, un documento, un servidor, el software, el hardware, etc.

Se recomienda realizar una clasificación de activos previa, lo autores de este trabajo de grado sugieren utilizar la herramienta disponible por el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia para realizar esta clasificación. Dentro de las características de esta clasificación se debe tener en cuenta la numeración, descripción del activo, la clasificación, el propietario del activo dentro de la organización y finalmente la valoración con respecto a confidencialidad, integridad y disponibilidad como se muestra en la *tabla 6-8*, en donde se detalla una pequeña parte de la identificación de los activos de información.

| Numero de activo | procedimiento | Nombre del activos | descripción | Clasificación | Propietario | valoración | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | C | I | D |
| ACT01 | DMA | Computador 1 | Computador con alguna documentación | No primordial | Ing. oidor | 3 | 3 | 2 |
| ACT01 | DMA | Computador 2 | Computador donde se desarrollan las aplicaciones y se almacena el código fuente | primordial | Ing. oidor | 5 | 5 | 3 |
| ACT02 | DMA | Computador 3 | Computador donde se desarrollan las aplicaciones y se almacena el código fuente | primordial | Carlos C | 5 | 5 | 3 |

***Tabla 6-8.*** *Clasificación de activos de informacion*

Una vez que se han terminado de definir los activos de información, el siguiente paso es la utilización de la herramienta proporcionada por MEHARI para el análisis y la valoración de los riesgos. La metodología MEHARI cuenta con una herramienta

llamada “Base de Reconocimiento de MEHARI” la versión más reciente es la versión MEHARI 2010 con soporte para ISO 27002:2013.

La valoración, análisis y gestión de los riegos se materializa en esta herramienta, por lo que es importante saber cómo proceder. La información recolectada hasta el momento servirá para completar la información dentro de esta Base de Reconocimiento. La estructura de la Base de Reconocimiento es mostrada en la *ilustración 6-9.*

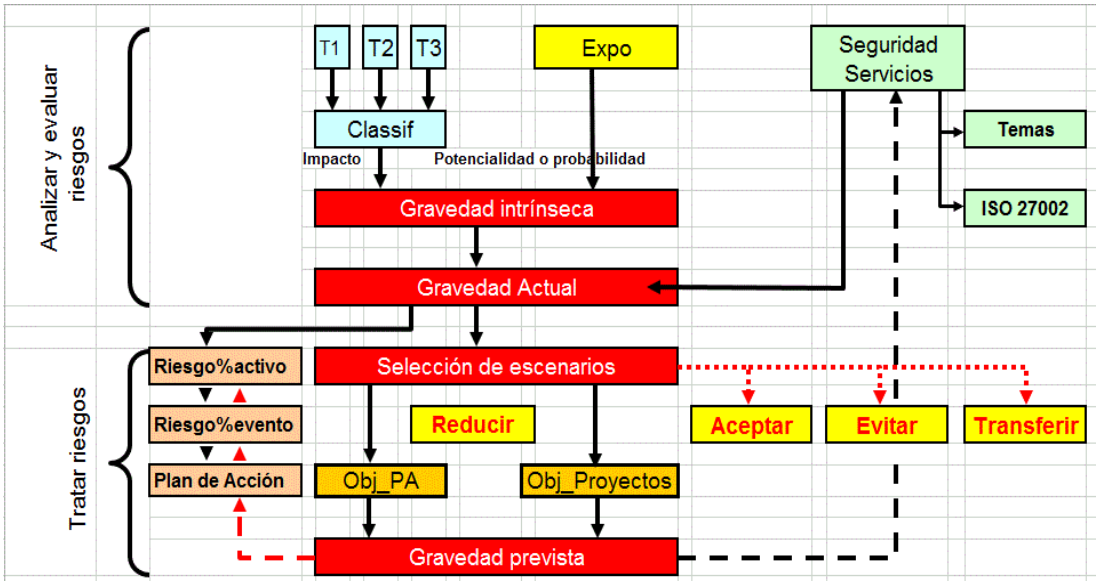



***Ilustración 6-9.*** *Estructura de la base de datos de reconocimiento de MEHARI*

La estructura de la base de reconocimiento de MEHARI está dividida en dos partes, en la parte superior se encuentra el análisis y evaluación de los riesgos, en la parte inferior el tratamiento de los riesgos. Es importante tener en cuenta la estructura de herramienta ya que se detallara cada módulo en lo que sigue de ese capítulo.

Dentro de la herramienta, las tres primeras tablas de Excel como se muestra en la *ilustración 6-10* representan lo siguiente:

- **Intro**: Es la interfaz inicial la cual muestra el contenido de toda la base de reconocimiento, en donde se pueden además enmascarar u ocultar algunas hojas de cálculo con el fin de facilitar la utilización.

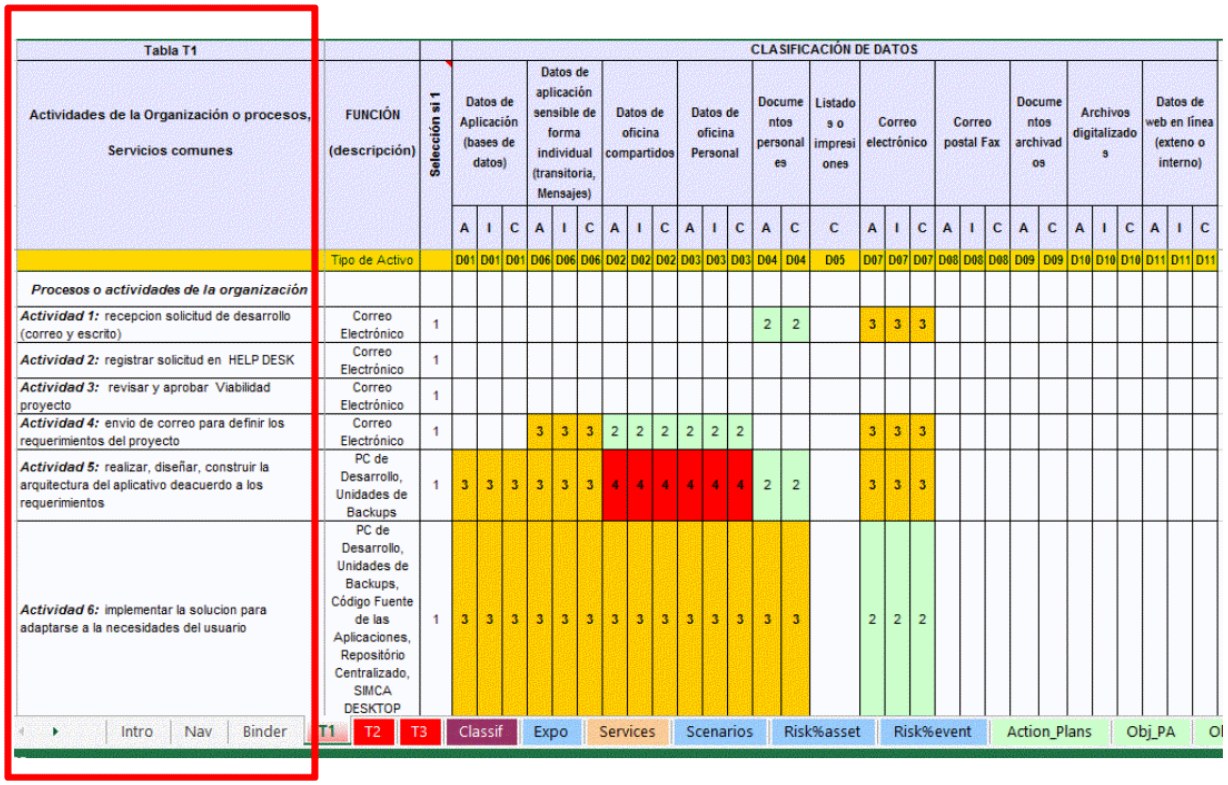
- **Nav**: Muestra de manera conceptual la estructura de la base de reconocimiento.

- **Binder**: Sirve para crear una etiqueta y personalizar la herramienta para la organización.


***Ilustración 6-10.*** *Navegación por la base de reconocimiento de MEHARI*

Continuando con el desarrollo de la metodología, dentro de la Base de Reconocimiento se tienen tres tablas siguientes a la tabla “Binder”, estas son “Tabla de Clasificación de Datos – T1”, “Tabla de Clasificación de Servicios – T2” y “Tabla de Clasificación de Cumplimiento – T3”. Todos los activos, sus funciones y sus respectivas valoraciones de mal funcionamiento deben introducirse en estas tablas. A continuación se explica cómo se realiza este proceso.

En esta tabla se deben ubicar las actividades que se identificaron anteriormente en "Stake análisis y clasificación de activos" como lo muestra la *ilustración 6-11* en donde se remarca el área en donde van las actividades de la organización previamente identificadas.

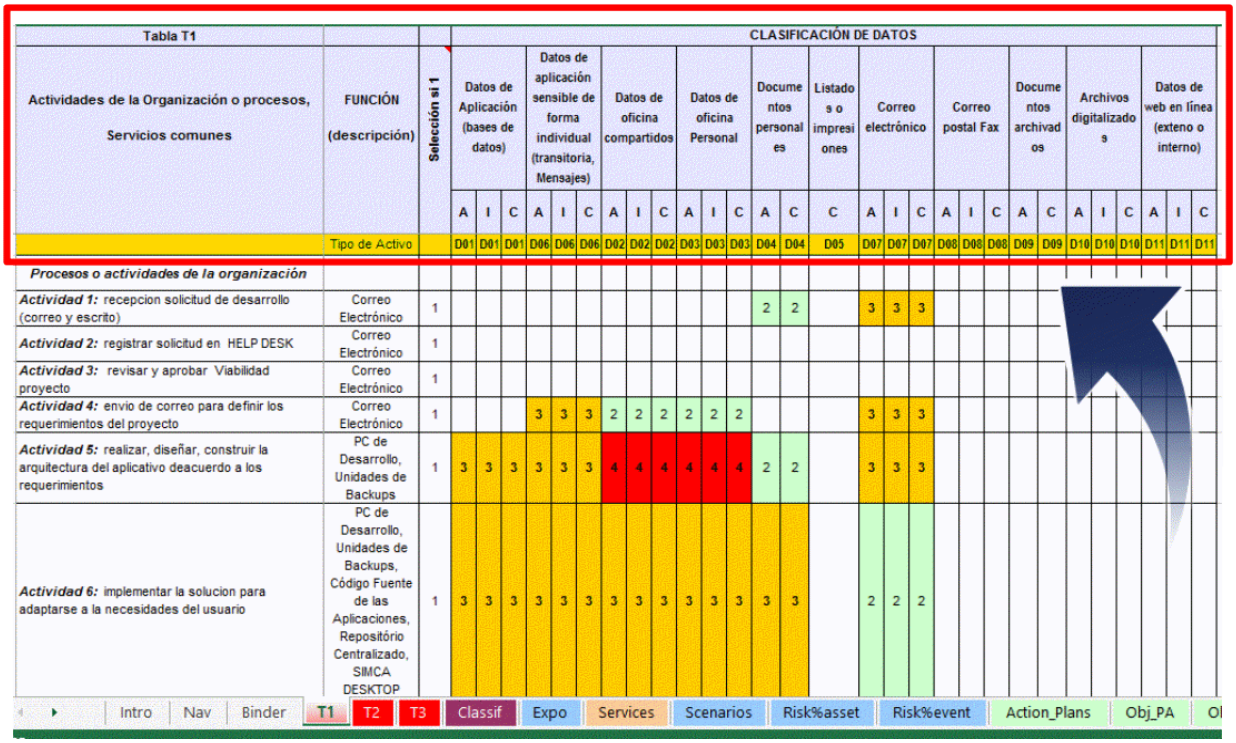


| Tabla T1 | | | CLASIFICACIÓN DE DATOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Actividades de la Organización o procesos, Servicios comunes | FUNCIÓN (descripción) | Selección si 1 | Datos de Aplicación (bases de datos) | | | Datos de aplicación sensible de forma individual (transitoria, Mensajes) | | | Datos de oficina compartidos | | | Datos de oficina Personal | | | Documentos personales | | Listados o impresiones | Correo electrónico | | | Correo postal Fax | | | Documentos archivados | | Archivos digitalizados | | | Datos de web en línea (exteno o interno) | | |
| | | | A | I | C | A | I | C | A | I | C | A | I | C | A | C | C | A | I | C | A | I | C | A | C | A | I | C | A | I | C |
| | Tipo de Activo | | D01 | D01 | D01 | D06 | D06 | D06 | D02 | D02 | D02 | D03 | D03 | D03 | D04 | D04 | D05 | D07 | D07 | D07 | D08 | D08 | D08 | D09 | D09 | D10 | D10 | D10 | D11 | D11 | D11 |
| ***Procesos o actividades de la organización*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 1:*** recepcion solicitud de desarrollo (correo y escrito) | Correo Electrónico | 1 | | | | | | | | | | | | | 2 | 2 | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 2:*** registrar solicitud en HELP DESK | Correo Electrónico | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 3:*** revisar y aprobar Viabilidad proyecto | Correo Electrónico | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 4:*** envio de correo para definir los requerimientos del proyecto | Correo Electrónico | 1 | | | | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | | | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 5:*** realizar, diseñar, construir la arquitectura del aplicativo deacuerdo a los requerimientos | PC de Desarrollo, Unidades de Backups | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 6:*** implementar la solucion para adaptarse a la necesidades del usuario | PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositório Centralizado, SIMCA DESKTOP | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | | 2 | 2 | 2 | | | | | | | | | | | | |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | Services | Scenarios | Risk%asset | Risk%event | Action_Plans | Obj_PA

***Ilustración 6-11.*** *Ubicación de las actividades o procesos de la organización*

En la parte superior de la tabla, la metodología agrupa los activos de información de acuerdo a la categoría. "Tabla de Clasificación de Datos – T1", "Tabla de Clasificación de Servicios – T2" y "Tabla de Clasificación de Cumplimiento – T3". En la *ilustración 6-12* se muestra los activos agrupados en la categoría de clasificación de datos T1.



| Tabla T1 | | | CLASIFICACIÓN DE DATOS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Actividades de la Organización o procesos, Servicios comunes | FUNCIÓN (descripción) | Selección si 1 | Datos de Aplicación (bases de datos) | | | Datos de aplicación sensible de forma individual (transitoria, Mensajes) | | | Datos de oficina compartidos | | | Datos de oficina Personal | | | Documentos personales | | Listados o impresiones | Correo electrónico | | | Correo postal Fax | | | Documentos archivados | | Archivos digitalizados | | | Datos de web en línea (exteno o interno) | | |
| | | | A | I | C | A | I | C | A | I | C | A | I | C | A | C | C | A | I | C | A | I | C | A | C | A | I | C | A | I | C |
| | Tipo de Activo | | D01 | D01 | D01 | D06 | D06 | D06 | D02 | D02 | D02 | D03 | D03 | D03 | D04 | D04 | D05 | D07 | D07 | D07 | D08 | D08 | D08 | D09 | D09 | D10 | D10 | D10 | D11 | D11 | D11 |
| ***Procesos o actividades de la organización*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 1:*** recepcion solicitud de desarrollo (correo y escrito) | Correo Electrónico | 1 | | | | | | | | | | | | | 2 | 2 | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 2:*** registrar solicitud en HELP DESK | Correo Electrónico | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 3:*** revisar y aprobar Viabilidad proyecto | Correo Electrónico | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Actividad 4:*** envio de correo para definir los requerimientos del proyecto | Correo Electrónico | 1 | | | | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | | | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 5:*** realizar, diseñar, construir la arquitectura del aplicativo deacuerdo a los requerimientos | PC de Desarrollo, Unidades de Backups | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 2 | | 3 | 3 | 3 | | | | | | | | | | | | |
| ***Actividad 6:*** implementar la solucion para adaptarse a la necesidades del usuario | PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositório Centralizado, SIMCA DESKTOP | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | | 2 | 2 | 2 | | | | | | | | | | | | |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | Services | Scenarios | Risk%asset | Risk%event | Action_Plans | Obj_PA

***Ilustración 6-12.*** *Agrupación de activos en la categoría de datos según MEHARI*

Finalmente y con la ayuda de la identificación de las principales actividades y la identificación de las malfunciones realizada anteriormente se valora cada actividad con su activo de información relacionado teniendo en cuenta la confidencialidad, disponibilidad e integridad, como se resalta en la *ilustración 6-13*, es importante mencionar que algunos activos no aplican para algunas actividades en tal caso simplemente se omite la valoración dejándola en blanco.

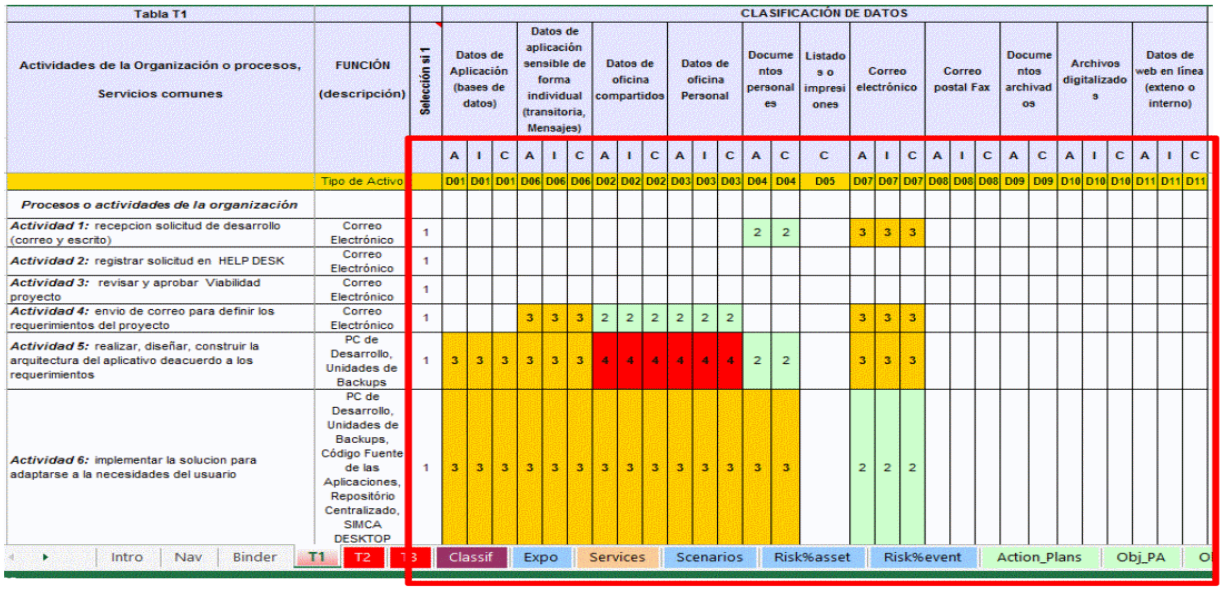



***Ilustración 6-13.*** *Valoración de los activos de información utilizados por las actividades*

a. Tabla de Clasificación de Datos – T1

La clasificación de activos en la categoría de datos se puede detallar en la *ilustración 6-14*

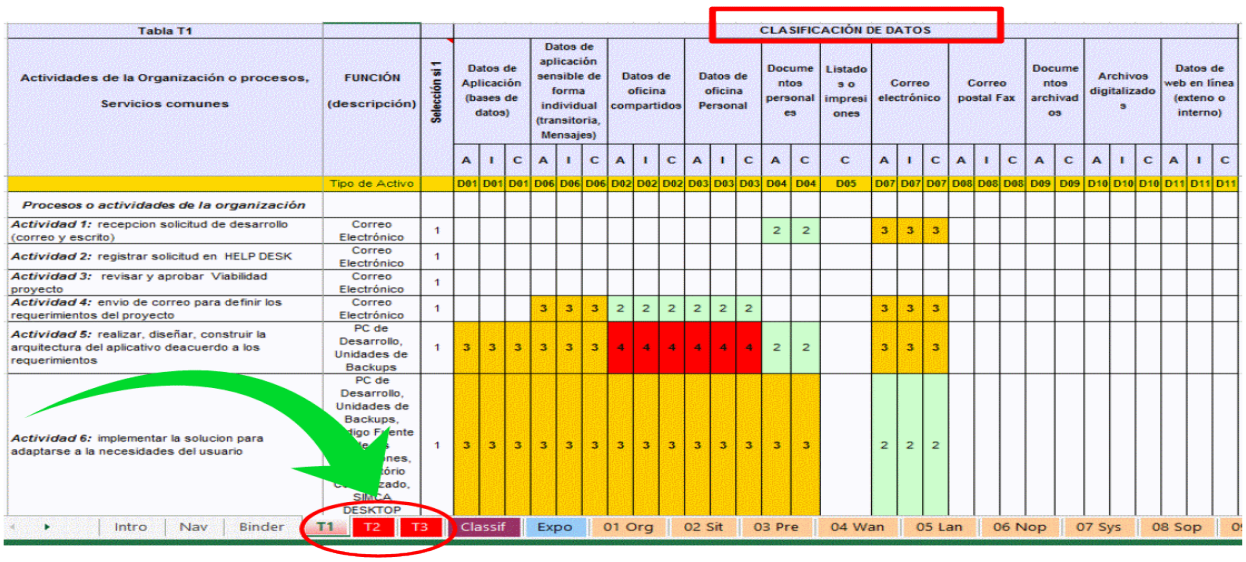
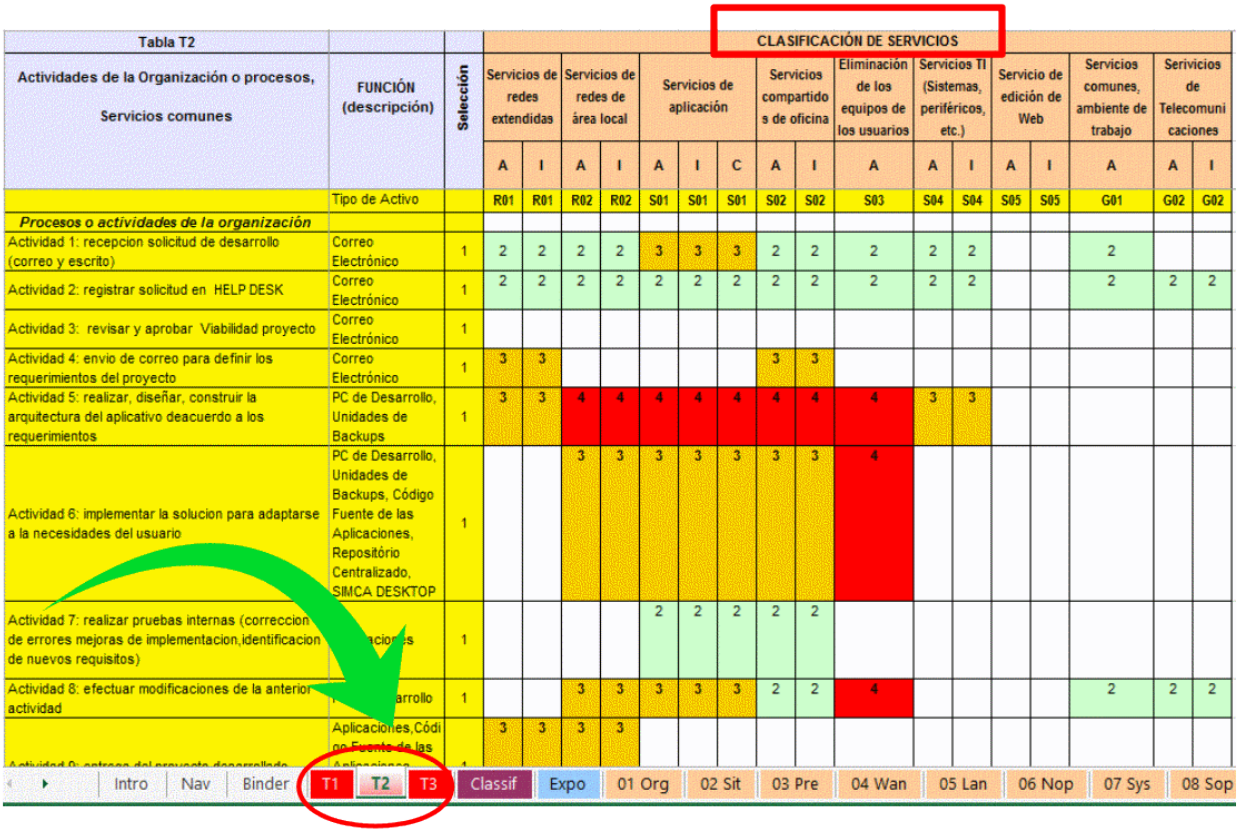



***Ilustración 6-14.*** *Tabla de clasificación T1 en la categoría de datos*

b. Tabla de Clasificación de Servicio – T2

La clasificación de activos en la categoría de servicios se puede detallar en la *ilustración 6-15*



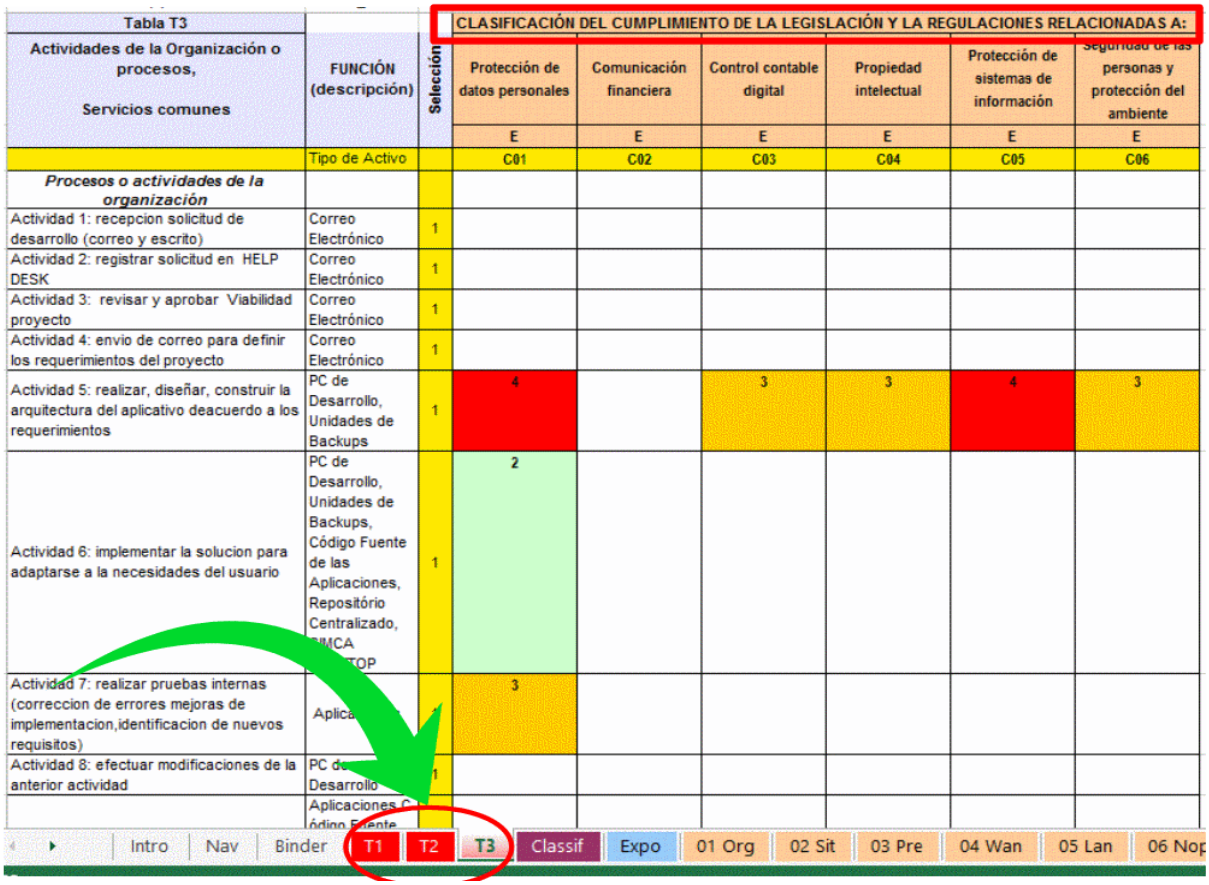
| Tabla T2 | | | CLASIFICACIÓN DE SERVICIOS | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Actividades de la Organización o procesos, Servicios comunes | FUNCIÓN (descripción) | Selección | Servicios de redes extendidas | | Servicios de redes de área local | | Servicios de aplicación | | | Servicios compartidos de oficina | | Eliminación de los equipos de los usuarios | Servicios TI (Sistemas, periféricos, etc.) | | Servicio de edición de Web | | Servicios comunes, ambiente de trabajo | Serivicios de Telecomunicaciones | |
| | | | A | I | A | I | A | I | C | A | I | A | A | I | A | I | A | A | I |
| | Tipo de Activo | | R01 | R01 | R02 | R02 | S01 | S01 | S01 | S02 | S02 | S03 | S04 | S04 | S05 | S05 | G01 | G02 | G02 |
| *Procesos o actividades de la organización* | | | | | | | | | | | | | | | | | | | |
| Actividad 1: recepcion solicitud de desarrollo (correo y escrito) | Correo Electrónico | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | | | 2 | | |
| Actividad 2: registrar solicitud en HELP DESK | Correo Electrónico | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | | 2 | 2 | 2 |
| Actividad 3: revisar y aprobar Viabilidad proyecto | Correo Electrónico | 1 | | | | | | | | | | | | | | | | | |
| Actividad 4: envio de correo para definir los requerimientos del proyecto | Correo Electrónico | 1 | 3 | 3 | | | | | | 3 | 3 | | | | | | | | |
| Actividad 5: realizar, diseñar, construir la arquitectura del aplicativo deacuerdo a los requerimientos | PC de Desarrollo, Unidades de Backups | 1 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | | | | | |
| Actividad 6: implementar la solucion para adaptarse a la necesidades del usuario | PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositório Centralizado, SIMCA DESKTOP | 1 | | | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | | | | | | | |
| Actividad 7: realizar pruebas internas (correccion de errores mejoras de implementacion,identificacion de nuevos requisitos) | | 1 | | | | | 2 | 2 | 2 | 2 | 2 | | | | | | | | |
| Actividad 8: efectuar modificaciones de la anterior actividad | | 1 | | | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 4 | | | | | 2 | 2 | 2 |
| | Aplicaciones,Código Fuente de las | | 3 | 3 | 3 | 3 | | | | | | | | | | | | | |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | 01 Org | 02 Sit | 03 Pre | 04 Wan | 05 Lan | 06 Nop | 07 Sys | 08 Sop

***Ilustración 6-15.*** *Tabla de clasificación T2 en la categoría de servicios*

c. Tabla de Clasificación de Cumplimiento – T3

La clasificación de activos en la categoría de cumplimiento se puede detallar en la *ilustración 6-16*



| Tabla T3 | | | CLASIFICACIÓN DEL CUMPLIMIENTO DE LA LEGISLACIÓN Y LA REGULACIONES RELACIONADAS A: | | | | | |
|---|---|---|---|---|---|---|---|---|
| Actividades de la Organización o procesos, Servicios comunes | FUNCIÓN (descripción) | Selección | Protección de datos personales | Comunicación financiera | Control contable digital | Propiedad intelectual | Protección de sistemas de información | Seguridad de las personas y protección del ambiente |
| | | | E | E | E | E | E | E |
| | Tipo de Activo | | C01 | C02 | C03 | C04 | C05 | C06 |
| *Procesos o actividades de la organización* | | | | | | | | |
| Actividad 1: recepcion solicitud de desarrollo (correo y escrito) | Correo Electrónico | 1 | | | | | | |
| Actividad 2: registrar solicitud en HELP DESK | Correo Electrónico | 1 | | | | | | |
| Actividad 3: revisar y aprobar Viabilidad proyecto | Correo Electrónico | 1 | | | | | | |
| Actividad 4: envio de correo para definir los requerimientos del proyecto | Correo Electrónico | 1 | | | | | | |
| Actividad 5: realizar, diseñar, construir la arquitectura del aplicativo deacuerdo a los requerimientos | PC de Desarrollo, Unidades de Backups | 1 | 4 | | 3 | 3 | 4 | 3 |
| Actividad 6: implementar la solucion para adaptarse a la necesidades del usuario | PC de Desarrollo, Unidades de Backups, Código Fuente de las Aplicaciones, Repositório Centralizado, [illegible] | 1 | 2 | | | | | |
| Actividad 7: realizar pruebas internas (correccion de errores mejoras de implementacion,identificacion de nuevos requisitos) | Aplica[illegible] | 1 | 3 | | | | | |
| Actividad 8: efectuar modificaciones de la anterior actividad | PC d[illegible] Desarrollo | 1 | | | | | | |
| | Aplicaciones C[illegible] | | | | | | | |

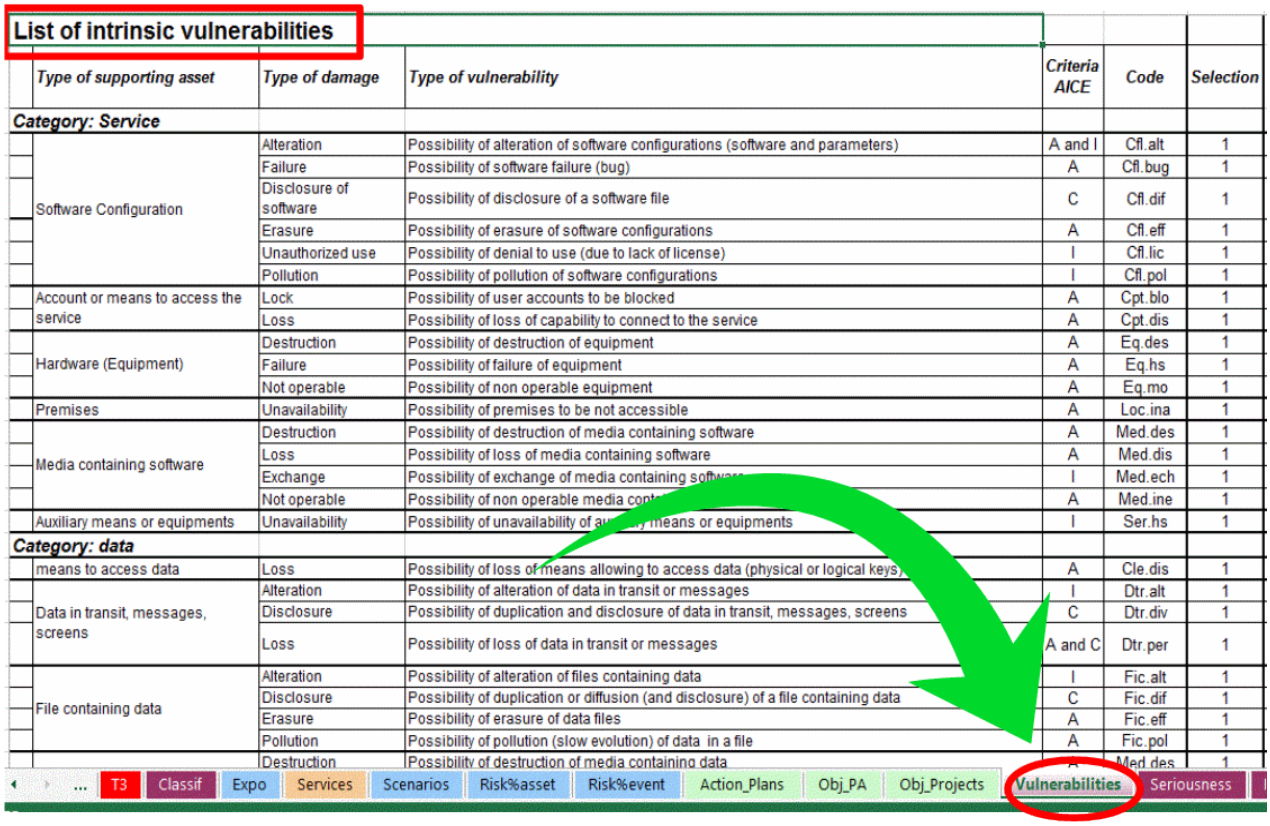
Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | 01 Org | 02 Sit | 03 Pre | 04 Wan | 05 Lan | 06 Nop

***Ilustración 6-16.*** *Tabla de clasificación T3 en la categoría de cumplimiento*

En la parte inferior de cada tabla se encuentran los campos para ser diligenciados por el personal que está realizando la valoraciones de los activos y actividades, los autores sugieren diligenciar estos campos para que el Jefe de Información o Auditor lleve un registro del trabajo que se ha realizado.

Una vez que se han diligenciado las tablas T1, T2 y T3 de la herramienta, se deben seleccionar los activos de soporte o conocidos como activos secundarios, esto se realiza en la hoja “vulnerabilidades” como se muestra en la *ilustración 6-17,* en la

columna selección se deben considerar los activos de soporte, el tipo de daño al activo y el tipo de vulnerabilidad del activo, de acuerdo a los que apliquen para la organización.



**List of intrinsic vulnerabilities**

| | Type of supporting asset | Type of damage | Type of vulnerability | Criteria AICE | Code | Selection |
|---|---|---|---|---|---|---|
| **Category: Service** | | | | | | |
| | Software Configuration | Alteration | Possibility of alteration of software configurations (software and parameters) | A and I | Cfl.alt | 1 |
| | | Failure | Possibility of software failure (bug) | A | Cfl.bug | 1 |
| | | Disclosure of software | Possibility of disclosure of a software file | C | Cfl.dif | 1 |
| | | Erasure | Possibility of erasure of software configurations | A | Cfl.eff | 1 |
| | | Unauthorized use | Possibility of denial to use (due to lack of license) | I | Cfl.lic | 1 |
| | | Pollution | Possibility of pollution of software configurations | I | Cfl.pol | 1 |
| | Account or means to access the service | Lock | Possibility of user accounts to be blocked | A | Cpt.blo | 1 |
| | | Loss | Possibility of loss of capability to connect to the service | A | Cpt.dis | 1 |
| | Hardware (Equipment) | Destruction | Possibility of destruction of equipment | A | Eq.des | 1 |
| | | Failure | Possibility of failure of equipment | A | Eq.hs | 1 |
| | | Not operable | Possibility of non operable equipment | A | Eq.mo | 1 |
| | Premises | Unavailability | Possibility of premises to be not accessible | A | Loc.ina | 1 |
| | Media containing software | Destruction | Possibility of destruction of media containing software | A | Med.des | 1 |
| | | Loss | Possibility of loss of media containing software | A | Med.dis | 1 |
| | | Exchange | Possibility of exchange of media containing software | I | Med.ech | 1 |
| | | Not operable | Possibility of non operable media cont | A | Med.ine | 1 |
| | Auxiliary means or equipments | Unavailability | Possibility of unavailability of au means or equipments | I | Ser.hs | 1 |
| **Category: data** | | | | | | |
| | means to access data | Loss | Possibility of loss of means allowing to access data (physical or logical keys) | A | Cle.dis | 1 |
| | Data in transit, messages, screens | Alteration | Possibility of alteration of data in transit or messages | I | Dtr.alt | 1 |
| | | Disclosure | Possibility of duplication and disclosure of data in transit, messages, screens | C | Dtr.div | 1 |
| | | Loss | Possibility of loss of data in transit or messages | A and C | Dtr.per | 1 |
| | File containing data | Alteration | Possibility of alteration of files containing data | I | Fic.alt | 1 |
| | | Disclosure | Possibility of duplication or diffusion (and disclosure) of a file containing data | C | Fic.dif | 1 |
| | | Erasure | Possibility of erasure of data files | A | Fic.eff | 1 |
| | | Pollution | Possibility of pollution (slow evolution) of data in a file | A | Fic.pol | 1 |
| | | Destruction | Possibility of destruction of media containing data | | Med.des | 1 |

... T3 Classif Expo Services Scenarios Risk%asset Risk%event Action_Plans Obj_PA Obj_Projects Vulnerabilities Seriousness

***Ilustración 6-17.*** *Selección de los activos de soportes*

Una vez se ha terminado de configurar las tablas anteriores, la herramienta MEHARI arroja una tabla llamada “Tabla de Impacto intrínseco” la cual muestra el resultado de la valoración del mal funcionamiento (impacto) de las tablas T1, T2 y T3 y los activos secundarios o de soporte. Esta tabla se muestra en la *ilustración 6-18.*

| Tabla de Impacto Intrínseco | | | | | Selección de Activos |
|---|---|---|---|---|---|
| **Activos de datos y de información** | | **A** | **I** | **C** | |
| ***Datos e información*** | | | | | |
| D01 | Archivos de datos y bases de datos que se acceden por aplicaciones | 4 | 4 | 4 | 1 |
| D02 | Archivos y datos compartidos en la oficina | 4 | 4 | 4 | 1 |
| D03 | Archivos de oficina personales (en estaciones de trabajo de usuarios y equipos) | 4 | 4 | 4 | 1 |
| D04 | Información escrita o impresa y datos almacenado por usuarios y los archivos personales | 4 | | 3 | 1 |
| D05 | Documentos impresos o listados | | | | 0 |
| D06 | Intercambio de mensajes, vistas de pantalla, datos individuales sensibles | 4 | 4 | 4 | 1 |
| D07 | Correo Electrónico | 3 | 3 | 3 | 1 |
| D08 | (Postal) Correos postales y faxes | 2 | 2 | 2 | 1 |
| D09 | Archivos patrimoniales y documentos utilizados como pruebas | 2 | | 1 | 1 |
| D10 | Archivos relacionados con TI | | | | 0 |
| D11 | Datos e información publicada en sitios públicos o internos | | | | 0 |
| | | | | | |
| **Activos de servicio** | | **A** | **I** | **C** | |
| ***Servicios generales*** | | | | | |
| G01 | Espacio de trabajo del usuario y el ambiente | 3 | | | 1 |
| G02 | Servicios de telecomunicaciones (voz, fax, audio y video conferencias, etc.) | 3 | 3 | | 1 |
| ***Servicios de redes y TI*** | | | | | |
| R01 | Servicios de redes extendidas | 3 | 3 | | 1 |
| R02 | Servicios d | 4 | 4 | | 1 |
| S01 | Ser s prestados por las aplica | 4 | 4 | 4 | 1 |
| S02 | Servicios compartidos de oficina (servi tión de documentos, impresoras compartidas, etc.) | 4 | 4 | | 1 |
| S03 | Disposición de equipos de usuarios (estacion bajo, impresoras locales, periféricos, interfaces específicas, etc.) | 4 | 3 | | 1 |
| S04 | Servicios comunes, ambiente de trabajo: mensaj impresiones, edición, etc. | 3 | 3 | | 1 |
| S05 | Servicio de edición de Web (interna o pública) | | | | 0 |
| | | | | | |
| **Proceso de gestión de tipo de activos** | | **E** | | | |
| ***Proccesos de gestión para el cumplimiento de las leyes o re amentaciones*** | | | | | |
| C01 | Cumplimiento a la leyes o regulaciones relacionadas a la protección de datos personales | 4 | | | 1 |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | 01 Org | 02 Sit | 03 Pre | 04 Wan

***Ilustración 6-18.****Impacto Intrínseco de los activos de información*

Posterior a esto, se debe diligenciar la tabla llamada “Tabla de eventos y exposición natural” en la hoja de cálculo “*expo* “como se muestra en la *ilustración 6-19* esta tabla describe las amenazas para los escenarios y la “potencialidad intrínseca” de la ocurrencia de esas amenazas para la organización.

En la primera columna de la tabla se describe el tipo de amenaza o la familia, en la segunda columna se asigna el identificador de esa amenaza, en la tercera columna se describe la amenaza en cuestión, en la cuarta columna se encuentra el código de la amenaza, en la quinta columna se le asigna un valora a la amenaza dependiendo de su gravedad para la organización (esta puntuación es la sugerida por la metodología MEHARI), en la sexta columna se evalúa la exposición natural según el criterio del auditor y de acuerdo a las necesidades de la organización,

finalmente en la séptima columna se tiene el resultado de la evaluación de cada una de las amenazas consideradas.

**Tabla of eventos : Tipos de eventos y exposición natural**

Fecha de la decisión del ajuste de la exposición natural: 18/03/2016

| *Tipo de Familia* | *Tipo de código* | *Descripción del Evento* | *Código* | *Exposición natural (estándar CLUSIF)* | *Exposición natural (decidido)* | *Exposición natural (resultante)* |
|---|---|---|---|---|---|---|
| Ausencia de personal debido a un accidente | AB.P | Ausencia del personal socio | AB.P.Pep | 3 | 2 | 2 |
| | | Ausencia del personal interno | AB.P.Per | 2 | 4 | 4 |
| Ausencia o indisponibilidad de servicio, debido a un accidente | AB.S | Ausencia de servicio : Aire acondicionado | AB.S.Cli | 2 | | 2 |
| | | Ausencia de servicio : Fuente de alimentación | AB.S.Ene | 3 | 4 | 4 |
| | | Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos | AB.S.Loc | 2 | 4 | 4 |
| | | Ausencia o imposibilidad de mantenimiento de software de aplicación | AB.S.Maa | 3 | 4 | 4 |
| | | Ausencia o imposibilidad de mantenimiento del sistema de información | AB.S.Mas | 2 | 2 | 2 |
| Accidente grave del ambiente | AC.E | Tormenta Eléctrica | AC.E.Fou | 2 | | 2 |
| | | Fuego | AC.E.Inc | 2 | 4 | 4 |
| | | Inundación | AC.E.Ino | 3 | | 3 |
| Accidente de Hardware | AC.M | Averías del equipo | AC.M.Equ | 3 | 3 | 3 |
| | | Averías de los accesorios del equipo | AC.M.Ser | 3 | 3 | 3 |
| Ausencia voluntaria del personal | | ...ido social con huelga | AV.P.Gre | 2 | 3 | 3 |
| Error conceptual | ER.L | ...queo o mal funcionamiento debido a un diseño o error de program... ...ware interno) | ER.L.Lin | 3 | 4 | 4 |
| Error de Hardware o error de comportamiento por el personal | ER.P | Perdida u olv... ...umento o media | ER.P.Peo | 3 | 2 | 2 |
| | | Error de operacio... ...no cumplimiento de un procedicmiento | ER.P.Pro | 3 | 3 | 3 |
| | | Error de ingreso dat... ...scrut...a | ER.P.Prs | 3 | 4 | 4 |
| Incidente debido al ambiente | IC.E | Daños debidos al env... ...e los equipos) | IC.E.Age | 2 | 3 | 3 |
| | | Daños por agua | IC.E.De | 3 | | 3 |
| | | Daños por contamina... | IC.E.Pol | 2 | | 2 |
| | | Sobre carga eléctrica | IC.E.Se | 2 | 2 | 2 |
| | | Incidente en producción | IE.L.Exp | 3 | 4 | 4 |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | 01 Org | 02 Sit | 03 Pre | 04 Wan | 05 Lan | 06 Nop | 07 Sys | 08 Sop

***Ilustración 6-19.*** *Tabla de Eventos y exposición natural de la Base de Reconocimiento de MEHARI*

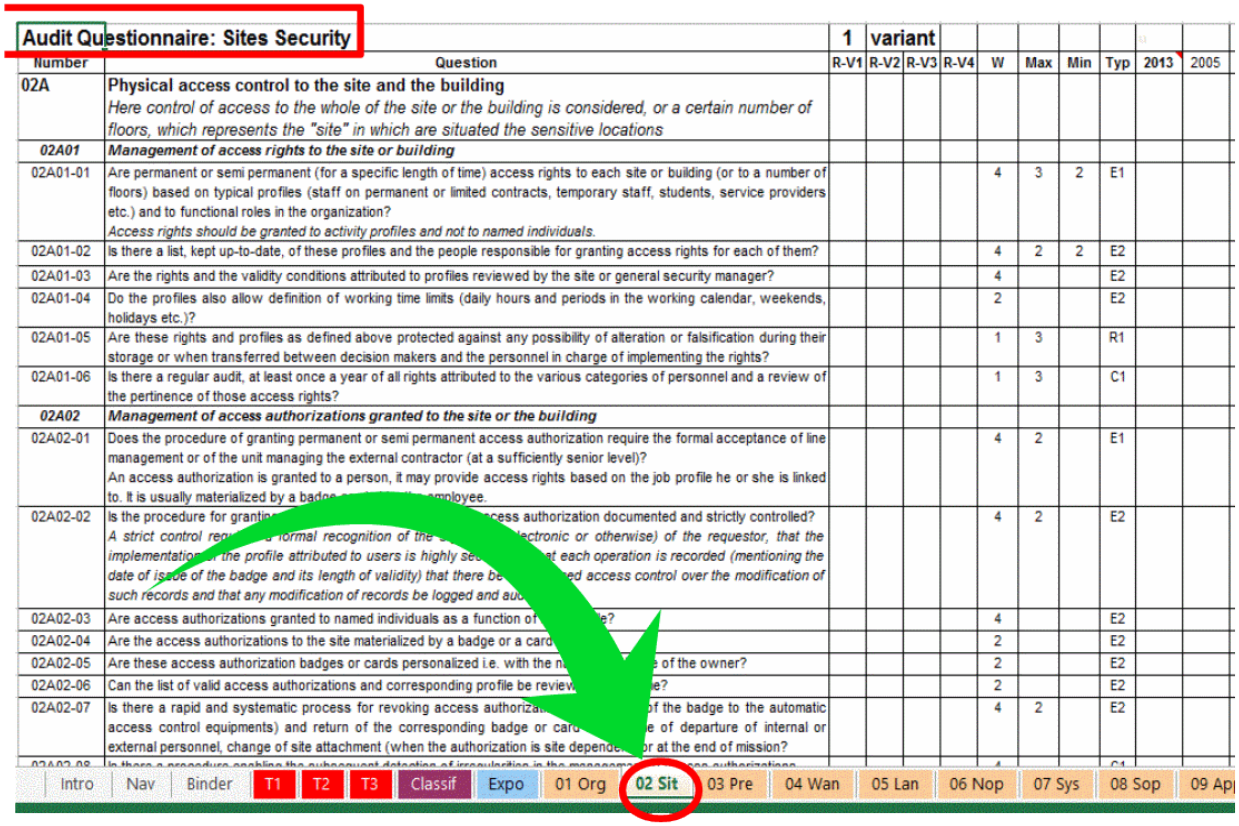
## 2. Diagnósticos de Servicios de Seguridad


***Ilustración 6-20.*** *Fase operacional "Diagnostico de servicios de seguridad" de la Metodología MEHARI*

En la sub fase anterior se definieron los activos con sus mal funcionamientos y el impacto de esos activos a través de la tabla de impacto intrínseco, también se definió la probabilidad o potencialidad a través de la tabla de eventos. MEHARI permite al Jefe de Seguridad realizar una revisión de cómo está la organización en términos de Seguridad de la Información antes de realizar la valoración del riesgo.

Este diagnóstico sirve para evidenciar que controles de la norma ISO/IEC 27002:2013 están implementados, documentados y en funcionamiento. A través de preguntas de auditoria la metodología MEHARI evalúa la presencia de controles de la norma ISO/IEC 27002:2013. Estas preguntas, dentro de la Base de Reconocimiento debe responderse con: 1, 0 o X que representan, si, no o irrelevante respectivamente. La metodología cuenta con más de 1000 preguntas de auditoria, estas preguntas deben ser respondidas por el Jefe de Seguridad o Auditor en compañía del personal de la organización.

La *ilustración 6-21* muestra las preguntas de auditora según la Base de Reconocimiento de MEHARI.



| Audit Questionnaire: Sites Security | | 1 | variant | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Number | Question | R-V1 | R-V2 | R-V3 | R-V4 | W | Max | Min | Typ | 2013 | 2005 |
| 02A | **Physical access control to the site and the building**<br>*Here control of access to the whole of the site or the building is considered, or a certain number of floors, which represents the "site" in which are situated the sensitive locations* | | | | | | | | | | |
| ***02A01*** | ***Management of access rights to the site or building*** | | | | | | | | | | |
| 02A01-01 | Are permanent or semi permanent (for a specific length of time) access rights to each site or building (or to a number of floors) based on typical profiles (staff on permanent or limited contracts, temporary staff, students, service providers etc.) and to functional roles in the organization?<br>*Access rights should be granted to activity profiles and not to named individuals.* | | | | | 4 | 3 | 2 | E1 | | |
| 02A01-02 | Is there a list, kept up-to-date, of these profiles and the people responsible for granting access rights for each of them? | | | | | 4 | 2 | 2 | E2 | | |
| 02A01-03 | Are the rights and the validity conditions attributed to profiles reviewed by the site or general security manager? | | | | | 4 | | | E2 | | |
| 02A01-04 | Do the profiles also allow definition of working time limits (daily hours and periods in the working calendar, weekends, holidays etc.)? | | | | | 2 | | | E2 | | |
| 02A01-05 | Are these rights and profiles as defined above protected against any possibility of alteration or falsification during their storage or when transferred between decision makers and the personnel in charge of implementing the rights? | | | | | 1 | 3 | | R1 | | |
| 02A01-06 | Is there a regular audit, at least once a year of all rights attributed to the various categories of personnel and a review of the pertinence of those access rights? | | | | | 1 | 3 | | C1 | | |
| ***02A02*** | ***Management of access authorizations granted to the site or the building*** | | | | | | | | | | |
| 02A02-01 | Does the procedure of granting permanent or semi permanent access authorization require the formal acceptance of line management or of the unit managing the external contractor (at a sufficiently senior level)?<br>An access authorization is granted to a person, it may provide access rights based on the job profile he or she is linked to. It is usually materialized by a badge [illegible] employee. | | | | | 4 | 2 | | E1 | | |
| 02A02-02 | Is the procedure for granti[illegible]cess authorization documented and strictly controlled?<br>*A strict control req[illegible] formal recognition of the [illegible]lectronic or otherwise) of the requestor, that the implementation[illegible] the profile attributed to users is highly se[illegible]t each operation is recorded (mentioning the date of issue of the badge and its length of validity) that there be[illegible]ed access control over the modification of such records and that any modification of records be logged and aud[illegible]* | | | | | 4 | 2 | | E2 | | |
| 02A02-03 | Are access authorizations granted to named individuals as a function of [illegible]e? | | | | | 4 | | | E2 | | |
| 02A02-04 | Are the access authorizations to the site materialized by a badge or a card[illegible] | | | | | 2 | | | E2 | | |
| 02A02-05 | Are these access authorization badges or cards personalized i.e. with the n[illegible]e of the owner? | | | | | 2 | | | E2 | | |
| 02A02-06 | Can the list of valid access authorizations and corresponding profile be review[illegible]e? | | | | | 2 | | | E2 | | |
| 02A02-07 | Is there a rapid and systematic process for revoking access authoriza[illegible]f the badge to the automatic access control equipments) and return of the corresponding badge or card[illegible]e of departure of internal or external personnel, change of site attachment (when the authorization is site dependen[illegible]r at the end of mission? | | | | | 4 | 2 | | E2 | | |
| 02A02-08 | Is there a procedure enabling the subsequent detection of irregularities in the manageme[illegible] authorizations | | | | | 4 | | | C1 | | |

Intro | Nav | Binder | T1 | T2 | T3 | Classif | Expo | 01 Org | 02 Sit | 03 Pre | 04 Wan | 05 Lan | 06 Nop | 07 Sys | 08 Sop | 09 Ap

***Ilustración 6-21.*** *Preguntas de auditoria de la Base de Reconocimiento de MEHARI*

La tabla anterior es un ejemplo del tipo de pregunta. En la columna después de la pregunta hay valores R-V1, R-V2, R-V3 y R-V4. Estas cuatro columnas representan cuatro variables, esto quiere decir que la metodología puede realizar hasta cuatro diagnósticos de seguridad al tiempo, el resto de columnas hacia la derecha son columnas que MEHARI configura por defecto para realizar los cálculos. Las últimas tres columnas son “2013”, “2005” y “comentarios”. La columna “2013” se refiere al control de la norma ISO/IEC 27002:2013 que representa esa pregunta, es decir, ese servicio de seguridad representa un control, la columna “2005’ indica lo mismo pero en la versión anterior de la norma ISO/IEC 27002. Por último la columna “comentarios”, es un campo abierto para escribir algún comentario por parte del auditor.

En lo posible se sugiere que se respondan todas las preguntas. En caso de que la organización no cuente con ningún SGSI y que el tema de Seguridad de la

Información sea desconocido para la organización, se podría omitir estas preguntas de auditoria, dado que no hay controles para evaluar. En la herramienta estas preguntas están en las tablas, “01 Org”, “02 Sit”, “03 Pre”, “04 Wan”, “05 Lan”, “06 Nop”, “07 Sys”, “08 Sop”, “09 App”, “10 Dev”, “11 Mic”, “12 Top”, “13 Man” y “14 ISM”. Como lo muestra la *ilustración 6-22.*

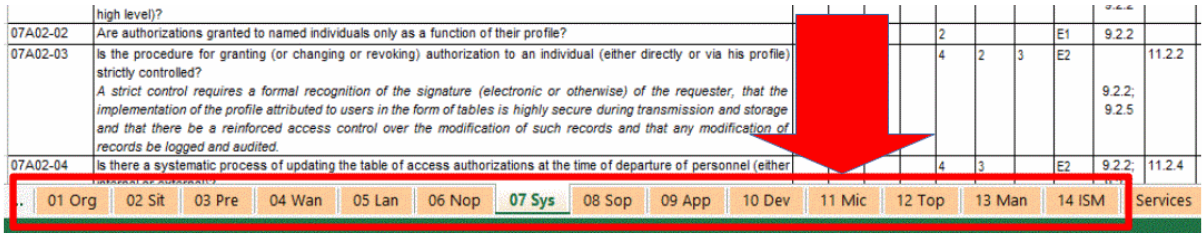



***Ilustración 6-22.*** *Agrupaciones de preguntas de seguridad o auditoria*

El resumen de las preguntas de auditoria se muestra en la hoja de cálculo “Services” y “Themes” como se muestra en la *ilustración 6-23 y 6-24* respectivamente, la metodología arroja el resultado del diagnóstico de los servicios de seguridad en estas dos tablas.

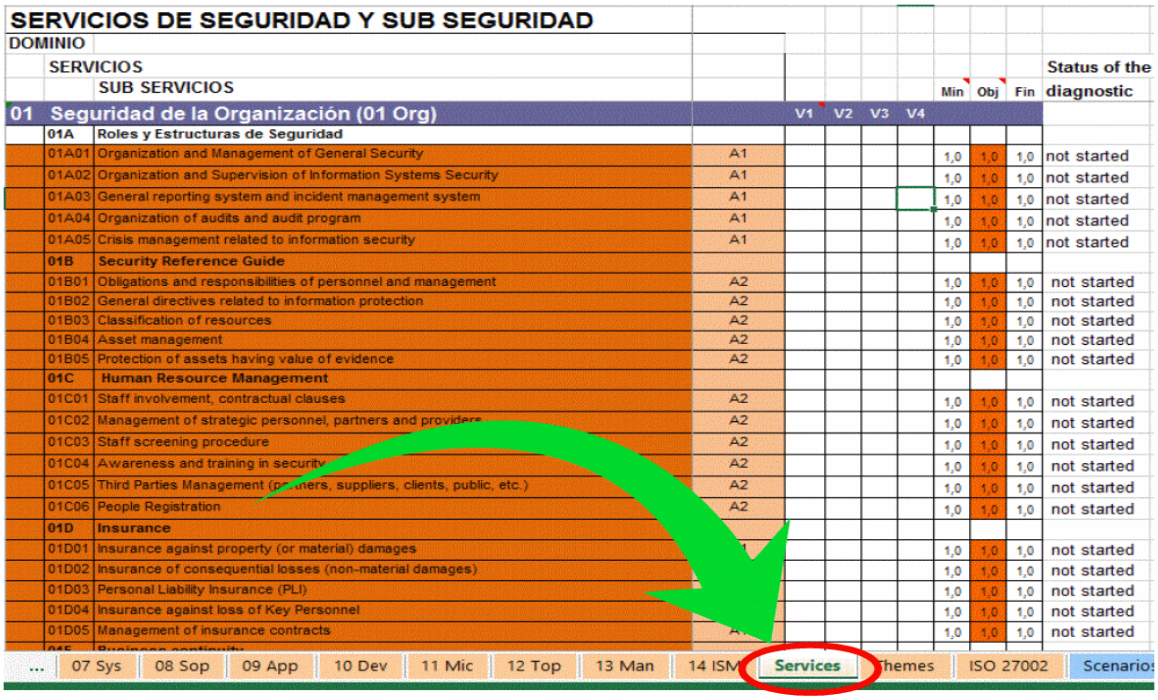
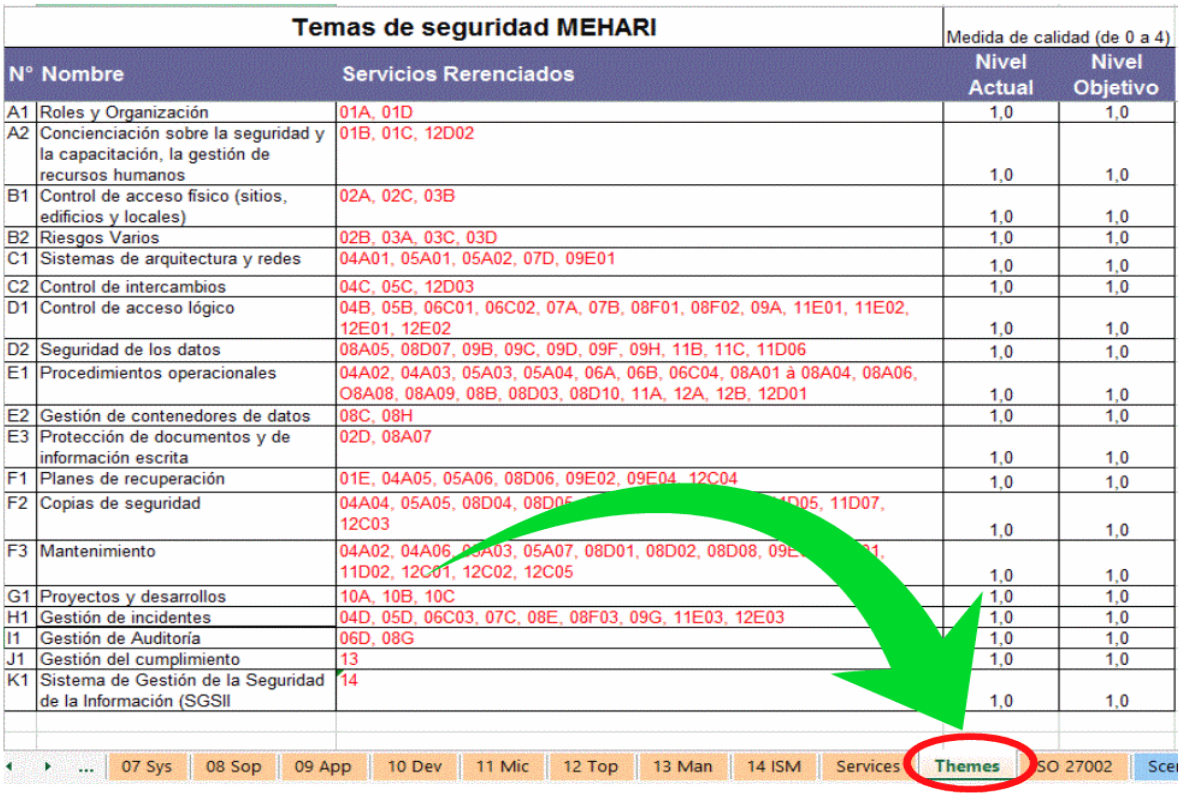



***Ilustración 6-23.*** *Resultado de la valoración de servicios de seguridad*

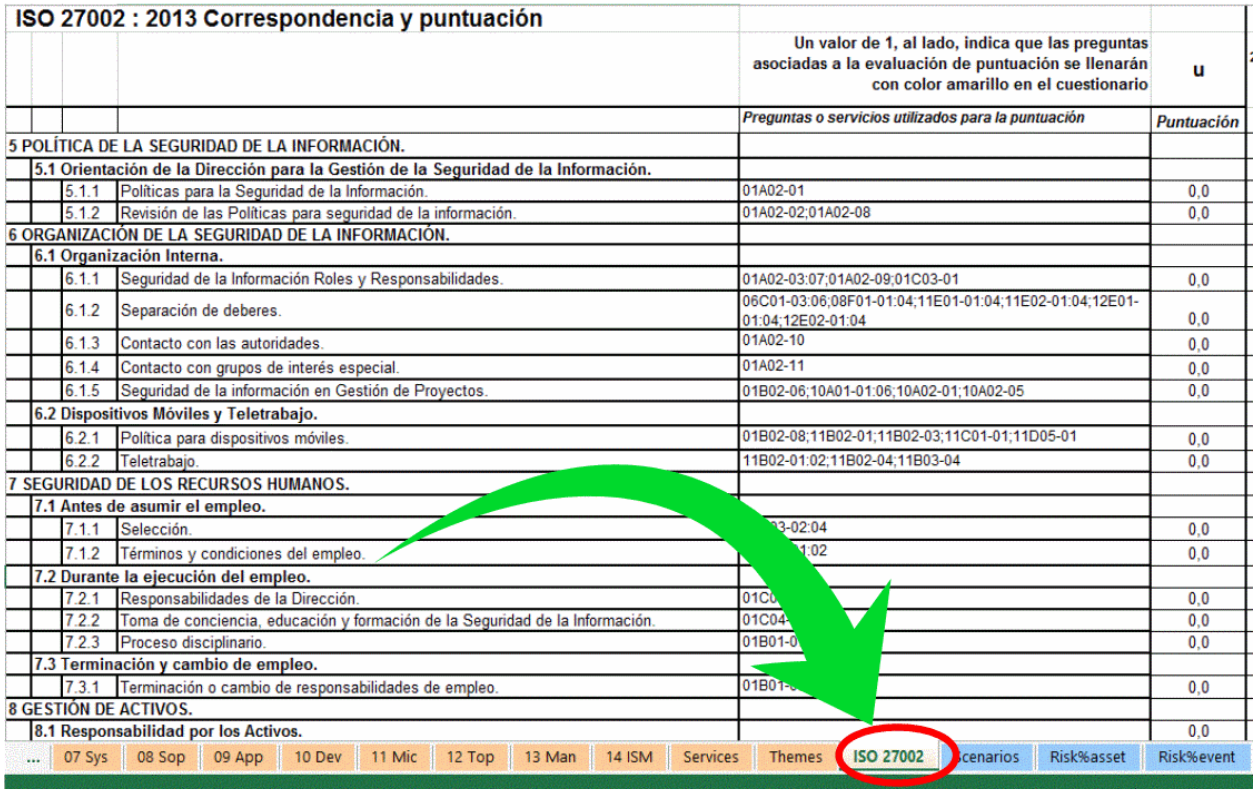


| Temas de seguridad MEHARI | | | Medida de calidad (de 0 a 4) | |
|---|---|---|---|---|
| N° | Nombre | Servicios Rerenciados | Nivel Actual | Nivel Objetivo |
| A1 | Roles y Organización | 01A, 01D | 1,0 | 1,0 |
| A2 | Concienciación sobre la seguridad y la capacitación, la gestión de recursos humanos | 01B, 01C, 12D02 | 1,0 | 1,0 |
| B1 | Control de acceso físico (sitios, edificios y locales) | 02A, 02C, 03B | 1,0 | 1,0 |
| B2 | Riesgos Varios | 02B, 03A, 03C, 03D | 1,0 | 1,0 |
| C1 | Sistemas de arquitectura y redes | 04A01, 05A01, 05A02, 07D, 09E01 | 1,0 | 1,0 |
| C2 | Control de intercambios | 04C, 05C, 12D03 | 1,0 | 1,0 |
| D1 | Control de acceso lógico | 04B, 05B, 06C01, 06C02, 07A, 07B, 08F01, 08F02, 09A, 11E01, 11E02, 12E01, 12E02 | 1,0 | 1,0 |
| D2 | Seguridad de los datos | 08A05, 08D07, 09B, 09C, 09D, 09F, 09H, 11B, 11C, 11D06 | 1,0 | 1,0 |
| E1 | Procedimientos operacionales | 04A02, 04A03, 05A03, 05A04, 06A, 06B, 06C04, 08A01 à 08A04, 08A06, O8A08, 08A09, 08B, 08D03, 08D10, 11A, 12A, 12B, 12D01 | 1,0 | 1,0 |
| E2 | Gestión de contenedores de datos | 08C, 08H | 1,0 | 1,0 |
| E3 | Protección de documentos y de información escrita | 02D, 08A07 | 1,0 | 1,0 |
| F1 | Planes de recuperación | 01E, 04A05, 05A06, 08D06, 09E02, 09E04, 12C04 | 1,0 | 1,0 |
| F2 | Copias de seguridad | 04A04, 05A05, 08D04, 08D05 [illegible] 1D05, 11D07, 12C03 | 1,0 | 1,0 |
| F3 | Mantenimiento | 04A02, 04A06, [illegible]A03, 05A07, 08D01, 08D02, 08D08, 09E[illegible]1, 11D02, 12C01, 12C02, 12C05 | 1,0 | 1,0 |
| G1 | Proyectos y desarrollos | 10A, 10B, 10C | 1,0 | 1,0 |
| H1 | Gestión de incidentes | 04D, 05D, 06C03, 07C, 08E, 08F03, 09G, 11E03, 12E03 | 1,0 | 1,0 |
| I1 | Gestión de Auditoría | 06D, 08G | 1,0 | 1,0 |
| J1 | Gestión del cumplimiento | 13 | 1,0 | 1,0 |
| K1 | Sistema de Gestión de la Seguridad de la Información (SGSII | 14 | 1,0 | 1,0 |



***Ilustración 6-24.*** *Niveles de servicios de seguridad*

Finalmente en la hoja de cálculo "ISO 27002" se detalla el cumplimiento del control de acuerdo a la ISO/IEC 27002:2013, esta tabla es el resultado de las preguntas de auditoria que fueron contestadas afirmativamente y permite ver que tan bien implementado esta un control de seguridad, asignando una puntación de 1 a 10 según el estado del control donde cero significa no implementado a 10 bien implementado y mantenido, la tabla es mostrada en la *ilustración 6-25*



| ISO 27002 : 2013 Correspondencia y puntuación | | | | Un valor de 1, al lado, indica que las preguntas asociadas a la evaluación de puntuación se llenarán con color amarillo en el cuestionario | u |
|---|---|---|---|---|---|
| | | | | *Preguntas o servicios utilizados para la puntuación* | *Puntuación* |
| 5 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN. | | | | | |
| | 5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información. | | | | |
| | | 5.1.1 | Políticas para la Seguridad de la Información. | 01A02-01 | 0,0 |
| | | 5.1.2 | Revisión de las Políticas para seguridad de la información. | 01A02-02;01A02-08 | 0,0 |
| 6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. | | | | | |
| | 6.1 Organización Interna. | | | | |
| | | 6.1.1 | Seguridad de la Información Roles y Responsabilidades. | 01A02-03:07;01A02-09;01C03-01 | 0,0 |
| | | 6.1.2 | Separación de deberes. | 06C01-03:06;08F01-01:04;11E01-01:04;11E02-01:04;12E01-01:04;12E02-01:04 | 0,0 |
| | | 6.1.3 | Contacto con las autoridades. | 01A02-10 | 0,0 |
| | | 6.1.4 | Contacto con grupos de interés especial. | 01A02-11 | 0,0 |
| | | 6.1.5 | Seguridad de la información en Gestión de Proyectos. | 01B02-06;10A01-01:06;10A02-01;10A02-05 | 0,0 |
| | 6.2 Dispositivos Móviles y Teletrabajo. | | | | |
| | | 6.2.1 | Política para dispositivos móviles. | 01B02-08;11B02-01;11B02-03;11C01-01;11D05-01 | 0,0 |
| | | 6.2.2 | Teletrabajo. | 11B02-01:02;11B02-04;11B03-04 | 0,0 |
| 7 SEGURIDAD DE LOS RECURSOS HUMANOS. | | | | | |
| | 7.1 Antes de asumir el empleo. | | | | |
| | | 7.1.1 | Selección. | 03-02:04 | 0,0 |
| | | 7.1.2 | Términos y condiciones del empleo. | 1:02 | 0,0 |
| | 7.2 Durante la ejecución del empleo. | | | | |
| | | 7.2.1 | Responsabilidades de la Dirección. | 01C0 | 0,0 |
| | | 7.2.2 | Toma de conciencia, educación y formación de la Seguridad de la Información. | 01C04- | 0,0 |
| | | 7.2.3 | Proceso disciplinario. | 01B01-0 | 0,0 |
| | 7.3 Terminación y cambio de empleo. | | | | |
| | | 7.3.1 | Terminación o cambio de responsabilidades de empleo. | 01B01- | 0,0 |
| 8 GESTIÓN DE ACTIVOS. | | | | | |
| | 8.1 Responsabilidad por los Activos. | | | | 0,0 |



***Ilustración 6-25.*** *Puntuación de servicios de seguridad respecto a controles de seguridad*

## 3. Análisis de riesgo y valoración


***Ilustración 6-26.*** *Fase operacional "Diagnostico de servicios de seguridad" de la Metodología MEHARI*

Esta es la sub fase más importante de toda la metodología, aquí es donde se realiza la valoración del riesgo, tomando en cuenta toda la información proporcionada en las tablas anteriores. La metodología MEHARI toma los activos de información seleccionados y los conjuga en más de 800 escenarios lo cuales representan

situaciones hipotéticas riesgosas para determinar si pueden o no suceder y que pasaría si sucediera. Se deben seleccionar de los más de 800 escenarios cuales, a consideración del Jefe de Información aplica para la organización. La hoja de cálculo en donde son colocados los activos de información para conjugarlos en diferentes escenarios riesgosos se muestra en la *ilustración 6-27*.

El funcionamiento de la hoja de cálculo “Scenarios” es descrita a continuación. En la columna A, se tiene la familia de escenarios, MEHARI agrupa los escenarios en familias para tener un orden en su forma de clasificación, en la columna B se tiene el código de la familia de escenarios, en la columna C se describe el tipo de activo (las agrupaciones que hizo MEHARI en las tablas T1, T2 y T3), la columna D representa el tipo de vulnerabilidad que se evalúa (Disponibilidad, Integridad, Confidencialidad o Eficiencia), la columna E es el activo relacionado, la columna F es el daño hipotético sufrido, la columna G representa el código del daño. La columna H representa el tipo de evento según la tabla de eventos, la columna I es el sub tipo del evento, las columnas de la J a la N tienen que ver con las circunstancias hipotéticas. La columna O es la descripción del escenario riesgoso hipotéticos.

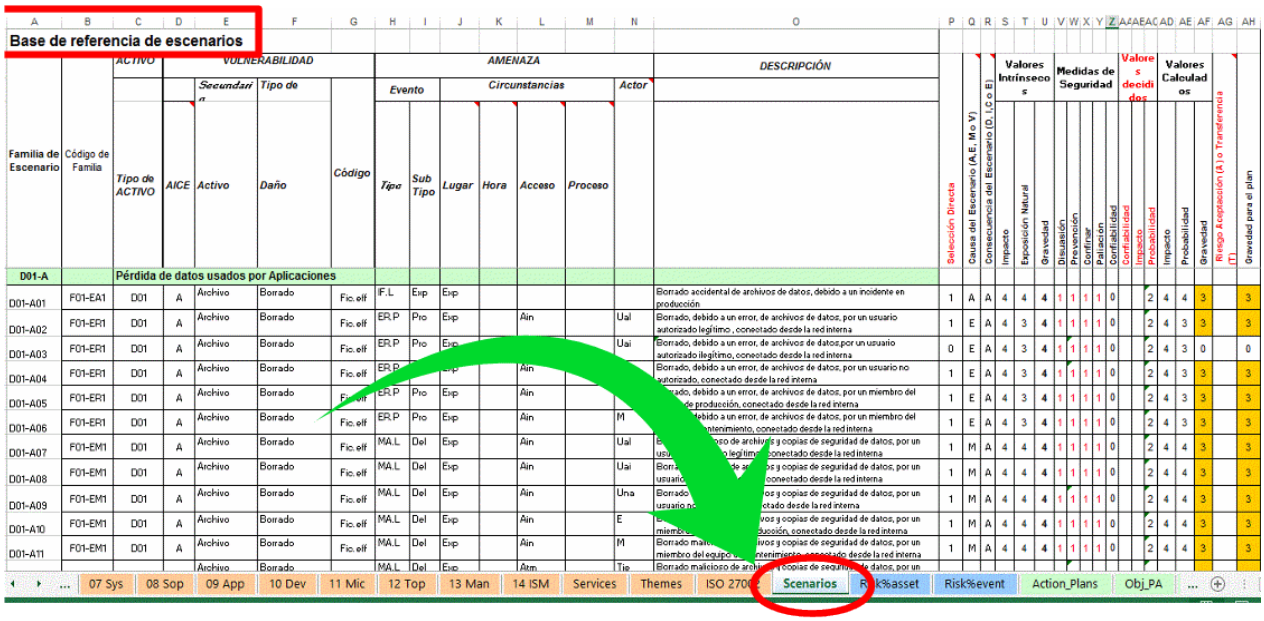



***Ilustración 6-27.*** *Escenarios para la valoración*

De las columnas P a la AH hay varias valoraciones, las que se encuentran en color negro son valoraciones y cálculos que hace MEHARI basado en información previamente introducida, los de color rojo son valores decidíos por el Jefe de Seguridad o Auditor. La primera columna P es la selección o no del escenario, se debe tomar una decisión en cada escenario si se va a valorar o no, las columnas Q a la Z son valores calculados por la metodología y se recomienda no modificar esos valores ya que son los resultados de las formulas propias de la Base de Reconocimiento. En las columnas AA, AB y AC se consignan valores de Seguridad de la Información a discreción del Auditor, en caso de que no se esté de acuerdo con la valoración de la metodología MEHARI en estas columnas se colocan valoraciones a consideración del Auditor esto puede darse en el caso de que el Auditor considera que el evento puede ser más grave o menos grave de la valoración propuesta por MEHARI y lo mismo sucede con la probabilidad.

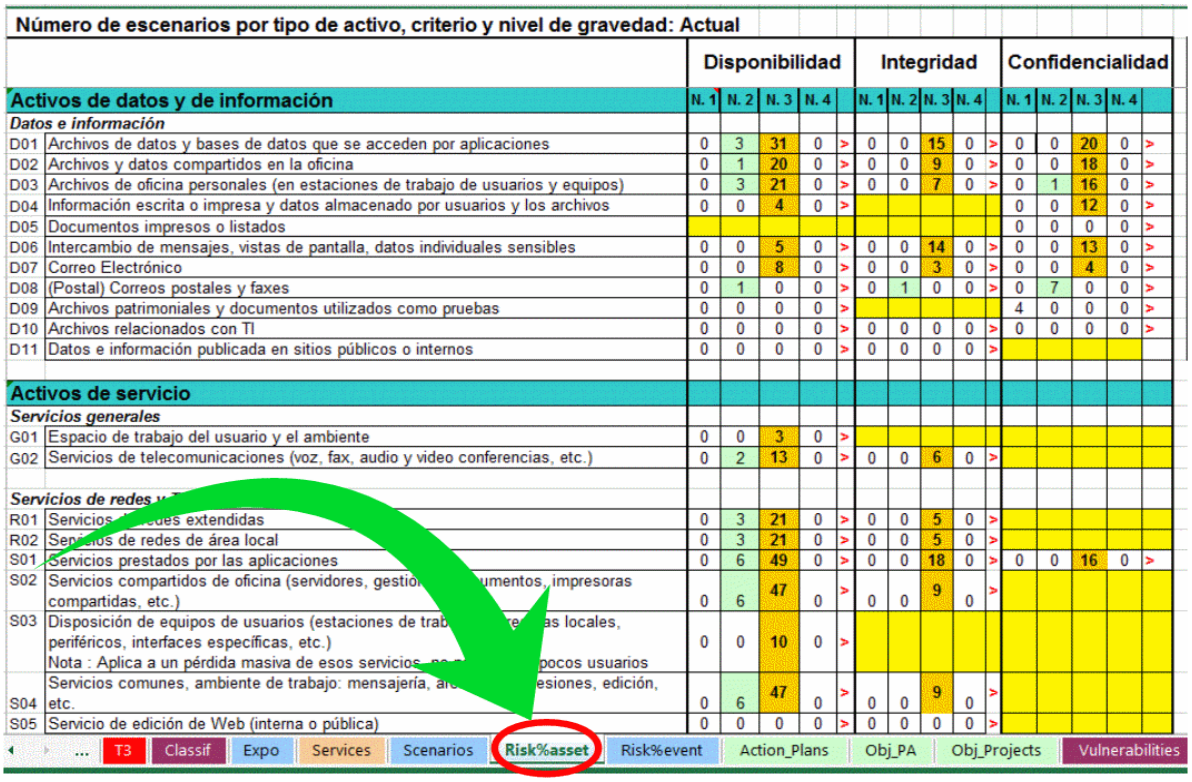
Por último la columna AG es una columna donde MEHARI proporciona una forma de tratar el riesgo de manera rápida el cual es “Aceptando” o “Transfiriendo”. Si el Auditor o Jefe de Seguridad decide tomar esta determinación, debe contar con una aprobación por parte de la alta dirección que avale esta decisión.

Una vez realizado esto en la columna AH la metodología arroja el resultado final de la valoración del riesgo o escenario riesgoso. Esta valoración servirá para determinar si se debe tratar o no, en esa columna queda consignado la valoración definitiva del escenario o riesgo.

En la hoja de cálculo “*Scenarios*”, se observa en la segunda fila dos nombres claves “Vulnerabilidad” y “Amenaza”. Para que exista un riesgo deben existir las dos al tiempo. Si solo existe una de las dos no se considera que exista un riesgo, debido que no existe amenaza que explote la vulnerabilidad. Las vulnerabilidades y amenazas dentro de la Base de Reconocimiento son casos hipotéticos que MEHARI recrea para evaluar los activos, poniéndolos a prueba en dichos escenarios para determinar si existe riesgo de que suceda ese escenario en consideración. En caso que exista, poder determinar qué tan grave, en términos de Seguridad de la Información es que suceda.

Una vez se terminada la realización de esta tabla, MEHARI arroja dos tablas de resultados de la valoración denominadas “Risk%Asset” y “Risk%event” como se muestra en la *ilustración 6-28 y 6-29*.

La tabla “Risk%Asset” arroja los resultados de la valoración en términos de Seguridad de la Información y muestra el número total de escenarios valorados. Se tiene los grupos de activos en la columna izquierda con sus respectivas nomenclaturas, los mismos grupos de activos que son consignados en las tablas T1, T2 y T3. En la parte derecha se tiene el resultado de la valoración realizada correspondiente a cada grupo de activo.

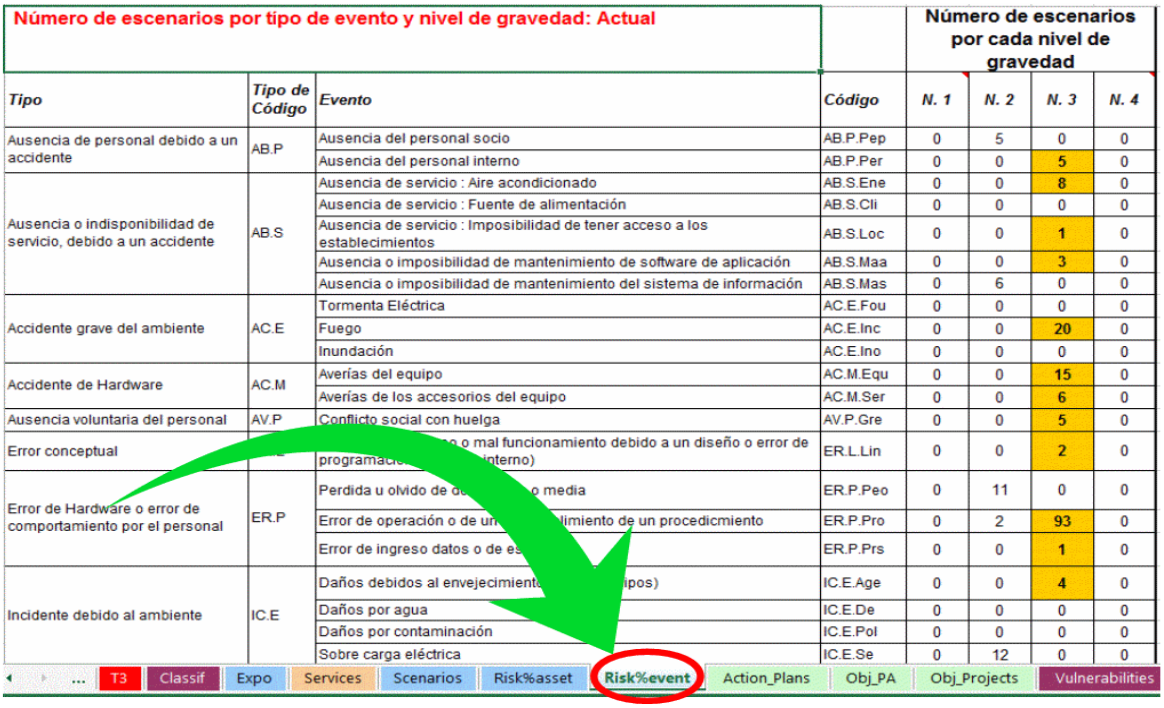


**Número de escenarios por tipo de activo, criterio y nivel de gravedad: Actual**

| | | Disponibilidad | | | | | Integridad | | | | | Confidencialidad | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Activos de datos y de información** | | N. 1 | N. 2 | N. 3 | N. 4 | | N. 1 | N. 2 | N. 3 | N. 4 | | N. 1 | N. 2 | N. 3 | N. 4 | |
| ***Datos e información*** | | | | | | | | | | | | | | | | |
| D01 | Archivos de datos y bases de datos que se acceden por aplicaciones | 0 | 3 | 31 | 0 | > | 0 | 0 | 15 | 0 | > | 0 | 0 | 20 | 0 | > |
| D02 | Archivos y datos compartidos en la oficina | 0 | 1 | 20 | 0 | > | 0 | 0 | 9 | 0 | > | 0 | 0 | 18 | 0 | > |
| D03 | Archivos de oficina personales (en estaciones de trabajo de usuarios y equipos) | 0 | 3 | 21 | 0 | > | 0 | 0 | 7 | 0 | > | 0 | 1 | 16 | 0 | > |
| D04 | Información escrita o impresa y datos almacenado por usuarios y los archivos | 0 | 0 | 4 | 0 | > | | | | | | 0 | 0 | 12 | 0 | > |
| D05 | Documentos impresos o listados | | | | | | | | | | | 0 | 0 | 0 | 0 | > |
| D06 | Intercambio de mensajes, vistas de pantalla, datos individuales sensibles | 0 | 0 | 5 | 0 | > | 0 | 0 | 14 | 0 | > | 0 | 0 | 13 | 0 | > |
| D07 | Correo Electrónico | 0 | 0 | 8 | 0 | > | 0 | 0 | 3 | 0 | > | 0 | 0 | 4 | 0 | > |
| D08 | (Postal) Correos postales y faxes | 0 | 1 | 0 | 0 | > | 0 | 1 | 0 | 0 | > | 0 | 7 | 0 | 0 | > |
| D09 | Archivos patrimoniales y documentos utilizados como pruebas | 0 | 0 | 0 | 0 | > | | | | | | 4 | 0 | 0 | 0 | > |
| D10 | Archivos relacionados con TI | 0 | 0 | 0 | 0 | > | 0 | 0 | 0 | 0 | > | 0 | 0 | 0 | 0 | > |
| D11 | Datos e información publicada en sitios públicos o internos | 0 | 0 | 0 | 0 | > | 0 | 0 | 0 | 0 | > | | | | | |
| **Activos de servicio** | | | | | | | | | | | | | | | | |
| ***Servicios generales*** | | | | | | | | | | | | | | | | |
| G01 | Espacio de trabajo del usuario y el ambiente | 0 | 0 | 3 | 0 | > | | | | | | | | | | |
| G02 | Servicios de telecomunicaciones (voz, fax, audio y video conferencias, etc.) | 0 | 2 | 13 | 0 | > | 0 | 0 | 6 | 0 | > | | | | | |
| ***Servicios de redes y*** | | | | | | | | | | | | | | | | |
| R01 | Servicios [illegible]edes extendidas | 0 | 3 | 21 | 0 | > | 0 | 0 | 5 | 0 | > | | | | | |
| R02 | Ser[illegible]os de redes de área local | 0 | 3 | 21 | 0 | > | 0 | 0 | 5 | 0 | > | | | | | |
| S01 | Servicios prestados por las aplicaciones | 0 | 6 | 49 | 0 | > | 0 | 0 | 18 | 0 | > | 0 | 0 | 16 | 0 | > |
| S02 | Servicios compartidos de oficina (servidores, gestio[illegible]umentos, impresoras compartidas, etc.) | 0 | 6 | 47 | 0 | > | 0 | 0 | 9 | 0 | > | | | | | |
| S03 | Disposición de equipos de usuarios (estaciones de trab[illegible]re[illegible]as locales, periféricos, interfaces específicas, etc.) Nota : Aplica a un pérdida masiva de esos servicios, [illegible]pocos usuarios | 0 | 0 | 10 | 0 | > | | | | | | | | | | |
| S04 | Servicios comunes, ambiente de trabajo: mensajería, ar[illegible]esiones, edición, etc. | 0 | 6 | 47 | 0 | > | 0 | 0 | 9 | 0 | > | | | | | |
| S05 | Servicio de edición de Web (interna o pública) | 0 | 0 | 0 | 0 | > | 0 | 0 | 0 | 0 | > | | | | | |

... T3 Classif Expo Services Scenarios Risk%asset Risk%event Action_Plans Obj_PA Obj_Projects Vulnerabilities

***Ilustración 6-28.*** *Resultados de la valoración del riesgo de la Base de Reconocimiento de MEHARI*



**Número de escenarios por tipo de evento y nivel de gravedad: Actual**

| Tipo | Tipo de Código | Evento | Código | Número de escenarios por cada nivel de gravedad N. 1 | N. 2 | N. 3 | N. 4 |
|---|---|---|---|---|---|---|---|
| Ausencia de personal debido a un accidente | AB.P | Ausencia del personal socio | AB.P.Pep | 0 | 5 | 0 | 0 |
| | | Ausencia del personal interno | AB.P.Per | 0 | 0 | 5 | 0 |
| Ausencia o indisponibilidad de servicio, debido a un accidente | AB.S | Ausencia de servicio : Aire acondicionado | AB.S.Ene | 0 | 0 | 8 | 0 |
| | | Ausencia de servicio : Fuente de alimentación | AB.S.Cli | 0 | 0 | 0 | 0 |
| | | Ausencia de servicio : Imposibilidad de tener acceso a los establecimientos | AB.S.Loc | 0 | 0 | 1 | 0 |
| | | Ausencia o imposibilidad de mantenimiento de software de aplicación | AB.S.Maa | 0 | 0 | 3 | 0 |
| | | Ausencia o imposibilidad de mantenimiento del sistema de información | AB.S.Mas | 0 | 6 | 0 | 0 |
| Accidente grave del ambiente | AC.E | Tormenta Eléctrica | AC.E.Fou | 0 | 0 | 0 | 0 |
| | | Fuego | AC.E.Inc | 0 | 0 | 20 | 0 |
| | | Inundación | AC.E.Ino | 0 | 0 | 0 | 0 |
| Accidente de Hardware | AC.M | Averías del equipo | AC.M.Equ | 0 | 0 | 15 | 0 |
| | | Averías de los accesorios del equipo | AC.M.Ser | 0 | 0 | 6 | 0 |
| Ausencia voluntaria del personal | AV.P | Conflicto social con huelga | AV.P.Gre | 0 | 0 | 5 | 0 |
| Error conceptual | | o mal funcionamiento debido a un diseño o error de programaci interno) | ER.L.Lin | 0 | 0 | 2 | 0 |
| Error de Hardware o error de comportamiento por el personal | ER.P | Perdida u olvido de d o media | ER.P.Peo | 0 | 11 | 0 | 0 |
| | | Error de operación o de ur limiento de un procedicmiento | ER.P.Pro | 0 | 2 | 93 | 0 |
| | | Error de ingreso datos o de e | ER.P.Prs | 0 | 0 | 1 | 0 |
| Incidente debido al ambiente | IC.E | Daños debidos al envejecimient ipos) | IC.E.Age | 0 | 0 | 4 | 0 |
| | | Daños por agua | IC.E.De | 0 | 0 | 0 | 0 |
| | | Daños por contaminación | IC.E.Pol | 0 | 0 | 0 | 0 |
| | | Sobre carga eléctrica | IC.E.Se | 0 | 12 | 0 | 0 |



***Ilustración 6-29.*** *Resultados de la valoración de eventos de la Base de Reconocimiento de MEHARI*

## 6.1.3 Fase de tratamiento

La fase de tratamiento se enfoca en la realización de la planificación del tratamiento del riesgo de todos los escenarios que dieron una valoraciones de 3 y 4. Posteriormente se realiza la planificación.

### 1. Planificación de medidas inmediatas

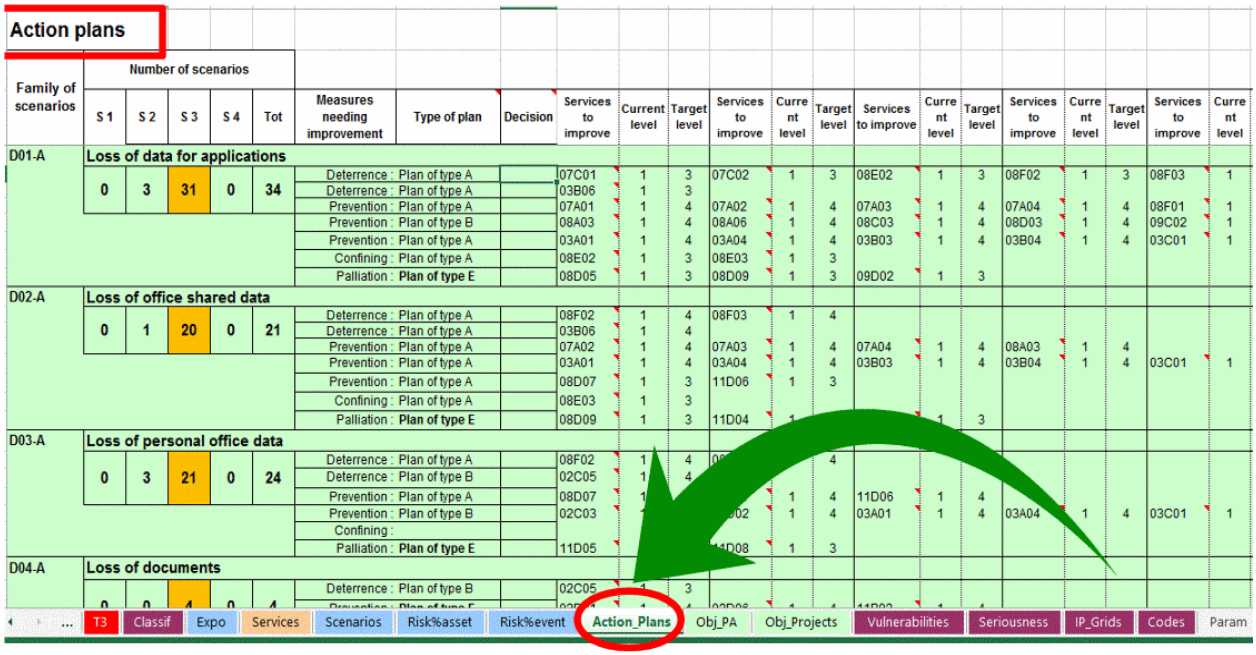

***Ilustración 6-30.*** *Fase tratamiento "planificación inmediata" de la Metodología MEHARI*

La planificación inmediata considera aquellos escenarios con valoración igual a 4, estos riesgos deben comunicarse y tratarse inmediatamente debido a que son los riesgos de mayor puntuación que tienen una alta probabilidad de suceder.

**2. Planificación de otras medidas**


***Ilustración 6-31.*** *Fase tratamiento "planificación de medidas" de la Metodología MEHARI*

Cuando se ha terminado de planificar los escenarios más graves, se procede a seleccionar los escenarios que obtuvieron valoración igual a 3. Una vez realizada la selección, se construye el plan de acción o plan de tratamiento. Aquí se observa la familia de escenarios para la identificación del riesgo en la columna izquierda de la *ilustración 6-32*, posteriormente se observa la valoración que obtuvo esa familia, seguido se observa planes de la A, a la E según el tipo de riesgo. MEHARI, según la información que ha suministrado, sugiere un plan para cada familia de escenario. Los autores de este trabajo de grado sugieren tomar las sugerencias que arroja la Base de Reconocimiento. La selección del plan debe hacerse escribiendo el número "1" al frente del plan que se ha seleccionado para mitigar ese riesgo. En esta misma línea se observan unas nomenclaturas, seguidas de unos valores que son el nivel objetivo y el nivel actual. Por lo general el nivel actual es mucho más bajo que el nivel objetivo (antes de realizar el plan y su ejecución). El punto de esta actividad es lograr que el nivel actual sea igual o superior al nivel objetivo, esto se realiza observando la nomenclatura del servicio a mejorar, a que control de seguridad corresponde de la norma ISO/IEC 27002. Es decir, se debe ir a la documentación y determinar el servicio que se debe mejorar y cómo hacer para mejorarlo según criterios del Jefe de Información.




| Family of scenarios | Number of scenarios | | | | | Measures needing improvement | Type of plan | Decision | Services to improve | Current level | Target level | Services to improve | Current level | Target level | Services to improve | Current level | Target level | Services to improve | Current level | Target level | Services to improve | Current level |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | S1 | S2 | S3 | S4 | Tot | | | | | | | | | | | | | | | | | |
| D01-A | **Loss of data for applications** | | | | | | | | | | | | | | | | | | | | | |
| | 0 | 3 | 31 | 0 | 34 | Deterrence : | Plan of type A | | 07C01 | 1 | 3 | 07C02 | 1 | 3 | 08E02 | 1 | 3 | 08F02 | 1 | 3 | 08F03 | 1 |
| | | | | | | Deterrence : | Plan of type A | | 03B06 | 1 | 3 | | | | | | | | | | | |
| | | | | | | Prevention : | Plan of type A | | 07A01 | 1 | 4 | 07A02 | 1 | 4 | 07A03 | 1 | 4 | 07A04 | 1 | 4 | 08F01 | 1 |
| | | | | | | Prevention : | Plan of type B | | 08A03 | 1 | 4 | 08A06 | 1 | 4 | 08C03 | 1 | 4 | 08D03 | 1 | 4 | 09C02 | 1 |
| | | | | | | Prevention : | Plan of type A | | 03A01 | 1 | 4 | 03A04 | 1 | 4 | 03B03 | 1 | 4 | 03B04 | 1 | 4 | 03C01 | 1 |
| | | | | | | Confining : | Plan of type A | | 08E02 | 1 | 3 | 08E03 | 1 | 3 | | | | | | | | |
| | | | | | | Palliation : | **Plan of type E** | | 08D05 | 1 | 3 | 08D09 | 1 | 3 | 09D02 | 1 | 3 | | | | | |
| D02-A | **Loss of office shared data** | | | | | | | | | | | | | | | | | | | | | |
| | 0 | 1 | 20 | 0 | 21 | Deterrence : | Plan of type A | | 08F02 | 1 | 4 | 08F03 | 1 | 4 | | | | | | | | |
| | | | | | | Deterrence : | Plan of type A | | 03B06 | 1 | 4 | | | | | | | | | | | |
| | | | | | | Prevention : | Plan of type A | | 07A02 | 1 | 4 | 07A03 | 1 | 4 | 07A04 | 1 | 4 | 08A03 | 1 | 4 | | |
| | | | | | | Prevention : | Plan of type A | | 03A01 | 1 | 4 | 03A04 | 1 | 4 | 03B03 | 1 | 4 | 03B04 | 1 | 4 | 03C01 | 1 |
| | | | | | | Prevention : | Plan of type A | | 08D07 | 1 | 3 | 11D06 | 1 | 3 | | | | | | | | |
| | | | | | | Confining : | Plan of type A | | 08E03 | 1 | 3 | | | | | | | | | | | |
| | | | | | | Palliation : | **Plan of type E** | | 08D09 | 1 | 3 | 11D04 | 1 | | | | 3 | | | | | |
| D03-A | **Loss of personal office data** | | | | | | | | | | | | | | | | | | | | | |
| | 0 | 3 | 21 | 0 | 24 | Deterrence : | Plan of type A | | 08F02 | 1 | 4 | | | 4 | | | | | | | | |
| | | | | | | Deterrence : | Plan of type B | | 02C05 | 1 | 4 | | | | | | | | | | | |
| | | | | | | Prevention : | Plan of type A | | 08D07 | 1 | | | 1 | 4 | 11D06 | 1 | 4 | | | | | |
| | | | | | | Prevention : | Plan of type B | | 02C03 | 1 | | 02 | 1 | 4 | 03A01 | 1 | 4 | 03A04 | 1 | 4 | 03C01 | 1 |
| | | | | | | Confining : | | | | | | | | | | | | | | | | |
| | | | | | | Palliation : | **Plan of type E** | | 11D05 | 1 | | 11D08 | 1 | 3 | | | | | | | | |
| D04-A | **Loss of documents** | | | | | | | | | | | | | | | | | | | | | |
| | 0 | 0 | 4 | 0 | 4 | Deterrence : | Plan of type B | | 02C05 | 1 | 3 | | | | | | | | | | | |



***Ilustración 6-32.*** *Plan de Acción o Plan de Tratamiento de la Base de Reconocimiento de MEHARI*

Para finalizar con el plan de tratamiento y la declaración de aplicabilidad, se debe dirigir al anexo A de la norma ISO/IEC 27002:2013 para determinar los controles de seguridad a implementar basados en los planes seleccionados en el Plan de Acción. Cada plan tiene consigo unos servicios y estos servicios tienen controles relacionados, se debe determinar que controles son los que están relacionados con esos servicios respecto a los planes seleccionados, para posteriormente seleccionarlos en la declaración de aplicabilidad. Cabe aclarar que todos los controles que se seleccionen deben estar plenamente justificados y una vez se tenga esta declaración debe entregarse a la alta dirección para que sea evaluado y aprobado, para dar por finalizada la fase de planeación de SGSI.

**3. Auditoria y Guía**

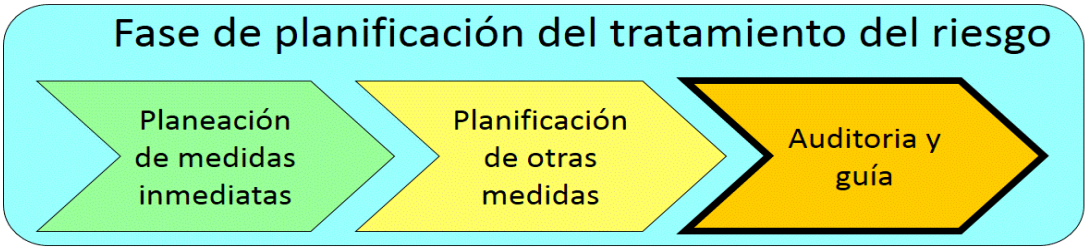



***Ilustración 6-33.*** *Fase tratamiento "auditoria y guía" de la Metodología MEHARI*

Esta sub fase tiene que ver con las fases de "Verificación" y "Actuación" del ciclo Deming. Una vez se ha planificado el tratamiento y en la fase siguiente de "Ejecución" se han implementado lo que se estipulo en el plan, MEHARI proporciona una forma de hacer una segunda valoración del riesgo ya con los controles de seguridad, servicios de seguridad y planes implementados. Estas comparaciones se realizan en las tablas del libro de Excel "Obj_PA" y "Obj_Projects". Además, debe configurarse una pequeña información en la tabla "Risk%Asset". Debido a que estas fases de ciclo Deming no están dentro del marco alcance de este proyecto de grado, no se abordara la "Auditoria y Guía".

## 6.2 APRENDIZAJES OBTENIDOS CON MEHARI

La metodología MEHARI es una metodología de gestión de riesgos que provee una extensa Base de Reconocimiento, no obstante la documentación disponible no es completamente clara y es necesaria la práctica para su completo entendimiento, sin embargo en este capítulo se ha detallado como se debe implementar la metodología en cualquier organización llenando el vacío que deja MEHARI.

Durante la ejecución del presente proyecto de grado se logró conocer mejor la metodología, la cual es compleja de entender para personas que exploran la metodología por primera vez. Se encuentra mucha documentación pero no se especifica de manera clara como ejecutar el análisis y la valoración de los riesgos con el uso de la herramienta que la metodología pone a disposición.

En este capítulo de detalló cómo debe seguirse la ejecución de la metodología pasando por cada una de sus fases, hasta llegar a el análisis y la valoración de los riesgos con el soporte de la herramienta dispuesta por MEHARI.

Se espera que la guía presentada en este capítulo pueda ayudar a cualquier persona encargada de la seguridad de una organización a la implementación de un SGSI con el soporte de una herramienta tan completa como lo es la metodología MEHARI.

# 7 CONCLUSIONES

- La aplicación de la metodología MEHARI al caso de estudio propuesto permitió la adaptación de la metodología y la identificación de los principales riesgos a los cuales estaba expuesta la organización.

- La metodología MEHARI es una metodología que proporciona una extensa herramienta libre y gratuita para poder llevar a cabo el análisis y la gestión de los riesgos que requiere en principio una complicada adaptación de la herramienta.

- La metodología MEHARI solo puede ser ejecutada junto con la “Base de Reconocimiento” la cual es una herramienta asociada a MEHARI.

- La metodología MEHARI tiene un enfoque riguroso de análisis de riesgo de forma directa, extensiva e individual que se diferencia de otro tipo de metodologías las cuales son muy simplistas.

- La metodología MEHARI está en conformidad con los estándares ISO de seguridad de la información, de este modo la metodología se integra fácilmente a los procesos de un SGSI cumpliendo con los requerimiento de la ISO/IEC 27001.

- La metodología MEHARI es ideal para organizaciones que tienen como objetivo mejorar un SGSI, esto quiere decir que las organizaciones que se están iniciando en un SGSI deberían seguir la ISO/IEC 27003 como guía de implementación, para posteriormente mejorar el SGSI realizando una evaluación con la metodología MEHARI la cual provee una extenso grupo de preguntas de auditoria que permiten evaluar de forma efectiva cualquier organización con respecto a los controles de seguridad establecidos en la ISO/IEC 27002.

- El ciclo de mejora continua Deming le permite a un SGSI estar constantemente actualizado frente a nuevas amenazas, la metodología MEHARI sigue un completo proceso de mejora similar al ciclo Deming lo cual hace que la metodología MEHARI sea la adecuada para los proceso de identificación de nuevos riesgos y de perfeccionamiento de un SGSI.

## 7.1 TRABAJOS FUTUROS

- Ejecutar la fase de planeación en la Seguridad de la Información en otro procedimiento críticos de la institución siguiendo como guía la adaptación de la metodología MEHARI presentada en este trabajo.

- Evaluar y analizar las diferentes metodologías de gestión de riesgos en comparación con la metodología MEHARI.

- Implementar la fase de ejecución de un SGSI para el Procedimiento de Desarrollo y Mantenimiento de Aplicaciones.

- Ejecutar la fase de planeación de un SGSI para los procedimientos más críticos relacionados con el procedimiento tratado en este trabajo de grado.

- Analizar los resultados de las diferentes metodologías de gestión de riesgos las cuales fueron ejecutadas paralelamente a este trabajo de grado.

# 8 BIBLIOGRAFÍA

**[1]** "El cibercrimen es un delito más rentable que el narcotráfico", *Dinero.com*, 2015. [En línea]. Disponible: http://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988. [Última Búsqueda: 27- Abril- 2016].

**[2]** "5 Cifras Espeluznantes de la Inseguridad Informática", *ENTER.CO*, 2016. [En línea]. Disponible: http://www.enter.co/chips-bits/seguridad/5-cifras-espeluznantes-de-la-inseguridad-informatica-disi-2010/. [Última Búsqueda: 27- Abril- 2016].

**[3]** *"Implantación y Certificación del Sistema de gestión de la Seguridad de la Información – SGSI de la Universidad del Cauca"*, R-005, Universidad del Cauca, 2015.

**[4]** *"Políticas del sistema de Seguridad de la Información de la Universidad del Cauca"*, R-785, Universidad del Cauca, 2015.

**[5]** "Inicio - Estrategia GEL", *Estrategia.gobiernoenlinea.gov.co*, 2016. [En línea]. Disponible: http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html. [Última Búsqueda: 27-Abril-2016].

**[6]** "MANUAL PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA EN LAS ENTIDADES DEL ORDEN NACIONAL DE LA REPÚBLICA DE COLOMBIA 2012-2015", *Ministerio de Tecnología de la Información y las Comunicaciones*, pag 14-94, v. 3.1, 2012. [En línea]. Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf. [Última Búsqueda: 27-Abril-2016].

**[7]** F. Pino, F. García, M. Piattini and H. Oktaba, "A research framework for building SPI proposals in small organizations: the COMPETISOFT experience", *Software Qual J,* 2015.

**[8]** L. N. Agustín y R. S. Javier, "Sistema de Gestión de la Seguridad de la Información", *Iso27000.es,* 2010. Disponible: http://www.iso27000.es/download/doc_sgsi_all.pdf. [Última Búsqueda: 27-Abril-2016].

**[9]** "ENTREGABLES 3, 4, 5 Y 6: INFORME FINAL – MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI – SGSI – MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA", Ministerio de Tecnología de la Información y las Comunicaciones, 2008. [En línea]. Disponible: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf. [Última Búsqueda: 27-Abril-2016].

**[10]** "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements", *ISO*, 2016. [En línea]. Disponible: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. [Última Búsqueda: 27- Abril- 2016].

**[11]** L. N. Agustín y R. S. Javier, "ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información", *Iso27000.es*, 2016. [En línea]. Disponible: http://www.iso27000.es/iso27000.html. [Última Búsqueda: 27- Abril - 2016].

**[12]** "Estándares de Seguridad ISO 27000", WeLiveSecurity.com, 2016. [En línea]. Disponible: http://www.welivesecurity.com/la-es/2014/09/10/estandares-seguridad-iso-27000-nuevo/. [Última Búsqueda: 10- Febrero - 2016].

**[13]** "El Ciclo de Deming", *Implementacionsig.com*, 2016. [En línea]. Disponible: http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-. [Última Búsqueda: 27- Abril - 2016].

**[14]** C. Marty, "ISO27k ISMS Implementation and Certification Process", *Iso27001security.com,* 2010. Disponible: http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_overview_v2.pptx. [Última Búsqueda: 27-Abril-2016].

**[15]** *MEHARI 2010 Introducción*, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf. [Última Búsqueda: 27-Abril-2016].

**[16]** "CLUSIF [English version]", *Clusif.asso.fr*, 2016. [En línea]. Disponible: http://clusif.asso.fr/en/clusif/present/. [Última Búsqueda: 27-Abril-2016].

**[17]** *MEHARI 2010 Security Stakes Analysis and Classification Guide*, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Stakes-Analysis-and-Classification-Guide.pdf. [Última Búsqueda: 27-Abril-2016].

**[18]** *MEHARI 2010 Risk Analysis and Treatment Guide*, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf. [Última Búsqueda: 27-Abril-2016].

**[19]** *MEHARI 2010 Fundamental concepts and functional specifications*, 1st ed. Paris: Clusif, 2010. [En línea]. Disponible: http://clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf. [Última Búsqueda: 27-Abril-2016].

**[20]** *MEHARI 2010 strategies for risk seriousness reduction and setting security level targets,* v. 36. Paris: Clusif, 2016.

**[21]** *División de Gestión de Recursos Tecnológicos Desarrollo y Mantenimiento de Aplicaciones,* Universidad del Cauca, Código: PA-GA-5.3.PR-8, v. 4, Popayán, 2016. [En línea]. Disponible: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PA-GA-5.3-PR-8%20Desarrollo%20y%20Mantenimiento%20de%20Aplicaciones._0.pdf. [Última Búsqueda: 27-Abril-2016].

**[22]** A. Alexander, "*Diseño de un sistema de gestión de seguridad de información"*. Bogotá: Alfaomega Colombiana, 2007.

**[23]** "Anexo 1: Metodología de Clasificación de Activos – Modelo de Seguridad de la Información para Estrategia de Gobierno en Línea", Ministerio de Tecnología de la Información y las Comunicaciones, 2011. [En línea]. Disponible: http://css.mintic.gov.co/ap/gel4/images/SeguridaddelaInformacion2_0_Anexo7_Clasificacion-de-Activos.pdf. [Última Búsqueda: 29-Abril-2016].

**[24]** "ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management", *ISO*, 2011. [En línea]. Disponible: http://www.iso.org/iso/catalogue_detail?csnumber=56742. [Última Búsqueda: 27-Abril-2016].

**[25]** MEHARI, "MEHARI 2010 with support ISO 27002:2013", v. 10.02.2016, Paris, 2016. [En línea]. Disponible: https://sourceforge.net/projects/mehari/files/MEHARI-Expert/Mehari%202010%20English/. [Última Búsqueda: 27- Abril - 2016].

**[26]** *MEHARI 2010 Reference Manual knowledge base updated for ISO 27002:2013 links*, 2st ed. Paris: Clusif, 2016.

**[27]** "ISO/IEC 27003:2010 - Information technology -- Security techniques -- Information security management system implementation guidance", *ISO*, 2013. [En línea]. Disponible: http://www.iso.org/iso/catalogue_detail?csnumber=42105. [Última Búsqueda: 27-Abril-2016].