ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA PLANTA CENTRAL DEL MINISTERIO DE CULTURA Y PATRIMONIO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

JOHAN MARCELO MONTENEGRO ZAMBRANO

MARÍA CRISTINA VIVAR HERRERA

DIRECTOR: MSc. PABLO WILIAN HIDALGO LASCANO

Quito, enero 2021

AVAL

Certifico que el presente trabajo fue desarrollado por Johan Marcelo Montenegro Zambrano y María Cristina Vivar Herrera, bajo mi supervisión.

_____

MSc. PABLO HIDALGO

DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Nosotros, Johan Marcelo Montenegro Zambrano y María Cristina Vivar Herrera, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejamos constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

JOHAN M. MONTENEGRO Z.	MARÍA C. VIVAR H.

DEDICATORIA

A Jehová, mi único Dios y Salvador. Fuera de Él, nada soy. Su Palabra es Verdad: es información segura.

A mi padre y mis hermanos, a los que amo por completo, por quienes daría mi vida, y a los que volvería a escoger una y otra vez si tuviera que elegir.

A la memoria de mi madre.

Al lector, que comprende cuán importante es la Seguridad de la Información.

Johan Montenegro

DEDICATORIA

El presente trabajo de titulación está dedicado a Dios y la virgen Dolorosa por guiarme por el buen camino, ser mi faro y darme fuerzas para seguir adelante a pesar de las vicisitudes que se han presentado.

A mis padres, por su amor, compresión y apoyo incondicional para alcanzar cada uno de mis objetivos y metas, por ser mi ejemplo para seguir siempre adelante y mi mayor fortaleza.

A mis abuelitos que son parte de mi vida.

M. Cristina Vivar

AGRADECIMIENTO

Estoy agradecido eternamente con Dios en todo.

Quiero expresar mi agradecimiento a María Cristina Vivar, mi compañera de Tesis, por creer en mí, por compartir todo su tiempo, esfuerzo y conocimientos conmigo en la consecución de este Trabajo, y por su invaluable amistad.

Quiero agradecer también a Pablo Wilian Hidalgo, profesor de la Escuela Politécnica Nacional, quien proporcionó toda la dirección y guía en el desarrollo del presente Trabajo de Titulación, contribuyó con sus amplios conocimientos en el ámbito, y sus valiosos consejos arrojaron luz y marcaron una gran diferencia en la forma de llevar a cabo de este trabajo. Especial gratitud a Xavier Calderón, también profesor de la EPN, por sus preciadas recomendaciones en la fase inicial de este proyecto.

Quiero expresar mi agradecimiento a mi padre, Marcelo Fabián Montenegro Murillo, quien aportó con sus conocimientos técnicos en un aspecto fundamental en este Trabajo.

Fue fructífera la participación de Milton Eduardo Estévez, Yésica Alexandra Calderón y Marcos David Mejía, técnicos de la DTICs del Ministerio de Cultura y Patrimonio, y amigos míos, en procesos clave de este Trabajo. Les agradezco. Agradezco también a Xavier Armando Castro, por su apoyo y aportes técnicos, y a César Augusto Robles y Lenin Fernando Calle, de la misma Dirección, quienes brindaron todo su apoyo y proveyeron las facilidades en todo cuanto pudieron, aún en contra de las adversidades, para que este trabajo surja. También cuentan entre mis amigos. Agradezco a todos los expertos y técnicos en el ámbito que estuvieron dispuestos a responder a las inquietudes y a los funcionarios que reconocieron la importancia de esta labor, y lo reflejaron con su aporte.

Y quiero manifestar mi más sincera gratitud a mi familia: una vez más a mi padre, a mis hermanos Bryan David Montenegro y Joel Andrés Montenegro, y a mis cuñadas, Andrea Franco de Montenegro y Stefany Ortega de Montenegro, no solo por ponerse toda la carga encima para que yo quede libre y trabaje con tranquilidad, sino también por todo lo que tuvieron que hacer para apoyarme; a mis pequeños sobrinos, por momentos inolvidables, y mi entrañable gratitud para Jennyfer Cristina Villegas, por su profundo cariño, por entenderme en todo, por mantenerse a mi lado y por brindarme su apoyo incondicional. Y a mis amigos, sobre todo con quienes compartí los últimos semestres en la EPN.

Johan Montenegro

AGRADECIMIENTO

Gracias a mis padres Sandra y Hernán por ser mi guía y pilar fundamental en mi vida, por sus consejos y amor, al Ing. Pablo Hidalgo nuestro director de tesis quien con sus orientaciones apoyo y seguimiento de este trabajo me ha hecho crecer profesionalmente, a mi compañero Johan con quien hemos tomado el reto para realizar este trabajo de titulación

A la EPN, a mis abuelitos Julia y Raúl, a mi tío Raúl Alejandro, a mis compañeros de trabajo Lenín, César, Xavier, Eduardo, Yesica, Santiago, a mis amigos y a cada una de las personas que me han brindado su apoyo incondicional.

M. Cristina Vivar

ÍNDICE DE CONTENIDO

6 ANEXOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente Trabajo de Titulación tiene como objetivo el diseñar un SGSI para la Planta Central del Ministerio de Cultura y Patrimonio.

El Capítulo 1 comprende toda la parte conceptual que engloba al proyecto: conceptos relacionados con SGSI, análisis y descripción de las normas ISO/IEC 27000, 27001, 27002 y 27005 en las que se fundamenta el proyecto, de las organizaciones de normalización y regulación pertinentes, del EGSI (versión 2.0) y de las metodologías MAGERIT y MEHARI.

El Capítulo 2 expone la Metodología desarrollada para este proyecto, basada en las normas mencionadas; se analiza y determina el contexto actual de la Institución; se desarrolla un Método de Análisis y Evaluación de Riesgos, que incluye técnicas de las metodologías estudiadas; se definen los criterios y umbrales de valoración, se identifican los activos y las dependencias entre éstos, se hace un Análisis de Riesgos determinando amenazas, vulnerabilidades, salvaguardas, impacto, probabilidad y riesgo potencial, y se desarrolla y aplica un *software* que permite agilizar los procesos de cálculo; se hace una Evaluación del Riesgo, y se desarrollan las opciones para el Tratamiento de Riesgos.

En el Capítulo 3 se definen controles y se desarrollan Políticas de Seguridad de la Información para abordar los riesgos.

El Capítulo 4 contiene las conclusiones y recomendaciones.

Se incluyen 20 Anexos, en los que constan la Matriz de Riesgos principal, la Declaración de Aplicabilidad, diagramas de dependencias, cuestionarios, el Plan de Capacitación, el Estudio de amenazas, vulnerabilidades y salvaguardas, entre otros.

PALABRAS CLAVE: SGSI, Seguridad de la Información, MAGERIT, MEHARI, ISO 27001, ISO 27002, ISO 27005, riesgo.

ABSTRACT

The objective of this Degree Project is to design an ISMS (Information Security Management System) for the Central Plant of the MCyP (Ministerio de Cultura y Patrimonio), of the Republic of Ecuador.

Chapter 1 includes the entire conceptual part that encompasses the project: concepts related to ISMS, analysis and description of the ISO / IEC 27000, 27001, 27002 and 27005 standards on which the project is based, of the relevant standardization and regulation organizations, of EGSI (version 2.0) and of MAGERIT and MEHARI methodologies.

Chapter 2 exposes the Methodology developed for this project, based on the aforementioned standards; the current context of the Institution is analyzed and determined; A Risk Analysis and Evaluation Method is developed, which includes techniques from the previously studied methodologies; Valuation criteria and thresholds are defined, assets and dependencies between them are identified, a Risk Analysis is carried out determining threats, vulnerabilities, safeguards, impact, probability and potential risk, and a PC program is developed and applied to expedite the calculation processes; A Risk Assessment is made, and options for Risk Treatment are developed.

In Chapter 3, controls are defined and Information Security Policies are developed to address risks.

Chapter 4 contains the conclusions and recommendations.

20 Annexes are included, which contain the main Risk Matrix, the Statement of Applicability (SoA), dependency diagrams, questionnaires, the Training Plan, the Study of threats, vulnerabilities and safeguards, among others.

KEYWORDS: ISMS, Information Security, MAGERIT, MEHARI, ISO 27001, ISO 27002, ISO 27005, risk.

1 INTRODUCCIÓN

No existe ningún sistema de información que sea completamente seguro; ni siquiera un ordenador desconectado de toda red. La Agencia Central de Inteligencia (CIA, por sus siglas en inglés), por ejemplo, diseñó un *software* capaz de infectar un ordenador aislado de la red y desplegar un paquete de herramientas con código malicioso que puede recolectar, almacenar y cifrar información del ordenador en una partición del disco duro, aunque, evidentemente, necesita de la intervención del ser humano, cuando éste inserta una memoria USB en el ordenador en cuestión, según reveló WikiLeaks en su portal [1].

Sorprendentemente, hay ataques con los que puede obtenerse información de un dispositivo electrónico desconectado de toda red, de forma remota, y sin necesidad de acercarse siquiera al dispositivo objetivo. Tal es el caso de los ataques TEMPEST [2], que aprovechan las emanaciones electromagnéticas de los dispositivos electrónicos, provocadas, por ejemplo, por las pulsaciones de las teclas en un teclado o simplemente por la imagen que sale de una pantalla de ordenador encendida, para reconstruir la señal en el dispositivo del delincuente, estando éste a varios metros de distancia.

Entonces, ¿resulta inútil todo esfuerzo por proteger la información? De ninguna manera. Con el creciente avance tecnológico del que se sirve la ciberdelincuencia, crecen las medidas de seguridad. El ideal es alcanzar el 100% de seguridad, pero en la realidad se busca mitigar los riesgos de seguridad de la información hasta un nivel aceptable.

Es por esto que surge la necesidad de gestionar los riesgos de seguridad de la información, de forma sistemática, en base a las recomendaciones y directrices proporcionadas por la pericia de expertos, profesionales y científicos en este ámbito, que estén debidamente actualizadas y que se ajusten a las necesidades de la organización cuya información se busca proteger. Sin embargo, se ha hallado que la mayor parte de las brechas de seguridad provienen de las malas prácticas del activo más débil de la organización: el talento humano.

Pero ¿necesita la Planta Central del Ministerio de Cultura y Patrimonio un Sistema de Gestión de Seguridad de la Información (SGSI)? Por supuesto. Esta Institución guarda información patrimonial, cultural, social, artística y científica valiosa, que ha sido vulnerada a falta de un SGSI y, además, debe hacerlo por disposición gubernamental. Este Trabajo de Titulación se ha enfocado en el diseño de un SGSI basado en las normas internacionales ISO/IEC 27001 [3], 27002 [4] y 27005 [5], y se ha servido del aporte de las metodologías MAGERIT y MEHARI, con las que se ha obtenido la solución que se propone a la Institución, que incluye al factor humano como un aspecto sumamente importante.

1.1 OBJETIVOS

1.1.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para la Planta Central del Ministerio de Cultura y Patrimonio.

1.1.2 OBJETIVOS ESPECÍFICOS

- Analizar la documentación asociada a la evaluación de riesgos de seguridad de la información del MCyP, Planta Central.
- Evaluar los riesgos en base a la solución obtenida de las metodologías MAGERIT y MEHARI.
- Definir controles de seguridad de la información.
- Validar algunos de los controles de seguridad de la información definidos.

1.2 ALCANCE

El presente Trabajo de Titulación abarca el diseño de un SGSI para la Planta Central del Ministerio de Cultura y Patrimonio, a fin de que sea dicha institución la que decida adoptarlo y posiblemente replicarlo a nivel nacional.

Para el diseño del SGSI se analiza toda la documentación que refleja el estado actual de la institución en cuanto a seguridad de la información. Así mismo, se analizan las normativas vigentes a la fecha que engloban al proceso; entre ellas las correspondientes a las Normas Técnicas Ecuatorianas ISO/IEC 27000:2016 [7], ISO/IEC 27001 [3], ISO/IEC 27002 [4] e ISO/IEC 27005 [5], así como el Acuerdo Ministerial 025-2019 [6], y se estudian las metodologías de evaluación de riesgos en la seguridad de la información MAGERIT y MEHARI, basadas en las normas mencionadas, que se adecúen a la realidad institucional y se adapten a las necesidades y requerimientos de la Planta Central de la Institución.

Luego de dicho estudio, se toma la información, criterios y procedimientos de las metodologías estudiadas, que se consideran necesarios, de tal forma que se establezca una solución que se adapte a la realidad de esta Cartera de Estado.

A continuación, se procede con el levantamiento de los activos de información; para ello, se realizan entrevistas y diagramas de tolerancia a indisponibilidad con los responsables y/o administradores de los sistemas de información de la Planta Central del MCyP, lo que permite determinar los activos de información clave para el funcionamiento de esta Cartera

de Estado, además de tener conocimiento más amplio del objetivo de cada sistema, tipo de información y relevancia correspondiente.

Posteriormente, se realiza la valoración de cada activo, principalmente en las dimensiones de confidencialidad, integridad y disponibilidad. Para esto, se usan los criterios de valoración establecidos en dichas dimensiones y, en conjunto con funcionarios de la Dirección de Tecnologías de la Información y Comunicación, se delibera y se define el valor propio de cada activo basado en dichos criterios.

Las dependencias entre activos son modeladas en diagramas de dependencias para cada activo y sus activos superiores (activos que dependen de él), y se desarrolla un programa computacional que permite agilizar el proceso de cálculo del valor acumulado de los activos. Se calcula el valor acumulado de cada activo considerando el valor propio, el grado de dependencia de cada activo superior (determinado bajo criterios establecidos) y sus valores propios.

Se determinan las amenazas potenciales correspondientes, incluyendo aquellas que afectan al personal de esta institución, debido a que es éste quien puede acceder, actualizar, eliminar o modificar la información.

Se analiza el impacto de cada amenaza sin considerar los controles existentes. Para el cálculo del impacto se considera el impacto acumulado y el impacto repercutido sobre cada activo.

El impacto acumulado tiene en cuenta el valor acumulado del activo en cuestión y el nivel de degradación causada por una amenaza efectiva sobre el mismo.

Para el impacto repercutido se modelan las dependencias del activo en cuestión y los activos inferiores (activos de los cuales depende).

El impacto repercutido tiene en cuenta el valor propio del activo analizado, el grado de dependencia de los activos inferiores y la degradación de los mismos al materializarse sus amenazas correspondientes.

La probabilidad (o potencialidad) de que cada amenaza pueda materializarse es analizada tomando en consideración los criterios de valoración establecidos y las vulnerabilidades identificadas.

Con el impacto acumulado, el impacto repercutido y la probabilidad (potencialidad) se hallan los riesgos de cada activo, en ausencia de controles.

Se identifican los controles (salvaguardas) existentes, y se define el grado de eficacia de cada uno frente a las amenazas.

El riesgo residual considera los riesgos acumulado y repercutido sobre un activo, y el grado de eficacia de los controles existentes.

Los resultados de dichos cálculos son organizados en una matriz final de riesgos.

Se determinan controles adaptados a las necesidades de seguridad de información de la institución.

Se brindan conclusiones y recomendaciones que podrán ser utilizadas para trabajos futuros.

En este Trabajo de Titulación no se presentará un producto final demostrable.

1.3 MARCO TEÓRICO

1.3.1 ANTECEDENTES

1.3.1.1 Antecedentes internacionales

1.3.1.1.1 Sobre la importancia de la seguridad de la información

Najar y Suárez (2015) realizaron un estudio sobre la importancia de la seguridad de la información debido a que la creciente tecnología, que facilita el darse a conocer en un mercado cada vez más amplio y globalizado, también trae consigo vulnerabilidades que exponen la información frente a cibercriminales, concluyendo que el activo más valioso para una organización, la información, se encuentra altamente expuesto [8].

Así mismo, Parra (2015) realizó un estudio sobre la importancia y la complejidad de la seguridad de la información a nivel global, puesto que ésta se posiciona como el activo más importante para una organización, advirtiendo sobre la poca o nula conciencia que países, empresas y personas tiene sobre este aspecto, razón por la que organizaciones públicas y privadas carecen de seguridad suficiente para protegerla [9].

Por otro lado, Zambrano (2019) realizó un estudio sobre la relación que existe entre la falta de conciencia y la seguridad de la información, afirmando que la mayor cantidad de los ciberataques se llevan a cabo aprovechándose del poco conocimiento de las personas en este aspecto, puesto que la información, aseguró, representa un capital muy importante y una parte vital del rendimiento y rentabilidad de las organizaciones, por lo que debe ser

gestionada y protegida, debiendo trabajarse a nivel de usuario, siendo este último el punto más vulnerable de la red [10].

Esto es corroborado por Safa, Sookhak, Von Solms, Furnell, Ghani y Herawan (2015) en en su proyecto de investigación en el que aplicaron como columna vertebral la Teoría de la Motivación de Protección y la Teoría de la Conducta Planificada y, a través del modelado de ecuaciones estructurales, comprobaron que la conciencia de seguridad de la información, la política de organización de seguridad de la información, la experiencia y la participación en la seguridad de la información, la actitud hacia la seguridad de la información, la evaluación de amenazas y la autoeficacia de la seguridad de la información, entre otros, tienen un efecto positivo en los usuarios quienes, según señalaron, son un factor importante en este ámbito [11].

1.3.1.1.2 Sobre la importancia de un SGSI

Tewamba, Kamdjoug, Bitjoka, Wamba, y Bahanag (2019) realizaron una investigación que reveló que un SGSI (en relación a calidad del sistema, servicio e información, nivel de madurez del proceso de gestión de riesgos de seguridad de la información) y el desempeño de la organización están directamente relacionados por un lado, e indirectamente por las capacidades de las Tecnologías de la Información de la organización por el otro. Esto demuestra que un SGSI es crucial para una organización, porque contribuye en gran manera al desempeño organizacional y mejora el soporte de sistemas de información tales como la gestión, habilidades personales e infraestructura de TI[1]. Las hipótesis fueron aprobadas por la técnica PLS-SEM[2] utilizando los datos recopilados de las encuestas realizadas a 136 profesionales de SI[3] y TI [12].

Por su parte, Flyktman (2016) realizó una investigación cuyo objetivo radicó en encontrar la cohesión en aspectos como el interés por la seguridad, el liderazgo y el desempeño organizacional. Para ello utilizó los datos de la investigación, recopilados durante varios años a partir de la literatura, principalmente en los campos de la administración, las ciencias militares, la seguridad de la información y las ciencias del comportamiento; esta investigación permitió concluir que es necesario tener en cuenta un Sistema de Gestión de Seguridad de la Información (SGSI) al formar los procesos de la empresa [13].

---

[1] TI: Tecnologías de la Información.
[2] PLS-SEM: (*Partial least squares – structural equation modeling*, Modelo de ecuaciones estructurales a través de mínimos cuadrados parciales, por sus siglas en inglés).
[3] SI: Sistemas de Información.

1.3.1.2 Antecedentes nacionales

1.3.1.2.1 Sobre la importancia de la seguridad de la información

Chilán y Pionce (2017) expusieron los referentes teóricos conceptuales con respecto a la seguridad de la información, recalcando que la información es uno de los principales recursos de las organizaciones y, por tanto, debe protegerse de todas las amenazas potenciales que puedan comprometer a la organización [14].

De igual modo, Hernández y Naranjo (2016), advirtieron sobre la importancia de la seguridad de la información, considerando a esta última como el aspecto más importante de una organización, indispensable para su funcionamiento y, consecuentemente, el punto determinante para el fracaso de una organización si se ve vulnerada. Por ello, diseñaron un plan estratégico de seguridad de información en una empresa del sector comercial [15].

Por otro lado, Flores (2018) realizó un análisis acerca del entendimiento sobre la importancia de la seguridad de la información por parte de usuarios de TI que han superado los 45 años de edad, que incluyó entrevistas que revelaron las falencias de conocimiento en materia de seguridad de la información de estos usuarios en Ecuador, contrastando con los trabajos de investigación que se han realizado en otros países de Sudamérica sobre esta problemática. Esto permitió que proporcione recomendaciones y lineamientos para ayudar a este segmento de la población en este tema, acorde a las vulnerabilidades halladas [16].

1.3.1.2.2 Proyectos de SGSI realizados en instituciones públicas

Terán (2018) desarrolló una Guía para la implantación de un SGSI alineado a la norma ecuatoriana NTE ISO/IEC 27000, a fin de mejorar la seguridad de la información del servicio de agendamiento de citas del Ministerio de Salud Pública del Ecuador (MSP) [17].

De igual modo, Molina (2016) diseñó un SGSI para el área del Centro de Operaciones de Redes NOC de la Corporación Nacional de Telecomunicaciones CNT EP, en la agencia matriz Doral, en base a la norma INEN-ISO/IEC 27001:2012 [18].

Guamán y Moncayo (2016), por su parte, desarrollaron un modelo de SGSI basado en las mejores prácticas de seguridad de informática, cuyo enfoque estuvo dirigido al estado de los datos y la información en ese tiempo, en la Agencia de Regulación y Control Hidrocarburífero (ARCH), evidenciando los riesgos de seguridad de la información de la organización, en base a la norma 27001:2007 y al Acuerdo 166 de la Secretaría Nacional de Administración Pública (SNAP) de la República del Ecuador [19].

1.3.1.2.3 Sobre las metodologías MAGERIT y MEHARI

Holguín y Lema (2019) desarrollaron un modelo para medir la madurez del análisis de riesgo de los activos de información en el contexto de las empresas navieras, dentro del cual incluyeron un análisis de las metodologías MAGERIT, MEHARI y también OCTAVE. Este modelo de validez teórica, a través de categorías de evaluación definidas y pertinencia de buenas prácticas encontradas en las mencionadas metodologías, los llevó a concluir que éstas tienen características propias pero complementarias entre sí, permitiendo que puedan combinarse para obtener un análisis de riesgo más robusto [20].

1.3.2 MARCO CONCEPTUAL

1.3.2.1 Dato

Un dato es un extracto de la realidad [21], un hecho aislado [22], con significado y valor inherentes, construido en base a una forma de lenguaje, registrado en algún tipo de soporte [23] y que, al presentarse solo, fuera de un contexto, puede no generar significado ni valor adicional para quien lo recibe. Un número de cédula, o la cantidad de horas que se ha trabajado en la semana, son ejemplos de datos. Los datos pueden representarse de varias formas, dependiendo de su tipo, como se ve en la Tabla 1.1.

Tabla 1.1. Tipos de datos y su representación [22]

Tipo de dato	Representación
Alfanumérico	Números, letras y otros caracteres
De imagen	Imágenes, gráficas y fotos
De audio	Sonidos, ruidos y tonos
De video	Imágenes en movimiento

1.3.2.2 Información

Información es el conjunto de datos organizados de tal forma que adquieren un significado y valor para quien lo recibe, adicional al valor inherente que tienen por sí solos [22], siendo ésta capaz de causar un cambio de estado de conocimiento del receptor. Puede presentarse como texto escrito, imágenes o formas intangibles como conceptos, conocimientos, ideas, marcas, etc.

La información puede clasificarse por niveles de importancia acorde a la utilidad o valor que tengan para una entidad, que puede verse reflejada en la forma en que sea capaz de

comprometer la marcha de una organización si es revelada indebidamente, manipulada, degradada o se pierde parcial o totalmente. Es el propietario de la información quien le atribuye un valor, independientemente de la forma en que ésta se encuentre presentada, almacenada o transmitida, de su origen o de la fecha en que fue generada [24].

La norma NTE INEN ISO/IEC 27001 [3] no establece en concreto cuáles son los niveles de clasificación de la información, pero deja a las instituciones que definan, en base a un análisis, los niveles en los que clasificará la información; por ejemplo, qué y cuándo la información es confidencial, para uso interno o de carácter público, o si es crítica, sensible o de valor insignificante.

Una vez clasificada, es necesario establecer las acciones que se tomarán en cada nivel de categorización. Por ejemplo, si la información tiene un alto nivel de confidencialidad, debe haber procedimientos y controles que impidan el acceso a personas o entidades a las que no compete observar o manipular dicha información, que vele por que no sea adulterada indebidamente o que garantice al máximo que esté disponible cuando quien esté autorizado requiera de ella para llevar a cabo sus funciones.

1.3.2.3 Activo de información

Activo es todo aquello que tiene valor para la organización [7]. Debido al enfoque, activo de información es todo activo relacionado con la información, ya sea que la presente, la almacene, la transmita o le provea soporte [4] [5]; puede ser víctima de una amenaza, cuya acción degrade a la información según el nivel de dependencia que tenga de éste [5] y, por tanto, hay necesidad de protegerlo. La información en sí misma cuenta como un activo [7].

1.3.2.4 Informática

Informática, o “INFORmación autoMÁTICA”, es una ciencia que abarca un conjunto de técnicas y conocimientos científicos orientados al estudio del tratamiento de la información a través de ordenadores o “máquinas automáticas”. El ordenador es una máquina que realiza el procesamiento de datos de entrada a través de cálculos aritméticos y lógicos de forma automática, es decir, sin necesidad de la intervención del recurso humano, siguiendo el conjunto de instrucciones de un programa almacenado en su memoria. El resultado de dicho procesamiento se muestra finalmente en un dispositivo o medio de salida [25].

- ***Hardware***: Todo aquello del ordenador que es palpable. Comprende todo el soporte físico: cubierta externa del equipo, dispositivos electrónicos y electromecánicos, circuitería, cables, etc.

- ***Software***: Todo aquello del ordenador que es impalpable. Comprende todo el soporte lógico: programas, sistemas operativos, entornos de desarrollo, ofimática, bases de datos, etc.

1.3.2.5 Seguridad informática

Seguridad informática es un conjunto de medidas, técnicas, prácticas, métodos o controles [26] [27] [28] enfocados a la protección de la información que es almacenada, procesada y comunicada [29] en un sistema o medio informáticos [26] [27], en las dimensiones de confidencialidad, integridad y disponibilidad [26] [28].

1.3.2.6 Ciberseguridad

Según el Glosario de Términos de Seguridad de la Información de la NIST[4], Ciberseguridad es la capacidad de defender o proteger el uso del ciberespacio[5] de ciberataques, es decir, de ataques dirigidos al uso del ciberespacio por parte de una organización con el fin de interrumpir, deshabilitar, destruir o controlar malintencionadamente un entorno o infraestructura informática, robar la información o destruir la integridad de los datos [32]. Dicha capacidad abarca un conjunto de controles de seguridad y prácticas que protejan a los usuarios y demás activos de información cuando sea necesario el uso del ciberespacio [33].

1.3.2.7 Seguridad de la información

La Seguridad de la Información es una disciplina [34] enfocada en el resguardo y protección de la información [35], independientemente de su formato; es decir, de la forma, lugar, espacio, origen o fecha de generación en que es presentada, almacenada, procesada o transmitida. La Seguridad de la Información no solo engloba a los otros aspectos como la Seguridad Informática y la Ciberseguridad, sino que va mucho más allá al buscar garantizar también la seguridad de la información en otros formatos [27] [36], como cuando esta última se encuentra impresa en papel, almacenada en medios extraíbles u otros contenedores como el recurso humano, las instalaciones, etc., en las dimensiones principales de la seguridad: confidencialidad, integridad y disponibilidad [7] [36].

---

[4] NIST (*National Institute of Standards and Technology*), es uno de los laboratorios de ciencias físicas más antiguos de los Estados Unidos de Norteamérica y proporciona estándares orientados a productos y servicios que, de alguna manera, dependen de la tecnología [30].

[5] Ciberespacio: Un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de sistemas de información que incluye Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados [32].

1.3.2.7.1 Confidencialidad

Dimensión de seguridad de la información orientada a la protección de la información del acceso de agentes no autorizados; es decir, que pueda acceder a ella únicamente quien está autorizado.

1.3.2.7.2 Integridad

Dimensión de seguridad de la información orientada a la protección de la información de todo tipo de adulteración o modificación no autorizada; es decir, garantizar que la información se presente tal y como es.

1.3.2.7.3 Disponibilidad

Dimensión de seguridad de la información orientada a la protección de la información a fin de garantizar que pueda accederse a ella el momento en que ésta sea requerida y durante el tiempo en que sea requerida.

1.3.2.7.4 Amenaza

Todo evento o acción potencial, natural, accidental o deliberada, que pueda comprometer la seguridad de la información y degradarla en una o más dimensiones de seguridad, al explotar una vulnerabilidad. La amenaza puede ejercerse sobre un activo de información. Una amenaza de seguridad es descartable si no existe vulnerabilidad que pueda ser explotable por la misma.

1.3.2.7.5 Vulnerabilidad

Toda falencia o carencia de seguridad de la información en un activo, que pueda hacer posible la materialización de una amenaza potencial. Una vulnerabilidad es descartable si no existe una amenaza asociada a la misma.

1.3.2.7.6 Impacto

Nivel de daño que puede sufrir un activo de información en una dimensión de seguridad si una amenaza llega a materializarse al explotar una vulnerabilidad.

1.3.2.7.7 Probabilidad

Nivel de certeza de que una amenaza pueda materializarse, según los factores del escenario en que pueda llevarse a cabo.

1.3.2.7.8 Riesgo

El riesgo es el consenso entre el impacto y la probabilidad de que una amenaza pueda materializarse, y se calcula como el producto entre ambos factores. Para evaluar el riesgo deben considerarse los posibles escenarios [5] en los que puede desarrollarse una amenaza, ajustándolos a la realidad de la organización. Por ejemplo, al analizar una amenaza potencial, si la probabilidad de que ésta ocurra en un escenario específico es muy alta, pero el impacto que pueda causar es insignificante, el riesgo podría resultar muy bajo.

El riesgo se evalúa sin salvaguardas y con salvaguardas, a fin de verificar si el rendimiento de cada una justifica el costo de las mismas para la organización. El riesgo debe ser clasificado por niveles para que la organización tome las medidas que considere pertinentes. Puesto que la seguridad total es ideal, en el mejor de los casos se espera que el riesgo descienda hasta un nivel aceptable.

1.3.2.7.9 Salvaguarda

Medida de seguridad cuyo propósito es la mitigación del riesgo. Se descarta como salvaguarda a la medida que no produce mitigación alguna, o no esté amparada en una política de seguridad. Por ejemplo, el hecho de que el administrador de la red actúe bajo ética profesional y por buenos principios y valores no garantiza que la información esté asegurada si no existe una política regulatoria que pueda punir malas prácticas, dificultando así toda acción que pueda tomarse al no poder controlar la conducta de un segundo administrador, si éste viene como reemplazo del primero.

La salvaguarda se mide por el grado de eficacia de seguridad que pueda proporcionarle a un activo de información frente a una posible amenaza (a través de su factor de reducción), sea para prevenir (y reducir la probabilidad) o para corregir (y reducir el impacto).

- **Origen del control:** El control puede surgir de una de tres fuentes: a) políticas, normativas o procesos formalizados y documentados, b) por buenas prácticas, el empirismo o la experiencia, o c) por leyes, decretos o seguros.
- **Mecanismo de control:** Un mecanismo de control determina la forma en que se mitiga un riesgo. Puede ser cualquiera de dos: a) preventivo, cuya aplicación evita que la amenaza llegue a materializarse; o b) correctivo, cuya aplicación disminuye el daño cuando se ha materializado la amenaza [37].
- **Tipo de control:** Puede ser de cualquiera de tres tipos [38]:

- **Administrativo:** cuando la salvaguarda es aplicada, y está orientada a, las personas.
- **Técnico:** cuando la salvaguarda es de carácter tecnológico y está aplicada a contenedores de tipo técnico.
- **Físico:** cuando la salvaguarda está orientada al control de acceso físico y está aplicada a contenedores de tipo físico.

1.3.3 ORGANIZACIONES DE NORMALIZACIÓN Y REGULACIÓN

Una organización de normalización o estandarización es una entidad conformada por científicos y profesionales capacitados en áreas específicas, con el propósito de proporcionar y redactar normas que garanticen la calidad, seguridad y funcionamiento adecuado de elementos físicos, administrativos, técnicos y tecnológicos, sin descuidar la responsabilidad social, ambiental y económica. Debido a la continua evolución económica, tecnológica y social, a los hallazgos científicos recientes y al surgimiento de nuevos desafíos, estas organizaciones revisan, generan y actualizan constantemente las normas.

Dentro del campo de seguridad de la información, las organizaciones de estandarización proporcionan normas orientadas a garantizar un nivel aceptable de seguridad, que deben ser adaptadas por la institución que acoge dichas normas según su realidad institucional.

También están las organizaciones de regulación, como las instituciones gubernamentales competentes, que pueden adoptar normas internacionales o generarlas a nivel local y proporcionar disposiciones que debe cumplir toda institución que está bajo su control a fin de que exista coherencia con la realidad nacional.

1.3.3.1 Organización Internacional de Estandarización (ISO)

ISO (*International Organization for Standarization*) es una organización independiente, desligada de toda institución gubernamental, fundada en 1947, cuya Secretaría Central se encuentra en Ginebra, Suiza, y constituye una red global de organismos nacionales de estandarización. Hoy en día cuenta con miembros de 164 países [39].

Esta organización se dedica a la creación de documentos que proporcionan especificaciones, requerimientos, guías o características que pueden ser usadas por una organización para garantizar qué productos, materiales, procesos y servicios cumplen fielmente con el propósito con el que fueron creados, proveyendo con esto considerables beneficios en todo sector imaginable. Las normas desarrolladas brindan apoyo tecnológico que garantizan la calidad esperada [40].

Cada miembro representa a la ISO en su propio país, en una de tres categorías: En la categoría de *membresía completa* (u *organismos miembro*), los organismos tienen voto y participación en el desarrollo y estrategia de las normas ISO, y pueden adoptar y vender las normas ISO a nivel nacional. En la categoría de *miembros corresponsales*, los organismos actúan únicamente como observadores, pudiendo también vender y adoptar dichas normas a nivel nacional. En la categoría de *miembros suscriptores*, los organismos pueden mantenerse al día en el trabajo con las ISO, pero no pueden participar en él, ni vender o adoptar las ISO nacionalmente. [41] El Servicio Ecuatoriano de Normalización (INEN) es un miembro con *membresía completa*. [41] [42]

La ISO se organiza actualmente en 785 *Comités y Subcomités Técnicos* [39], los mismos que cumplen un rol específico de acuerdo al fin con el que fueron creados, dentro de 248 sectores hasta el momento [43]. El correspondiente al sector de interés, *Information Technology* (Tecnología de la Información), es el *Comité Técnico Conjunto JTC 1*.

1.3.3.2 Comisión Electrotécnica Internacional (IEC)

IEC (*International Electrotechnical Commission*) es una organización sin fines de lucro, cuasi-gubernamental, fundada en 1906 [44], cuya Oficina Central se encuentra en Ginebra, Suiza [45], y cuenta con un total de 86 miembros (países) alrededor de todo el mundo en la actualidad [46], con un único Comité Nacional (NC por sus siglas en inglés) por cada país miembro. Los NCs actúan como miembros dentro de la IEC, y cada miembro disfruta de beneficios de acuerdo con el nivel de membresía que posea dentro de la organización.

Como organización global, la IEC tiene como función el publicar normas internacionales que sirven como fundamento para la estandarización nacional, y como una referencia en la redacción de contratos y licitaciones a nivel internacional. Administra, además, sistemas de evaluación de conformidad para electrotecnología; es decir, para sistemas, productos y servicios eléctricos y electrónicos, con el fin de identificar el grado de cumplimiento de dichos elementos con la normativa establecida. [47]

Existen dos categorías, o niveles de membresía, en la IEC. La categoría de *membresía completa* comprende a los organismos (NCs) que tienen acceso a todas las actividades y funciones administrativas y técnicas, incluyendo el derecho total a voto y participación en cada reunión. Por otro lado, la categoría de *miembros asociados* comprende a los organismos (NCs) que tienen acceso a todo documento de trabajo, pero están limitados en cuanto al derecho de participación y voto en el trabajo técnico y no tienen ninguna opción de elección en la parte administrativa dentro de la organización [48].

Ecuador actúa como país afiliado, dentro del Programa de Países Afiliados a la IEC [42], fuera de ambas categorías de membresía.

La IEC cuenta además con la participación de *expertos* y *delegados* cuya actividad dentro de la institución representa un aporte importante, más no son considerados miembros o NCs. Los primeros son especialistas que actúan en un campo técnico en particular y son solicitados por cada NC para tomar parte en un trabajo técnico específico a través de grupos de trabajo, equipos de mantenimiento y equipos para gestionar proyectos; los segundos actúan como representantes de su Comité Nacional (NC) o Subcomité (SC) en las reuniones, y deben estar completamente informados por su NC antes de asistir, para poder ejercer su voz y voto en la toma de decisiones. [49]

1.3.3.3 Servicio Ecuatoriano de Normalización (INEN)

El Servicio Ecuatoriano de Normalización (INEN) es el organismo ecuatoriano encargado de la regulación, normalización, metrología y certificación técnica, adscrito al Ministerio de Industrias y Productividad [50]. Fue fundado como Instituto Ecuatoriano de Normalización el 28 de agosto de 1970 mediante Decreto Supremo No. 357, publicado en el Registro Oficial No. 54 del 7 de septiembre de 1970 [51]. Su sede principal se encuentra en la ciudad de Quito, capital de la República del Ecuador, teniendo direcciones zonales en Cuenca, Guayaquil y Riobamba [52].

Este organismo funge en la formulación de las Normas Técnicas Ecuatorianas (NTE), con el fundamento de satisfacer las necesidades del país y facilitar el comercio nacional e internacional [51]. El INEN, en colaboración con entidades gubernamentales, académicas e industriales, es responsable del desarrollo, publicación y promoción de estándares ecuatorianos y otros, contribuyendo a la economía nacional, desarrollo sostenible, salud, seguridad, tecnología, bienestar laboral y protección del consumidor, velando por la garantía de la calidad del sistema de producción y competitividad nacional, agregando el valor del talento humano y cumpliendo con los requisitos regulatorios y legales. [50]

El INEN tiene participación como miembro con nivel de *membresía completa* dentro de la ISO [41] [42] y como país afiliado a la IEC [42].

El nombre NTE INEN ISO/IEC en cada una de las normas ecuatorianas proporciona una breve descripción de la norma adoptada como Norma Técnica Ecuatoriana (NTE) por el Servicio Nacional de Normalización (INEN), del sistema internacional de estandarización conformado por la Organización Internacional de Estandarización y la Comisión Electrotécnica Internacional (ISO/IEC), seguido de la numeración de la norma específica.

1.3.3.4 Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)

El Ministerio de Telecomunicaciones y de la Sociedad de la Información es una entidad del Estado ecuatoriano, creada el 13 de agosto de 2009, mediante Decreto Ejecutivo Nro. 8 [53], encargada de la regulación del desarrollo de las TICs[6] dentro del territorio ecuatoriano. Esta entidad emite políticas, normativas y planes generales que deben ser implementadas por las instituciones, dentro de las cuales está el Ministerio de Cultura y Patrimonio. Lleva un seguimiento y evaluación periódica de la implementación de dichas disposiciones, a fin de que, en coordinación con los actores de los sectores estratégicos, se garantice el acceso a los servicios de forma igualitaria y se promueva el uso efectivo de los mismos [54].

El MINTEL, como ente regulador, y en función de sus objetivos, trabaja con entidades adscritas a éste, velando por asegurar el funcionamiento correcto de éstas [55] [56]:

- **ARCOTEL:** Agencia de Regulación y Control de las Telecomunicaciones, creada el 18 de febrero de 2015 con la Ley Orgánica de Telecomunicaciones [57], es la entidad encargada del control y regulación de los servicios de telecomunicaciones, así como de la designación de frecuencias del espectro radioeléctrico.
- **DINARDAP**: Dirección Nacional de Registro de Datos Públicos, entidad encargada, junto con otras, del Sistema Nacional de Registro de Datos Públicos[7], que incluye normas técnicas; su propósito es garantizar el acceso y transparencia de datos e información públicos. Dentro de las instituciones que publican en el portal está el Ministerio de Cultura y Patrimonio, de entre un gran número de instituciones.
- **CNT-EP:** Corporación Nacional de Telecomunicaciones - Empresa Pública, creada el 14 de enero de 2010, como empresa pública por decreto presidencial [58]. Provee servicios convergentes de telecomunicaciones y TICs, tales como telefonía fija, local e internacional, acceso a Internet fijo y móvil y televisión satelital.
- **DIGERCIC:** Dirección Nacional de Registro Civil, Identificación y Cedulación, creada el 29 de octubre de 1900 [59]. Es la encargada de la emisión de certificados electrónicos, cedulación, inscripciones de nacimiento, reconocimientos, etc.
- **ARCPostal:** Agencia de Regulación y Control Postal, creada el 7 de octubre de 2015 [60]. Es la entidad encargada de la regulación y administración de los servicios postales.

---

[6] TICs: Tecnologías de la Información y Comunicación.
[7] Dentro de este sistema se encuentran instituciones públicas, la información pública de instituciones privadas, normas, instrumentos, procesos, etc.

- **CDE-EP:** Correos del Ecuador – Empresa Pública, entidad creada el 2 de mayo de 1831 [61]. Brinda al país servicios postales, envíos y recepciones de paquetería. A partir del 19 de mayo de 2020, con el Decreto Ejecutivo 1056 [62], se dispuso la extinción de esta empresa, pero en el Decreto Ejecutivo 1123 [63], dado el 6 de agosto de 2020, se reformó el decreto anterior, indicando que la Administración de esta empresa continuará brindando el Servicio Postal Universal, hasta la designación del nuevo operador postal.

1.3.4 NORMAS Y ESTÁNDARES

Los términos "norma" y "estándar" se usan comúnmente como sinónimos, aunque el primero parece tener una connotación más estricta que el segundo. Según el DRAE[8], una de las acepciones de norma es "regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.", y una de las acepciones de estándar es "que sirve como tipo, modelo, norma, patrón o referencia". Se puede ver que, en la acepción del segundo término, éste es catalogado como norma en un sentido más estricto, pero también como una referencia, en el sentido menos estricto.

Las normas consideradas para la gestión de seguridad de la información en la Planta Central del Ministerio de Cultura y Patrimonio son las de la familia ISO 27000, adaptadas y traducidas idénticamente de las normas internacionales de la familia ISO/IEC 27000 por el INEN, que se enlistan a continuación:

- NTE INEN ISO/IEC 27000: 2016 [7]
- NTE INEN ISO/IEC 27001: 2013 [3]
- NTE INEN ISO/IEC 27002: 2013 [4]
- NTE INEN ISO/IEC 27005: 2012 [5]

Además, debido a que en este aspecto el Ministerio de Cultura y Patrimonio está regulado por el MINTEL, deben seguirse y adaptarse los lineamientos establecidos en el Acuerdo Ministerial No. 025-2019 [64], a través del cual se expone el Esquema Gubernamental de Seguridad de la Información (EGSI), versión 2.0.

1.3.4.1 Familia ISO/IEC 27000

La familia ISO/IEC 27000 está conformada por un conjunto de normas en desarrollo y mejora continua por la ISO y por la IEC, las cuales facilitan un marco de gestión de

[8] DRAE. Diccionario de la Real Academia Española.

seguridad de la información, que puede ser aplicado y utilizado en cualquier organización, independientemente de su tamaño, función y/o relación con otras instituciones.

1.3.4.2 ISO/IEC 27000: 2016

Dentro de la familia (o serie) 27000, la norma 27000 proporciona de manera general el propósito de la publicación, alcance y campo de acción de cada norma integrante. En ella se redactan todas las definiciones utilizadas en la serie [65] y se introduce a la importancia de la implementación de un SGSI en una organización. Fue publicada el 1 de mayo de 2009 como 1ra edición, revisada el 1 de diciembre de 2012 como 2da edición, el 14 de enero de 2014 como 3ra edición y en febrero de 2016 como 4ta edición. La norma técnica ecuatoriana correspondiente es la NTE INEN ISO/IEC 27000:2016 [7].

De acuerdo con la exigencia estatal y a la realidad institucional, las normas que se aplicarán dentro de la familia ISO/IEC 27000 serán: ISO/IEC 27001 [3], ISO/IEC 27002 [4] e ISO/IEC 27005 [5].

1.3.4.2.1 Resumen / estructura del documento

De manera general, la norma NTE INEN ISO/IEC 27000:2016 está estructurada por los siguientes elementos: prólogo, introducción, objeto y campo de aplicación, términos y definiciones, sistemas de gestión de seguridad de la información, familia de normas del SGSI, los anexos A y B de la norma, y la bibliografía. A lo largo del documento se han colocado pequeñas notas intermedias.

El documento comienza con un prólogo en el que se expone brevemente qué son y qué cumplen la ISO, el IEC y los JTC[9], siendo el JTC1 el encargado del campo de Tecnologías de la Información. Como introducción hace una descripción general del documento, indicando la importancia de un SGSI, y enlista las normas que conforma la serie 27000. Más adelante se indica el propósito de la norma y su campo de aplicación en organizaciones de todo tipo y tamaño. Además, proporciona un listado de 83 términos para los cuales se han descrito sus correspondientes definiciones.

En los apartados siguientes se desarrolla el tema del SGSI, su importancia y los beneficios que trae la adopción de la familia de normas SGSI para la organización. Cubre temas como la seguridad de la información, tratamiento de riesgos y la necesidad de que la institución establezca su política y objetivos. Según describe la norma, deben implementarse

[9] JTC. Comité Técnico Conjunto, en español.

controles de seguridad y debe hacerse uso de formulación y procedimientos, directrices y políticas aplicables para la organización.

También plantea un enfoque basado en procesos. Este enfoque ha constituido un problema en el Ministerio de Cultura y Patrimonio puesto que, hasta la fecha no se han establecido procesos definidos, y los procesos sustantivos se encuentran en etapa de análisis y cambios. Esto último provocó la omisión del uso de este enfoque y, en su lugar, resultó necesario el diseño del SGSI de forma generalizada, según la realidad institucional.

Con mayor profundidad, describe los pasos que debe seguir una organización para el establecimiento, monitoreo, mantenimiento y mejoramiento del SGSI, la necesidad de identificar los requisitos de seguridad de la información y la importancia de definir un método para la evaluación de riesgos (recomienda el uso de la norma ISO/IEC 27005 como referente), el tratamiento que deba aplicarse a los riesgos, los controles (recomienda el uso de la norma 27002) y las acciones a incluirse en el proceso de mejora continua del SGSI. Proporciona ejemplos de factores críticos para el éxito del SGSI, a fin de que la organización aumente la probabilidad de alcanzar estos factores al implementar el SGSI.

El apartado de familia de normas del SGSI incluye una lista de normas clasificadas según su campo de aplicación y objeto, y las relaciones que hay entre ellas (Figura 1.1); Se enlistan y describen normas que especifican requisitos (ISO/IEC 27001 e ISO/IEC 27006),normas que proveen directrices generales (ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC TR 27008[10], ISO/IEC 27013, ISO/IEC 27014 e ISO/IEC TR 27016) y normas que proveen directrices específicas sectoriales (ISO/IEC 27010, ISO/IEC 27011, ISO/IEC TR 27015[11], ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019 e ISO/IEC 27799).

Incluye anexos al final del documento. En el Anexo A se aclara que, salvo por imposición legislativa o por contrato, nadie está obligado a aplicar las normas de la familia SGSI. En el Anexo B, aclara que el propietario del término en la familia ISO/IEC 27000 es aquella norma que define el término inicialmente, siendo responsable de su definición (provisión, revisión, actualización y retiro), y proporciona una lista de términos de algunas nomas utilizados en esta norma.

Finalmente, la bibliografía consta de referencias a las normas ISO e ISO/IEC.

---

[10] Esta versión está actualmente retirada. En su lugar está la norma ISO/IEC TS 27008:2019.
[11] Esta versión está actualmente retirada.

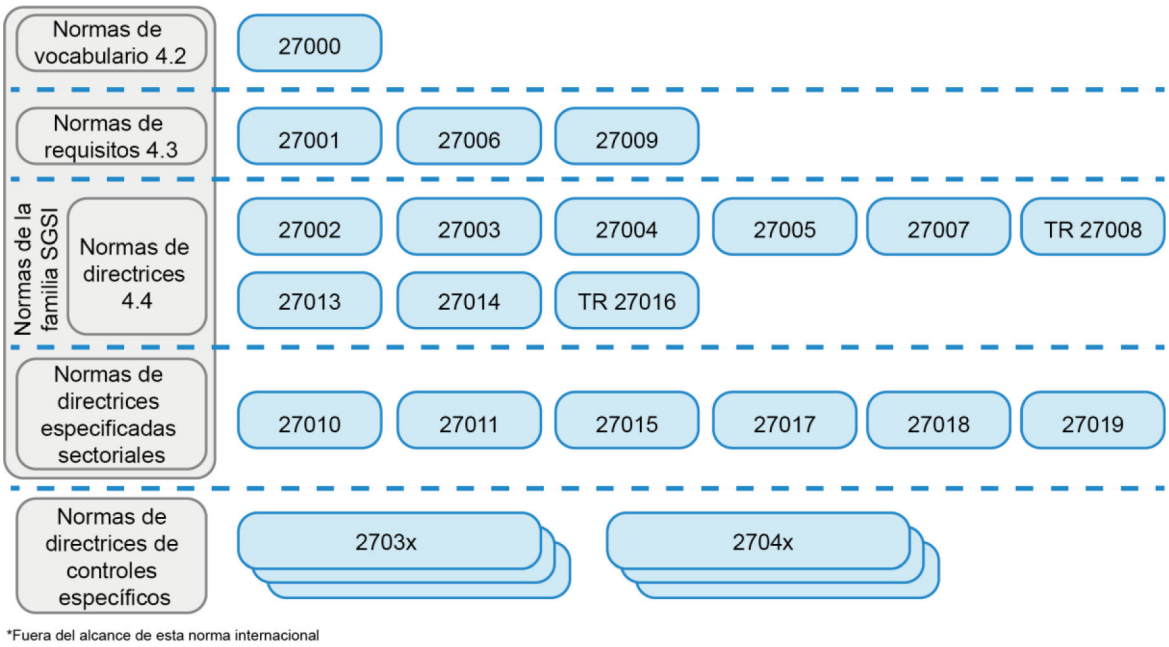


Figura 1.1. Relaciones entre las normas de la familia SGSI [7]

1.3.4.3 ISO/IEC 27001: 2013

La ISO/IEC 27001 es una norma desarrollada por el Comité Técnico Conjunto ISO/IEC JTC 1/SC 27, *Information Security, cybersecurity and privacy protection* (Seguridad de la Información, ciberseguridad y protección de privacidad), con el título "Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requerimientos" (título original en inglés, "Information technology - Security techniques - Information security management systems - Requirements"). [66] La norma técnica ecuatoriana correspondiente es la NTE INEN ISO/IEC 27001:2013 [3].

Todos los requerimientos manifestados en la norma son genéricos, es decir, que se han desarrollado para que puedan ser utilizados en todo tipo de organización, sea grande o pequeña, sin importar su naturaleza, dejando a cada institución la decisión de adaptar dichos requerimientos a la realidad institucional. Cada organización puede optar por usar los requerimientos de la norma que considere importantes y prioritarios, pudiendo prescindir de aquellos que no considere aplicables dentro de su institución.

Los requisitos son especificados para establecer, implementar, dar mantenimiento y mejora continua a un Sistema de Gestión de Seguridad de la Información, incluyendo otros para evaluación y tratamiento de riesgos de seguridad de la información según la realidad institucional [66].

La norma ISO/IEC 27001 se centra en el concepto de un SGSI, el mismo que constituye un proceso sistemático, debidamente documentado, difundido y conocido en toda la organización [67]. Este documento hace referencia a directrices de la norma ISO 31000, más no deben tomarse como obligatorias debido a que en la referencia consta como nota.

La gestión de la seguridad de la información no se acota únicamente a la seguridad de tecnologías de la información, sino que abarca a todas las áreas pertenecientes a la institución.

1.3.4.3.1 Resumen / estructura del documento

La norma NTE INEN-ISO/IEC 27001:2013 consta de los siguientes elementos: prólogo nacional, prólogo, introducción, objeto y campo de aplicación, referencias normativas, términos y definiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño, mejoras, anexo A y bibliografía. También se han colocado notas intermedias.

El documento se presenta como una traducción idéntica a la norma internacional ISO/IEC 27001:2013, y da una breve explicación sobre la participación de los organismos nacionales en el sistema especializado de normalización mundial ISO/IEC. Se aclara que esta versión sustituye a la versión 27001:2005.

Como introducción expone de forma general su propósito, y recalca sobre la importancia de establecer un SGSI y su aplicación a partes internas o externas, para dar cumplimiento con los requerimientos de seguridad de la información institucional. Expone, además, la compatibilidad con otras normas de SGSI que han adoptado el Anexo RL[12]. Más adelante, En el apartado de objeto y campo de aplicación se explica el propósito de la norma de especificar requisitos genéricos de establecimiento, implementación, mantenimiento, mejora continua de un SGSI y tratamiento de riesgos. Para los términos y definiciones, se hace referencia a la aplicación de los establecidos en la norma ISO/IEC 27000.

La norma enfatiza en la necesidad de la organización de comprender el contexto en el que se encuentra (hace referencia a la ISO 31000 sobre el establecimiento del contexto interno y externo) y las necesidades y expectativas de las partes interesadas. Es deber de la

[12] El Anexo RL o “estructura de alto nivel”, se constituye como marco de referencia para un sistema de gestión genérico, que permite la integración, sincronización y combinación de las normas a través de una estructura común. En 2019 cambió el nombre a Anexo K.

organización determinar y documentar el alcance del SGSI al implementarlo acorde con los requisitos de esta norma.

En el apartado de liderazgo se hace hincapié del compromiso y deberes que tiene la alta dirección de la organización con el SGSI y con la Política de Seguridad de la Información y las características principales que debe tener para ser apropiada en la organización.

El apartado de planificación trata de las acciones para abordar los riesgos y oportunidades, los objetivos de seguridad de la información y la planificación para alcanzarlos. Aborda la necesidad de definir y aplicar un proceso de apreciación de riesgos que incluya criterios que permitan obtener resultados consistentes, y con el que se identifique, analice y evalúe los riesgos de seguridad de la información. Este proceso debe documentarse debidamente.

El apartado de soporte expone sobre la obligación de la organización de determinar y proporcionar recursos para dar cumplimiento al SGSI, de asegurarse de que el personal sea competente en el desempeño de sus responsabilidades, sea concientizado sobre su papel dentro del SGSI y sea comunicado de todo lo concerniente al SGSI. Este proceso debe estar debidamente documentado.

El apartado de operación señala que debe existir planificación y control operacional, que incluya la implementación de controles necesarios para cumplir con los requerimientos de seguridad de la información, la apreciación de riesgos en los tiempos que se haya definido y el tratamiento respectivo de los riesgos. Esto debe documentarse apropiadamente

La organización tiene la responsabilidad de planificar y determinar la forma y tiempos en que debe monitorearse, medirse, analizarse y evaluarse el desempeño del SGSI, y de llevar a cabo auditorías internas. Adicionalmente, en el proceso de mejora debe incluirse la no conformidad y acciones correctivas necesarias, revisando la eficacia de éstas y realizando cualquier cambio al SGSI cuando sea necesario, para así mejorar de manera continua la eficacia, idoneidad y adecuación del SGSI.

El Anexo A constituye el elemento más extenso de esta norma. Contiene objetivos de control y controles enumerados en una tabla, alineados con los de la norma ISO/IEC 27002:2013 (capítulos del 5 al 18), utilizados en el contexto de tratamiento de riesgos de seguridad de la información. La Figura 1.2 muestra la estructura de la Tabla A.1 del Anexo A, conformada por los capítulos correspondientes a la ISO/IEC 27002, las categorías de cada uno y los objetivos de control y controles de seguridad de cada categoría.

Finalmente, la bibliografía referencia a algunas normas pertenecientes a la ISO y al conjunto ISO/IEC.

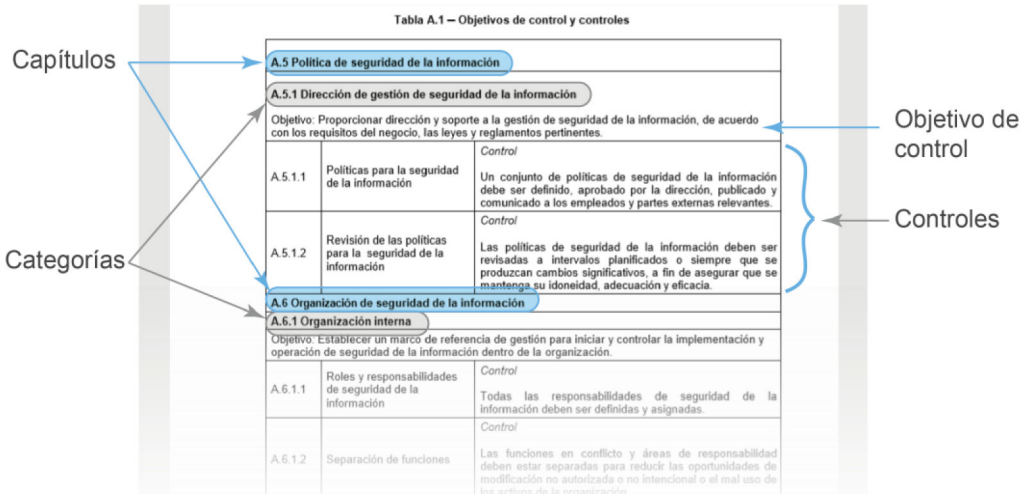


Figura 1.2. Estructura de la Tabla A.1 del Anexo A de la ISO/IEC 27001:2013 [3]

1.3.4.4 ISO/IEC 27002: 2013

La ISO/IEC 27002 es una norma desarrollada por el Comité Técnico Conjunto ISO/IEC JTC 1/SC 27, *Information Security, cybersecurity and privacy protection* (Seguridad de la Información, ciberseguridad y protección de privacidad), con el título "Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información." (título original en inglés, "*Information technology — Security techniques — Code of practice for information security controls*"). [68] La norma técnica ecuatoriana correspondiente es la NTE INEN ISO/IEC 27002:2013 [4].

Esta norma proporciona directrices para los estándares de seguridad de la información, en las que se incluyen la selección e implementación de controles de seguridad de un sistema de seguridad de la información basado en la norma ISO / IEC 27001, según los escenarios de riesgo dentro del contexto de la organización, además de alentar a la organización a que desarrolle sus propias pautas de gestión de seguridad de la información [68].

1.3.4.4.1 Resumen / estructura del documento

El documento ISO/IEC 27002:2013 está conformado por: prologo nacional, prólogo, introducción, objeto y campo de aplicación, referencias normativas, términos y definiciones, estructura de la norma, políticas de seguridad de la información, organización de la seguridad de la información, seguridad en recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad en las comunicaciones, adquisición, desarrollo y mantenimiento del sistema, relaciones con proveedores, gestión de incidentes de seguridad de la información,

aspectos de seguridad de la información para la gestión de la continuidad del negocio, cumplimiento y bibliografía.

Este documento se presenta como una traducción idéntica de la norma internacional correspondiente, salvo ciertos términos adaptados. Este documento reemplaza a la versión 27002:2005.

El documento manifiesta que esta norma fue creada como referencia en la selección de controles de seguridad de la información de un SGSI basado en la norma ISO/IEC 27001, o como guía de controles comúnmente aceptados; además, se habla sobre los antecedentes y contexto (que incluyen amenazas de seguridad y la necesidad de controles), los requisitos de seguridad, la libertad de la organización de adoptar los controles propuestos en esta norma y/o desarrollar sus propias directrices, la consideración del ciclo de vida de los activos y su posible retiro. Tanto en el apartado de referencias normativas como en el de términos y definiciones se hace referencia a la ISO/IEC 27000.

También se describe la estructura de la norma, misma que regirá para los apartados siguientes, conocidos como capítulos (14 capítulos en total), del capítulo cinco al capítulo dieciocho, de la siguiente manera:

- **Capítulo:** conformado por una o más categorías de controles de seguridad. Hay 14 capítulos. El primero de los 14 capítulos comienza con la numeración 5, y el último con la numeración 18.
- **Categoría de control:** conformado por un objetivo de control y uno o más controles. Hay, en total, 35 categorías.
    - **Control:** define el control con que se pretende alcanzar el objetivo. Hay 114 controles en total.
    - **Guía de implementación:** que detalla la forma en la que se puede llevar a cabo el control, pudiendo no ser apropiado o suficiente en todos los casos si no se ajusta a los requisitos de la organización.
    - **Otra información:** proporciona información adicional, que puede incluir referencias a otras normas o a consideraciones legales.

Finalmente, en la bibliografía se hace referencia a normas pertenecientes de la ISO y al conjunto ISO/IEC.

1.3.4.5 ISO/IEC 27005: 2012

La ISO/IEC 27005 es una norma desarrollada por el Comité Técnico Conjunto ISO/IEC JTC 1/SC 27, *Information Security, cybersecurity and privacy protection* (Seguridad de la

Información, ciberseguridad y protección de privacidad), con el título “Tecnología de la información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información.” (título original en inglés, “*Information technology — Security techniques — Information security risk managemen*t”) [69]. La Norma técnica ecuatoriana correspondiente es la NTE INEN ISO/IEC 27005:2012 [5].

Esta norma provee directrices acordes a la norma NTE INEN-ISO/IEC 27001 orientadas a la gestión de riesgos de seguridad de la información, aunque lo hace de manera genérica; es decir, no se especifica ninguna metodología de gestión de riesgos de seguridad de la información, dando paso a que sea la propia organización la que defina la metodología conveniente, acorde a la estructura de esta norma. La organización tomará esta decisión según su enfoque, el alcance de su SGSI, el contexto en que se desenvuelve y los riesgos de seguridad de información que ambiciona mitigar [5].

Esta norma es aplicable para toda organización, independientemente de su tamaño o naturaleza. Es importante conocer las terminologías, conceptos y modelos que se describen en las normas ISO/IEC 27001 e ISO/IEC 27002 [69].

1.3.4.5.1 Resumen / estructura del documento

El documento está dividido en los siguientes elementos: antecedentes, introducción, alcance, referencias normativas, términos y definiciones, estructura de la norma, información general, visión general del proceso de gestión de riesgo de seguridad de la información, establecimiento del contexto, valoración del riesgo de seguridad de la información, tratamiento del riesgo de la seguridad de la información, aceptación del riesgo de la seguridad de la información, comunicación de los riesgos de la seguridad de la información, monitoreo y revisión del riesgo de la seguridad de la información, anexos A, B, C, D, E y F de la norma, bibliografía y apéndice Z.

El documento indica de forma general el propósito de la norma de servir como un referente en la gestión de riesgos de seguridad de la información, aclarando que la organización debe definir su enfoque para la gestión de riesgos. Se advierte que el documento es pertinente para directores y personal involucrado en la gestión de riesgos de seguridad de la información, incluyendo a partes externas cuando sea necesario. Señala, además, que su finalidad es suministrar directrices de riesgo de seguridad de la información, y que su campo de aplicación cubre a todo tipo de organización.

Tanto en las terminologías como en las referencias normativas se hace referencia a las normas NTE INEN ISO/IEC 27001 y NTE INEN ISO/IEC 27002. En términos y definiciones

se referencia a las mismas, a más de los siguientes términos: impacto, riesgo de la seguridad de la información, evitar el riesgo, comunicación del riesgo, estimación del riesgo, identificación del riesgo, y los relacionados con el tratamiento de riesgos.

Como información general, la norma indica la importancia de un enfoque sistemático para la gestión de riesgos de seguridad de la información y de la creación de un SGSI alineado a las necesidades de la organización, debiendo ser un proceso continuo, aplicable a toda la organización, a través de un plan de tratamiento, a fin de implementar decisiones y recomendaciones necesarias para reducir el riesgo hasta un nivel aceptable.

La norma expone una visión general de los procesos de gestión de riesgos de seguridad de la información, mismos que son detallados en los siguientes numerales, siguiendo un enfoque iterativo en las actividades de valoración o tratamiento del riesgo, como se muestra en la Figura 1.3, a fin de economizar el tiempo y el esfuerzo, así como garantizar que los riesgos altos sean valorados adecuadamente.

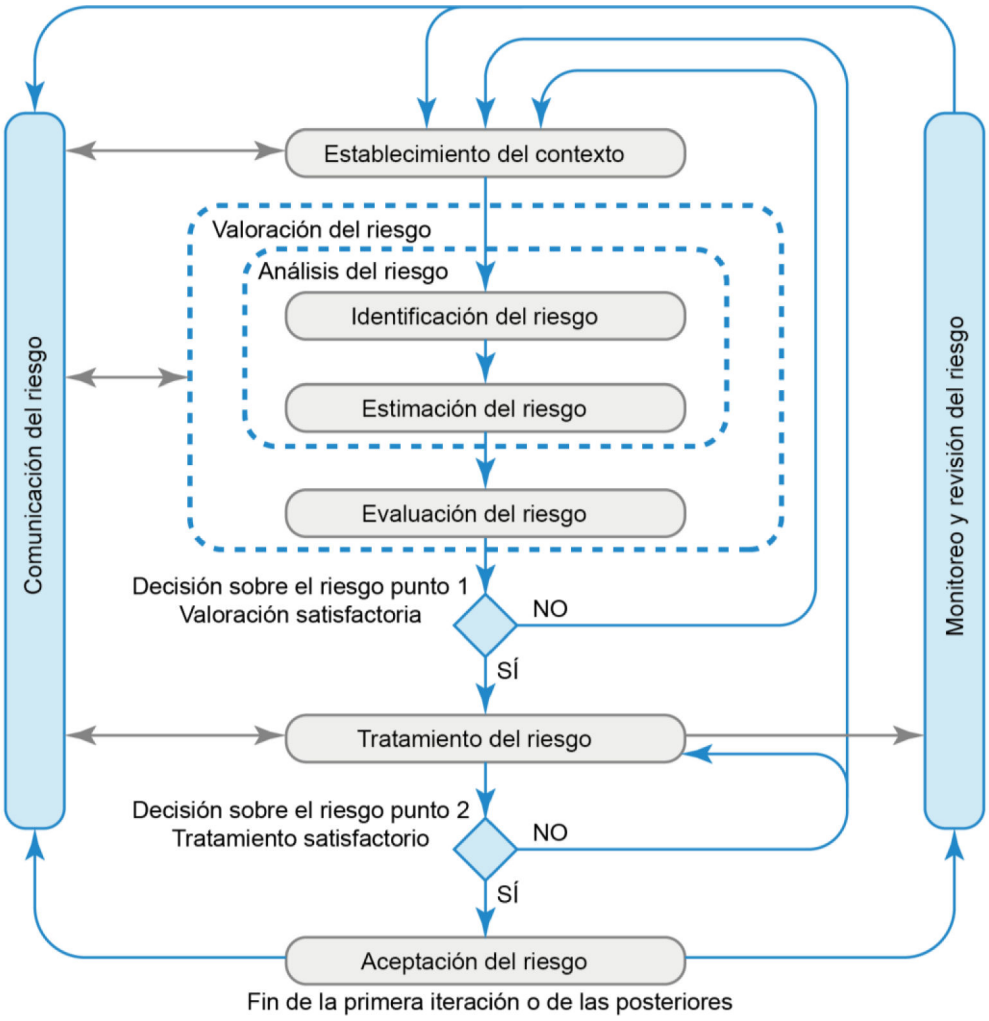


Figura 1.3. Proceso de gestión del riesgo de la seguridad de la información. [5]

Dentro del establecimiento del contexto, la norma expone las consideraciones generales, los criterios básicos con la aplicación de un enfoque adecuado para la gestión del riesgo que considere criterios de evaluación del riesgo, criterios de impacto y criterios de aceptación del riesgo, se advierte sobre la obligación de la organización de definir el alcance y los límites de la gestión de riesgos de seguridad de la información considerando los objetivos estratégicos, procesos, funciones y estructura del negocio, etc. Trata también sobre la organización para la gestión de los riesgos de seguridad de la información, misma que debe ser aprobada por los directores correspondientes en la institución.

Los apartados siguientes del documento tiene el siguiente esquema: entrada, acción, guía para la implementación y salida. También presenta el resumen de las cuatro fases dentro del proceso de gestión de riesgos de seguridad de la información (ciclo PDCA[13]) relacionados con el esquema de la Figura 1.3 y que se muestra en la Tabla 1.2.

Tabla 1.2. Alineamiento del SGSI y el proceso de Gestión de Riesgos [5]

Proceso del SGSI	Proceso de gestión de riesgos de seguridad de la información
Planificar (Plan)	Establecimiento del contexto.
	Valoración del riesgo.
	Planificación del tratamiento del riesgo.
	Aceptación del riesgo.
Hacer (Do)	Implementación del plan del tratamiento del riesgo.
Verificar (Check)	Monitoreo y revisión continua del riesgo.
Actuar (Act)	Mantener y mejorar el proceso de gestión del riesgo de seguridad de la información.

La etapa de valoración del riesgo de la seguridad de la información encierra dos etapas: la etapa de análisis del riesgo, que incluye la identificación del riesgo (identificación de activos, amenazas, controles existentes, vulnerabilidades y consecuencias) y la estimación del riesgo (a través de metodologías que permitan la estimación cualitativa o cuantitativa del riesgo), y la etapa de evaluación del riesgo.

Para la etapa de tratamiento del riesgo, la norma define 4 opciones (ver Figura 1.4): a) reducción del riesgo, según el accionar de los controles elegidos considerando restricciones financieras, técnicas, operativas, etc.; b) retención del riesgo, si satisface ciertos criterios para aceptarlo, evitando implementar controles adicionales; c) evitación del riesgo, si los riesgos son muy altos o los costos de implementación exceden a los

[13] PDCA: siglas correspondientes a las etapas del ciclo de un SGSI: *Plan* (Planificar), *Do* (Hacer), *Check* (Verificar) y *Act* (Actuar).

beneficios; y d) transferencia del riesgo, al compartir el riesgo con partes externas a través de, por ejemplo, seguros.

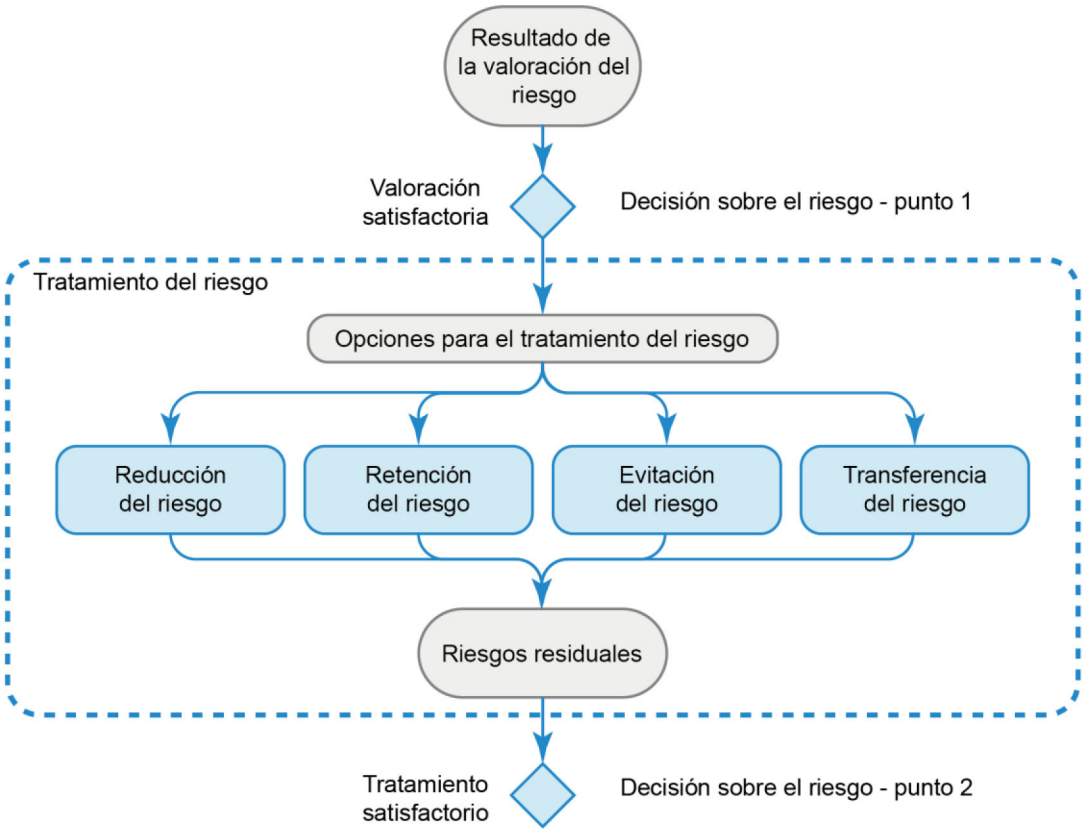


Figura 1.4. Actividad para el tratamiento del riesgo [5]

La norma señala que la aceptación del riesgo se realiza a través de una decisión registrada formalmente en base a criterios de aceptación, y justificada formalmente si se han omitido criterios de aceptación de riesgo en la toma de decisiones. Además, describe la actividad de comunicación como la compartición o intercambio de la información de los riesgos entre los encargados de la toma de decisiones y demás partes involucradas, de forma bidireccional, con el objeto de que haya compresión sobre las razones para las decisiones y acciones tomadas. Recomienda la creación de un comité en el que se pueda analizar, debatir y tomar decisiones sobre los riesgos, su prioridad, tratamiento y aceptación.

Debido a que los riesgos, amenazas, vulnerabilidades, probabilidad o impacto pueden cambiar de forma abrupta en cualquier momento, se enfatiza en la necesidad de que se realice el monitoreo y revisiones constantes del riesgo de seguridad de la información, puesto que esta actividad permitiría la detección de dichos cambios. El monitoreo, revisión y mejora continua de la gestión del riesgo debe abordar aspectos como el contexto legal, ambiental, de competencia, criterios de evaluación y aceptación del riesgo, etc.

Los anexos de la norma ocupan cerca de la mitad del documento, siendo el Anexo B el más extenso de todos. Estos son de carácter informativo, y proporcionan información detallada que puede tomarse como referencia en el diseño de un SGSI.

El Anexo A de la norma provee directrices para la definición del alcance y los límites del proceso de gestión de riesgo de seguridad de la información.

El Anexo B de la norma proporciona directrices para identificar y valorar activos e impacto, a través de ejemplos de clasificación de activos (primarios y de soporte), recomendaciones de valoración de activos proporcionando enfoques a considerarse, a través de escalas y grados de dependencia entre activos que acumulan sus valores, y finalmente recomendaciones de valoración de impacto, el cual puede ser inmediato (operacional, ya sea directo o indirecto), o tener un efecto a futuro financieramente.

El Anexo C de la norma proporciona ejemplos de amenazas comunes según su tipo y su origen, organizadas en una tabla, así como la fuente de éstas, la motivación que puede tener un atacante y las acciones amenazantes que puede tomar, organizadas en otra tabla.

El Anexo D de la norma provee ejemplos de vulnerabilidades correlacionadas con las amenazas comunes en una tabla, y sugiere la utilización de métodos para valorarlas.

El Anexo E de la norma proporciona enfoques para valorar los riesgos de seguridad de la información, que incluye ejemplos de matriz de riesgos, clasificación de amenazas, y determinación de probabilidad y consecuencias posibles de los riesgos.

El Anexo F de la norma recomienda la consideración de restricciones para la reducción de riesgos de diferentes tipos: de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, entre otras.

La bibliografía incluye referencias a normas ISO/IEC y de otras instituciones como la NIST.

El apéndice Z previene sobre los documentos normativos que deben consultarse, referenciando a las normas ISO/IEC 27001 e ISO/IEC 27002.

La NTE INEN ISO/IEC 27005 incluye información complementaria al final del documento, en el que constan los integrantes del Subcomité Técnico y la institución representada en Ecuador.

1.3.5 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información es importante porque permite la protección de la información de amenazas potenciales que pueden ponerla en riesgo

afectando su confidencialidad, integridad y disponibilidad. La gestión de riesgos de seguridad de la información debe adaptarse a la realidad institucional, por lo que es importante determinar qué es lo que se quiere proteger para otorgarle la seguridad que se espera.

1.3.6 ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

El Esquema Gubernamental de Seguridad de la Información (EGSI) es una disposición gubernamental documentada y enfocada a la seguridad de la información. Su propósito es conducir a las Instituciones de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID) del hacia el incremento y mejora de la seguridad de la información a través de la aplicación de procedimientos basados en estándares y normas técnicas de la familia ISO 27000, pertinentes a esta materia. Para el efecto, el EGSI proporciona un conjunto de directrices y recomendaciones para la gestión permanente de la seguridad de la información en cada organización, siendo obligatorio el implementar este esquema.

1.3.6.1 Versión 1.0

La Secretaría Nacional de Administración Pública (SNAP), actualmente extinta[14], considerando la importancia de la seguridad de la información en las instituciones públicas, tanto a nivel interno como interinstitucional, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011, respectivamente, a través de los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, conformada en su momento por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), la Secretaría Nacional de Inteligencia (Senain[15]) y la SNAP. Dicha comisión realizó un análisis de la situación en lo referente a la gestión de la seguridad de la información en las Instituciones de la APCID, estudio que reveló la necesidad de desarrollar y establecer el EGSI, versión 1.0 [70], basado en la norma técnica ecuatoriana NTE INEN ISO/IEC 27002, a través del Acuerdo Ministerial No. 166, de 25 de septiembre de 2013.

---

[14] La SNAP fue suprimida por Decreto Presidencial No. 5, emitido el 24 de mayo de 2017 [71].
[15] La Secretaría de Inteligencia (Senain) fue suprimida por Decreto Ejecutivo No. 526, el 21 de septiembre de 2018, y en su lugar se creó el Centro de Inteligencia Estratégica (CIES) como ente rector del Sistema Nacional de Inteligencia [72].

1.3.6.2 Versión 2.0

Mediante Decreto Ejecutivo No. 8, de 13 de agosto de 2009, se creó el MINTEL, como órgano rector del desarrollo de las TICs, incluyendo las telecomunicaciones y el espectro radioeléctrico. Con la supresión de la Senain y la SNAP, le corresponde al MINTEL ejercer como ente evaluador del estado de cumplimiento del EGSI. A través del Acuerdo Ministerial No. 025-2019 [64], de 20 de septiembre de 2019, se deroga el Acuerdo Ministerial No. 166, imponiéndose en su lugar el EGSI versión 2.0, basado en las normas técnicas ecuatorianas INEN ISO/IEC 27000.

1.3.6.3 Comparativa entre las versiones

En la Tabla 1.3 se exponen los aspectos en que se diferencia la versión actual de la versión anterior.

Tabla 1.3. Comparativa de las versiones del EGSI. [Elaboración propia]

Versión	Fecha expedición / entrada en vigor	Acuerdo Ministerial	Norma base	Emisor	Evaluador	Características
1.0	25-09-2013	166	NTE INEN ISO/IEC 27002	SNAP	MINTEL	Fases I: 126 hitos prioritarios. Fase II. No incluye directrices para elaborar la matriz de riesgos. El OSI[16] no puede pertenecer al área de TICs.
2.0	20-09-2019 / 13-01-2020	025-2019	Normas NTE INEN ISO/IEC 27000	MINTEL	MINTEL	Documento detallado, más elaborado y extenso. Directrices actualizadas. Incluye recomendaciones y ejemplos de aplicación en la elaboración de la matriz de riesgos. Incluye una Guía para la Implementación. [73] El OSI puede pertenecer al área de TICs.

1.3.7 METODOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN

Metodología es el estudio y validación de los métodos orientados a conseguir los objetivos planteados, dentro de un marco de investigación científica. Los métodos comprenden un conjunto de procesos o acciones racionales y ordenados, que persiguen la consecución del conocimiento científico, y la metodología conjunta un grupo de éstos, velando porque mantengan propiedades confiables dentro del trabajo de investigación. La aplicación de un

[16] OSI. Oficial de Seguridad de la Información.

método depende de la o las personas que, a través de su libertad valorativa, seleccionan el objeto de estudio, el sistema de conceptos y la forma en que se desarrollará la investigación. [74]

Las metodologías de seguridad de la información proveen procedimientos definidos y sistematizados, a fin de conseguir el aseguramiento de la información.

1.3.8 ELECCIÓN DE LAS METODOLOGÍAS DE REFERENCIA

Existen diversas metodologías de seguridad de la información, pero se ha decidido trabajar con MAGERIT[17] y MEHARI[18], pues ambas se alinean a las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, normas referenciales en este proyecto. MAGERIT se enfoca principalmente en la primera, y extiende su alcance con el uso de la norma ISO 31000 (alineada con la norma ISO/IEC 27001, sobretodo en el establecimiento del contexto de la organización y el tratamiento del riesgo), mientras que MEHARI declara explícitamente el uso de las tres primeras como los enfoques con los que se alinea y compatibiliza.

Como refuerzo para esta decisión, se ha tomado en cuenta el estudio realizado por Alemán y Rodríguez (2014). En el artículo señalan que las metodologías más relevantes de análisis de riesgos son OCTAVE, MAGERIT, MEHARI, NIST SP 800:30, CORAS, CRAMM y EBIOS, analizadas en un cuadro comparativo en el que se destacan sus ventajas y desventajas en cada ámbito de aplicación definido [75].

A partir de ese estudio, Holguín y Lema (2019) diseñan un modelo para medir la madurez del análisis de riesgo de los activos de información, acotando que las metodologías MAGERIT, MEHARI y OCTAVE son escogidas por encima de las demás debido a que su proceso de análisis de riesgo es análogo, y excluyen las otras metodologías porque, según indican, requieren un costo de licencia que las convierte en poco atractivas para su implementación [20].

Consecuentemente, y en base a los análisis mencionados, para este proyecto se escoge MAGERIT y MEHARI por su ámbito de aplicación enfocado principalmente a organizaciones gubernamentales, y se descarta OCTAVE debido a que está enfocado a principalmente a Pymes y, además, muestra más desventajas con respecto a los otros dos.

---

[17] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
[18] MEHARI: Methode Harmonisée d'Analyse de Risques - Método de Análisis de Riesgos Armonizado, en español.

1.3.9 METODOLOGÍA MAGERIT

MAGERIT es una metodología de gestión de riesgos de seguridad de la información, de origen español, desarrollada por el CSAE[19], acoplada principalmente a la norma ISO/IEC 27001 para el análisis y tratamiento de riesgos en su contexto (aunque hace referencia a la norma ISO 31000 como el esquema de gestión de riesgos estructurada a utilizar). Esta metodología, en su versión 3.0, se ha estructurado en tres libros:

- Libro I: Método [76].
- Libro II: Catálogo de elementos [77].
- Libro III: Guía de técnicas [78].

MAGERIT propone el uso de evaluaciones cuantitativas o cualitativas, para las cuales ha determinado métodos y fórmulas acorde con el enfoque con el que se decida trabajar.

1.3.9.1 Compatibilidad con las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005

1.3.9.1.1 Compatibilidad con la norma ISO/IEC 27001

MAGERIT se plantea como una metodología para el desarrollo de un SGSI, enmarcada en las cuatro etapas formalizadas del ciclo PDCA, de la norma ISO/IEC 27001 (se amplía el contexto de la organización con el uso de la norma ISO 31000).

1.3.9.1.2 Compatibilidad con la norma ISO/IEC 27002

MAGERIT sirve como el modelo de funcionamiento de la herramienta PILAR[20], utilizada como soporte en la aplicación de esta metodología. Una de sus funciones es el cálculo de calificaciones de seguridad en base a los lineamientos de la norma ISO/IEC 27002. En los libros de MAGERIT se toma a esta norma como referencia.

1.3.9.1.3 Compatibilidad con la norma ISO/IEC 27005

MAGERIT referencia a esta norma en la sección de técnicas específicas en el tercer libro de esta metodología. Además, el criterio de valoración de activos incluye el valor

---

[19] CSAE: Consejo Superior de Administración Electrónica, de España. Ha sido reemplazado por la Comisión de Estrategia TIC.

[20] PILAR: Procedimiento Informático-Lógico para el Análisis de Riesgos. PILAR es un software creado por el Centro Nacional de Inteligencia de España como soporte en la gestión de riesgos de seguridad de la información conforme a la metodología MAGERIT.

acumulado de los activos a través del grado de dependencias existentes entre éstos, tal como propone la norma ISO/IEC 27005 en su Anexo B.

1.3.9.2 Resumen

1.3.9.2.1 MAGERIT: Libro I – Método

Este documento está conformado por los siguientes elementos: introducción, visión de conjunto, método de análisis de riesgos, proceso de gestión de riesgos, proyectos de análisis de riesgos, plan de seguridad, desarrollo de sistemas de información, consejos prácticos, y seis anexos. El marco de trabajo de MAGERIT se resume en la Figura 1.5.

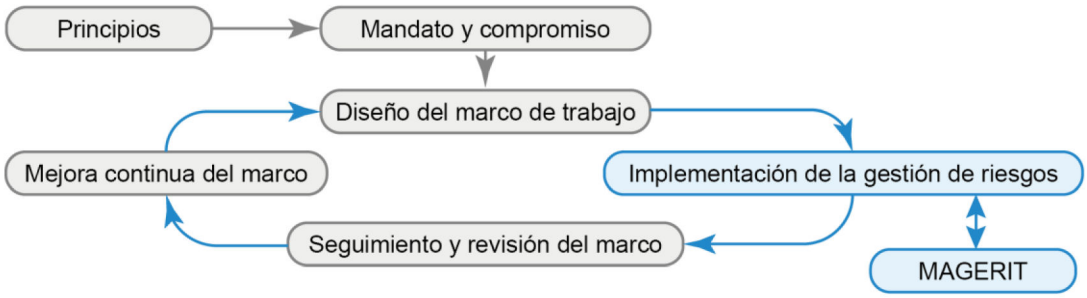


Figura 1.5. Marco de trabajo para la gestión de riesgos – MAGERIT [76]

En este libro se indica cómo están organizadas las guías de la metodología, el modo de empleo, un breve resumen del catálogo de elementos y la guía de técnicas, y la importancia del análisis de riesgos en los procesos de evaluación, certificación, auditoría y acreditación.

MAGERIT expone una visión del conjunto de dos tareas a realizar dentro de la gestión de riesgos: el análisis de riesgos y el tratamiento de los riesgos (Figura 1.6). Señala que el análisis de riesgos es la pieza clave para el control de todas las actividades con fundamento, y el tratamiento de riesgos es la fase que estructura las acciones para satisfacer los requisitos de seguridad detectadas durante el análisis.

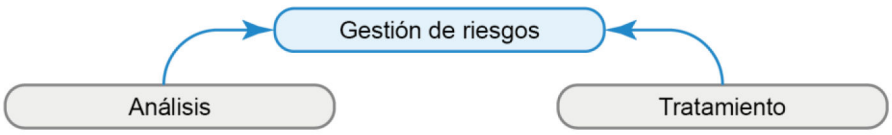


Figura 1.6. Visión de conjunto de gestión de riesgos – MAGERIT [76].

Se considera importante que haya una concienciación y formación del personal involucrado en el sistema de información (y especialmente que la seguridad sea practicada por la Dirección) en base a tres pilares: la Política de seguridad difundida y entendible por todos, la normativa de seguridad que aclare la postura de la institución en áreas específicas de

actividad, y la formación continua; además, es importante que todos puedan reportar y canalizar las incidencias de seguridad correctamente a quienes toman decisiones.

MAGERIT propone el Método de Análisis de Riesgos (MAR). Para este método hay que seguir una serie de pasos (Figura 1.7) (los pasos son tratados a detalle en el Libro III):

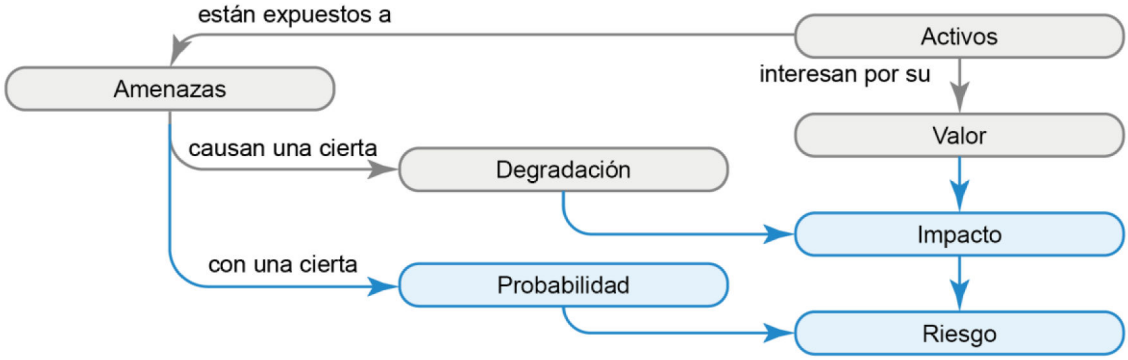


Figura 1.7. Elementos del análisis de riesgo potenciales – MAGERIT [76].

1. Determinar los activos relevantes para la institución, las dependencias existentes entre ellos, el valor propio y el valor acumulado de cada activo, las dimensiones en que serán valorados y el tipo de valoración (cuantitativa o cualitativa).
2. Determinar las amenazas que puedan causar degradación en el valor de un activo (y valorarse según el daño causado suponiendo que ocurre), el impacto acumulado, el impacto repercutido (considerando el valor propio del activo y las amenazas que actúan sobre los activos inferiores de los cuales depende) y el riesgo potencial (según el impacto y la probabilidad de ocurrencia del incidente causado por una amenaza); este último puede dividirse en zonas de riesgo (Figura 1.8): zona 1, riesgos con probabilidad e impacto muy altos; zona 2, riesgos de impacto moderado y probabilidad relativa; zona 3, riesgos con bajo impacto e improbables; y zona 4, riesgos con impacto muy alto pero improbables.

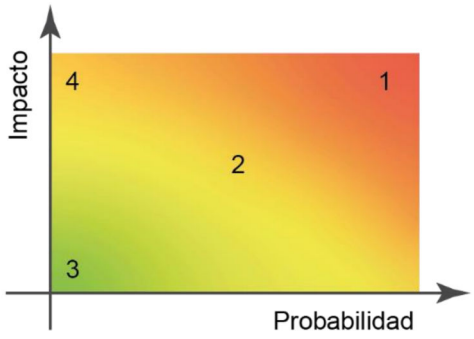


Figura 1.8. Riesgo en función del impacto y la probabilidad – MAGERIT [76].

El riesgo acumulado toma en cuenta el impacto acumulado y la probabilidad de la amenaza. El riesgo repercutido toma en cuenta el impacto repercutido y la probabilidad de la amenaza.

3. Identificar y seleccionar las salvaguardas existentes y determinar el efecto de éstas sobre el impacto (limitando el daño causado) o sobre la probabilidad (si previenen de la ocurrencia de la incidencia) como se muestra en el esquema de la Figura 1.9.

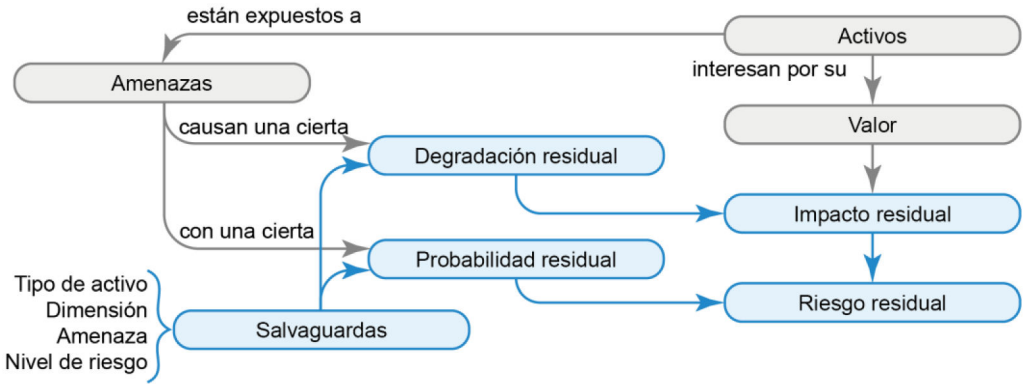


Figura 1.9. Elementos del análisis de riesgos residual – MAGERIT [76].

4. Calcular el impacto residual. El impacto residual es el remanente del impacto después del efecto de las salvaguardas, repitiendo el proceso de cálculo anterior, pero con el nuevo nivel de degradación.
5. Calcular el riesgo residual aplicando el mismo principio.

Las actividades deben formalizarse a través de las tareas MAR, que vienen especificadas tal como se muestra en la Tabla 1.4. MAGERIT provee un formato para documentarlas.

Tabla 1.4. Tareas a cumplir dentro del Método de Análisis de Riesgos (MAR) [76].

Tarea		Sub – tarea		Resultados
MAR. 1	Caracterización de los activos	MAR. 11	Identificación de los activos	Informe: Modelo de valor
		MAR. 12	Dependencias entre activos	
		MAR. 13	Valoración de los activos	
MAR. 2	Caracterización de las amenazas	MAR. 21	Identificación de las amenazas	Informe: Mapa de riesgos
		MAR. 22	Valoración de las amenazas	
MAR. 3	Caracterización de las salvaguardas	MAR. 31	Identificación de las salvaguardas pertinentes	Informes: Declaración de aplicabilidad (SoA), Evaluación de salvaguardas, Insuficiencias
		MAR. 32	Valoración de las salvaguardas	
MAR. 4	Estimación del estado de riesgo	MAR. 41	Estimación del impacto	Informes: Estado de riesgo, Insuficiencias
		MAR. 42	Estimación del riesgo	

Dentro del proceso de gestión de riesgos, la metodología describe las alternativas y criterios para el tratamiento de riesgos. Puede determinarse si un riesgo es crítico (atención urgente), grave (requiere atención), apreciable (objeto de estudio) o asumible (aceptable). De aquí se desprenden dos pasos sobre los que regirán las decisiones (Figura 1.10) de la dirección de la Institución: la evaluación y el tratamiento (incluyendo la aceptación) de riesgos. Debe ponerse especial atención a las vulnerabilidades si los valores residuales son iguales a los valores previos a las medidas de control.

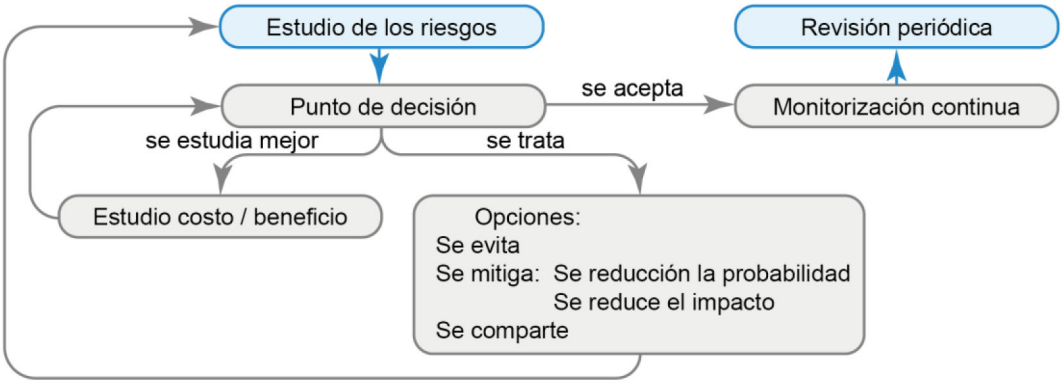


Figura 1.10. Posibles decisiones de tratamiento de riesgos – MAGERIT [76].

La dirección de la organización debe determinar y aceptar formalmente los niveles de impacto y riesgo aceptables. Para el tratamiento de riesgo deben tomarse dos grandes decisiones: reducir el riesgo residual (aceptando un menor riesgo) o ampliar el riesgo residual (aceptando un mayor riesgo), según las zonas de riesgo de la Figura 1.8. Un estudio cuantitativo de costo / beneficio en la implementación de las salvaguardas es clave para la toma de decisiones.

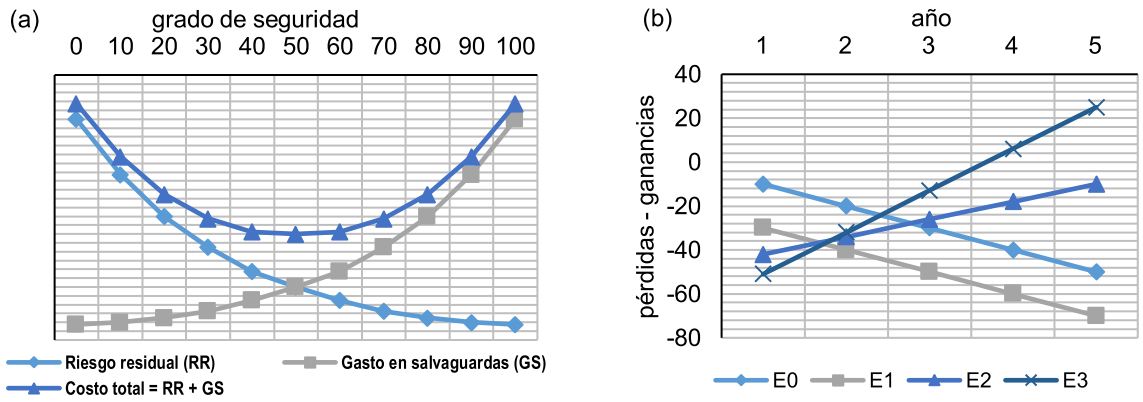


Figura 1.11. Estudios costo / beneficio. (a) Gasto en seguridad vs. Riesgo residual. (b) Ejemplo de decisiones de tratamiento de riesgos – MAGERIT [76].

Según MAGERIT, la gráfica (a) de la Figura 1.11, aunque parezca una opción lógica de estudio del costo / beneficio con equilibrio en el punto central, no es aplicable en la práctica;

en la gráfica (b), en cambio, se analizan escenarios (E_i) con diversas combinaciones de salvaguardas (valores negativos son pérdidas, y positivos, ganancias). E_0 representa el escenario en el que no se toman acciones. El más atractivo de todos es E_3 que, aunque inicialmente se hace un gran desembolso, a partir del año 5 se empiezan a percibir beneficios significativos. En un estudio cualitativo del costo / beneficio aparecen aspectos intangibles (como la reputación) que no pueden calcularse en un punto de equilibrio; por esto, un estudio mixto de dicha relación puede ser una opción.

El riesgo puede eliminarse, mitigarse, compartirse o financiarse (reservando fondos para responder a consecuencias si se acepta un riesgo). Las actividades en el proceso de gestión de riesgos deben ser formalizadas, a través de roles y funciones para jerarquizar y responsabilizar a los actores de la gestión de riesgos. Debe establecerse el contexto (externo e interno) en el que funciona la institución, y definirse criterios de valoración con umbrales de impacto, probabilidad, riesgo, etc.

Las medidas de seguridad, la normativa y la Política de Seguridad deben estar apoyadas por la Dirección, y deben ser claras, concisas y directas; debe haber un contacto permanente con la máxima autoridad, usuarios y técnicos de sistemas y los proveedores. Debe realizarse una monitorización permanente del sistema bajo indicadores clave de riesgo, que se lleva a cabo según las responsabilidades de los actores y sus roles en la seguridad de la información, incluyendo a los proveedores. El proceso debe documentarse internamente (definiciones y criterios de evaluación) y para otros (Plan de Seguridad). MAGERIT provee una lista de indicadores de control del proceso de gestión de riesgos.

En los Proyectos de Análisis de Riesgos (PAR) se toman 3 consideraciones: actividades preliminares, elaboración del análisis de riesgos y comunicación de resultados. En el transcurso de la puesta en marcha de un proyecto deben definirse roles específicos para llevarlo a cabo de manera efectiva. Las etapas del PAR se describen en la Tabla 1.5

Tabla 1.5. Tareas a cumplir dentro del Proyecto de Análisis de Riesgos (PAR) [76]

Tarea		Sub – tarea		Resultados
PAR. 1	Actividades preliminares	PAR. 11	Estudio de oportunidad	Informe: Preliminar
		PAR. 12	Determinación del alcance del proyecto	Perfil de proyecto de análisis de análisis de riesgos
		PAR. 13	Planificación del proyecto	Plan de trabajo para el proyecto, Procedimientos de trabajo
		PAR. 14	Lanzamiento del proyecto	Cuestionarios para las entrevistas, Catálogo del tipo de activos, Relación de dimensiones de seguridad, Criterios de valoración.
PAR. 2	Elaboración del análisis de riesgos			Documentación de las tareas
PAR. 3	Comunicación de resultados			Informe ejecutivo final

También expone la formalización de Planes de Seguridad (PS) a través de tareas. Estos planes de seguridad, al igual que en los procesos MAR y PAR, están especificados en un formato proporcionado por la metodología. Proporciona una lista de control para verificar el cumplimiento de las tareas.

Este libro incluye un capítulo centrado en el desarrollo de sistemas de información y la seguridad del proceso de desarrollo (SPD) desde su concepción hasta su puesta en producción. Formula un tratamiento sistemático y homogéneo para la gestión de la actualización y mejora de los sistemas, considerando que el análisis de riesgos debe ajustarse a las necesidades reales del sistema de información, y que cada modificación del sistema requerirá un nuevo análisis de riesgos en la fase de operación. Puede usarse MÉTRICA[21] versión 3 para sistematizar las tareas que deben cumplirse dentro del ciclo de vida del *software*, cubriendo todas las fases de este proceso.

Se proporcionan consejos prácticos a fin de esclarecer posibles problemas que suelen ser recurrentes durante el proceso de análisis de riesgos: el modelado de dependencias, valoración de activos y de amenazas, selección de salvaguardas, entre otros.

En el Apéndice 1 se expone un glosario de más de 50 términos (en español) en el que se definen términos y expresiones usados en, y relacionadas con, la seguridad de la información. Cada término y expresión cuenta con una o más definiciones tomadas de MAGERIT v2 o de otras fuentes con su respectiva cita. Incluye también una sección de términos anglosajones y su significado en español.

El Apéndice 2 contiene las referencias. El Apéndice 3 expone el marco legal alrededor del Proceso de Gestión de Riesgos. Las leyes y normativas mencionadas son las aplicadas en España.

El Apéndice 4 corresponde al marco de evaluación y certificación. Aquí se define lo que es un SGSI, sus 4 etapas dentro del ciclo PDCA y lo que es una certificación (y se aclara que en el caso de MAGERIT, la norma competente es la ISO/IEC 27001:2007). Se habla también de la credibilidad del certificado de acreditación y cómo se construye la confianza de éste. Se adiciona una terminología que incluye 12 términos y expresiones relacionadas con la acreditación y sus definiciones. Incluye aspectos de interés como requisitos de seguridad y uso de productos certificados.

---

[21] MÉTRICA es una metodología para sistematización del ciclo de vida de las aplicaciones, promovida por el antiguo Ministerio de Administraciones Públicas, España.

El Apéndice 5 proporciona información sobre las herramientas de soporte de la metodología, entre ellas PILAR.

El apéndice 6 hace una comparación de las versiones anteriores con la versión 3 de MAGERIT, indicando cambios y mejoras.

1.3.9.2.2 MAGERIT: Libro II – Catálogo de Elementos

Este documento está conformado por los siguientes elementos: introducción, tipos de activos, dimensiones de valoración, criterios de valoración, amenazas, salvaguardas, y cuatro anexos. A partir del capítulo 2, cada capítulo incluye un apartado de referencias.

El documento expone como finalidades el facilitar el análisis de riesgos para las personas involucradas, y el homogenizar los resultados del análisis a través de terminologías y criterios para comparar e integrar análisis llevados a cabo por diferentes equipos.

Aquí se explica sobre la tipificación de los activos y se proporciona un catálogo con los tipos de activos. Cada tipo de activo se especifica bajo un formato común, presentado como una tabla de columna única que contiene un campo con el nombre y una etiqueta con su identificador, un campo con los activos que entran en el tipo de activo, con sus respectivas etiquetas (incluyen números al final para esclarecerlos en el siguiente campo), y un campo con la descripción y definición de cada referencia indicada en el campo anterior. Un activo puede ser, al mismo tiempo, de varios tipos. Se incluye un apartado para publicar las clasificaciones, que incluye el uso del lenguaje de etiquetado XML.

En el libro se definen las dimensiones de valoración en las que se valorarán los activos. Se exponen las dimensiones canónicas de seguridad: disponibilidad [D], integridad de los datos [I] y confidencialidad de la información [C]. También se exponen las dimensiones derivadas: autenticidad [A] y trazabilidad [T]. Trata también sobre los criterios de valoración, recomendando el uso de una escala común y homogéneo para todas las dimensiones, y una escala logarítmica que permita relativizar las diferencias entre valores. Se proponen tablas con escalas estándar de valoración de activos. Se incluyen, como en el caso anterior, apartados para la publicación según XML.

Se proporciona un catálogo de amenazas clasificadas según su origen: natural [N], industrial [I], errores y fallos no intencionados [E] y ataques intencionados [A]. Dentro de cada origen de amenaza se han clasificado las amenazas, se especifican los activos que pueden verse afectados por éstas y las dimensiones a las cuales enfoca su impacto una amenaza particular, todo esto organizado en un formato común, que incluye una

descripción de la amenaza y una referencia a la amenaza equivalente en EBIOS[22]. Para la tipificación de las amenazas se incluye también su respectiva publicación en XML. Incluye una tabla de correlación entre amenazas y ataques, y la sintaxis y esquema para publicar nuevas amenazas o actualizaciones de las descritas previamente.

Se proporciona también un catálogo de salvaguardas, ordenadas y clasificadas según concreciones materiales, tecnológicas, organizativas o procedimentales. En el catálogo se muestran las agrupaciones de las salvaguardas por tipo de activo (al principio incluye salvaguardas generales), si corresponden continuidad de operaciones, si corresponden a externalización (relaciones externas, personal subcontratado, etc.) y por adquisición y desarrollo.

El Apéndice 1 contiene la descripción detallada de los formatos XML usados en los capítulos.

El Apéndice 2 proporciona fichas para el registro de datos durante un proyecto de análisis y gestión de riesgos. Las fichas contienen formatos que incluyen campos para el registro del activo. Se incluyen fichas adicionales para valorar la información en las dimensiones de seguridad pertinentes.

El Apéndice 3 proporciona un formato XML para poder intercambiar modelos de activos entre distintas herramientas.

El Apéndice 4 proporciona índices para la presentación de los informes especificados en los capítulos del libro I.

1.3.9.2.3 MAGERIT: Libro III – Guía de Técnicas

El documento contiene los siguientes elementos: introducción, técnicas específicas y técnicas generales. En la introducción se expone el objetivo del documento, relacionado a describir algunas técnicas a utilizar en los procesos de análisis y gestión de riesgos.

Las técnicas específicas son:

- **Análisis mediante tablas:** mediante una escala de 5 niveles: muy bajo (MB), bajo (B), medio (M), alto (A), muy alto (MA). Esta escala se usa tanto para la estimación del impacto como para la estimación del riesgo. Propone una tabla de ejemplo para interpretar el significado de las escalas para la estimación del impacto, probabilidad

[22] EBIOS, *Expression des Besoins et Identification des Objectifs de Sécurité*, Expresión de Necesidades e Identificación de Objetivos de Seguridad. Metodología Francesa.

y riesgo en escalas cualitativas, y propone un cuadro de cálculo de riesgo como la combinación de impacto y probabilidad.

- **Análisis algorítmico:** presenta dos enfoques algorítmicos: modelo cualitativo y modelo cuantitativo; también se presenta un modelo escalonado.
    - **Modelo cualitativo:** Los activos deben valorarse en cada dimensión de seguridad según una escala de valores simbólicos: $V=\{0,...,v_0,v_1,...,v_i,...\}$, en orden de menor a valor. Son despreciables los valores por debajo de v_0. Para las expresiones que siguen, interprétese el símbolo → como dependencia directa, y ⇒ como dependencia indirecta o directa, según el caso. Las dependencias ($A \rightarrow B$, que se lee: "A depende – directamente – de B") entre activos pueden ser transitivas: $(A \rightarrow B) \wedge (B \rightarrow C)$, y pueden llegar a dependencias más complejas, como en la Figura 1.12, en donde $(A \rightarrow B_1) \wedge (A \rightarrow B_2) \wedge (B_1 \rightarrow C) \wedge (B_2 \rightarrow C)$. En otras palabras: $A \Rightarrow C \Leftrightarrow \exists B, (A \Rightarrow B) \wedge (B \rightarrow C)$, que se lee: "A depende indirectamente de C si y solo si existe al menos un activo intermedio B, tal que A depende directa o indirectamente de B, y B depende directamente de C".

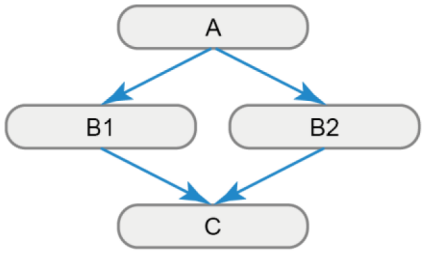


Figura 1.12. Dependencias – Modelo cualitativo – MAGERIT [78]

El valor acumulado de un activo es el mayor valor entre el propio y el de cualquiera de sus superiores. La degradación que una amenaza pueda causar está entre 0 (0%) y 1 (100%). El impacto se determina con el valor acumulado y el porcentaje de degradación. El impacto repercutido equivale a la degradación que sufre un activo dependiente cuando la amenaza ocurre sobre el activo del que depende. La probabilidad de una amenaza se evalúa en una escala de valores simbólicos, $P=\{0,..., p_0, p_1,..., p_i,...\}$, y el riesgo en una escala semejante, $R=\{0,..., r_0, r_1, ..., r_i, ...\}$, y está en función del impacto y la probabilidad. Los valores P_0 y r_0 e inferiores se consideran despreciables. Los riesgos acumulado y repercutido se determinan a partir de los impactos acumulado y repercutido respectivamente. La eficacia del paquete de salvaguardas se mide desde 0 (nada) hasta 1 (plenamente

eficaz), y a partir de éstas se obtienen las probabilidades residuales, y los impactos y riesgos, acumulados y repercutidos, residuales.

- **Modelo cuantitativo:** como en el modelo cualitativo, los activos deben evaluarse en cada dimensión de seguridad con un valor real positivo, siendo "v_0" y los valores inferiores a éste despreciables. Las dependencias siguen el mismo principio especificado en el modelo cualitativo. El grado de dependencia se calcula con la Ecuación 1.1, y las sumas de la fórmula Ecuación 1.1 se realizan con la Ecuación 1.2; ésta última tomada del cálculo de probabilidades de Bayes, para garantizar que la dependencia resultante no salga del intervalo que va del 0% al 100%.

$$\text{grado}(A \Rightarrow C) = \sum_i \{\text{grado}(A \Rightarrow B_i) \cdot \text{grado}(B_i \rightarrow C)\} \quad (1.1)$$

$$a + b = 1 - (1 - a)(1 - b) \quad (1.2)$$

Ejemplos del cálculo son los que están en la Figura 1.13.

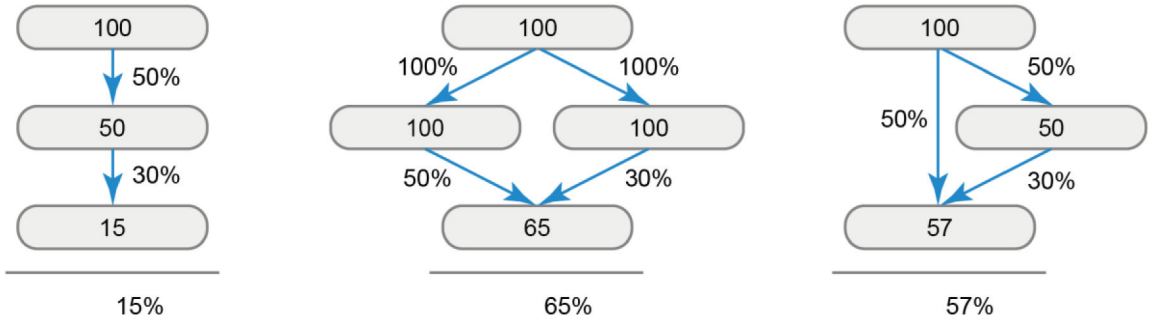


Figura 1.13. Dependencias – Modelo cuantitativo – MAGERIT [78].

El valor acumulado se calcula con la Ecuación 1.3.

$$\text{valor}_{\text{acumulado}} = \text{valor}(B) + \sum_i \{\text{valor}(A_i) \cdot \text{grado}(A_i \Rightarrow B)\} \quad (1.3)$$

La degradación del valor de un activo se calcula con un valor real entre 0 y 1 (degradación del 0% y 100%, respectivamente). El impacto (acumulado) es el equivalente producto del valor acumulado "v" del activo y el valor de degradación "d" que adquiere, según la Ecuación 1.4.

$$\text{impacto} = \text{i} = \text{v} \cdot \text{d} \quad (1.4)$$

El impacto repercutido equivale al producto del valor propio "v" del activo en cuestión, el grado de dependencia hacia el activo del que depende y la degradación "d" causada sobre el activo del que depende, siguiendo la Ecuación 1.5.

$$\text{impacto}_{\text{repercutido}} = \text{v} \cdot \text{d} \cdot \text{grado}\ (A \Rightarrow B) \tag{1.5}$$

La probabilidad de una amenaza puede basarse en la frecuencia esperada de ocurrencia ARO[23], siendo un valor real positivo, y considerando despreciable cualquier valor igual o menor que "f_0". Consecuentemente, el riesgo se calcula usando la Ecuación 1.6 genérica.

$$\text{riesgo} = \text{impacto} \cdot \text{frecuencia} \tag{1.6}$$

El riesgo acumulado y el riesgo repercutido se calculan con el impacto acumulado y repercutido, respectivamente. El valor de la eficacia "e^p" se calcula según la Ecuación 1.7, en donde e^i y e^f corresponden a la eficacia frente al impacto y la probabilidad, respectivamente.

$$(1 - e^i) \cdot (1 - e^f) = 1 - e \tag{1.7}$$

La degradación, impacto, frecuencia y riesgo residuales son los remanentes después de la salvaguarda. El riesgo residual se calcula como el producto del impacto residual y la frecuencia residual, según la Ecuación 1.8.

$$\text{riesgo}_{\text{residual}} = \text{impacto}_{\text{residual}} \cdot \text{frecuencia}_{\text{residual}} \tag{1.8}$$

Modelo escalonado: corresponde al análisis del impacto sobre la disponibilidad de los sistemas de información. Responden a esquemas como el de la Figura 1.14, en donde los escalones reflejan tiempos de detención, cuyos valores se ordenan de menor a mayor: $E=\{e_1, e_2,...,e_n\}$. Cada activo recibe un valor "$v[e_i]$" en cada escalón, cualitativo o cuantitativo, en orden de menor a mayor correspondientemente con cada escalón. Para determinar las dependencias, cualitativamente se usarán dos valores (sí o no), mientras que, cuantitativamente, se les definirá un grado. El valor acumulado, como el valor propio, se calcula de forma paralela e independiente en cada escalón. La degradación del valor de un activo se ubicará en el escalón "e_i" si la amenaza en cuestión provoca ese escalón de detención. El impacto es el valor "$v[e_i]$" de ese escalón. El impacto acumulado tomará el valor acumulado del activo afectado directamente, mientras que el impacto repercutido tomará el valor propio en el escalón de

[23] ARO (*Annual Rate of Occurrence*). Frecuencia estimada con el que ocurre una amenaza en un año.

la degradación correspondiente al activo afectado directamente del que depende.

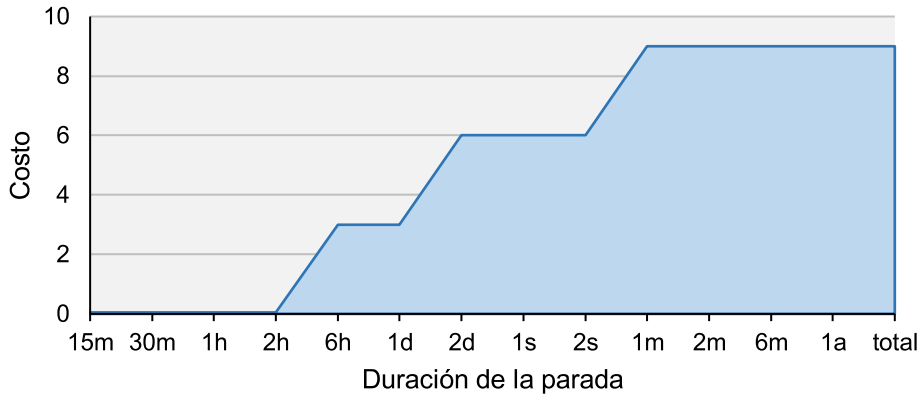


Figura 1.14. Costo de la interrupción de la disponibilidad – MAGERIT [78].

La eficacia de la salvaguarda (frente al impacto) se califica por el tiempo de reacción (respuesta garantizada) para reponer el servicio, teniendo que ser su escalón menor al escalón de degradación. El paquete de salvaguardas alternativas requiere que al menos una sea efectiva, pero en las salvaguardas concurrentes, el valor de eficacia es el peor de ellas. La degradación residual "e_r" se obtiene por acción de las salvaguardas que colocarán al activo, que en un principio (sin protección) se encontraba en el escalón de degradación "e_d", en el escalón de eficacia "e_s", modulado por la eficacia frente al impacto "e^i". El impacto residual toma el valor del escalón residual: $\text{impacto}_{\text{residual}}=\text{valor}[e_r]$. La frecuencia y el riesgo residuales se hallan según el modelo cuantitativo o cualitativo que les corresponda.

- **Modelo para estimar la eficacia de un paquete de salvaguardas:** un paquete de salvaguardas es un grupo de éstas que se acumulan sobre un activo. La eficacia "e" de cada una de las salvaguardas "s" se evalúa con un número real entre 0 (0%) y 1 (100%), según el razonamiento de la Tabla 1.6.

Tabla 1.6. Valoración de las salvaguardas – MAGERIT [78]

Eficacia e	Razonamiento
$e = 1$	Si una salvaguarda es idónea (100% eficaz)
$0 < e < 1$	Si una salvaguarda no es suficiente
$e = 0$	Si una salvaguarda no tiene ningún efecto
$e = na$	Si una salvaguarda está fuera de contexto

El paquete de salvaguardas "ps" puede ser concurrente (*todas* las salvaguardas "s" son necesarias), excluyente (*sólo una* salvaguarda "s" del paquete surte efecto) o aditiva (mientras haya más, mejor). La Tabla 1.7 indica las condiciones para evaluar la eficacia del paquete de salvaguardas.

Tabla 1.7. Valoración del paquete de salvaguardas – MAGERIT [78]

Eficacia e(ps)	Razonamiento
$e(ps) = e(s)$	Si s es singular
$e(ps) = media_k\{e(ps_k)\}$	Si ps = todas (ps_k)
$e(ps) = min\{1, 0, \Sigma_k\ e(ps_k)\}$	Si ps = algunas (ps_k)
$e(ps) = max_k\{e(ps_k)\}$	Si ps = una (ps_k)

La eficacia ponderada de un paquete de salvaguardas es la media aritmética de éstas, introduciendo una ponderación "p" a cada salvaguarda (si se considera que no todas son de la misma naturaleza; en caso de que fueran igual de importantes, p = 1), según la Ecuación 1.9.

$$e(ps) = \frac{\sum_k e(ps_k) \cdot p_k}{\sum_k p_k} \tag{1.9}$$

La eficacia frente al impacto, la frecuencia o ambas, de una amenaza se calculan mediante la Ecuación 1.7.

- **Árboles de ataque:** Para construir un árbol de ataque se comienza por el objetivo del atacante, que sirve de raíz del árbol; a continuación, se despliegan objetivos secundarios (intermedios) como ramas, que permiten conseguir el objetivo principal. Cada rama puede contener sub-objetivos (nuevas ramas) que pueden ser concurrentes (AND, todas los sub-objetivos son necesarios) o alternativas (OR, cualquiera de los sub-objetivos puede realizarse). Véase la Figura 1.15.

  Cada nodo OR o AND puede tener atributos que proveen información a detalle del atacante (conocimientos, inversión, riesgo que percibe, etc.) a fin de obtener escenarios simplificados correspondientes. El riesgo residual puede lograrse incrementando, por ejemplo, el nivel de conocimiento que requiere el atacante o la inversión que tendría que pagar para efectuar el ataque. Lo ideal es eliminar todas las ramas del árbol. Para la construcción del árbol puede acudirse a la experiencia (propia o ajena), a encuentros en grupos de reflexión o a herramientas que sugieran ataques según la naturaleza de los activos.

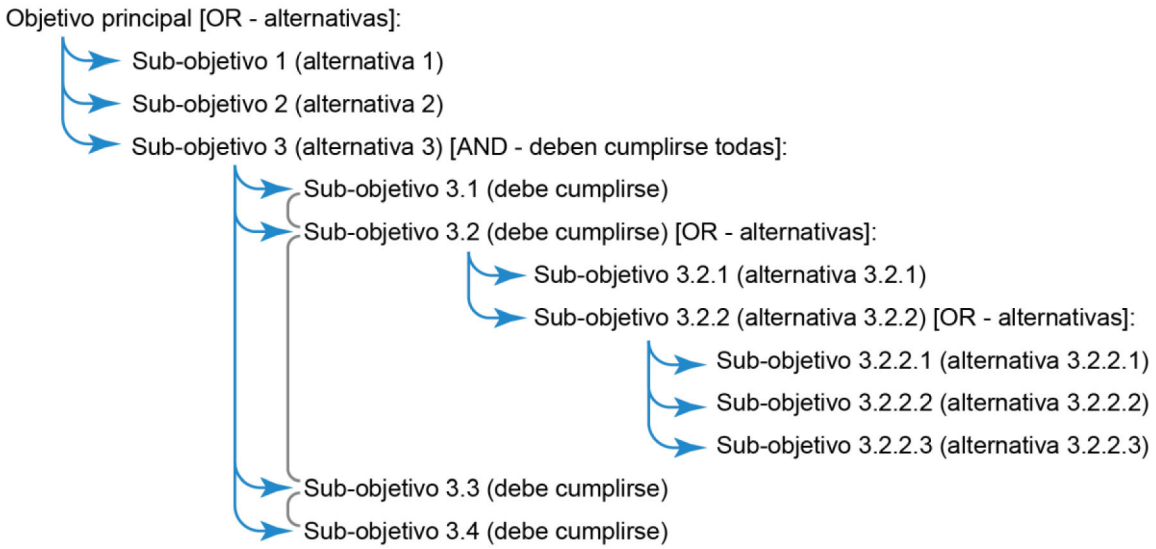


Figura 1.15. Ejemplo de estructura de un árbol de ataque – MAGERIT [78].

MAGERIT sugiere la utilización de técnicas generales usadas en el desarrollo de proyectos de análisis y gestión de riesgos, pudiendo ser éstas:

- **Técnicas gráficas:** como histogramas (puntos y líneas, barras, radar), diagramas de Pareto o diagramas de tarta (ver Figura 1.16):

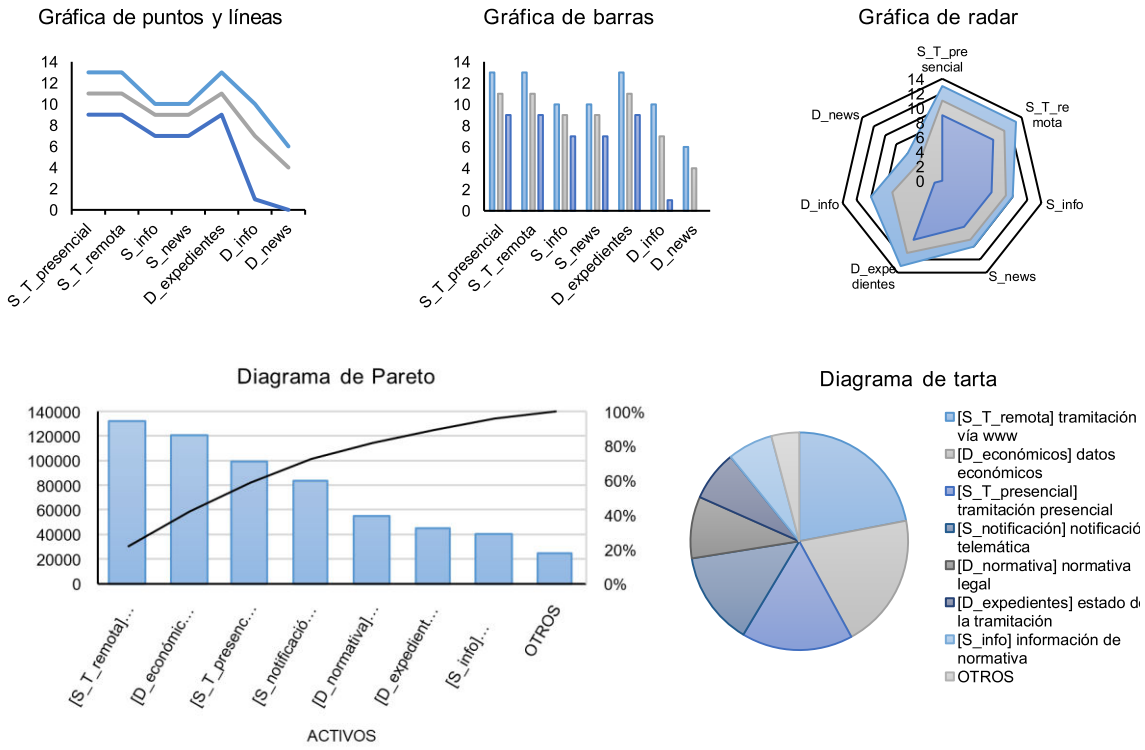


Figura 1.16. Técnicas gráficas – MAGERIT [78]

- **Sesiones de trabajo:** en las que se obtiene información a través de entrevistas y reuniones, y se comunica resultados con presentaciones. Para las entrevistas, se proporcionan directrices necesarias a tener en cuenta durante la preparación de la entrevista y durante la entrevista. También se proporcionan directrices para llevar a cabo reuniones y presentaciones.
- **Valoración Delphi:** Técnica cualitativa que consiste en tomar la opinión consensuada de expertos. Lo ideal es que participen entre 15 y 35 expertos. Esta técnica provee alta precisión en problemas técnicamente complejos. Para el resumen ejecutivo se prepara un cuestionario con los temas a valorar, el cual es distribuido y llenado por los expertos de forma anónima. Si hay un consenso en las respuestas, se termina; de otro modo, se resuelven las ambigüedades o inquietudes posibles, y se entrega nuevamente el mismo cuestionario, hasta que se llegue a un consenso. Se recomiendan dos rondas. De no lograr el objetivo, puede convocarse a una reunión para llegar a un consenso. Si el análisis es estadístico, se usarán medidas de tendencia central, medidas de dispersión, cuartiles y rango intercuartílico con las respuestas de cada ronda; si el análisis es a través de votaciones, se determina la respuesta con mayor acogida en cada valoración.

1.3.10 METODOLOGÍA MEHARI

MEHARI es una metodología de evaluación y gestión de riesgos de seguridad de la información, de origen francés, desarrollada por el CLUSIF[24], acoplada a los requerimientos de las normas ISO/IEC 27001, ISO/IEC 27002 y principalmente de la ISO/IEC 27005, con un enfoque de análisis en base a escenarios de riesgo.

MEHARI, al igual que MAGERIT, permite una evaluación cualitativa o cuantitativa. Esta evaluación se realiza sobre los factores estructurales (u organizacionales, independientes de las medidas de seguridad y orientadas al contexto y actividades de la organización), o de reducción de riesgo (directamente relacionadas con las medidas de seguridad) a través de sus herramientas y base de conocimientos acorde a la norma ISO/IEC 27005 [80]. MEHARI incluye un software llamado RISCARE[25], cuyo uso no es obligatorio. Los documentos de MEHARI son los siguientes:

---

[24] CLUSIF: Club de la Sécurité de l'Information *Français*, Club Francés de Seguridad de la Información en español, es una asociación para la promoción de la ciberseguridad, que reúne a empresas y administraciones en torno al desarrollo de buenas prácticas para la seguridad digital [79].

[25] RISCARE es un software que brinda soporte en la etapa de evaluación de riesgos y genera informes de auditoría automáticos. Es una marca registrada de BUC S.A.

- Introducción. [80]
- Conceptos Fundamentales y Especificaciones Funcionales. [81]
- Conceptos y Mecanismos. [82]
- Guía de Análisis y Clasificación de Amenazas de Seguridad. [83]
- Guía de Análisis y Tratamiento de Riesgos. [84]
- Guía de Evaluación de Servicios de Seguridad [85]

1.3.10.1 Compatibilidad con las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 [80]

1.3.10.1.1 Compatibilidad con la norma ISO/IEC 27001

MEHARI cubre completamente con las tareas para la creación de las bases de un SGSI, la implementación y gestión del SGSI, evaluación del riesgo residual y mejoras de las medidas de seguridad, y el empleo de controles y mejora continua del SGSI.

1.3.10.1.2 Compatibilidad con la norma ISO/IEC 27002

MEHARI proporciona tablas comparativas de correspondencia alineadas con los indicadores desglosados en la norma ISO/IEC 27002, para poder comprobar el cumplimiento de la norma.

1.3.10.1.3 Compatibilidad con la norma ISO/IEC 27005

MEHARI cumple con los requerimientos descritos en la ISO/IEC 27005 para el establecimiento de un SGSI: identificación de activos principales y de soporte, identificación de amenazas, identificación y cuantificación de la eficacia de las salvaguardas, escenarios de riesgo y selección de salvaguardas para los planes de reducción de riesgos.

1.3.10.2 Resumen

1.3.10.2.1 MEHARI: Introducción

En este documento se indica cómo debe usarse la metodología y las herramientas asociadas; expone breves descripciones sobre análisis, evaluaciones, clasificaciones, escalas, etc., los objetivos y la compatibilidad que tiene con las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, y el propósito de servir como soporte para un Oficial de Seguridad de la Información (OSI). La metodología se describe detalladamente en guías, manuales y bases de datos de conocimiento.

1.3.10.2.2 MEHARI: Conceptos Fundamentales y Especificaciones Funcionales

Este documento está organizado de forma similar a la estructura de alto nivel que siguen las normas ISO/IEC. Está comprendido por los siguientes elementos: introducción, propósito, referencias normativas, términos y definiciones, evaluación de riesgos, tratamiento de riesgos, gestión de riesgos y los Anexos A1 y A2.

En cuanto al propósito del documento, indica el interés de éste por precisar los principios y especificaciones funcionales y cómo cumplirlas para llevar a cabo la gestión de riesgos. Dentro de sus objetivos están el identificar, cuantificar y reducir el riesgo, la implementación de la metodología como herramienta de gestión y seguimiento permanente, y la resolución de los riesgos según el tratamiento decidido. Como referencias normativas, se señalan las normas ISO/IEC 27001 e ISO/IEC 27005.

En el apartado de términos y definiciones se describen los conceptos relacionados con la seguridad de la información, tales como amenaza de seguridad, impacto para la organización, impacto intrínseco, potencialidad (probabilidad), potencialidad intrínseca, escenario de riesgo, servicio de seguridad, entre otros.

Se exponen tres pasos a seguir para llevar a cabo este proceso de evaluación de riesgos:

- **Identificar los riesgos:** deben especificarse elementos como los activos (primarios y de soporte), las vulnerabilidades intrínsecas, el nivel de daño a los activos, las amenazas potenciales (eventos, actores y circunstancias) y los escenarios de riesgo; deben listarse estos elementos y los riesgos teóricamente posibles.
- **Estimar los riesgos:** se deben definir y poder estimar la gravedad intrínseca (sin salvaguardas) y gravedad potencial del riesgo (con salvaguardas); deben definirse niveles de estimación de impacto y potencialidad intrínsecos, niveles de eficacia de las salvaguardas y niveles de estimación de impacto y potencialidad residuales para evaluar el riesgo.
- **Evaluar el riesgo:** debe decidirse cómo se categorizará el riesgo (si es aceptable o inaceptable), a fin de tomar las medidas necesarias sobre éste. MEHARI proporciona una tabla de ejemplo de evaluación de riesgo, como se indica en la Figura 1.17: riesgos intolerables (requieren medidas de emergencia), riesgos inadmisibles (deben reducirse o eliminarse en algún momento, en un ciclo de planificación), y riesgos aceptables.

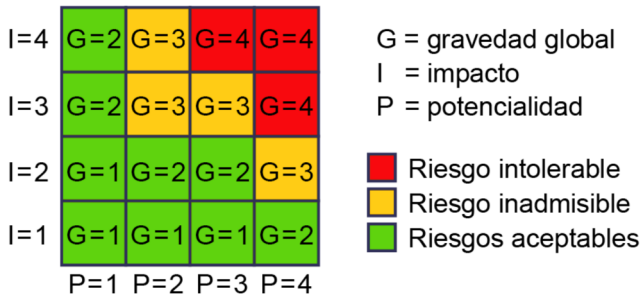


Figura 1.17. Cuadro de aceptabilidad del riesgo – MEHARI [81].

El tratamiento de riesgos comprende las cuatro opciones descritas en la norma ISO/IEC 27005: a) retener el riesgo, es decir, aceptar el riesgo y no hacer nada al respecto; b) reducir el riesgo, disminuyendo su probabilidad o impacto con servicios de seguridad, adaptados al riesgo, que cumplan con la calidad objetivo; c) transferir el riesgo, cargando parte de la pérdida (financiera) a un tercero; y d) evitar el riesgo, similar a reducirlo, pero a través de medidas estructurales (puede hacerse con la ayuda de una caracterización detallada de los escenarios de riesgo).

Para la gestión de riesgos se proponen tres fases para su cumplimiento: desarrollar planes de acción, implementar dichos planes y realizar un seguimiento y gestión del riesgo:

- **Desarrollar planes de acción:** para lo cual deben considerarse los siguientes pasos: Elegir objetivos prioritarios en términos de seguridad para implementar y optimizar los mismos (considerando qué medidas deben implementarse primero si hay dificultades o limitaciones económicas); transformar dicha elección en planes de acción (eligiendo soluciones basadas en mecanismos organizativos o técnicos); elegir posibles medidas estructurales y de prevención de riesgos; y validar (aprobar) la toma de decisiones con respecto a los pasos anteriores.
- **Implementar los planes de acción:** para lo cual es importante especificar los riesgos que cada plan de acción debe reducir a fin de determinar la mejor respuesta.
- **Seguimiento y gestión del riesgo:** para lo cual se han establecido 2 niveles de verificación: verificación de calidad y verificación del cumplimiento de la implementación de soluciones (Figura 1.18). La primera puede hacerse a través de una base de conocimientos (MEHARI propone una en la Guía de evaluación de servicios de seguridad) y la segunda a través de definición de las respuestas esperadas.

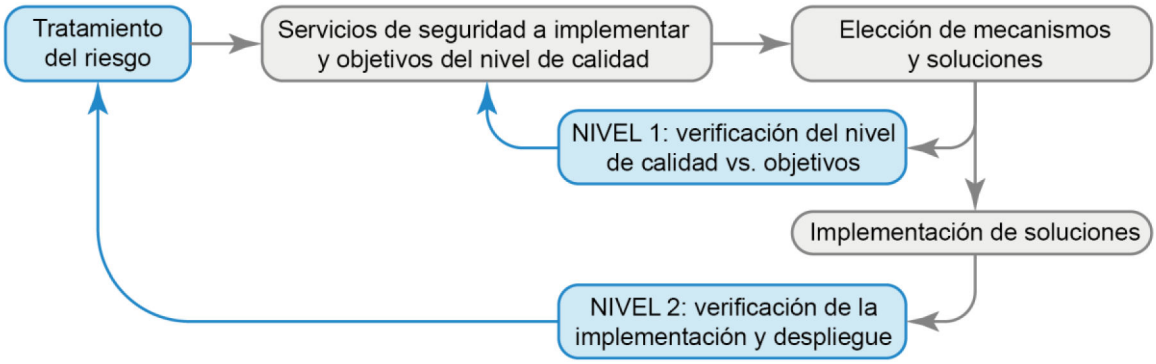


Figura 1.18. Verificaciones en el seguimiento y gestión de riesgos – MEHARI [81]

Muestra de las bases de conocimientos de MEHARI se adjuntan como anexos en el documento en cuestión:

- Anexo A1: Clasificación de activos primarios – Base de conocimiento MEHARI 2010. Consta de una tabla en la que se listan los activos clasificados según su tipo (datos, información y servicio) y las dimensiones de seguridad correspondientes (confidencialidad, disponibilidad y/o integridad). También se listan procesos según su tipo y el nivel de eficiencia en cumplimiento de leyes y reglamentos.
- Anexo A2: Clasificación de activos de soporte – Base de conocimiento MEHARI 2010. Consta de una tabla en la que se ha separado por su categoría (servicios, datos o proceso de gestión).
- Anexo B: Clasificación de vulnerabilidades intrínsecas – Base de conocimiento MEHARI 2010. Consta de una tabla con un listado de los activos de soporte, el tipo de daño correspondiente (amenaza), el tipo de vulnerabilidad correlacionada, y la o las dimensiones de seguridad en las que puede verse afectado.
- Anexo C1: Clasificación de los eventos – Base de conocimiento MEHARI 2010. Consta de una tabla con el tipo de familia del evento (amenazas), y los subtipos de evento, es decir, eventos que pertenecen a esta familia. Por ejemplo, la familia puede ser *Accidente ambiental grave*, y los subtipos de eventos: *relámpago, fuego, inundación.*
- Anexo C2: Clasificación de los actores primarios – Base de conocimiento MEHARI 2010. Consta de una tabla en la que se clasifican los actores por su categoría y su tipología. Por ejemplo, un actor categorizado como *Personal no autorizado*, puede ser de dos tipos: un *tercero no autorizado*, o un *vándalo o terrorista*.

El Anexo C de la metodología provee dos escalas de cuatro niveles cada una para evaluar los niveles de impacto y potencialidad (probabilidad) respectivamente.

1.3.10.2.3 MEHARI: Conceptos y Mecanismos

Este documento consta de los siguientes elementos: introducción general, evaluación de amenazas y clasificación de la información y los activos, evaluación del estado de seguridad, análisis de situaciones de riesgo, identificación de situaciones de riesgo, uso de los módulos MEHARI, y revisión y comparación con versiones anteriores. Cada capítulo contiene su propia introducción. Como introducción general se habla de la importancia de que el Oficial de Seguridad de la Información conozca su papel y sus desafíos, la necesidad de usar una metodología de gestión de riesgos de seguridad de la información y cuáles son los enfoques y herramientas que provee esta metodología.

La metodología indica el propósito de una evaluación de amenazas de seguridad y cuándo debería realizarse; considera importante definir las amenazas a través de escalas de fallas de funcionamiento posibles, clasificar de la información y los activos y seguir un proceso de análisis de amenazas con el modelo de la *Guía de Análisis y Clasificación de Amenazas de Seguridad* de la metodología.

En el apartado de evaluación del estado de seguridad se exponen se definen conceptos sobre servicios de seguridad (salvaguardas), sub-servicios (complementarios para los servicios de seguridad), mecanismos (algoritmos, procedimientos o tecnologías para que un servicio funcione), soluciones de seguridad (implementación real de un mecanismo), tipos de servicios como medidas generales (a nivel de organización y sin efecto directo sobre el riesgo) y medidas técnicas (con efectos directos e inmediatos), y evaluación del nivel de calidad del servicio de seguridad (según su eficiencia, robustez y permanencia).

Propone la evaluación directa de los servicios a través de sus guías y un proceso de revisión de vulnerabilidades (a través de un plan de auditoría que identifique las diferencias de las áreas de soluciones a nivel técnico por separado y un proceso de revisión posterior), y los entregables del plan de auditoría, la evaluación de seguridad por dominio y un resumen de las vulnerabilidades. Se enfatiza en el análisis de situaciones o escenarios de riesgo, en el que es útil considerar el tipo de consecuencia, sus causas y el tipo de activo o activos involucrados.

El análisis de un escenario de riesgo se hace a través de la potencialidad (MEHARI prefiere este término en lugar de *probabilidad*), y el impacto, para lo cual provee de escalas de evaluación para cada uno de ellos, de forma cuantitativa. Para la potencialidad deben considerarse tres parámetros (Figura 1.19.a): exposición natural al riesgo: medidas disuasivas (o disuasorias) y medidas preventivas. Para el impacto deben considerarse 4 parámetros (Figura 1.19.b): gravedad de las consecuencias, medidas limitantes, medidas

paliativas (limitan las consecuencias indirectas luego de haber aplicado las medidas limitantes), y medidas de recuperación (a través de la transferencia de riesgo).

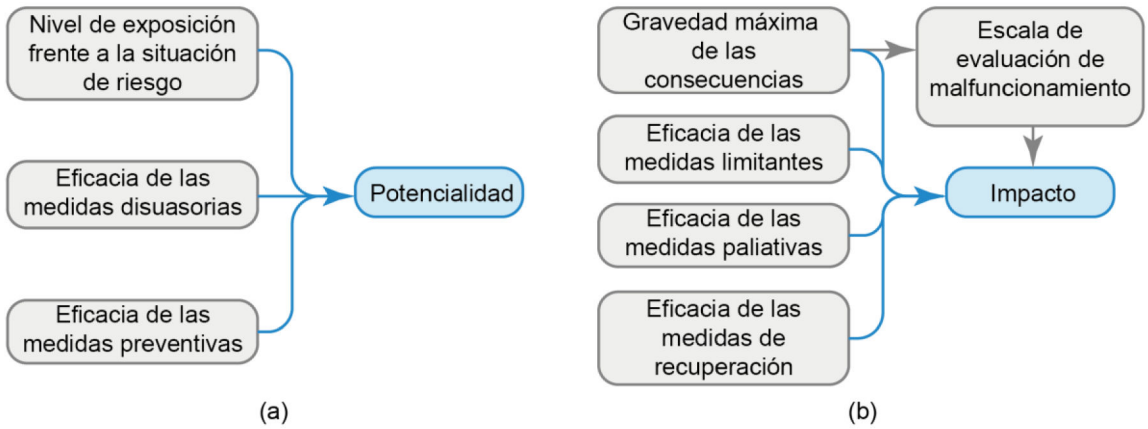


Figura 1.19. Evaluación del escenario de riesgo en (a) potencialidad y (b) impacto – MEHARI [82]

Se evalúa la gravedad del escenario según las categorías propuestas en el libro *Conceptos Fundamentales y Especificaciones Funcionales,* según el cuadro de aceptabilidad de la Figura 1.17. El proceso de análisis de riesgo se resume en la Figura 1.22, mismo que puede realizarse con las herramientas de soporte de MEHARI. La identificación de situaciones de riesgos puede hacerse mediante dos enfoques: directo (usando escalas de valores destacando las actividades más relevantes), y la identificación sistemática a partir de la base de conocimientos (siguiendo un proceso automatizado y más detallado).

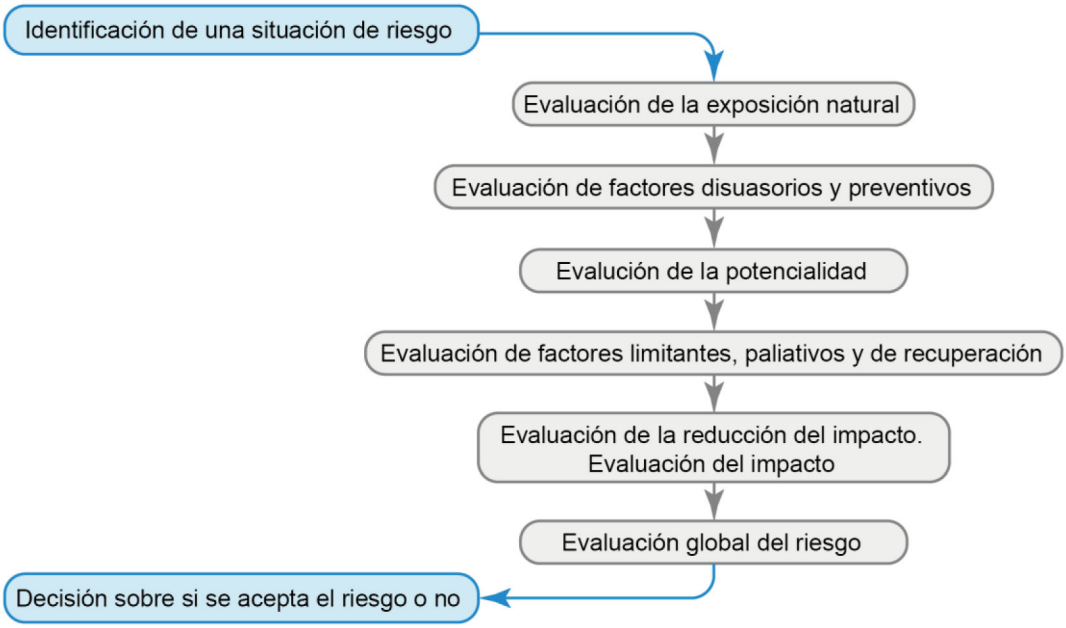


Figura 1.20. Proceso de análisis (de situaciones) de riesgos – MEHARI [82].

El capítulo seis, uso de los módulos de MEHARI, señala que pueden tomarse diferentes enfoques de gestión de seguridad que pueden beneficiarse de esta metodología, por lo que no es obligatorio hacer un uso estándar de los módulos. Presenta tres enfoques:

- Planes de seguridad basados en el análisis de riesgos, que involucran dos niveles de decisión: estratégicos (de largo plazo, centralizadas, adecuadas a intereses colectivos e independientes de los procesos o tecnología que se está implementando) y operativos (de corto plazo, separadas en unidades de negocio, con resultados propios, en función de los procesos y la tecnología que se está implementando).
- Planes de seguridad basados en una auditoría, que incluye una revisión de las vulnerabilidades, la identificación de servicios con bajo nivel de calidad y la selección de medidas necesarias para mejorar dichos servicios. Puede hacerse a través de una evaluación simple del estado de seguridad y su principal debilidad o a través de una evaluación detallada, verificando todos los aspectos de servicios de seguridad (según su efectividad, robustez y permanencia).
- Seguridad de proyectos de desarrollo, orientado a un proyecto específico ignorando la diferencia entre los niveles estratégicos y operativos, estableciendo un nivel de servicio de seguridad estándar en la fase inicial del proyecto. Se realiza un análisis de amenazas específicas del proyecto, un análisis de riesgos principales dentro de escenarios de riesgo definidos por los líderes del proyecto. Los requisitos de seguridad serán deducidos del análisis de riesgos anterior y distribuidos a los administradores de infraestructura general para que los integren en sus planes.

Finalmente, se realiza una revisión comparativa con versiones anteriores a fin de exponer las mejoras de esta versión (2010).

1.3.10.2.4 MEHARI: Guía de Análisis y Clasificación de Amenazas de Seguridad

Este documento consta de los siguientes elementos: introducción, escala de valor de fallas de funcionamiento, clasificación de la información y los activos de soporte, construcción de la tabla de impacto intrínseco, consejos prácticos, y los anexos 1 y 2. El documento provee ejemplos para un mejor entendimiento. Como introducción, se habla de dos resultados que se obtienen del análisis de amenazas: la escala de valor de fallas de funcionamiento y la clasificación (o valoración) de los activos relacionados con la información.

El proceso de obtención de una escala de valores para fallas de funcionamiento, según el documento, se da a través de cuatro etapas: a) identificación de las principales actividades

y sus objetivos; b) identificación de fallas de funcionamiento potenciales asociadas a cada actividad; c) análisis de amenazas de seguridad, en las que se evalúe el nivel de gravedad que puede causar una amenaza (se proponen cuatro niveles) y se establezcan criterios y umbrales de criticidad; y d) compilación de los diversos resultados para cada actividad, evaluados en una tabla que contienen la escala de valor con descripción definida.

El apartado siguiente trata sobre la clasificación de la información y de los activos de soporte. Se recalca la necesidad de identificar los activos a clasificar, algunos de forma individual y otros agrupados. Los activos primarios pueden identificarse como se especifica en el libro *MEHARI: Conceptos Fundamentales y Especificaciones Funcionales*. Las bases de conocimiento de MEHARI proporcionan tablas como soporte, y el documento provee un ejemplo del uso de éstas. Para los criterios de clasificación deben considerarse los aspectos de confidencialidad, integridad y disponibilidad, y otro para leyes, regulaciones y requisitos contractuales.

Deben clasificarse los activos de soporte, y cómo se afectan en las tres dimensiones de seguridad, usando la escala propuesta. La construcción de la tabla de impacto intrínseco puede completarse con la información de las tablas de clasificación anteriores.

Se proporciona un consejo práctico sobre los puntos importantes que deben considerarse en la construcción de una escala de valor: primero, un enfoque en los procesos más críticos (evitando considerar todos los escenarios de riesgo posibles, proceso en el que debe estar involucrada principalmente la alta dirección); segundo, las fallas de funcionamiento y su impacto deben identificarse ignorando los controles existentes; tercero, debe mantenerse una consistencia entre diferentes tipos de fallas de funcionamiento con niveles de gravedad equivalentes (como puede verse en el anexo 1 del documento en cuestión); y cuarto, una decisión formal y seriamente consensuada en el establecimiento de la escala de valor.

También deben considerarse aspectos importantes durante la clasificación, como el agrupar los activos con objetivos similares para evitar analizar una gran cantidad de objetos. Por último, debería desarrollarse un plan de acción enfocado a las acciones más urgentes. El Anexo 1 provee un ejemplo completo de aplicación de una escala de valor aplicada a una empresa industrial, y el Anexo 2 muestra un ejemplo del uso de la tabla de impacto intrínseco.

1.3.10.2.5 MEHARI: Guía de Análisis y Tratamiento de Riesgos

El documento está conformado por: introducción, evaluación de riesgos, tratamiento del riesgo, consejos prácticos y cinco anexos. Se hace una revisión de los principios generales

de MEHARI, y se indica que ha adoptado la organización descrita en la ISO/IEC 27005 que puede verse en el diagrama de la Figura 1.21, en el que se muestran las tres fases de la gestión de riesgos.

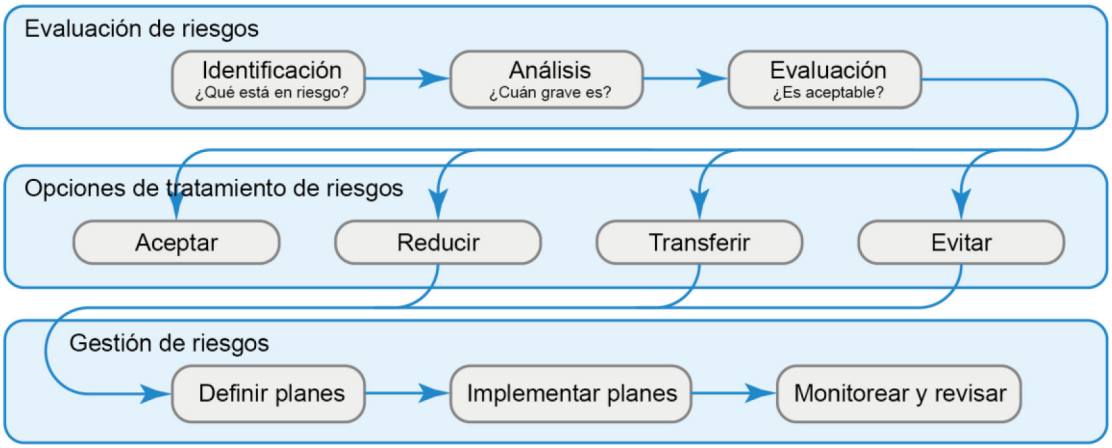


Figura 1.21. Fases de una gestión de riesgos – MEHARI [84].

En la evaluación de riesgos se incluyen tres etapas: a) identificación del riesgo, que puede hacerse a través de la base de conocimientos de MEHARI y las vulnerabilidades asociadas a los escenarios de riesgo; b) análisis de la gravedad de un escenario, según la potencialidad e impacto intrínsecos, a través de una tabla de impacto como se muestra en el Anexo 3 del documento; y c) una etapa de evaluación del riesgo, para determinar si se considera aceptable o no. El software RISCARE permite el manejo de hasta ocho criterios.

Puede realizarse una evaluación de factores de reducción de riesgos a través de una auditoría de seguridad basada en la base de conocimientos de MEHARI. MEHARI propone fórmulas en la base de conocimientos, como se había dicho anteriormente, en hojas de cálculo.

La probabilidad residual puede ser evaluada de forma automatizada con la base de conocimientos en función de los niveles de las medidas disuasivas y preventivas. El impacto residual también puede ser evaluado de la misma forma, pero en función de las medidas limitantes (o de protección) y paliativas. La evaluación de la gravedad de un escenario puede llevarse a cabo según lo especificado en el documento *MEHARI: Conceptos Fundamentales y Especificaciones Funcionales*.

Para el tratamiento del riesgo puede utilizarse la base de conocimientos de MEHARI automatizada, que incluye una vista global (escenarios y su gravedad agrupados por tipo de activo primario), o una vista de los escenarios agrupados por tipo de amenaza.

El Anexo 1 incluye una tabla de exposición natural al riesgo. El Anexo 2 proporciona una escala de cuatro niveles para evaluar el nivel de exposición natural. El Anexo 3 proporciona nuevamente la tabla de impacto intrínseco. El Anexo 4 proporciona escalas de cuatro niveles para evaluar cada uno de los tipos de medidas reductoras (disuasivas, preventivas, limitantes o de protección, y paliativas), y el Anexo 5 proporciona cuadrículas de evaluación estándar para evaluar la potencialidad en escenarios de riesgo.

1.3.10.2.6 MEHARI: Guía de Evaluación de Servicios de Seguridad

Esta guía consta de los siguientes elementos: introducción, definiciones, proceso de evaluación, evaluaciones personalizables, entregables y consejo práctico. Se hace referencia al documento "MEHARI: Conceptos fundamentales y especificaciones funcionales", que proporciona los requerimientos del uso apropiado de la base de conocimientos que incluye definiciones y una lista de servicios de seguridad y cuestionarios.

Se provee definiciones concernientes al proceso de evaluación de servicios de seguridad. Define las expresiones *servicio de seguridad*, *sub-servicio*, *mecanismo*, *solución de seguridad*, *topología de los servicios de seguridad*, *eficiencia, robustez y permanencia de un servicio de seguridad*, como se describen en el documento *MEHARI: Conceptos y Mecanismos.*

Se advierte que el proceso de evaluación debe incluir un esquema de auditoría. MEHARI incluye cuestionarios de auditoría acoplados según el esquema mencionado. El siguiente nivel en la auditoría tiene que ver con estrategias técnicas y se aconseja que, en el proceso de auditoría se agreguen comentarios que registren las explicaciones a las respuestas de los cuestionarios de la auditoría; como todas las respuestas deben ser "sí" o "no", cualquier respuesta dudosa debe ser manejada como "no". Se advierte que el auditor debe ser un profesional de seguridad experimentado.

En los siguientes y últimos capítulos se expone la posibilidad de realizar evaluaciones personalizables, en la que los cuestionarios de auditoría puedan limitarse a contener solo preguntas clave, que incluyan el tipo de pregunta y el nivel de seguridad que aborda la pregunta; la necesidad de presentar entregables con los cuestionarios como evidencia y los comentarios y análisis respectivos (que pueden incluir gráficos o diagramas). Se aconseja, además, que los cuestionarios de auditoría incluyan preguntas similares para diferentes grupos a fin de realizar comparativas útiles.

2 METODOLOGÍA

La metodología que se plantea para el SGSI está basada en las normas ISO/IEC 27001 [3], ISO/IEC 27002 [4] e ISO/IEC 27005 [5]; estas normas proveen directrices generales que, adaptadas a la realidad institucional e influenciadas por las metodologías MAGERIT y MEHARI, proveen herramientas útiles para el análisis y gestión de riesgos. En base al estudio de las normas ISO/IEC y de las metodologías indicadas, se ha desarrollado la metodología para la gestión de riesgos de la seguridad de la información. Ésta incluye un método de análisis de riesgos que hace uso de un modelo híbrido, de la avenencia entre los modelos cualitativo y cuantitativo, cuyos procesos tienen influencia de las metodologías antes mencionadas.

La metodología consta de las siguientes partes:

- Establecimiento del contexto.
- Método de análisis y evaluación de riesgos (valoración del riesgo).
- Tratamiento del riesgo.

2.1 CONTEXTO DE LA ORGANIZACIÓN

Las normas ISO ponen énfasis en la necesidad de establecer el contexto; la norma ISO/IEC 27001:2013 [3] indica que es necesario determinar las cuestiones externas e internas esenciales que permitan el cumplimiento de su propósito y que influyen en la capacidad de lograr los resultados deseados para el SGSI, al tiempo que la norma ISO/IEC 27005:2012 [5] indica que es necesario recabar información que contribuya al establecimiento del contexto de la gestión de la seguridad de la información. En conjunto, deben establecerse los contextos interno y externo, los criterios de valoración, el alcance y los límites del SGSI.

2.1.1 CULTURA ORGANIZACIONAL

2.1.1.1 Misión

La Planta Central del Ministerio de Cultura y Patrimonio, como parte de la Organización, se debe a la misión:

“El Ministerio de Cultura y Patrimonio ejerce la rectoría del Sistema Nacional de Cultura para fortalecer la identidad Nacional y la Interculturalidad; proteger y promover la diversidad de las expresiones culturales; incentivar la libre creación artística y la producción, difusión, distribución y disfrute de bienes y servicios culturales; y salvaguarda de la memoria social y el patrimonio cultural, garantizando el ejercicio pleno de los derechos culturales a partir

de la descolonización del saber y del poder; y de una nueva relación entre el ser humano y la naturaleza, contribuyendo a la materialización del Buen Vivir" [86].

2.1.1.2 Visión

"El Ministerio de Cultura y Patrimonio ejercerá la rectoría de las políticas públicas culturales y del Sistema Nacional de Cultura; garantizará el ejercicio de los derechos culturales e incidirá en la integración simbólica del Ecuador y en el cambio cultural de la sociedad" [86].

2.1.1.3 Valores

El Ministerio de Cultura y Patrimonio se fundamenta en los valores de liderazgo, servicio, compromiso, honestidad y transparencia [86].

2.1.1.4 Objetivo

De manera general, esta Cartera de Estado persigue el siguiente objetivo:

"Establecer un modelo participativo de gestión, que contribuya al cumplimiento de la misión y objetivos estratégicos institucionales dentro del marco de los lineamientos establecidos por la Constitución de la República del Ecuador, por el proceso de Reforma Democrática del Estado coordinado por la SENPLADES[26], que permitan aplicar las facultades y competencias que le corresponden, bajo los principios de desconcentración, servicios públicos de calidad y rendición de cuentas" [87].

2.1.2 ESTRUCTURA ORGANIZACIONAL INTERNA

La Figura 2.1 muestra la estructura de la organización interna de la Planta Central del Ministerio de Cultura y Patrimonio, que excluye a las coordinaciones zonales puesto que no están en la Planta Central.

2.1.2.1 Metas y objetivos de las unidades administrativas

Las metas y objetivos de las unidades administrativas de la Planta Central del MCyP se encuentran especificadas en del portal de la institución [89], según especifica la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), misma que debe ser actualizada constantemente y publicada de forma obligatoria.

---

[26] SENPLADES: Secretaría Nacional de Planificación y Desarrollo. Actualmente se identifica como Secretaría Técnica de Planificación "Planifica Ecuador".

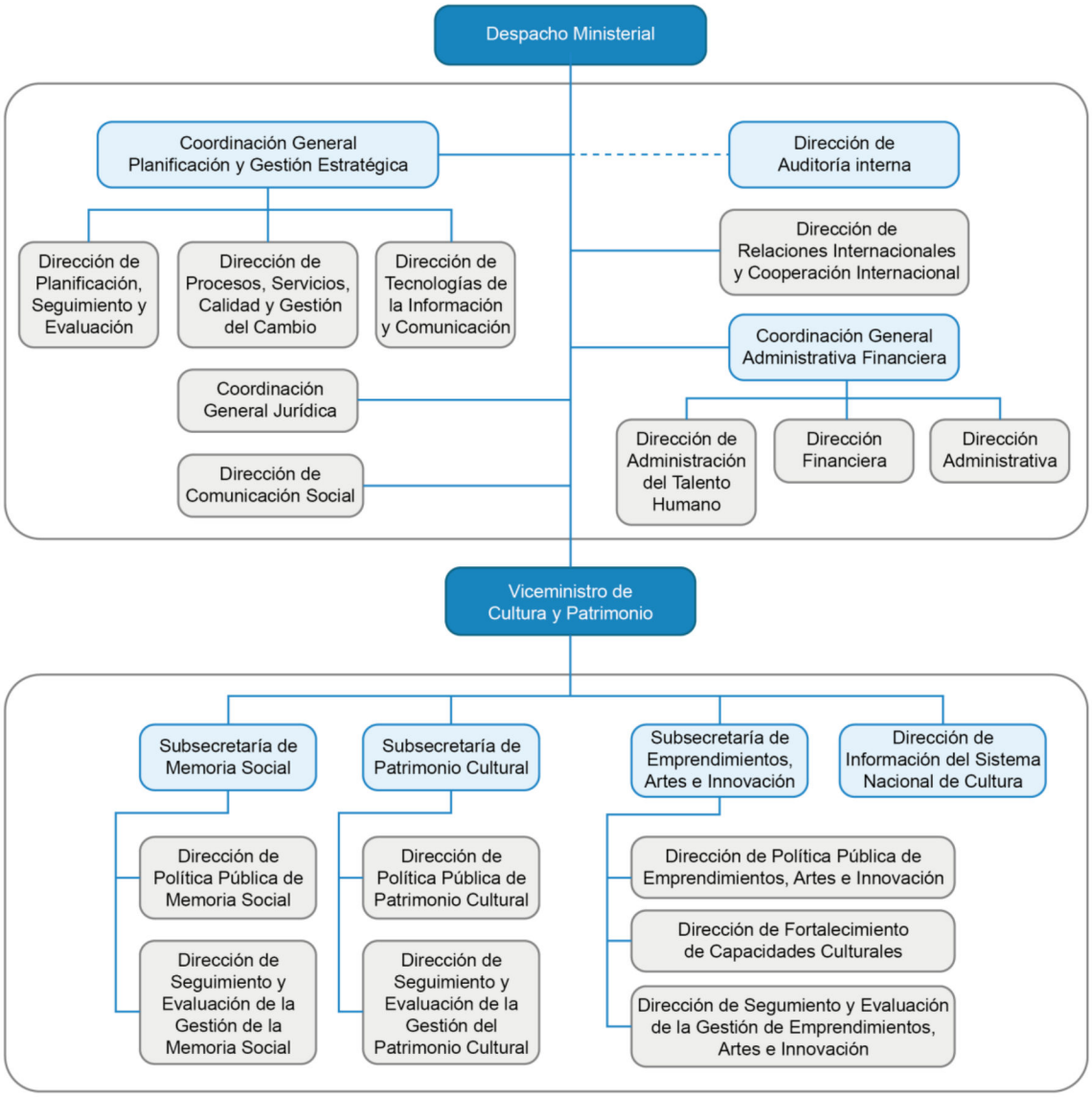


Figura 2.1. Estructura de la organización interna del MCyP - Planta Central [88]

2.1.3 PARTES INTERESADAS

Las partes interesadas son todas aquellas personas e instituciones cuya actividad afecta o influencia en el sistema de gestión de seguridad de la información, y que, recíprocamente, la actividad de la institución afecta o influye en los objetivos o sistemas de gestión de éstas. Las normas ISO/IEC 27001 [3] e ISO/IEC 27005 [5] denotan la importancia de tomar en cuenta las expectativas y percepciones de las partes interesadas en la gestión de riesgos puesto que pueden impactar sobre aspectos importantes como el buen nombre y reputación de la Institución, y deben considerarse las consecuencias negativas que puedan desprenderse si existen fallos de la seguridad que involucren a dichas partes. La Tabla 2.1

agrupa las partes interesadas y sus respectivos intereses y expectativas con respecto a la institución.

Tabla 2.1. Expectativas de las partes interesadas
[Elaboración propia]

Parte interesada (*stakeholder*)		Temas de responsabilidad	Interés de la parte interesada	Interés de la institución
Clientes / usuarios	Artistas y gestores culturales. Historiadores, investigadores y científicos. Usuarios nacionales e internacionales.	Calidad de servicios. Reputación. Confidencialidad. Disponibilidad. Integridad.	Servicio de calidad, disponibilidad e integridad de la información de los servicios utilizados. Confidencialidad de sus datos personales.	Proveer información íntegra y disponible. Presentar servicios confiables. Preservar y/o mejorar la reputación y el buen nombre.
Empleados	Funcionarios del MCyP: Curadores, gerencia, nivel jerárquico superior, asistentes, técnicos, secretarios, limpieza, guardianía, despacho, etc.	Derechos. Sueldo. Ambiente laboral. Recursos. Confidencialidad.	Garantías de derechos humanos y laborales. Pago puntual. Buen clima laboral. Recursos adecuados para laborar. Confidencialidad de su información personal.	Acuerdos de confidencialidad debidamente pactados. Conciencia en seguridad de la información. Registros. Puntualidad. No repudio. Uso debido de los recursos.
Proveedores	Antivirus, Antispam, Firewall, Internet, Full Time, Guardianía, Limpieza	Compromisos. Garantías. Confidencialidad. Integridad. Disponibilidad.	Contrato de largo plazo. Pago puntual. Proveer un mejor servicio que la competencia.	Acuerdos de confidencialidad debidamente pactados. Servicio de calidad. Bajos precios. Garantías. Integridad y disponibilidad del servicio. Mantenimiento y actualizaciones. Valor agregado.
Administración Pública	MINTEL EOD's[27] DINARDAP	Legislación. Disposiciones gubernamentales. EGSI versión 2.0	Cumplimiento de la legislación. Implementación del EGSI. Gestión adecuada por parte del MCyP.	Cumplimiento de la legislación. Reputación según el cumplimiento del EGSI. Cumplimiento de las disposiciones gubernamentales. Cumplimiento LOTAIP.
Sociedad	Sociedad ecuatoriana. Pueblos y nacionalidades indígenas. Sociedad internacional. Activistas del medioambiente.	Memoria Social, Patrimonio y Cultura. Medio ambiente. Transparencia. Reputación.	Responsabilidad con el medio ambiente. Preservación de la identidad cultural, patrimonio, memoria social y cultural.	Preservar y salvaguardar el patrimonio, la memoria social, cultural y toda la información relacionada. Guardar la reputación de la institución. Publicar información transparente según LOTAIP.

[27] Entidades Operativas Desconcentradas.

2.1.4 UBICACIÓN Y CARACTERÍSTICAS GEOGRÁFICAS

La Planta Central del MCyP se encuentra ubicada en el sector Mariscal Sucre, del Distrito Metropolitano de Quito, al norte de la Sierra Ecuatoriana, en la cordillera occidental de los Andes (Figura 2.2). Debido a la ubicación del Distrito Metropolitano de Quito, y propiamente del edificio de la Planta Central, resulta de especial interés el analizar los riesgos asociados, por lo que es útil el servirse de los estudios del Atlas de Amenazas Naturales del Distrito Metropolitano de Quito [90] y del Plan Especial "La Mariscal" [91]. La Tabla 2.2 contiene información de la ubicación y los datos del lote global de la institución, mientras que la Tabla 2.3 contiene las características geográficas del entorno.

Figura 2.2. Mapa físico del Distrito Metropolitano de Quito (Fuente: Google Earth)

Tabla 2.2. Ubicación y datos del lote global de la Planta central del MCyP

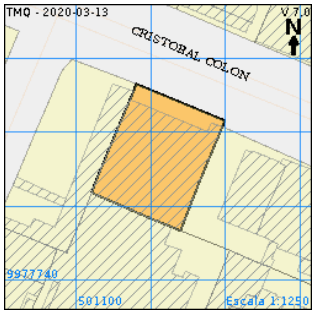
Datos del lote global	Valor	Implantación del lote	Fuente
Cantón	Distrito Metropolitano de Quito		Cédula Catastral Informativa en Propiedad Horizontal (Anexo A)
Zona Metropolitana	Norte		
Parroquia	Mariscal Sucre		
Barrio / Sector	Mariscal Sucre		
Clasificación del suelo	Urbano		
Área según escritura	832 m^2		
Área gráfica	824.50 m^2		
Frente total	27.56 m		
Dirección	N25 Cristóbal Colón – E5 – 34		

Tabla 2.3. Resumen de las características geográficas del entorno [Elaboración propia]

Sector del DMQ	Aspecto físico		Estado actual	Fuentes
Mariscal Sucre	Tipografía y relieve	Llanura. Parte más baja del centro-norte.	Pendiente 0%-6%	Atlas de Amenazas Naturales y Exposición a Infraestructura del D.M.Q. [90] Plan Especial "La Mariscal" [91]
	Hidrografía	Relleno de quebradas (4 cuencas hidrográficas)	Sin hidrografía actualmente	
	Riesgos y amenazas	Inundación	Alta susceptibilidad	
		Riesgos sísmicos	Vulnerabilidad constante	
		Amenazas volcánicas	Sin amenaza	

2.1.5 MARCO LEGAL

La Tabla 2.4 contiene la base legal que rige a esta Cartera de Estado en lo que a responsabilidad con la información y protección de datos respecta, con información derivada de la publicación oficial de la institución en su portal [92], en cumplimiento del Artículo 7, literal a, de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).

Tabla 2.4. Marco legal del MCyP [92]

Tipo de la Norma	Norma Jurídica	No. Registro Oficial	Fecha de publicación
Carta Suprema	Constitución de la República del Ecuador	R. O. No. 449	20 de octubre de 2008
Código	Código Orgánico de Planificación y Finanzas Públicas	R. O. S. No. 306	22 de octubre 2010
	Código del Trabajo	R. O. Suplemento No. 167	16 de diciembre de 2005
	Código Orgánico Integral Penal (COIP)	R. O. Suplemento No. 180	20 de febrero de 2014
Ley Orgánica	Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)	R. O. S. No. 337	18 de mayo de 2004
	Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP)	R. O. No. 395	04 de agosto de 2008
	Ley Orgánica de Servicio Público (LOSEP)	R. O.S. No. 294	06 de octubre de 2010
	Ley Orgánica de la Contraloría General del Estado	R. O. No. 595	12 de junio de 2002
	Ley Orgánica de Cultura	R. O.S. No. 913	30 de diciembre de 2016

2.1.6 SERVICIOS INSTITUCIONALES

Según su portal [93], el Ministerio de Cultura y Patrimonio proporciona los servicios que se describen en la Tabla 2.5.

Tabla 2.5. Servicios del MCyP [93]

No.	Denominación del servicio	Descripción del servicio
1	Tutela Jurídica de fundaciones y Corporaciones Culturales	Servicio orientado a garantizar el derecho de asociación y reunión a personas naturales y jurídicas
2	Declaratoria de Bienes Patrimoniales Nacionales e Incorporación en la Lista Representativa del Patrimonio Cultural Inmaterial	Servicio orientado a la ciudadanía e instituciones quienes a través de los GAD's Municipales realizarán el proceso con el Instituto Nacional de Patrimonio Cultural para la Declaratoria de Bienes Patrimoniales o Incorporación en la lista representativa del Patrimonio Cultural Inmaterial, mediante un Acuerdo Ministerial emitido por el Ministerio de Cultura y Patrimonio.
3	Registro de artistas y gestores culturales	Servicio Orientado al registro de artistas, profesionales en la cultura, académicos, colectivos y asociaciones culturales, mediante el registro y calificación de su perfil artístico en el sistema del Registro Único de Actores RUAC

2.1.7 ALCANCE DEL SGSI

Según la norma ISO/IEC 27001 [3], el alcance de la institución puede ser diferente del de otra debido al tamaño, sus servicios, sus actividades, sus procesos y su complejidad, y la competencia de sus funcionarios. Por esta razón, la norma afirma que es deber de la institución el determinar y documentar el alcance del SGSI, en el que se debe considerar el contexto, interno y externo, de la organización.

De forma complementaria, la norma ISO/IEC 27005 [5] indica que el alcance de la gestión del riesgo está alineado con el alcance del SGSI, y debe definirse garantizando que todos los activos relevantes sean tomados en cuenta en el proceso de valoración del riesgo, y reafirma que los controles implementados dentro del alcance, el contexto y los límites del SGSI deben basarse en el riesgo. En el Anexo B se propone una definición del alcance para la institución.

2.1.8 POLÍTICA DE SEGURIDAD

La norma ISO/IEC 27001 [3], en el apartado 5.2 declara que es deber de la alta dirección el establecer una política de seguridad de la información, que sea adecuada y alineada al propósito de la organización; que incluya: los objetivos de seguridad de la información o provea un marco de referencia para establecerlos, un compromiso de cumplimiento de los requerimientos aplicables relacionados con la seguridad de la información y un compromiso de mejora continua del SGSI. Además, debe:

- Estar documentada y disponible para la Institución.
- Ser difundida en la Institución.
- Estar disponible para las partes interesadas, según sea necesario.
- Ser revisada a intervalos planificados o cuando haya cambios significativos.
- Formar parte del proceso de concientización.

En el Capítulo 3 se propone una Política de Seguridad de la Información para la Institución.

2.1.9 ROLES Y RESPONSABILIDADES EN EL SGSI

La norma ISO/IEC 27001 [3], en el apartado de Liderazgo, dispone que los roles y responsabilidades, con respecto a la Seguridad de la Información, deben ser asignados por parte de la máxima autoridad. El Esquema Gubernamental de Seguridad de la Información (EGSI versión 2.0) [64] establece, además, que debe conformarse un Comité de Seguridad de la Información (CSI) designado por la máxima autoridad. Este Comité será el responsable de designar a un funcionario como Oficial de Seguridad de la Información (OSI).

2.1.9.1 Comité de Seguridad de la Información (CSI)

Según el artículo 5 del Acuerdo Ministerial No. 025-2019 (EGSI versión 2.0) [64], el Comité de Seguridad de la Información debe estar integrado por los responsables o delegados de las siguientes áreas:

- Talento Humano
- Administrativa
- Planificación y Gestión Estratégica
- Comunicación Social
- Tecnologías de la Información
- Unidades Agregadores de Valor
- El Área Jurídica, que participará como asesor.

2.1.9.1.1 Responsabilidades

Las responsabilidades del CSI se encuentran documentadas tanto en el Acuerdo Ministerial No. 025-2019 [64], artículo 6, como en la Guía de Implementación del EGSI [73]. Éstas son:

- Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.

- Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
- Promover la difusión de la seguridad de la información dentro de la institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- El comité deberá convocarse trimestralmente o cuando las circunstancias lo ameriten; se deberá llevar registros y actas de las reuniones.
- Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información.
- Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información.
- Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información.

2.1.9.2 Oficial de Seguridad de la Información (OSI)

Según el artículo 7 del mismo Acuerdo Ministerial [64], el Oficial de Seguridad de la Información debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, y se recomienda que el OSI no sea parte del área de Tecnologías de la Información. Debe tener cualidades de liderazgo, ser capaz de lograr acuerdos y consensos, poder de gestión, entre otras, y debe contar con la aceptación y el apoyo de toda la organización, razón por la cual es importante que sea elegido por consenso.

2.1.9.2.1 Responsabilidades

Las responsabilidades del OSI están dispuestas de forma general en el artículo 8 del Acuerdo [64], redactadas de la siguiente manera:

- Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
- Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información.

- Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes Áreas.
- Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información.
- Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.
- Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
- Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
- Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.
- Mantener la documentación de la implementación del EGSI debidamente organizada.
- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad establecidos.
- Informar al Comité de Seguridad de la información, el avance de la implementación del EGSI, así como las alertas que impidan su implementación.
- Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad; en caso de ausencia, al Comité de Seguridad de la Información.
- La Guía de Implementación del EGSI [73] desarrolla con mayor detalle cada uno de los puntos del Acuerdo Ministerial en cuestión.

2.1.10 CRITERIOS DE VALORACIÓN

Según la norma ISO/IEC 27005 [5], es menester establecer los criterios con los cuales se evaluará el riesgo, impacto, entre otros. Estos criterios son la base para la estimar valores en el Método de Análisis y Evaluación de Riesgos (MAER) desarrollado para este proyecto.

2.1.10.1 Criterios de valoración de activo de información

El valor del activo viene definido en las dimensiones de confidencialidad, disponibilidad e integridad, así como el costo por recuperar las dos últimas (puesto que no es posible recuperar la confidencialidad si se ha revelado la información). Una vez que hayan sido levantados los activos de información, deben ser valorados a través de estos criterios, cuyos valores son estimados cuando se ha llegado a un consenso entre los evaluadores.

2.1.10.1.1 Confidencialidad

Los activos de información son valorados en la dimensión de confidencialidad según los efectos legales que pueda representar si su información es revelada y/o se llega a incumplir los acuerdos de confidencialidad. La Tabla 2.6 contiene los umbrales de valoración de la confidencialidad según los dos factores mencionados.

Tabla 2.6. Confidencialidad: criterios de valoración según efecto legal
[Elaboración propia]

Cualidad:		**Efecto legal**	
La divulgación del activo o su información representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Problemas legales y sanciones penales muy altas.
4	Alto	A	Problemas legales y sanciones penales altas.
3	Medio	M	Problemas legales y sanciones penales moderadas.
2	Bajo	B	Problemas legales y sanciones penales bajas.
1	Muy bajo	MB	Ningún problema legal.
La divulgación o exposición de la información			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Incumple totalmente con el acuerdo de confidencialidad.
4	Alto	A	Puede incumplir gravemente con el acuerdo de confidencialidad.
3	Medio	M	Puede incumplir levemente con el acuerdo de confidencialidad.
2	Bajo	B	Puede incumplir insignificantemente con el acuerdo de confidencialidad.
1	Muy bajo	MB	No incumple con ningún acuerdo de confidencialidad.

Así mismo, se valoran los activos en la dimensión de confidencialidad según la cantidad de datos personales que puedan exponerse a través de este activo.

La Tabla 2.7 contiene los criterios de valoración del activo en la dimensión de confidencialidad según el efecto personal.

También se valoran los activos en la dimensión de la confidencialidad según la cantidad de información confidencial que pueda ser revelada, así como la información del activo pueda facilitar al secuestro de la información y cómo puede verse afectada la reputación de la institución (Tabla 2.8).

Tabla 2.7. Confidencialidad: criterios de valoración según efecto personal [Elaboración propia]

Cualidad:		**Efecto personal**	
La divulgación del activo o su información causa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Muy alta exposición de información personal privada.
4	Alto	A	Alta exposición de la información personal privada.
3	Medio	M	Moderada exposición de la información personal privada.
2	Bajo	B	Leve exposición de la información personal privada.
1	Muy bajo	MB	No hay exposición de información personal privada.

Tabla 2.8. Confidencialidad: criterios de valoración según efecto institucional [Elaboración propia]

Cualidad:		**Efecto institucional**	
La divulgación del activo o su información causa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Muy alta exposición de información institucional confidencial.
4	Alto	A	Alta exposición de la información institucional confidencial.
3	Medio	M	Moderada exposición de la información institucional confidencial.
2	Bajo	B	Leve exposición de la información institucional confidencial.
1	Muy bajo	MB	No hay exposición de información institucional confidencial.
La divulgación del activo o su información causa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Muy alta facilidad para el secuestro y fuga de la información crítica.
4	Alto	A	Alta facilidad para el secuestro y fuga de la información crítica.
3	Medio	M	Leve facilidad para el secuestro y fuga de la información crítica.
2	Bajo	B	Muy baja facilidad para el secuestro y fuga de la información crítica.
1	Muy bajo	MB	Nula o insignificante facilidad para el secuestro y fuga de la información.
La divulgación del activo o su información causa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Grave (o total) pérdida de reputación y confianza de los usuarios.
4	Alto	A	Alta pérdida de reputación y confianza de los usuarios.
3	Medio	M	Moderada pérdida de reputación y confianza de los usuarios.
2	Bajo	B	Insignificante pérdida de reputación y confianza de los usuarios.
1	Muy bajo	MB	Ninguna pérdida de reputación o confianza de los usuarios.

2.1.10.1.2 Integridad

Los activos de información son valorados en la dimensión de integridad según el efecto legal que incluya problemas y sanciones penales, si se adultera la información de éstos o su información. La Tabla 2.9 contiene los criterios de valoración según estas consideraciones.

Tabla 2.9. Integridad: criterios de valoración según efecto legal
[Elaboración propia]

Cualidad:		**Efecto legal**	
La adulteración del activo o su información representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Problemas legales y sanciones penales muy altas.
4	Alto	A	Problemas legales y sanciones penales altas.
3	Medio	M	Problemas legales y sanciones penales moderadas.
2	Bajo	B	Problemas legales y sanciones penales bajas.
1	Muy bajo	MB	Ningún problema legal.

Como en la confidencialidad, los activos se evalúan en la dimensión de integridad según los problemas que puede acarrear la adulteración de los datos personales. La Tabla 2.10 contiene los criterios de valoración según esta consideración.

Tabla 2.10. Integridad: criterios de valoración según efecto personal
[Elaboración propia]

Cualidad:		**Efecto personal**	
La adulteración de la información personal representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Un problema muy grave en el desempeño del activo.
4	Alto	A	Un problema grave en el desempeño del activo.
3	Medio	M	Un problema moderado en el desempeño del activo.
2	Bajo	B	Un problema leve en el desempeño del activo.
1	Muy bajo	MB	Ningún problema en el desempeño del activo.

Un activo es valorado en la dimensión de integridad si la adulteración de la información institucional puede afectar el desempeño, la actividad normal, la reputación de la institución, o la actividad de terceras partes relacionadas. La Tabla 2.11 contiene los criterios de valoración del activo en las consideraciones mencionadas.

Tabla 2.11. Integridad: criterios de valoración según efecto personal
[Elaboración propia]

Cualidad:		**Efecto institucional**	
La adulteración de la información institucional representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Un problema muy grave en el desempeño del activo.
4	Alto	A	Un problema grave en el desempeño del activo.
3	Medio	M	Un problema moderado en el desempeño del activo.
2	Bajo	B	Un problema leve en el desempeño del activo.
1	Muy bajo	MB	Ningún problema en el desempeño del activo.
La adulteración de la información administrativa representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Un problema extremadamente grave en la actividad normal de la institución.
4	Alto	A	Un problema grave en la actividad normal de la institución.
3	Medio	M	Un problema importante en la actividad normal de la institución.
2	Bajo	B	Un problema leve en la actividad normal de la institución.
1	Muy bajo	MB	Podría no ser necesario detener las actividades de la institución para reestablecer la integridad de este archivo.
La adulteración del activo o su información provoca			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Grave (o total) pérdida de reputación y confianza de los usuarios.
4	Alto	A	Alta pérdida de reputación y confianza de los usuarios.
3	Medio	M	Moderada pérdida de reputación y confianza de los usuarios.
2	Bajo	B	Insignificante pérdida de reputación y confianza de los usuarios.
1	Muy bajo	MB	Ninguna pérdida de reputación o confianza de los usuarios.
La integridad del activo o su información afecta			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Gravemente a las actividades de usuarios o terceras partes.
4	Alto	A	Considerablemente a las actividades de usuarios o terceras partes.
3	Medio	M	Moderadamente a las actividades de usuarios o terceras partes.
2	Bajo	B	Levemente a las actividades de usuarios o terceras partes.
1	Muy bajo	MB	En ninguna forma a las actividades de usuarios o terceras partes.

2.1.10.1.3 Disponibilidad

Un activo es valorado en la dimensión de disponibilidad según el efecto legal que puede acarrear el no estar disponible cuando se lo requiera. La Tabla 2.12 contiene los criterios de valoración según esta consideración.

Tabla 2.12. Disponibilidad: criterios de valoración según efecto legal
[Elaboración propia]

Cualidad:		**Efecto legal**	
La indisponibilidad del activo o su información representa			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Problemas legales y sanciones penales muy altas.
4	Alto	A	Problemas legales y sanciones penales altas.
3	Medio	M	Problemas legales y sanciones penales moderadas.
2	Bajo	B	Problemas legales y sanciones penales bajas.
1	Muy bajo	MB	Ningún problema legal.

En el aspecto institucional, se valora en cómo la indisposición del activo o su información puede afectar a la operación interna, a terceras partes relacionadas o a la reputación de la institución. La Tabla 2.13 contiene los criterios de valoración según estas consideraciones.

Tabla 2.13. Disponibilidad: criterios de valoración según efecto institucional
[Elaboración propia]

Cualidad:		**Efecto institucional**	
La indisponibilidad del activo o su información provoca:			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Grave afectación o estancamiento en la operación interna.
4	Alto	A	Considerable o estancamiento afectación en la operación interna.
3	Medio	M	Moderada o estancamiento afectación en la operación interna.
2	Bajo	B	Poca afectación o estancamiento en la operación interna.
1	Muy bajo	MB	Nula o insignificante afectación o estancamiento en la operación interna.
La indisponibilidad del activo o su información afecta:			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Gravemente a las actividades de usuarios o terceras partes.
4	Alto	A	Considerablemente a las actividades de usuarios o terceras partes.
3	Medio	M	Moderadamente a las actividades de usuarios o terceras partes.
2	Bajo	B	Levemente a las actividades de usuarios o terceras partes.
1	Muy bajo	MB	En ninguna forma a las actividades de usuarios o terceras partes.
La indisponibilidad del activo o su información provoca:			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Grave (o total) pérdida de reputación y confianza de los usuarios.
4	Alto	A	Alta pérdida de reputación y confianza de los usuarios.
3	Medio	M	Moderada pérdida de reputación y confianza de los usuarios.
2	Bajo	B	Insignificante pérdida de reputación y confianza de los usuarios.
1	Muy bajo	MB	Ninguna pérdida de reputación o confianza de los usuarios.

2.1.10.1.4 Costo

Para la valoración del costo se ha tomado una escala de valor cualitativa, para que guarde homogeneidad en el proceso de valoración de activos de información. Además, se consideran los costos por recuperación solo en las dimensiones de integridad y disponibilidad, puesto que no se puede recuperar la confidencialidad si ha sido violada. La Tabla 2.14 contiene los criterios de valoración del costo de un activo.

Tabla 2.14. Costo: criterios de valoración del costo
[Elaboración propia]

Cualidad:		**Costo**	
La pérdida de integridad del activo genera			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Muy alto costo por recuperación de la integridad.
4	Alto	A	Alto costo por recuperación de la integridad.
3	Medio	M	Costo moderado por recuperación de la integridad.
2	Bajo	B	Bajo costo por recuperación de la integridad.
1	Muy bajo	MB	Costo insignificante por recuperación de la integridad.
La pérdida de disponibilidad del activo genera			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Muy alto costo por recuperación de la disponibilidad.
4	Alto	A	Alto costo por recuperación de la disponibilidad.
3	Medio	M	Costo moderado por recuperación de la disponibilidad.
2	Bajo	B	Bajo costo por recuperación de la disponibilidad.
1	Muy bajo	MB	Costo insignificante por recuperación de la disponibilidad.
La indisponibilidad del activo o su información provoca			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Grave pérdida material y/o financiera.
4	Alto	A	Alta pérdida material y/o financiera.
3	Medio	M	Moderada pérdida material y/o financiera.
2	Bajo	B	Baja pérdida material y/o financiera.
1	Muy bajo	MB	Insignificante o ninguna pérdida material y/o financiera.

2.1.10.2 Criterios de valoración de los niveles de dependencia

El grado de dependencia indica en qué porcentaje un activo depende de otro, a fin de conocer cómo puede verse afectado si el o los activos de los cuales depende son impactados por una amenaza. Los criterios que se presentan en las tablas siguientes no evalúan el grado de dependencia directamente, sino que permiten la estimación de los niveles de dependencia en cada dimensión de seguridad, y con éstos se procede al cálculo del grado de dependencia como se indica en el método de análisis y evaluación de riesgos

más adelante. La Tabla 2.15 contiene los criterios de valoración de los niveles de dependencia en las dimensiones canónicas de la seguridad de la información.

Tabla 2.15. Dependencia: criterios de valoración en dimensiones canónicas [Elaboración propia]

Dependencia: confidencialidad			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Toda la información (flujo de información) del activo dependiente puede ser develada en este activo.
4	Alto	A	Una gran parte de la información (flujo de información) del activo dependiente puede ser develada en el activo actualmente analizado.
3	Medio	M	Una moderada parte de la información (flujo de información) del activo dependiente puede ser develada en el activo actualmente analizado.
2	Bajo	B	La información (flujo de información) del activo dependiente puede ser develada en muy poco en este activo.
1	Muy bajo	MB	La información (flujo de información) del activo dependiente no puede ser develada en este activo.
X	No aplica	NA	No hay dependencia directa.
Dependencia: integridad			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Toda la información (flujo de información) del activo dependiente puede ser adulterada en este activo.
4	Alto	A	Una gran parte de la información (flujo de información) del activo dependiente puede ser adulterada en el activo actualmente analizado.
3	Medio	M	Una moderada parte de la información (flujo de información) del activo dependiente puede ser adulterada en el activo actualmente analizado.
2	Bajo	B	La información (flujo de información) del activo dependiente puede ser adulterada en muy poco en este activo.
1	Muy bajo	MB	La información (flujo de información) del activo dependiente no puede ser adulterada en este activo.
X	No aplica	NA	No hay dependencia directa.
Dependencia: disponibilidad			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Toda la información (flujo de información) del activo dependiente puede ser bloqueada o quedar indisponible con o a través del activo actualmente analizado.
4	Alto	A	Una gran parte de la información (flujo de información) del activo dependiente puede ser bloqueada o quedar indisponible con o a través del activo actualmente analizado.
3	Medio	M	Una parte moderada de la información (flujo de información) del activo dependiente puede ser bloqueada o quedar indisponible con o a través del activo actualmente analizado.
2	Bajo	B	La información (flujo de información) del activo dependiente puede ser bloqueada en muy poco o quedar indisponible con o a través del activo actualmente analizado.
1	Muy bajo	MB	La información (flujo de información) del activo dependiente no puede ser bloqueada o quedar indisponible con o a través del activo actualmente analizado.
X	No aplica	NA	No hay dependencia directa.

También se estima el nivel de dependencia según la facilidad que tenga el atacante de llevar a cabo un ataque hacia un activo dependiente, según el nivel de conocimiento y los recursos que requiera, y cuán graves perciba que son las acciones penales en su contra. La Tabla 2.16 contiene los criterios de dependencia según estas consideraciones.

Tabla 2.16. Dependencia: criterios de valoración según las consideraciones del atacante [Elaboración propia]

Dependencia: recursos del atacante y nivel de conocimiento			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	El atacante puede ser cualquier persona (dentro, fuera o que sepa algo de la institución), capaz de burlar la seguridad sin necesidad de medios especiales para llevar a cabo el ataque.
4	Alto	A	El atacante puede ser una persona con conocimientos suficientes, capaz de burlar la seguridad sin necesidad de medios especiales para llevar a cabo el ataque.
3	Medio	M	El atacante puede ser un profesional, sin necesidad de herramientas especiales (fuera de los disponibles en la profesión) para llevar a cabo el ataque.
2	Bajo	B	El atacante puede ser un especialista o un profesional, con herramientas o medios especiales, o un grupo de profesionales que, usando medios o herramientas colectivos, pueden burlar la seguridad y llevar a cabo el ataque.
1	Muy bajo	MB	El atacante puede ser un experto. Solo pocos expertos determinados, con medios excepcionales, pueden burlar la seguridad y llevar a cabo el ataque.
X	No aplica	NA	No hay dependencia directa.
Dependencia: penalización al atacante			
Valor	**Nivel**	**Abrev.**	**Descripción**
5	Muy alto	MA	Las acciones penales contra el atacante son muy leves. El atacante puede considerar lógicamente que no corre ningún riesgo personal, no ser identificado o usar argumentos sólidos en su defensa.
4	Alto	A	Las acciones penales contra el atacante son leves. El atacante puede considerar lógicamente que corre un pequeño riesgo personal y podría no ser identificado.
3	Medio	M	Las acciones penales contra el atacante son moderadas. El atacante puede considerar lógicamente que corre un mediano riesgo personal, pero aún soportable. Podría no ser identificado.
2	Bajo	B	Las acciones penales contra el atacante son graves. El atacante puede considerar lógicamente que corre un alto riesgo personal, y hay una gran posibilidad de ser identificado.
1	Muy bajo	MB	Las acciones penales contra el atacante son muy graves. El atacante se da cuenta de la seguridad con que será identificado y de que corre un grave riesgo personal.
X	No aplica	NA	No hay dependencia directa.

2.1.10.3 Criterios de valoración de nivel de degradación para el impacto

2.1.10.3.1 Nivel de degradación para el impacto

Estos niveles dependen de cuánto afecta una amenaza determinada a un activo en una dimensión en particular, y se expresa como un porcentaje de daño. La escala de la Tabla 2.17 ha sido tomada del documento Ayuda de PILAR Basic [94], basado en MAGERIT.

Tabla 2.17. Niveles de degradación [Elaboración propia, basada en [94]]

Porcentaje	Nivel	Abrev.	Descripción
100%	Total	T	La amenaza degrada totalmente al activo en la dimensión actual.
90%	Muy alta	MA	La amenaza causa muy alta degradación en el activo en la dimensión actual.
50%	Alta	A	La amenaza causa alta degradación en el activo en la dimensión actual.
10%	Media	M	La amenaza causa degradación moderada en el activo en la dimensión actual.
1%	Baja	B	La amenaza causa baja o insignificante degradación en el activo en la dimensión actual.

2.1.10.3.2 Impacto

El impacto se calcula según se indica en el Método de Análisis y Evaluación de Riesgos (MAER) de este proyecto. El impacto máximo equivale al producto entre el mayor valor acumulado de todos los activos y el 100% de degradación (Ecuación 2.1). El impacto resultante se jerarquiza por niveles siguiendo una escala logarítmica base 10, usando como referencia el impacto máximo. Los niveles han sido establecidos en forma de umbrales que definen los rangos dentro de los que se clasificarán los valores de impacto, puesto que éstos toman valores reales dentro de un rango continuo de valores (Tabla 2.18).

$$Impacto_{(MÁX)} = VA_{(MÁX)} \times degr_{(MÁX)} \tag{2.1}$$

Tabla 2.18. Valoración del impacto [Elaboración propia]

	Nivel	Abrev.	Descripción
100% $Impacto_{(MÁX)}$			
	Muy alto	MA	El impacto es vital
10% $Impacto_{(MÁX)}$			
	Alto	A	El impacto es muy grave
1% $Impacto_{(MÁX)}$			
	Medio	M	El impacto es grave
0.1% $Impacto_{(MÁX)}$			
	Bajo	B	El impacto es considerable
0.01% $Impacto_{(MÁX)}$			
	Muy bajo	MB	El impacto es insignificante
0%			

2.1.10.4 Criterios de valoración de la probabilidad

MEHARI prefiere el término “potencialidad” para evaluar la posibilidad de que una amenaza pueda materializarse de forma cualitativa, pues explica que “probabilidad” es una perspectiva cuantitativa. Por esta razón, la probabilidad es calculada a partir de escalas de potencialidad. Dichas escalas se han dividido según el origen de la amenaza: si es deliberada o si es natural o accidental.

a. **Deliberada:** llevada a cabo por un atacante según su interés y la facilidad para realizarla.
b. **Natural / accidental:** ocurre según las condiciones del entorno, por la susceptibilidad y la frecuencia con que ocurre.

2.1.10.4.1 Potencialidad de una amenaza deliberada

La potencialidad total de un ataque se evalúa en dos factores de potencialidad: facilidad para llevar a cabo el ataque, y el interés del atacante en hacerlo.

MEHARI explica que es necesario considerar el nivel de facilidad que pueda representar a un atacante en particular el llevar a cabo un ataque determinado. Para esto puede considerarse, por ejemplo, el nivel de preparación y los recursos necesarios que se requieran para efectuar dicho ataque según las condiciones en las que se encuentra el activo objetivo en particular. La Tabla 2.19 contiene los criterios de valoración de este factor, tomados de la escala de probabilidad del documento Ayuda de PILAR Basic [94].

Tabla 2.19. Criterios de valoración de potencialidad por facilidad para el atacante [Elaboración propia, basada en [94]]

Valor p(f)	Nivel	Abrev.	Descripción
100%	Fácil	F	El atacante podría llevar a cabo el ataque con gran facilidad.
10%	Medio	M	El atacante podría llevar a cabo el ataque con moderada facilidad.
1%	Difícil	D	El atacante podría llevar a cabo el ataque con dificultad.
0.1%	Muy difícil	MD	El atacante podría llevar a cabo el ataque, pero con alta dificultad.
0.01%	Extremadamente difícil	ED	El atacante podría llevar a cabo el ataque con dificultad extrema.

Así mismo, MEHARI considera que es necesario tener en cuenta el nivel de interés que tenga un atacante en llevar a cabo un ataque particular (reflejado también en el interés que

tenga por el activo objetivo en cuestión). La Tabla 2.20, contiene los criterios de valoración de la potencialidad por interés del atacante.

Tabla 2.20. Criterios de valoración de potencialidad por interés del atacante [Elaboración propia]

Valor	Nivel	Abrev.	Descripción
100%	Alto interés	AI	El atacante podría tener un alto interés en el activo.
10%	Medio interés	MI	El atacante podría tener un interés moderado en el activo.
1%	Muy poco interés	MPI	El atacante podría tener muy poco interés en el activo.
0.1%	Escaso interés	EI	El atacante podría tener un escaso interés en el activo.
0.01%	Sin interés	SI	El atacante podría no tener interés alguno por él activo.

2.1.10.4.2 Potencialidad de una amenaza natural o accidental

La potencialidad total de un evento de este origen se evalúa en dos factores de potencialidad: la susceptibilidad y la frecuencia.

La susceptibilidad es la sensibilidad con que se es capaz de recibir la amenaza y sus efectos. Ésta se encuentra relacionada con el riesgo en cuanto al nivel al que está expuesto un activo en particular al medio. MEHARI llama a esto “exposición natural”. La Tabla 2.21 contiene los criterios de valoración de potencialidad según este factor.

Tabla 2.21. Criterios de valoración de potencialidad por susceptibilidad [Elaboración propia]

Valor	Susceptibilidad	Abrev.	Descripción
100%	Muy susceptible	MS	Alta susceptibilidad.
10%	Moderadamente Susceptible	S	Susceptibilidad media.
1%	Poco susceptible	N	Susceptibilidad baja.
0.1%	Muy poco susceptible	PS	Susceptibilidad muy baja.
0.01%	No susceptible	MPS	Susceptibilidad insignificante.

La frecuencia de ocurrencia es otro factor a considerar. Se recurre normalmente a la tasa anual de ocurrencia (ARO – *Annual Rate of Occurrence*) como medida de probabilidad, tomando como referencia un año. El libro 1 de MAGERIT [76] proporciona una escala de valores como la que se presenta en la Tabla 2.22.

Tabla 2.22. Criterios de valoración de potencialidad por frecuencia
[Elaboración propia, basada en [76]]

Valor	Nivel	Abrev.	Descripción
100%	Muy frecuente	MF	A diario – varias veces al mes.
10%	Frecuente	F	Mensualmente – varios meses al año.
1%	Normal	N	Una vez al año.
0.1%	Poco frecuente	PF	Cada varios años.
0.01%	Muy poco frecuente	MPF	Siglos.

2.1.10.4.3 Probabilidad resultante

La probabilidad resultante se calcula como el producto de los factores de cada par, según el origen de la amenaza, como se indica en el método de análisis y evaluación de riesgos, y se organiza siguiendo el esquema de la matriz de probabilidad de la Tabla 2.23. La evaluación de la probabilidad para cada origen se encuentra en el apartado de evaluación del riesgo.

Tabla 2.23. Matriz de probabilidad [Elaboración propia]

Factor de potencialidad 2					
100%	0.01%	0.1%	1%	10%	100%
10%	0.001%	0.01%	0.1%	1%	10%
1%	0.0001%	0.001%	0.01%	0.1%	1%
0.1%	0.00001%	0.0001%	0.001%	0.01%	0.1%
0.01%	0.000001%	0.00001%	0.0001%	0.001%	0.01%
	0.01%	0.1%	1%	10%	100%
	Factor de potencialidad 1				

2.1.10.5 Criterios de valoración del riesgo

Los niveles del riesgo se ajustan a una escala logarítmica del porcentaje (base 10), siendo el máximo valor de riesgo un valor en función de los máximos valores de impacto y probabilidad posibles, como se muestra en la Ecuación 2.2.

$$Riesgo_{(MÁX)} = Impacto_{(MÁX)} \times Probabilidad_{(MÁX)} \quad (2.2)$$

La descripción de los niveles, así como los colores, han sido adaptados de los niveles de emergencia según el triaje de Mánchester, tal y como se observa en la Tabla 2.24.

Tabla 2.24. Niveles de riesgo en escala logarítmica [Elaboración propia]

	Nivel	Abrev.	Descripción
100% $Riesgo_{(MÁX)}$			
	Muy alto	MA	Muy alto riesgo. Riesgo de atención inmediata (crítico).
10% $Riesgo_{(MÁX)}$			
	Alto	A	Alto riesgo. Riesgo de emergencia (emergencia de primer nivel).
1% $Riesgo_{(MÁX)}$			
	Medio	M	Riesgo moderado. Riesgo de urgencia (emergencia de segundo nivel).
0.1% $Riesgo_{(MÁX)}$			
	Bajo	B	Bajo riesgo. Riesgo de urgencia menor (riesgo estándar).
0.01% $Riesgo_{(MÁX)}$			
	Aceptable	AC	Riesgo aceptable. Riesgo no urgente o descartable.
0%			

2.1.10.6 Criterios de valoración de eficacia de las salvaguardas

Las salvaguardas son medidas de control con las que pueden mitigarse los riesgos que corren los activos de información. MEHARI establece que las medidas de control pueden diferenciarse según su mecanismo: prevenir de la ocurrencia de una amenaza sobre un activo, o corregir o recuperar un activo si la amenaza llega a ocurrir [84]. Las tablas con los criterios de valoración de eficacia de las medidas de control han sido adaptadas de MEHARI [82], ajustando las escalas de valor a 5 niveles, y asociando a cada nivel un factor de reducción.

La eficacia de una salvaguarda se evalúa según el factor de reducción correspondiente: a menor factor de reducción, mayor eficacia. El factor de reducción es definido por un porcentaje. Los umbrales han sido definidos en 5 niveles entre 0% y 100%, en una escala logarítmica base $\sqrt[5]{100}$. La Tabla 2.25 contiene los factores de reducción, en porcentajes redondeados, con los que se evaluará la eficacia de las medidas de control.

Tabla 2.25. Factor de reducción para medir el nivel de eficacia de una salvaguarda [Elaboración propia]

Nivel de eficacia	Factor de reducción %	Factor de reducción (aprox.) %	Descripción
Muy alta	$\left(\sqrt[5]{100}\right)^{1}$ %	3 %	Muy alta eficacia, con muy alta capacidad de reducción.
Alta	$\left(\sqrt[5]{100}\right)^{2}$ %	6 %	Alta eficacia, con alta capacidad de reducción.
Media	$\left(\sqrt[5]{100}\right)^{3}$ %	16 %	Eficacia media, con capacidad de reducción moderada.
Baja	$\left(\sqrt[5]{100}\right)^{4}$ %	40 %	Baja eficacia, con capacidad de reducción considerable.
Muy baja o nula	$\left(\sqrt[5]{100}\right)^{5}$ %	100 %	Eficacia insignificante, con capacidad de reducción nula.

2.1.10.6.1 Salvaguardas frente al impacto

Según su mecanismo, las medidas de control que hacen frente al impacto son correctivas, y se aplican cuando una amenaza se ha materializado. MEHARI establece que existen tres mecanismos de medidas correctivas [81]: limitantes (protección), paliativas y de recuperación.

- **Medidas limitantes o de protección**: limitan las consecuencias de directas de una amenaza en espacio y en tiempo. Por ejemplo, puede haber medidas de detección, post-controles integrados en procesos informáticos y aplicaciones, capacidades de intervención rápida, etc. La Tabla 2.26 ha sido adaptada de la escala de valor de medidas limitantes de MEHARI [84], ajustada a 5 niveles.

Tabla 2.26. Criterios de valoración de eficacia de medidas limitantes [Elaboración propia, basada en [84]]

Mecanismo:	Correctivo		
Tipo de control:	Limitante o de protección		
Nivel de eficacia	**Factor de reducción %**	**Factor de reducción**	**Descripción**
Muy alta	3 %	0.03	El daño y sus consecuencias directas son limitadas rápidamente, puesto que la detección y la reacción son inmediatas.
Alta	6 %	0.06	El daño y sus consecuencias directas pueden limitarse considerablemente porque el tiempo de detección y el de reacción son altos.
Media	16 %	0.16	El daño y sus consecuencias directas pueden limitarse moderadamente, y el tiempo de detección es moderado, igual que el tiempo de reacción.
Baja	40 %	0.4	El daño y sus consecuencias directas pueden limitarse, pero el tiempo en detectarlas aún es alto y el tiempo de reacción es moderado.
Muy baja	100 %	1	El daño y sus consecuencias directas no se pueden limitar, o no se detectarán durante un largo tiempo, y el tiempo de reacción es lento.

- **Medidas paliativas**: Aquellas que actúan para reducir las consecuencias indirectas de una amenaza. Puede haber, por ejemplo, análisis previos sobre qué sistemas, procesos o servicios indispensables deben ofrecerse mínimamente, preparación de planes de mantenimiento, planes de respaldo y restauración (*backups*), etc. En la Tabla 2.27 se encuentran los factores de reducción para evaluar la eficacia de las medidas paliativas, adaptada de MEHARI [84].

Tabla 2.27. Criterios de valoración de eficacia de medidas paliativas
[Elaboración propia, basada en [84]]

Mecanismo:		Correctivo	
Tipo de control:		Paliativa	
Nivel de eficacia	**Factor de reducción %**	**Factor de reducción**	**Descripción**
Muy alta	3 %	0.03	Las actividades normales de la institución continuarán sin interrupción observable.
Alta	6 %	0.06	Se ha planificado con mucho cuidado y detalle, y las medidas paliativas han sido probadas y validadas. El tiempo de recuperación de las actividades normales de la institución puede predecirse con precisión y en corto tiempo.
Media	16 %	0.16	Se ha planificado soluciones, aunque faltan detalles, pero la actividad normal de la institución podría recuperarse en un tiempo moderado.
Baja	40 %	0.4	Se ha planificado con poco cuidado. No se conoce con precisión el tiempo para restaurar la actividad normal de la institución.
Muy baja	100 %	1	No existe planificación. Uso de medidas completamente improvisadas o sin ningún efecto.

- **Medidas de recuperación**: También conocidas como "medidas de transferencia de riesgo", puesto que éstas permiten la recuperación transfiriendo las pérdidas a terceros mediante seguros o procesos penales. Los criterios adaptados de MEHARI se ven en la Tabla 2.28.

Tabla 2.28. Criterios de valoración de eficacia de medidas de recuperación
[Elaboración propia, basada en [84]]

Mecanismo:		Correctivo	
Tipo de control:		De recuperación	
Nivel de eficacia	**Factor de reducción %**	**Factor de reducción**	**Descripción**
Muy alta	3 %	0.03	Las actividades normales de la institución continuarán sin interrupción observable.
Alta	6 %	0.06	Lo que puede recuperarse a través de procesos legales o por seguros es suficiente para mitigar el daño, y las operaciones de la organización pueden continuar.
Media	16 %	0.16	Lo que puede recuperarse a través de procesos legales o por seguros es considerable, pero las actividades de la organización podrían recuperarse en un tiempo moderado.
Baja	40 %	0.4	Lo que puede recuperarse es poco, y la organización es la responsable de la mayor parte del impacto. No es seguro que la transferencia permita continuar con las operaciones.
Muy baja	100 %	1	Lo que puede recuperarse es insignificante o nulo en comparación con el daño causado.

2.1.10.6.2 Salvaguardas frente a probabilidad

Según su mecanismo, las medidas de control que hacen frente a la probabilidad son preventivas, y se aplican antes de la materialización de una amenaza. MEHARI establece que existen dos mecanismos de medidas de prevención [81]: disuasivas y preventivas.

- **Medidas disuasivas**: Reducen la probabilidad de ocurrencia de una amenaza deliberada. Cuanto mayor sea la percepción del riesgo para el delincuente, menor será la probabilidad de que el delincuente intente llevar a cabo un ataque. Ejemplos de estas medidas son la regulación con penalizaciones severas, tener registros, tener sistemas de detección y grabación, difundir la existencia de tales sistemas, etc. De los criterios de valoración de MEHARI [84] se ha adaptado a la Tabla 2.29:

Tabla 2.29. Criterios de valoración de eficacia de medidas disuasivas
[Elaboración propia, basada en [84]]

Mecanismo:	Preventivo		
Tipo de control:	Disuasivo		
Nivel de eficacia	**Factor de reducción %**	**Factor de reducción**	**Descripción**
Muy alta	3 %	0.03	El atacante puede considerar lógicamente que debe abandonar cualquier idea de realizar la acción. Sabe sin duda que será identificado, y que el castigo resultante superará cualquier ganancia potencial.
Alta	6 %	0.06	El atacante puede considerar lógicamente que corre un alto riesgo. Sabe que puede ser identificado con gran probabilidad y que el castigo será grave.
Media	16 %	0.16	El atacante potencial puede, lógicamente, considerar que corre solo un mediano riesgo. En cualquier caso, cualquier posible perjuicio personal será soportable.
Baja	40 %	0.4	El atacante puede considerar lógicamente que solo corre un pequeño riesgo personal. En cualquier caso, percibiría un posible perjuicio personal soportable y leve.
Muy baja o nula	100 %	1	El atacante puede considerar lógicamente que no corre ningún riesgo personal. Pueden considerar que no será identificado, o puede usar argumentos sólidos para refutar cualquier acusación relacionada con las acciones realizadas, o que cualquier castigo será muy leve.

- **Medidas preventivas**: Aquellas que actúan para reducir las consecuencias indirectas de una amenaza. Puede haber, por ejemplo, análisis previos sobre qué sistemas, procesos o servicios indispensables deben ofrecerse mínimamente,

preparación de planes de mantenimiento, planes de respaldo y restauración (*backups*), etc. En la Tabla 2.30 se encuentran los factores de reducción para evaluar la eficacia de las medidas paliativas, adaptada de MEHARI [84]:

Tabla 2.30. Criterios de valoración de eficacia de medidas preventivas [Elaboración propia, basada en [84]]

Mecanismo:	Preventivo		
Tipo de control:	Preventiva		
Nivel de eficacia	**Factor de reducción %**	**Factor de reducción**	**Descripción**
Muy alta	3 %	0.03	Las actividades normales de la institución continuarán sin interrupción observable.
Alta	6 %	0.06	Se ha planificado con mucho cuidado y detalle, y las medidas paliativas han sido probadas y validadas. El tiempo de recuperación de las actividades normales de la institución puede predecirse con precisión y en corto tiempo.
Media	16 %	0.16	Se ha planificado soluciones, aunque faltan detalles, pero la actividad normal de la institución podría recuperarse en un tiempo moderado.
Baja	40 %	0.4	Se ha planificado con poco cuidado. No se conoce con precisión el tiempo para restaurar la actividad normal de la institución.
Muy baja o nula	100 %	1	No existe planificación. Uso de medidas completamente improvisadas o sin ningún efecto.

2.2 MÉTODO DE ANÁLISIS Y EVALUACIÓN DE RIESGOS

El presente Método de Análisis y Evaluación del Riesgo (MAER) involucra el uso de los métodos cuantitativo y cualitativo durante el proceso. El modelo cuantitativo permite que los valores numéricos puedan operarse con el uso de fórmulas matemáticas, lo que requiere de mucho esfuerzo y genera un abanico de valores dentro de un rango continuo, mientras que el modelo cualitativo se limita a valoraciones relativas, lo que permite que se agilice el proceso de valoración. Los valores obtenidos del modelo cuantitativo han debido ser ubicados dentro de niveles establecidos cualitativamente a fin de hacer más fácil la comprensión del estado en el que se encuentra un objeto de juicio (el riesgo, por ejemplo).

Para la valoración de los activos en cada dimensión canónica de seguridad se utilizan escalas cualitativas ordinales, cuyos umbrales han sido definidos por valores numéricos, a fin de tratarlas como escalas cuantitativas discretas. Esto permite que los valores cualitativos, ahora representados en números, puedan operarse entre sí para obtener un

valor discreto final para cada activo. Por otro lado, el valor acumulado de cada activo, que se calcula con el valor propio del activo, el valor de los activos que dependen de él y el grado de dependencia de éstos, toma un valor real no discreto, que responde a un modelo cuantitativo-continuo, como se ilustra en el ejemplo de la Figura 2.3. Esto puede observarse en la Matriz de Riesgos, en el Anexo T.

Los grados de dependencia, el nivel de degradación de cada activo en cada dimensión, la probabilidad de ocurrencia y el nivel de eficacia de las salvaguardas han sido definidos dentro de escalas de valor cualitativas, a las que se asignan valores numéricos de escalas cuantitativas-discretas para que sean utilizadas en fórmulas, a fin de obtener los riesgos acumulados y residuales que toman valores reales dentro un rango continuo de valores.

Finalmente, aunque los valores de riesgos sean números reales dentro de un rango de valores continuo, han sido clasificados dentro de una escala de valor cualitativa, a la que también se le han asignado umbrales numéricos para clasificar el riesgo.

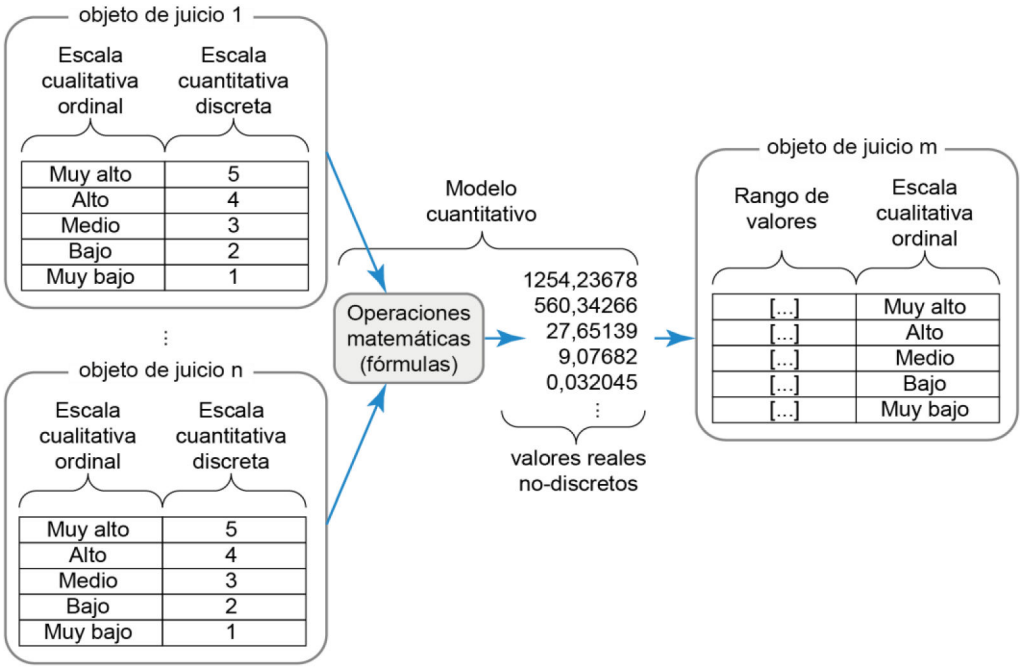


Figura 2.3. Ejemplo de tratamiento de valores en un modelo híbrido
[Elaboración propia]

Procesos típicos dentro un método de análisis de riesgos son: levantamiento, clasificación y valoración de activos, análisis de amenazas y vulnerabilidades, estimación de valores de impacto, probabilidad de ocurrencia y riesgo, identificación de las salvaguardas, estimación de la eficacia de las salvaguardas y estimación del riesgo residual. La Figura 2.4 muestra el Método de Análisis y Evaluación de Riesgos (MAER) a utilizar, desarrollado para este proyecto. El Anexo T se constituye como evidencia del resultado de todo este proceso.

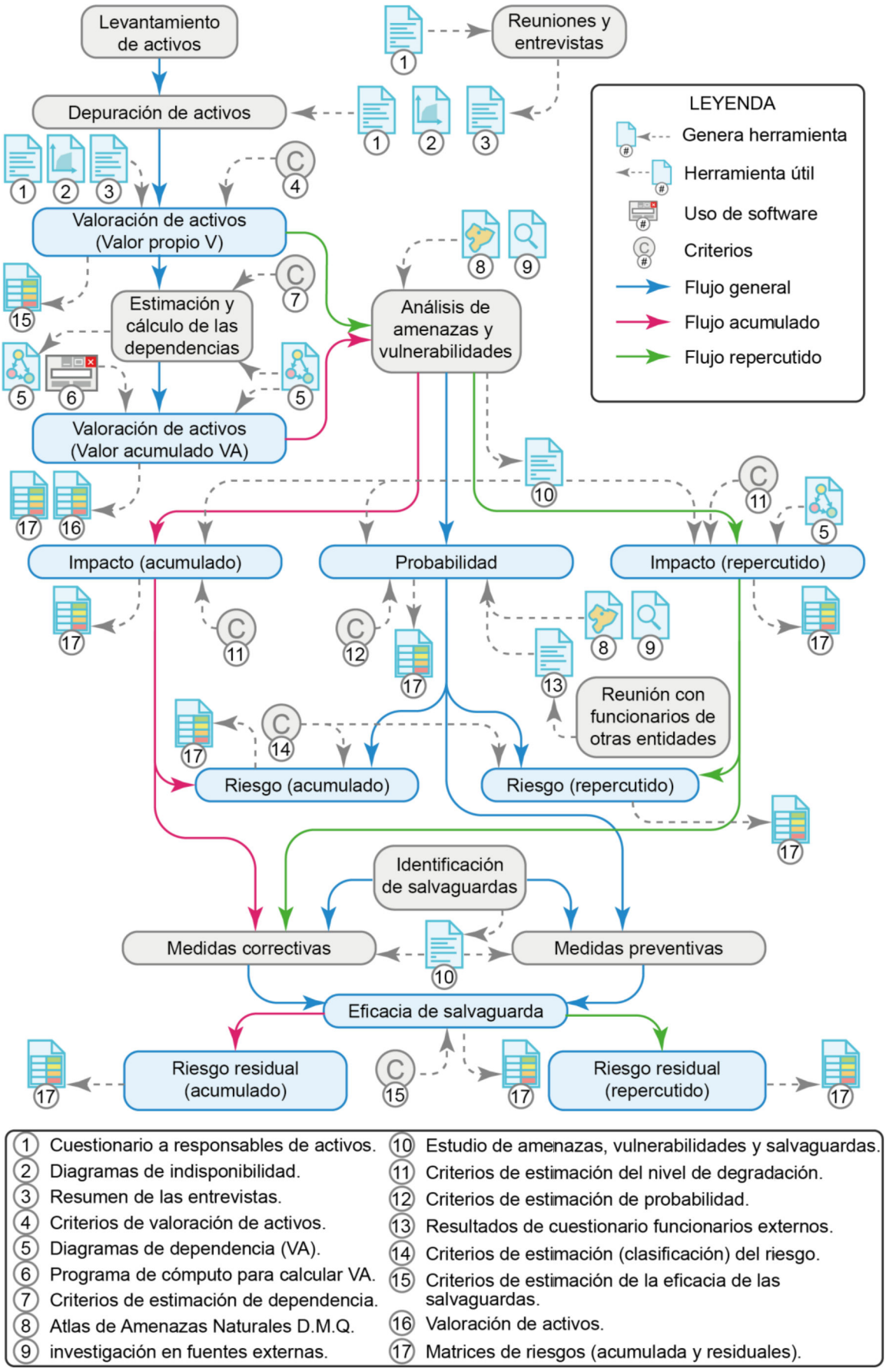


Figura 2.4. Método de análisis y evaluación de riesgos (MAER) [Elaboración propia].

2.2.1 LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN

2.2.1.1 Identificación de los activos de información

El anexo B de la norma ISO 27005 [5] proporciona un ejemplo de identificación de los activos de información que ha servido como base para su clasificación. Se ha establecido un esquema de codificación alfanumérica (ver Figura 2.5), según la clase y el tipo de activo de información como se indica en la Tabla 2.31.

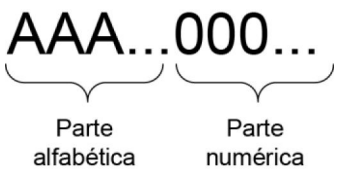


Figura 2.5. Esquema para identificación de activos de información [Elaboración propia]

Tabla 2.31. Identificación de activos de información [Elaboración propia]

Clase	Tipo	Sub-Tipo	Código
Activos primarios	Actividades del negocio		PAN000
	Información		INF000
Activos de soporte	Hardware	Equipo transportable	HWET00
		Equipo fijo	HWEF00
		Periféricos para procesamiento	HWPP00
		Medios para datos	HWMD00
	Software	Sistema operativo	SWSO00
		Software de servicio, mantenimiento y administración	SWSS00
		Paquetes de software o software estándar	SWPS00
		Aplicaciones del negocio	SWAN00
	Red	Medios de soporte	RDMS00
		Relevos pasivos o activos	RDPA00
	Personal	Personal a cargo de toma de decisiones (Jerárquico)	PEJE00
		Usuarios	PEUS00
		Personal de operaciones / mantenimiento	PEOM00
	Sitio	Ubicación	SIUB00
		Servicios esenciales	SISE00
	Organización	Subcontratistas, proveedores o fabricantes	ORPF00

Para el levantamiento de activos se ha considerado que se analicen por grupos según el tipo y sus características, salvo aquellas circunstancias en las que los activos requieran de un análisis individual. Por ejemplo, activos como las computadoras de escritorio se han analizado de forma segmentada por grupos según el tipo de usuario, puesto que comparten características similares, pero los sistemas y las bases de datos se analizan de forma individual puesto que son muy distintas en sus características como su relación con la misión, las normativas que las rigen, el tipo de información que albergan, etc.

2.2.1.2 Depuración de sistemas

Tabla 2.32. Etapa de depuración de sistemas [Elaboración propia]

Entrada	Proceso	Salida
• *Cuestionario lleno de los responsables y/o administradores de los sistemas (Anexo C)* • *Resumen de las entrevistas (Anexo D)* • *Diagramas de intolerancia a la no disponibilidad (Anexo E)*	• Depuración de sistemas que sin justificación han superado el tiempo de inactividad establecido para su vigencia.	• Sistemas que ingresarán en la gestión del riesgo.

MAGERIT señala que puede valorarse la interrupción del servicio de un activo según el tiempo que permanezca inactivo. Se ha adaptado este principio para poder ejercer la depuración de los sistemas que alberga la Planta Central del Ministerio de Cultura y Patrimonio, basado en el tiempo de inactividad[28]. Con la información recabada de los cuestionarios sobre los sistemas (Anexo C), el resumen de las entrevistas (Anexo D) y los diagramas de intolerancia a la no disponibilidad (Anexo E), se procede a la depuración. El proceso de depuración se indica en la Figura 2.6.

Este proceso permite tomar decisiones sobre aquellos sistemas que hayan superado los seis meses de inactividad. Por ejemplo, si un sistema ha superado este tiempo, se consulta con el responsable. Si el sistema es importante, pero una amenaza causó su interrupción, o es parte de un programa misional, y por su naturaleza requiere que su periodicidad de actualización sea mayor a seis meses (como el caso del sistema de CACAO del MCyP); en ambos casos, debe tomarse en cuenta el sistema en el análisis y evaluación de riesgos.

[28] No debe confundirse tiempo de interrupción con tiempo de inactividad. El primero se debe a una amenaza en la dimensión de la disponibilidad, mientras que el segundo es un concepto más amplio, es decir, que puede ser debido a una amenaza en la disponibilidad, o simplemente no ha sido necesitado, no ha sido utilizado o actualizado durante ese tiempo, o no es indispensable.

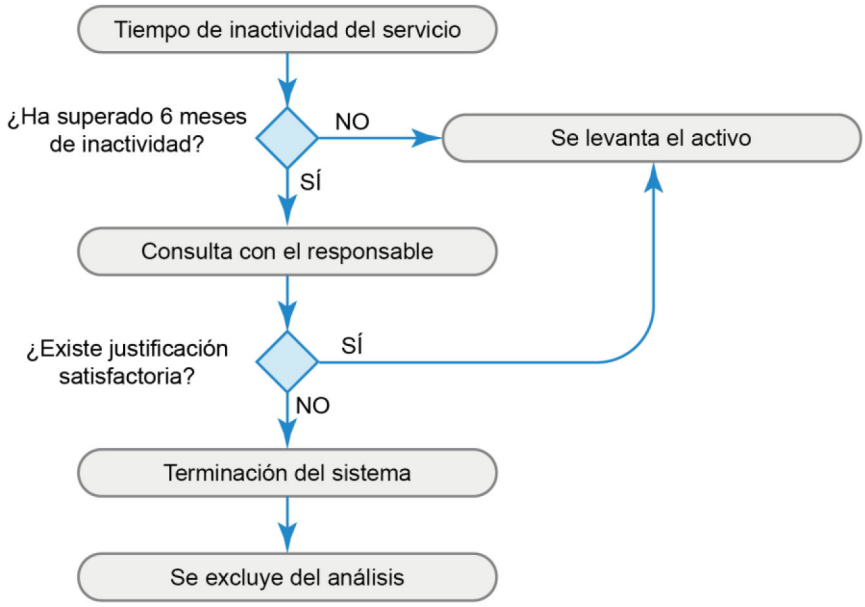


Figura 2.6. Proceso de depuración de sistemas [Elaboración propia].

Por otro lado, si el sistema no tiene la justificación debida para su mantención o si ya ha cumplido con su objetivo, debe darse de baja puesto que consume recursos innecesariamente, y debe excluirse del análisis y evaluación de riesgos. La Tabla 2.33 lista los sistemas que han sido dados de baja siguiendo este proceso.

Tabla 2.33. Sistemas eliminados en la depuración [Elaboración propia]

Nombre del sistema	Dominio
Kallari Yuyai	bpm.culturaypatrimonio.gob.ec
SIGCOMP	compromisos.culturaypatrimonio.gob.ec
CROMÏA 2015	cromia.culturaypatrimonio.gob.ec
Lo más destacado del MCYP	cultura.culturaypatrimonio.gob.ec
4to Concurso Fondo Fonográfico 2014	fondofonografico.culturaypatrimonio.gob.ec
Plataf. de Postulaciones a Fondos Concursables 2015	fondos.culturaypatrimonio.gob.ec
Resultados de Fondos Concursables 2015	fondosconcursables.culturaypatrimonio.gob.ec
Recorrido Informativo de la Diversidad Cultural 2015	furgoncultural.culturaypatrimonio.gob.ec
Ganadores del Fondo Fonográfico 2013	ganadores.culturaypatrimonio.gob.ec
Convocatoria los 100 de Cromía	los100decromia.culturaypatrimonio.gob.ec
Tour Virtual 3D	museos3d.culturaypatrimonio.gob.ec
Reg. Agrup. Infanto Juv., Sinfónico Corales, y de Trad.	orquestasj.culturaypatrimonio.gob.ec
Wikipedia de Patrimonio Alimentario del Ecuador	patrimonioalimentario.culturaypatrimonio.gob.ec/wiki
Prop. culturales para la Feria Internacional del Libro	propuestasfil.culturaypatrimonio.gob.ec
Concha Acústica Parque Samanes: Reg.de artistas…	psamanes.culturaypatrimonio.gob.ec
Convoc. QHAPAQ ÑAN - Sistema Vial Andino 2014	qhapaqnan.culturaypatrimonio.gob.ec
QHAPAQ ÑAN: archivos digitales y buscador	qn.culturaypatrimonio.gob.ec/qn/qn
Residencia de Gestión Cultural en Amazonía 2015	residenciasartisticas.culturaypatrimonio.gob.ec
Software Asociado a Equipos de Video Conferencia	videoconferencia.culturaypatrimonio.gob.ec
Proyecto Erotopías 2014	erotopias.com.ec
Fondo Fonográfico	fondofonograficoec.com
Red de Museos Nacionales	museos.gob.ec
Colecciones de Fondos Culturales	portalcultural.gob.ec
Sistema del Festival de Artes vivas de Loja	www.festivaldeloja.gob.ec

2.2.2 VALORACIÓN DE ACTIVOS

2.2.2.1 Estimación del valor propio

Tabla 2.34. Etapa de estimación del valor propio de los activos [Elaboración propia]

Entrada	Proceso	Salida
• *Cuestionario lleno de los responsables y/o administradores (Anexo C)* • *Resumen de las entrevistas (Anexo D)* • *Anexo E* • *Criterios de valoración de activos (Sección 2.1.10.1)*	• Estimación de valores en las dimensiones canónicas más el costo para cada activo • Aplicación de fórmulas para el cálculo del valor de las dimensiones y el costo • Aplicación de la fórmula para calcular el valor propio	• Valor propio de cada activo (Anexo F)

El valor propio de los activos se define por la estimación de valores en cada una de las dimensiones canónicas de seguridad y el costo, aplicando los criterios de valoración de activo de información definidos en la sección 2.1.10.1.

Para este proceso se usan los cuestionarios realizados a los responsables de los activos, algunos de los cuales se adjuntan en el Anexo C, y los resúmenes de las entrevistas efectuadas a los mismos junto con los diagramas de intolerancia a la no disponibilidad, que complementan con información relevante que no se contempla en los cuestionarios, los cuales se encuentran en los Anexos D y E, respectivamente, herramientas generadas de las reuniones y entrevistas con los funcionarios, a fin de que esta información pueda ser usada para poder estimar los valores.

En los cuestionarios se consideran factores como la relación directa de un activo con la misión de la organización, las obligaciones legales, la reputación, entre otros.

Con los valores obtenidos, se procede al cálculo del valor propio de cada activo usando las fórmulas que se indican a continuación. MAGERIT advierte sobre la necesidad del uso de una escala común para todas las dimensiones a fin de que se pueda comparar riesgos.

Tomando en cuenta este aviso, se calcula la media aritmética de los valores de los criterios de cada una de las dimensiones (incluyendo el costo), y el resultado es redondeado al entero más cercano. Así, el valor final de cada dimensión recae en un valor entero dentro de una escala de 5 niveles; es decir, que cada dimensión y el costo se evalúan sobre el mismo peso para el cálculo del valor propio. De esta forma, se garantiza el cumplimiento de la recomendación de MAGERIT.

Con la fórmula de la Ecuación 2.3 se obtiene el valor del activo en la dimensión de la confidencialidad.

$$V_C \approx \frac{P_{LSP} + A_C + E_{IPP} + E_{IIC} + S_{FIC} + R_{CU}}{6}; \quad V_C \in \mathbb{Z}^+ \ \wedge \ 0 < V_C \leq 5 \qquad (2.3)$$

Donde:

V_C	Valor del activo en la dimensión de confidencialidad
P_{LSP}	Problemas legales y sanciones penales
A_C	Acuerdo de confidencialidad
E_{IPP}	Exposición de la información personal privada
E_{IIC}	Exposición de la información institucional confidencial
S_{FIC}	Secuestro y fuga de la información crítica
R_{CU}	Reputación y confianza de los usuarios

Con la fórmula de la Ecuación 2.4 se obtiene el valor del activo en la dimensión de la integridad.

$$V_I \approx \frac{P_{LSP} + A_{PDA} + P_{DA} + P_{ANI} + R_{CU} + A_{UTP}}{6}; \quad V_I \in \mathbb{Z}^+ \ \wedge \ 0 < V_I \leq 5 \qquad (2.4)$$

Donde:

V_I	Valor del activo en la dimensión de integridad
P_{LSP}	Problemas legales y sanciones penales
A_{PDA}	Adulteración personal en el desempeño del activo
P_{DA}	Problemas en el desempeño del activo
P_{ANI}	Problemas en la actividad normal de la institución
R_{CU}	Reputación y confianza de los usuarios
A_{UTP}	Afectación a usuarios y terceras partes

Con la fórmula de la Ecuación 2.5 se obtiene el valor del activo en la dimensión de la disponibilidad.

$$V_D \approx \frac{P_{LSP} + A_{DOI} + A_{UTP} + R_{CU} + N_I}{5}; \quad V_D \in \mathbb{Z}^+ \ \wedge \ 0 < V_D \leq 5 \qquad (2.5)$$

Donde:

V_D	Valor del activo en la dimensión de disponibilidad
P_{LSP}	Problemas legales y sanciones penales
A_{DOI}	Afectación del desempeño de la operación interna
A_{UTP}	Afectación a usuarios y terceras partes
R_{CU}	Reputación y confianza de los usuarios
N_I	Nivel de intolerancia

MAGERIT expone que es muy frecuente valorar el costo del activo de forma cualitativa. Con la Ecuación 2.6 se obtiene el valor cualitativo del costo del activo.

$$V_{Costo} \approx \frac{C_{RI} + C_{RD} + P_{MF}}{3}; \quad V_{Costo} \in \mathbb{Z}^+ \ \wedge \ 0 < V_{Costo} \leq 5 \tag{2.6}$$

Donde:

V_{Costo}	Valor (cualitativo) del costo del activo
C_{RI}	Costo por recuperación de la integridad
C_{RD}	Costo por recuperación de la disponibilidad
P_{MF}	Pérdida material / financiera

El valor propio no requiere de este principio, y revela más si en lugar de hallar la media aritmética se acumulan los valores de las dimensiones y el costo, pudiendo tomar un valor entero positivo máximo de 20. Por ello, una vez calculados los valores, se usa la Ecuación 2.7 para hallar el valor propio del activo.

$$V = V_C + V_I + V_D + V_{Costo}; \quad V \in \mathbb{Z}^+ \ \wedge \ 0 < V \leq 20 \tag{2.7}$$

Donde:

V	Valor (propio) del activo
V_C	Valor del activo en la dimensión de confidencialidad
V_I	Valor del activo en la dimensión de integridad
V_D	Valor del activo en la dimensión de disponibilidad
V_{Costo}	Valor del costo del activo

Por ejemplo, si se tiene un activo X al que se desea evaluar, se estiman sus valores según los criterios de la sección 2.1.10.1. A continuación se muestran ejemplos del uso de las fórmulas para hallar los valores de un activo X, suponiendo que se han hecho las estimaciones y cálculos como se indica a continuación.

A partir de los valores del ejemplo de la Tabla 2.35, se calcula el valor del activo X en la confidencialidad con la Ecuación 2.3, obteniendo el valor de la Ecuación 2.8.

Tabla 2.35. Ejemplo de valoración en la confidencialidad [Elaboración propia]

CRITERIOS						
EFECTO LEGAL		EFECTO PERSONAL	EFECTO INSTITUCIONAL			
Problemas legales y sanciones penales	Acuerdo de Confidencialidad	Exposición de la información personal privada	Exposición de la información institucional confidencial.	Secuestro y fuga de la información crítica	Reputación y confianza de los usuarios	Valor Confidencialidad
1	5	1	1	1	1	2

$$V_C \approx \frac{P_{LSP} + A_C + E_{IPP} + E_{IIC} + S_{FIC} + R_{CU}}{6} = \frac{1+5+1+1+1+1}{6} = \frac{10}{6} = 1.\overline{6} \cong 2 \qquad (2.8)$$

Con los valores de integridad del ejemplo de la Tabla 2.36, se calcula el valor del activo X en la integridad usando la Ecuación 2.4, obteniéndose el valor de la Ecuación 2.9.

Tabla 2.36. Ejemplo de valoración en la integridad [Elaboración propia]

CRITERIOS						
EFECTO LEGAL	**EFECTO PERSONAL**	**EFECTO INSTITUCIONAL**				
Problemas legales y sanciones penales	**Adulteración personal en el desempeño del activo**	**Problemas en el desempeño del activo**	**Problemas en la actividad normal de la institución**	**Reputación y confianza de los usuarios**	**Afectación a usuarios y terceras partes**	Valor de Integridad
5	1	5	4	1	5	4

$$V_I \approx \frac{P_{LSP} + A_{PDA} + P_{DA} + P_{ANI} + R_{CU} + A_{UTP}}{6} = \frac{5+1+5+4+1+5}{6} = \frac{21}{6} = 3.5 \cong 4 \qquad (2.9)$$

A partir de los valores del ejemplo de la Tabla 2.37, se calcula el valor del activo X en la disponibilidad con la Ecuación 2.5, obteniendo el valor de la Ecuación 2.10.

Tabla 2.37. Ejemplo de valoración en la disponibilidad [Elaboración propia]

CRITERIOS					
EFECTO LEGAL	**EFECTO INSTITUCIONAL**				
Problemas legales y sanciones penales	**Afectación en el desempeño de operación interna**	**Afectación a usuarios y terceras partes**	**Reputación y confianza por parte de los usuarios**	**Nivel de Intolerancia**	Valor Disponibilidad
1	2	3	2	5	3

$$V_D \approx \frac{P_{LSP} + A_{DOI} + A_{UTP} + R_{CU} + N_I}{5} = \frac{1+2+3+2+5}{5} = 2.6 \cong 3 \qquad (2.10)$$

El valor del costo del activo X se calcula con los valores de ejemplo la Tabla 2.38, usando la Ecuación 2.6, obteniéndose el valor de la Ecuación 2.11.

Tabla 2.38. Ejemplo de valoración del costo [Elaboración propia]

CRITERIOS			
INTEGRIDAD	**DISPONIBILIDAD**		
Costo por recuperación de la integridad	**Costos por recuperación de la disponibilidad**	**Pérdida material / financiera**	Costo Total (Valor costo)
5	3	3	4

$$V_{Costo} \approx \frac{C_{RI} + C_{RI} + P_{MF}}{3} = \frac{5+3+3}{3} = \frac{11}{3} = 3.\bar{6} \cong 4 \quad (2.11)$$

El valor propio del activo X se obtiene sumando todos los valores obtenidos en las Ecuaciones 2.8, 2.9, 2.10 y 2.11.

$$V_X = V_C + V_I + V_D + V_{Costo} = 2 + 4 + 3 + 4 \quad (2.12)$$

$$V_X = 13 \quad (2.13)$$

En el modelado de dependencias (Anexo G), el activo, como su valor propio, son representados en un bloque, como se indica en la Figura 2.7.

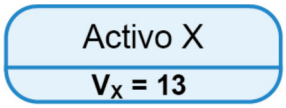


Figura 2.7. Representación del activo y su valor propio

El detalle de los valores para el cálculo del valor propio se encuentra tabulados en el Anexo F. El resultado de este trabajo se ve reflejado en el Anexo T.

2.2.2.2 Dependencias entre activos

Tabla 2.39. Etapa de estimación y cálculo de dependencias [Elaboración propia]

Entrada	Proceso	Salida
• *Criterios de valoración de niveles de dependencia directa (Sección 2.1.10.2)* • *Diagramas de dependencia para valor acumulado (Anexo G), antes de obtener los valores de los grados.*	• Estimación de niveles de dependencia. • Aplicación de la fórmula para calcular el grado de dependencia directa • Aplicación del principio probabilidades de Bayes para calcular el grado de dependencia indirecta	• Grado de dependencia entre activos • Diagramas de dependencia con valores de grados dependencia directa (Anexo G)

La norma ISO/IEC 27005 [5] recomienda identificar las dependencias entre activos, puesto que esto ayuda a garantizar que se obtenga el valor verdadero de los activos (valor acumulado). El Anexo G contiene los diagramas de dependencia para valor acumulado, con los que se hallarán los valores de dependencias que serán almacenados en el mismo anexo.

Las dependencias entre activos deben modelarse de forma jerárquica, descendente, en donde los activos superiores (dependientes) dependen de los activos inferiores, como puede verse en la Figura 2.8. En la cabeza del modelo se ubicarán los activos primarios de información, y debajo los activos de soporte. Es necesario aclarar que los términos "superior" e "inferior" son relativos, es decir, que un activo es superior con respecto a otro del cual depende, e inferior con respecto a otro que depende de éste, según lo que se analice en ese momento.

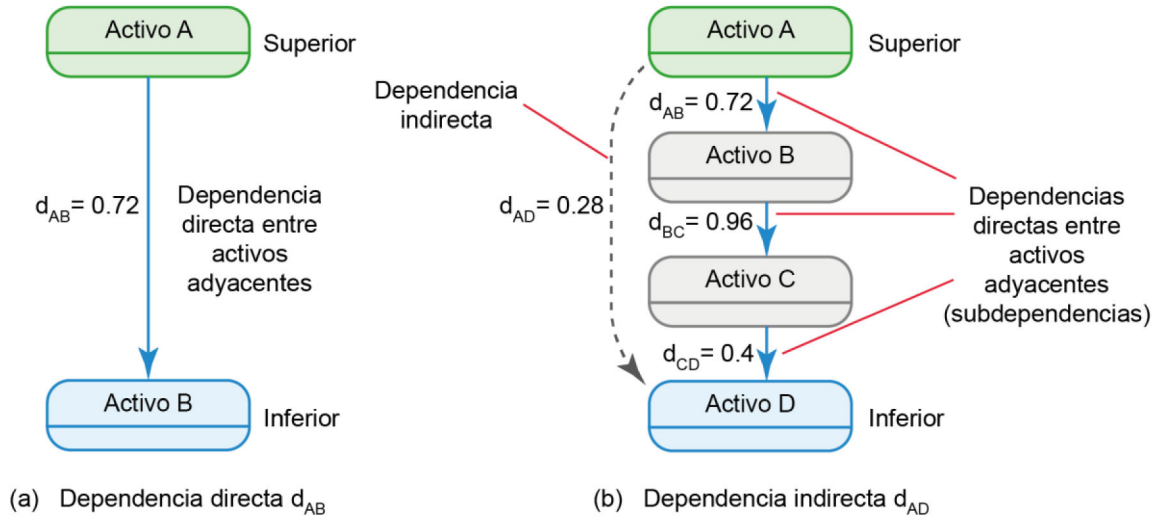


Figura 2.8. Tipos de dependencias entre activos [Elaboración propia]

El ejemplo de la Figura 2.8 muestra los tipos de dependencia que pueden existir entre dos activos determinados, y los valores de los grados de dependencia en estos casos, los cuales se expresan en porcentaje, en un rango entre 0 % y 100 %, o en forma decimal, dentro del rango comprendido entre 0 y 1. Para los cálculos, se toma la notación decimal.

- **Dependencia directa:** es la relación de dependencia que existe entre dos activos adyacentes, donde el uno (superior) es dependiente del otro (inferior).
  El grado de dependencia (directa) se calcula con los valores estimados según los criterios de valoración especificados en la sección 2.1.10.2., con la Ecuación 2.14.

$$d = \frac{d_C + d_I + d_D + d_R + d_P}{25}; \quad d \in \mathbb{R}^+ \ \wedge \ 0 < d \leq 1 \qquad (2.14)$$

Donde:

d	Grado de dependencia (directa) entre activos adyacentes
d_C	Estimación de nivel de dependencia en confidencialidad
d_I	Estimación de nivel de dependencia en integridad
d_D	Estimación de nivel de dependencia en disponibilidad
d_R	Estimación según los recursos y nivel de conocimiento que necesite el atacante
d_P	Estimación según la penalización o sanción que recae sobre el atacante

La fórmula no es la media aritmética de dichos valores, sino que con ella se calcula un valor real relativo comprendido entre 0 y 1, este último se alcanza si todos los valores en todos los criterios de valoración del nivel de dependencia son máximos e iguales a 5, y la suma de estos alcanza el valor máximo de 25. Es por esta razón que el denominador tiene este último valor. Si se quiere el valor del grado de dependencia en forma porcentual, basta con multiplicar el resultado por 100.

Para el ejemplo del diagrama de la Figura 2.8.a, se han colocado valores de ejemplo para hallar la dependencia directa en la Tabla 2.40.

Tabla 2.40. Ejemplo de estimación de dependencia del activo A al activo B según el diagrama de la Figura 2.8.a [Elaboración propia]

Criterio de dependencia	Confidencialidad	Integridad	Disponibilidad	Recursos	Penalización
Nivel	5	5	1	4	3

Con los valores de la Tabla 2.40 se obtiene el grado de dependencia directa de A hacia B (Ecuación 2.15):

$$d_{AB} = \frac{d_C + d_I + d_D + d_R + d_P}{25} = \frac{5 + 5 + 1 + 4 + 3}{25} = 0.72 \equiv 72\% \qquad (2.15)$$

Los valores de los grados de dependencia directa entre activos se encuentran en el Anexo G. Este trabajo se ve reflejado en el Anexo T.

- **Dependencia indirecta:** es la relación de dependencia que existe entre dos activos no adyacentes, pero que se encuentran conectados a través de activos intermedios. Uno (superior) es dependiente del activo que se encuentra en el extremo inferior de la relación. Los activos intermedios son, al mismo tiempo, inferiores al primero y

superiores al segundo. Aquí se introduce el concepto de “camino”, que es cada una de las trayectorias de interconexión del activo del extremo superior con el del extremo inferior.

Cada camino puede estar compuesto por varios activos intermedios, los que se encuentran conectados con dependencias directas entre ellos (sub-dependencias).

El valor de dependencia de un camino se calcula con el producto de los *n* grados de dependencia directa entre los activos adyacentes intermedios (sub-dependencias) que lo componen, como se indica en la Ecuación 2.16.

$$c = \prod_{i=1}^{n} subdep_i = subdep_1 \times subdep_2 \times \cdots \times subdep_n \qquad (2.16)$$

Donde:
- c Camino
- $subdep_i$ Cada uno de los grados de dependencia directa entre activos adyacentes intermedios del camino (sub-dependencias)
- n Total de sub-dependencias del camino

El grado de dependencia (indirecta en este caso) se calcula, según MAGERIT, en base a la fórmula tomada del cálculo de probabilidades de Bayes, para garantizar que la acumulación de los valores de dependencia de todos los caminos de la relación no supere el 100% (1 en decimales), como se muestra en la Ecuación 2.17.

$$d = 1 - \prod_{j=1}^{m} \left(1 - c_j\right) = 1 - (1 - c_1) \times (1 - c_2) \times \cdots \times (1 - c_m) \qquad (2.17)$$

Donde:
- d Grado de dependencia (indirecta) de la relación
- c_j Cada uno de los *m* caminos de la relación
- m Total de caminos de la relación

Para el ejemplo del diagrama de la Figura 2.8.b, la dependencia de A hacia B se calculó en la Ecuación 2.15 ($d_{AB} = 0.72$), y se han colocado los valores de las otras dependencias directas entre activos intermedios (sub-dependencias $d_{BC} = 0.96$ y $d_{CD} = 0.4$), suponiendo que fueron previamente calculados de la misma manera. En este caso, se tiene un solo camino, una trayectoria, con tres sub-dependencias. Se aplica la Ecuación 2.16 para hallar el valor del camino, como se indica en la Ecuación 2.18.

$$c = \prod_{i=1}^{3} subdep_i = d_{AB} \times d_{BC} \times d_{CD} = 0.72 \times 0.96 \times 0.4 = 0.27648 \qquad (2.18)$$

Y luego se halla el grado de dependencia total d_{AD} usando la Ecuación 2.17, cuyo cálculo es simple porque solo hay un camino, como se ve en la Ecuación 2.19.

$$d_{AD} = 1 - \prod_{j=1}^{1}(1 - c_j) = 1 - (1 - c) = 1 - (1 - 0.27648) \cong 0.28 \equiv 28\% \quad (2.19)$$

En el caso anterior, al tener un solo camino, el grado de dependencia de A hacia E puede hallarse solo con el valor del camino ($d_{AD} = c$), pero las fórmulas resultan imprescindibles cuando se tienen modelos de dependencia indirecta muy complejos, como el del ejemplo de la Figura 2.9.

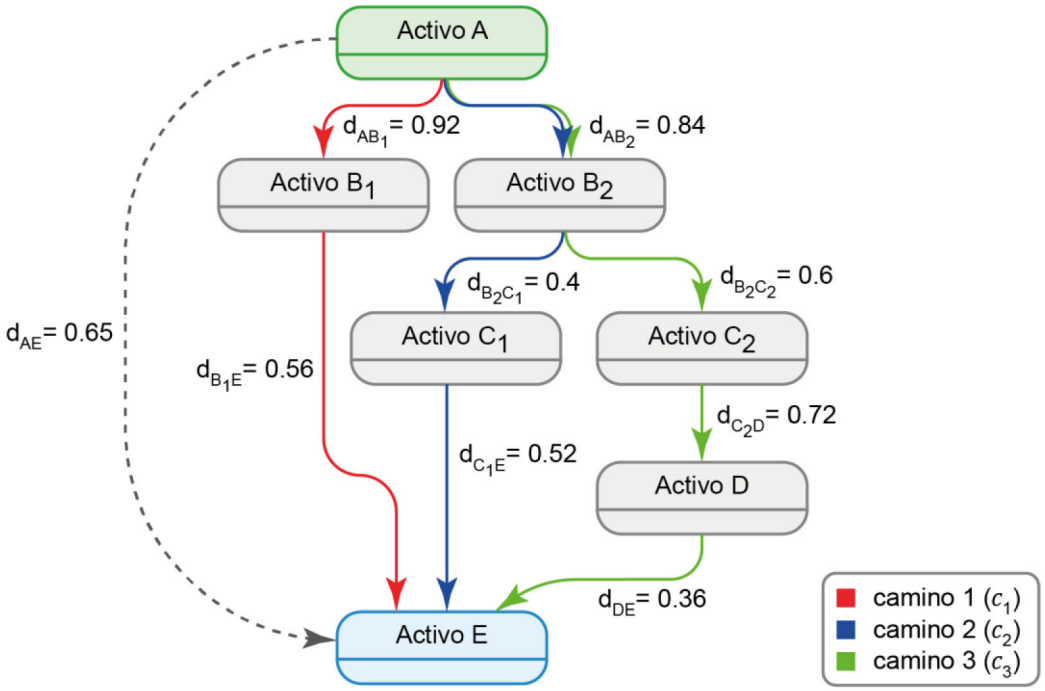


Figura 2.9. Ejemplo de modelo complejo de dependencia indirecta [Elaboración propia]

En el ejemplo modelo de la Figura 2.9, hay tres caminos desde A hacia B. El primero (rojo) tiene 2 sub-dependencias, el segundo (azul) tiene 3 sub-dependencias y el tercero (verde) tiene 4 sub-dependencias.

Los valores de cada uno de los tres caminos se calculan como sigue:

$$c_1 = \prod_{i=1}^{2} subdep_i = d_{AB_1} \times d_{B_1E} = 0.92 \times 0.56 = 0.5152 \quad (2.20)$$

$$c_2 = \prod_{i=1}^{3} subdep_i = d_{AB_2} \times d_{B_2C_1} \times d_{C_1E} = 0.84 \times 0.4 \times 0.52 = 0.17472 \quad (2.21)$$

$$c_3 = \prod_{i=1}^{4} subdep_i = d_{AB_2} \times d_{B_2C_2} \times d_{C_2D} \times d_{DE} = 0.84 \times 0.6 \times 0.72 \times 0.36$$

$$= 0.1306368 \quad (2.22)$$

Finalmente, se calcula el grado de dependencia de A hacia E usando los valores de los caminos hallados en las Ecuaciones 2.20, 2.21 y 2.22, aplicando la Ecuación 2.17, como se muestra en la Ecuación 2.23. Se ha aproximado la respuesta final hasta dos cifras decimales, como se muestra en la Ecuación 2.24.

$$d_{AE} = 1 - \prod_{j=1}^{3}\left(1 - c_j\right) = 1 - (1 - c_1)(1 - c_2)(1 - c_3) \quad (2.23)$$

$$d_{AE} = 1 - (1 - 0.5152)(1 - 0.17472)(1 - 0.1306368) \cong 0.65 \equiv 65\% \quad (2.24)$$

Puede verse la evidencia de estos cálculos en el Anexo G, en el que se incluyen otros factores utilizados para el cálculo del valor acumulado.

2.2.2.3 Cálculo del valor acumulado

Tabla 2.41. Etapa de cálculo del valor acumulado [Elaboración propia]

Entrada	Proceso	Salida
• *Valores propios.* • *Diagramas de dependencia para valor acumulado (Anexo G) con los valores de grados de dependencia directa.*	• Cálculo del valor acumulado a través de la aplicación de fórmulas. • Uso auxiliar del programa de cómputo desarrollado por los autores para este proyecto (Anexo H)	• Valor acumulado de los activos (Anexos F, H y T)

El valor acumulado de un activo es el valor que adquiere un activo en particular, considerando el peso de todos los activos que tienen un determinado grado de dependencia de él, además de su propio valor.

Sea *B* el activo a analizar, y A_k cada uno de los *n* activos dependientes de *B*, el valor acumulado del activo *B* equivale la suma de su valor propio con los productos de los *n* activos A_k dependientes de él (activos superiores a B) con sus respectivos grados de dependencia, sea esta directa o indirecta según su caso. La Ecuación 2.25 se usa para hallar el valor acumulado.

$$VA_B = V_B + \sum_{k=1}^{n}\left(V_{A_k} \times d_{A_kB}\right) = V_B + V_{A_1} \times d_{A_1B} + V_{A_2} \times d_{A_2B} + \cdots + V_{A_n} \times d_{A_nB} \quad (2.25)$$

Donde:

VA_B	Valor acumulado del activo *B*
V_B	Valor propio del activo *B*
V_{A_k}	Valor propio de cada activo A_k dependiente de *B*
d_{A_kB}	Grado de dependencia de A_k con respecto a *B*
n	Total de activos A_k dependientes de *B*

Continuando con el ejemplo, si a los activos de la Figura 2.9 se les colocan los valores propios, suponiendo que ya han sido calculados con los criterios de valoración (sección 2.1.10.1), se obtiene la Figura 2.10. El activo en que se realizará el cálculo del valor acumulado es el activo *E*.

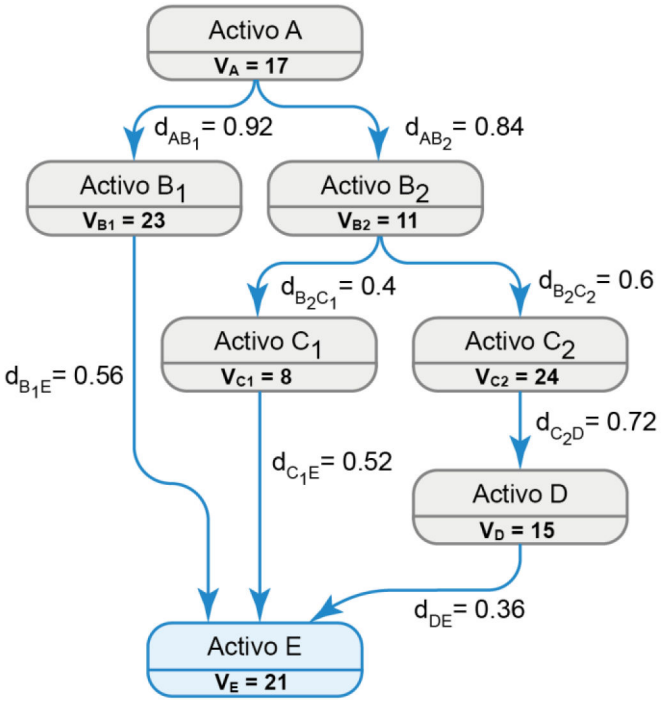


Figura 2.10. Diagrama de dependencias del activo E
[Elaboración propia]

Se calculan, primero, los grados de dependencia de cada uno de los activos dependientes (superiores) de *E,* aplicando las Ecuaciones 2.16 y 2.17. Debido a que son 6 activos dependientes, existen 6 dependencias, algunas de las cuales son indirectas. El valor de la dependencia de A hacia E se calculó siguiendo el proceso anterior, desde la Ecuación 2.20, hasta su obtención en la Ecuación 2.24, y cada uno de los grados de dependencia de los otros activos superiores con respecto a *E* se calculan siguiendo el mismo proceso de cálculo de la sección anterior. En las Figuras 2.11 a 2.16 se puede observar el proceso de obtención de los grados de dependencia.

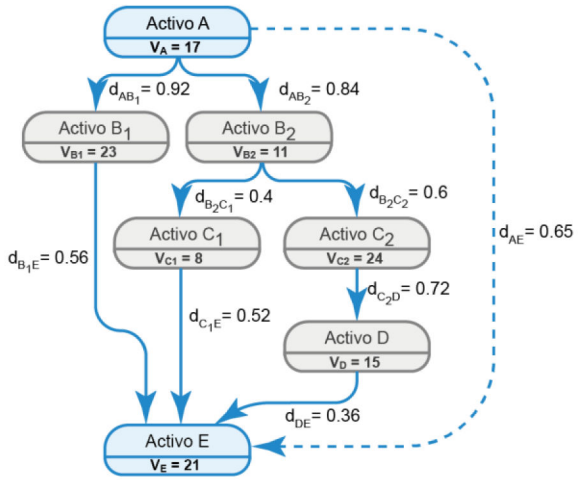


Figura 2.11. Dependencia: activo A de activo E

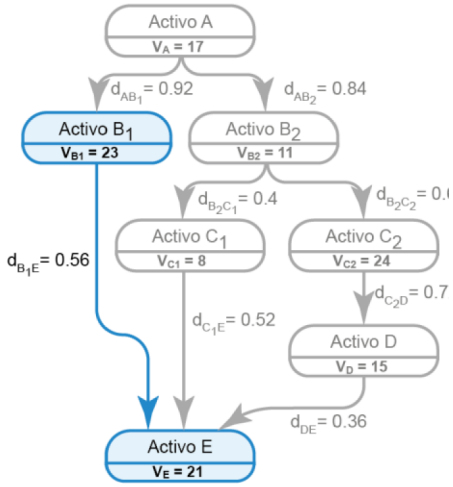


Figura 2.12. Dependencia: activo B1 de activo E

$$c_1 = 0.92 \times 0.56 = 0.5152$$

$$c_2 = 0.84 \times 0.4 \times 0.52 = 0.17472$$

$$c_3 = 0.84 \times 0.6 \times 0.72 \times 0.36 = 0.1306368$$

$$d_{AE} = 1 - (1 - 0.5152)(1 - 0.17472)(1 - 0.1306368)$$

$$d_{AE} = 0.65217148369 \cong 0.65 \qquad (2.26)$$

$$c_1 = 0.56$$

$$d_{B_1E} = 1 - (1 - 0.56)$$

$$d_{B_1E} = 0.56 \qquad (2.27)$$

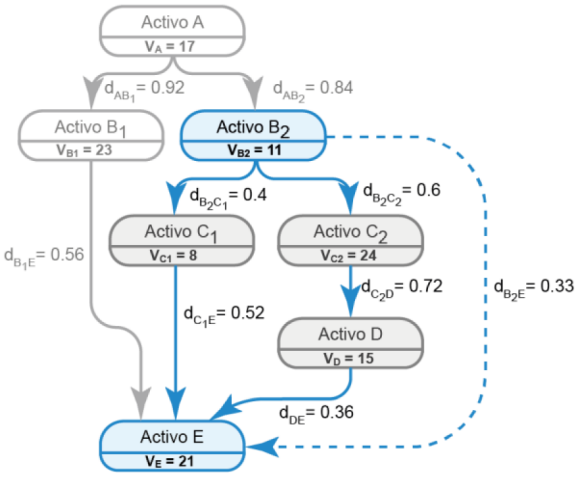


Figura 2.13. Dependencia: activo B2 de activo E

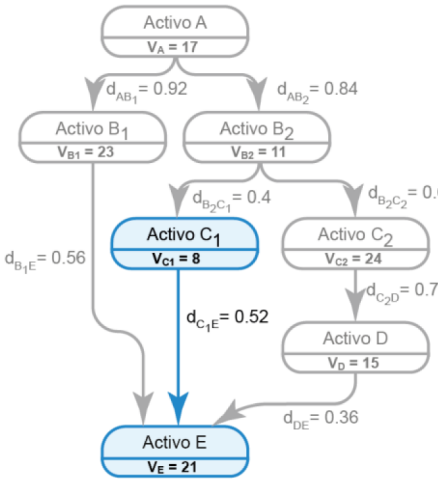


Figura 2.14. Dependencia: activo C1 de activo E

$$c_1 = 0.4 \times 0.52 = 0.208$$

$$c_2 = 0.6 \times 0.72 \times 0.36 = 0.15552$$

$$d_{B_2E} = 1 - (1 - 0.208)(1 - 0.15552)$$

$$d_{B_2E} = 0.33117184 \cong 0.33 \qquad (2.28)$$

$$c_1 = 0.52$$

$$d_{C_1E} = 1 - (1 - 0.52)$$

$$d_{C_1E} = 0.52 \qquad (2.29)$$

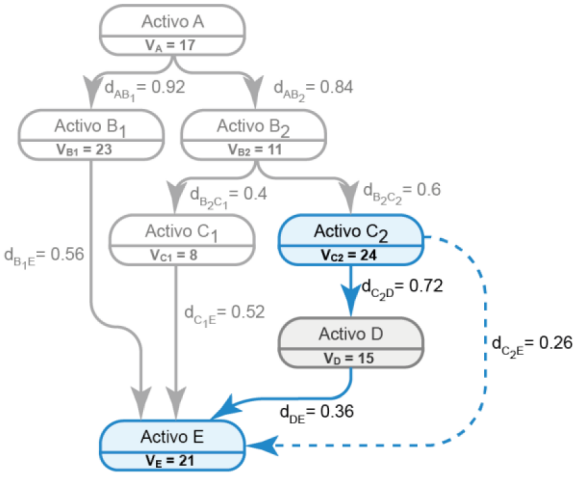


Figura 2.15. Dependencia: activo C2 de activo E

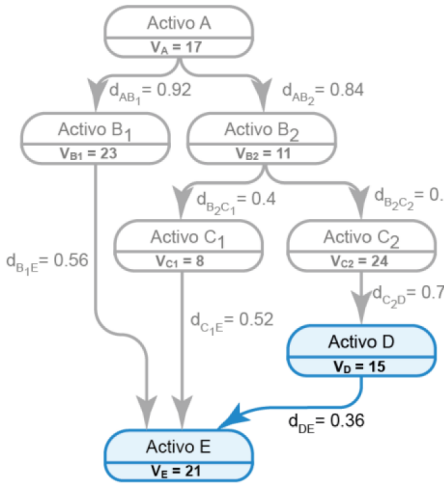


Figura 2.16. Dependencia: activo D de activo E

$$c_1 = 0.72 \times 0.36 = 0.2592$$
$$d_{C_2E} = 1 - (1 - 0.2592)$$
$$d_{B_2E} = 0.2592 \cong 0.26 \quad (2.30)$$

$$c_1 = 0.36$$
$$d_{C_1E} = 1 - (1 - 0.36)$$
$$d_{C_1E} = 0.36 \quad (2.31)$$

El valor acumulado del activo E se calcula aplicando la Ecuación 2.25, obteniéndose la Ecuación 2.32, en la que se substituyen los valores de las Ecuaciones 2.26 a 2.31, de donde se obtiene la Ecuación 2.33, que al clausurar se consigue finalmente el valor acumulado de E, en la Ecuación 2.34:

$$VA_E = V_B + V_A \times d_{AB} + V_{B_1} \times d_{B_1E} + V_{B_2} \times d_{B_2E} + V_{C_1} \times d_{C_1E} + V_{C_2} \times d_{C_2E} + V_D \times d_{DE} \quad (2.32)$$

$$VA_E = 21 + 17 \times 0.65 + 23 \times 0.56 + 11 \times 0.33 + 8 \times 0.52 + 24 \times 0.26 + 15 \times 0.36 \quad (2.33)$$

$$VA_E = 64.36 \quad (2.34)$$

Los valores acumulados de los activos pueden verse en la Matriz de Riegos del Anexo T, y su obtención en el Anexo G.

2.2.2.3.1 Uso del programa de cómputo desarrollado

El ejemplo anterior, que aparece como modelo complejo de dependencias, es simple en comparación a un modelado real de dependencias entre activos de información como el de la organización, pues contiene una gran cantidad de activos que se interrelacionan con conexiones más complejas. Por esta razón, aunque se disponga de una calculadora a la mano, se pueden cometer errores pequeños pero que afectarán gravemente al resultado final, además de que el proceso se vuelve muy lento y extenso. A partir de esto, surge la necesidad de un proceso automatizado que permita agilizar la obtención del valor acumulado, que provea resultados con exactitud; por ello fue necesario desarrollar un

programa por parte de los autores para este proyecto, cuya documentación se encuentra en el Anexo H. El programa lee el archivo de MS Excel[29] que almacena los valores de los activos, los caminos y las sub-dependencias, y procede a calcular, como en el ejemplo de la Figura 2.17. Para saber cómo usar el programa correctamente, y el formato del archivo de MS Excel, debe acudirse al Anexo I. Además, el programa permite exportar los resultados manual o automáticamente a un archivo de texto (.txt) o a un documento de MS Word (.doc).

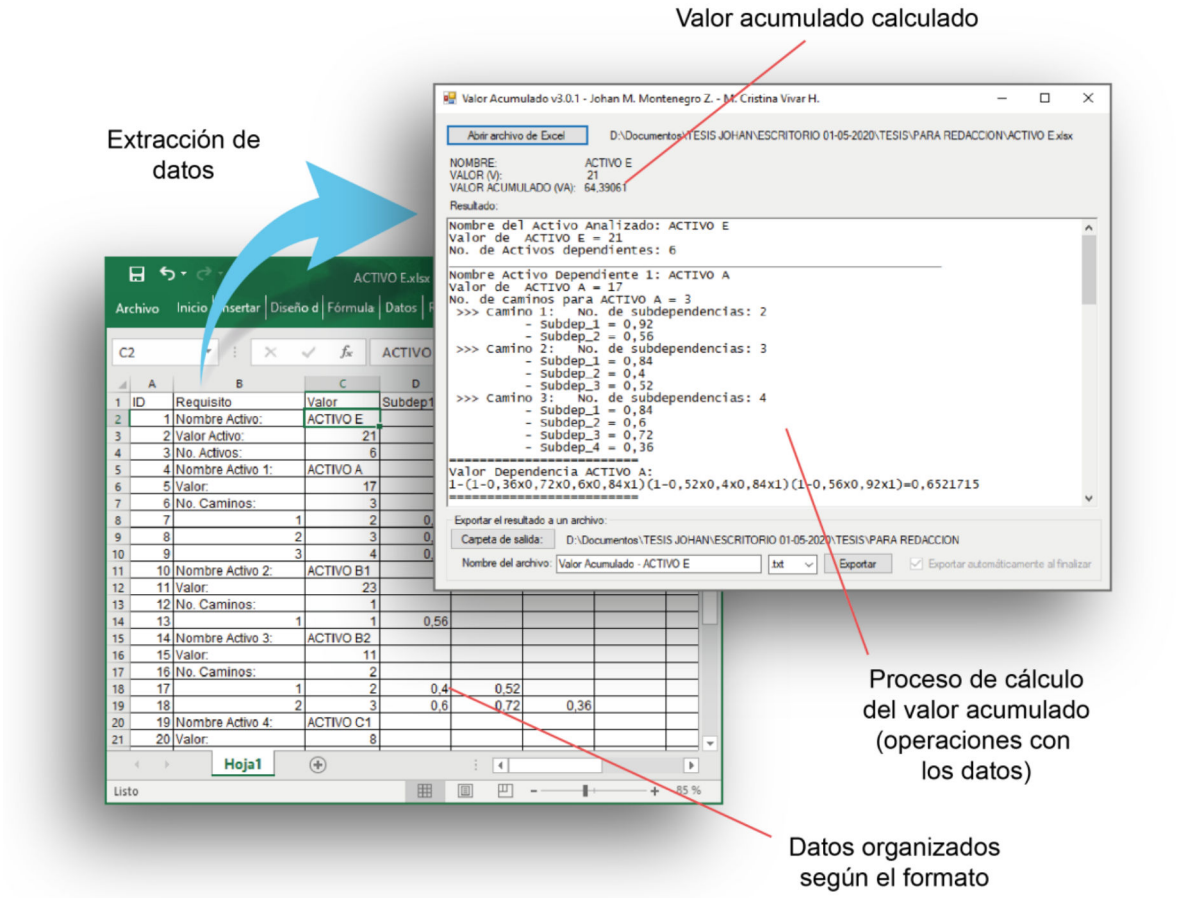


Figura 2.17. Ejemplo de uso del programa de cómputo
[Elaboración propia]

En la Figura 2.17, el programa calcula un valor de 64.39061 para el activo E, mientras que el cálculo realizado paso a paso durante el ejemplo ha arrojado un valor de 64.36. Esto es porque, durante los cálculos de ejemplo, se han aproximado los valores hasta dos cifras decimales, mientras que el programa utiliza hasta siete cifras decimales.

---

[29] El archivo de MS Excel debe estar abierto durante la ejecución del programa, y debe seguir rigurosamente el formato especificado en el Anexo I (Manual de Uso del Programa de Cómputo y Formato del Archivo MS Excel).

2.2.3 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES

Tabla 2.42. Etapa de análisis de amenazas y vulnerabilidades [Elaboración propia]

Entrada	Proceso	Salida
• *Atlas de Amenazas Naturales y Exposición a Infraestructura del Distrito metropolitano de Quito [90] y el Plan Especial "La Mariscal" [91]* • *Investigación en fuentes externas y observación en la institución.* • *Cuestionario a funcionarios externos, de la APCID (Anexo J).*	• Recopilación, tabulación, organización de la información recabada sobre amenazas potenciales, vulnerabilidades encontradas y salvaguardas.	• Estudio de amenazas, vulnerabilidades y salvaguardas (Anexo K)

El análisis de amenazas y vulnerabilidades es un proceso muy importante dentro del análisis y evaluación del riesgo, puesto que éste proporciona información fundamental para la estimación del impacto, probabilidad y, consecuentemente, del riesgo.

En el Anexo K se puede encontrar el estudio de las amenazas y vulnerabilidades que pueden afectar a los activos de información de la organización, desarrollado durante la elaboración de este proyecto para esta etapa del análisis. MEHARI indica que es importante identificar las amenazas potenciales considerando también la localización y situación geográfica, excluyendo aquellas que no se adapten a la realidad natural del entorno. Por esta razón, en el estudio se han incluido los registros encontrados en el Atlas de Amenazas Naturales y Exposición de Infraestructura del Distrito Metropolitano de Quito [90], sobre todo en el sector en el que se encuentra la Planta Central del MCyP, y en el Plan Especial "La Mariscal" [91].

No deben excluirse amenazas por falta de registros, puesto que la ausencia de un historial puede deberse a malas prácticas de seguridad. Deben incluirse amenazas que no hayan sucedido, pero tengan potencialidad de suceder, enmarcadas en la realidad institucional y el contexto de la organización. Según MAGERIT, puede ser útil tomar en cuenta las amenazas por la experiencia, de similares organizaciones. Es por esto que fue necesario registrar en un cuestionario los incidentes de seguridad ocurridos en otras instituciones de la APCID[30], cuestionario realizado a los responsables de la seguridad de la información en dichas instituciones, cuyos resultados se encuentran en el Anexo J.

En la Tabla 2.43 se muestra una lista de amenazas potenciales para los activos de información de la institución, principalmente tomadas del catálogo de amenazas de MAGERIT (Libro II), pero que guardan estrecha relación con el de MEHARI (Conceptos

[30] APCID. Administración Pública Central, Institucional y Dependiente [de la Función Ejecutiva].

Fundamentales y Especificaciones Funcionales [81], apéndice C1) y el Anexo C de la norma ISO/IEC 27005 [5].

Tabla 2.43. Amenazas y activos potencialmente vulnerables

Amenaza	Origen	Activos potenciales	Fuentes
Fuego	A, Accidental, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Daños por agua	N, Natural, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Desastres naturales	N, Natural, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, ISO/IEC 27005
Plaga (roedores, insectos)	N Natural	Equipos informáticos, equipamiento auxiliar, red, instalaciones	Investigación
Contaminación mecánica	A, Accidental, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Avería de origen físico	A, Accidental, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Corte del suministro eléctrico	A, Accidental, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Condiciones inadecuadas de temperatura y humedad	A, Accidental, D, Deliberado, I Industrial	Sistemas, equipos informáticos, red	MAGERIT, MEHARI, ISO/IEC 27005
Fallo del servicio de comunicaciones	A, Accidental, D, Deliberado, I Institucional	Red	MAGERIT, MEHARI, ISO/IEC 27005
Interrupción de servicios y suministros esenciales	A, Accidental, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, ISO/IEC 27005
Degradación de los equipos por el paso del tiempo	A, Accidental, D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Emanaciones electromagnéticas (TEMPEST)	D, Deliberado, I Industrial	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, ISO/IEC 27005
Errores de usuario	A Accidental	Sistemas, bases de datos, información	MAGERIT, MEHARI, ISO/IEC 27005
Errores de administrador	A Accidental	Sistemas, bases de datos, información, equipos informáticos, equipamiento auxiliar, red	MAGERIT, MEHARI, ISO/IEC 27005
Errores de monitorización	A Accidental	Sistemas, bases de datos, red	MAGERIT, MEHARI, ISO/IEC 27005
Errores de configuración	A Accidental	Sistemas, bases de datos, red	MAGERIT, MEHARI, ISO/IEC 27005
Deficiencias en la organización	A Accidental	Usuarios	MAGERIT, ISO/IEC 27005
Difusión de software dañino	A, Accidental, D Deliberado	Sistemas, bases de datos, equipos informáticos	MAGERIT, MEHARI, ISO/IEC 27005
Errores de [re-]encaminamiento	A Accidental	Sistemas, red	MAGERIT, ISO/IEC 27005
[Re-]encaminamiento de mensajes	D Deliberado	Sistemas, red	MAGERIT, MEHARI, ISO/IEC 27005
Errores de secuencia	A Accidental	Red	MAGERIT, ISO/IEC 27005
Alteración de secuencia	D Deliberado	Red	MAGERIT, ISO/IEC 27005

Alteración accidental de la información	A	Accidental	Bases de datos, información	MAGERIT, MEHARI, ISO/IEC 27005
Destrucción de la información	A, D	Accidental, Deliberado	Sistemas, bases de datos, información	MAGERIT, MEHARI, ISO/IEC 27005
Fugas de información	A	Accidental	Sistemas, bases de datos, información, usuarios, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Divulgación de la información	D	Deliberado	Sistemas, bases de datos, información, usuarios, instalaciones	MAGERIT, ISO/IEC 27005
Vulnerabilidades de los programas (Error de software)	A	Accidental	Sistemas	MAGERIT, MEHARI, ISO/IEC 27005
Errores de mantenimiento / actualización de programas (software)	A	Accidental	Sistemas, bases de datos,	MAGERIT, MEHARI, ISO/IEC 27005
Errores de mantenimiento / actualización de equipos (hardware)	A	Accidental	Equipos informáticos, equipamiento auxiliar, red	MAGERIT, ISO/IEC 27005
Caída del sistema por agotamiento de recursos	A	Accidental	Sistemas, equipos informáticos, red	MAGERIT, ISO/IEC 27005
Pérdida de equipos	A	Accidental	Equipos informáticos	MAGERIT, MEHARI, ISO/IEC 27005
Indisponibilidad de personal	A, D	Accidental, Deliberado	Usuarios	MAGERIT, MEHARI, ISO/IEC 27005
Manipulación de los registros de actividad (log)	D	Deliberado	Sistemas, red	MAGERIT, ISO/IEC 27005
Manipulación de la configuración	D	Deliberado	Sistemas, red	MAGERIT, MEHARI, ISO/IEC 27005
Suplantación de la identidad del usuario	D	Deliberado	Sistemas, bases de datos, información, equipos informáticos, red	MAGERIT, ISO/IEC 27005
Abuso de privilegios de acceso	D	Deliberado	Sistemas, bases de datos, información, equipos informáticos, red	MAGERIT, ISO/IEC 27005
Uso no previsto	D	Deliberado	Sistemas, bases de datos, equipamiento auxiliar, información, equipos informáticos, red	MAGERIT, ISO/IEC 27005
Acceso no autorizado	D	Deliberado	Sistemas, bases de datos, información, equipos informáticos, equipamiento auxiliar, instalaciones	MAGERIT, ISO/IEC 27005
Análisis de tráfico	D	Deliberado	Red	MAGERIT, ISO/IEC 27005
Repudio	D	Deliberado	Sistemas, instalaciones	MAGERIT, ISO/IEC 27005
Interceptación de la información	D	Deliberado	Red	MAGERIT, MEHARI, ISO/IEC 27005
Modificación deliberada de la información	D	Deliberado	Bases de datos, información	MAGERIT, MEHARI, ISO/IEC 27005
Manipulación de programas	D	Deliberado	Sistemas	MAGERIT, MEHARI, ISO/IEC 27005
Manipulación de los equipos	D	Deliberado	Equipos informáticos, equipamiento auxiliar, red	MAGERIT, MEHARI, ISO/IEC 27005
Denegación de servicio	D	Deliberado	Sistemas, equipos informáticos, red	MAGERIT, MEHARI, ISO/IEC 27005
Robo	D	Deliberado	Equipos informáticos, equipamiento auxiliar, red	MAGERIT, MEHARI, ISO/IEC 27005
Ataque destructivo	D	Deliberado	Equipos informáticos, equipamiento auxiliar, red, instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Ocupación enemiga	D	Deliberado	Instalaciones	MAGERIT, MEHARI, ISO/IEC 27005
Indisponibilidad del personal	D	Deliberado	Usuarios	MAGERIT, MEHARI, ISO/IEC 27005
Extorsión	D	Deliberado	Usuarios	MAGERIT, ISO/IEC 27005
Ingeniería social	D	Deliberado	Usuarios	MAGERIT, ISO/IEC 27005

2.2.4 IMPACTO

Tabla 2.44. Etapa de estimación y cálculo del impacto [Elaboración propia]

Entrada	Proceso	Salida
• *Valor propio y acumulado* • *Anexos L y H* • *Criterios de estimación del nivel de degradación (sección 2.1.10.3.1)*	• Generación de diagramas simplificados. • Cálculo del nivel de degradación, de los impactos acumulado y repercutido con el uso de fórmulas.	• Anexo L • Degradación e impacto en la Matriz de Riesgos (Anexo T)

El impacto no se estima directamente, sino que se evalúa según el nivel de degradación que puede sufrir un activo en una dimensión determinada. Ya que los niveles de degradación se expresan como porcentajes, es necesario que estos valores sean expresados en forma decimal, en el rango [0, 1], a fin de poder operar con ellos. Un activo puede tener tantos impactos como amenazas potenciales puedan caer sobre éste para degradarlo. Además, se analiza el impacto en dos aspectos:

a. **Acumulado:** considerando el valor acumulado del activo, y la relación de éste con los activos superiores.
b. **Repercutido:** considerando el valor propio del activo, y la relación de éste con los activos inferiores.

2.2.4.1 Estimación y cálculo del nivel de degradación

Con los valores de degradación estimados en cada dimensión según los criterios de valoración de la sección 2.1.10.3.1 se calcula el valor de la degradación del activo como la media aritmética de los valores. Se considera también que, si un activo no puede sufrir una degradación en una dimensión, su valor asignado es cero, y participa en la media, pues acorde al análisis no es coherente que la degradación total de un activo que pueda sufrir daños en las tres dimensiones sea menor que la degradación total de un activo que pueda sufrir daños en solo dos dimensiones o solo en una dimensión; por esta razón, el divisor siempre será tres. La Ecuación 2.35 permite obtener el nivel de degradación.

$$degr = \frac{degr_C + degr_I + degr_D}{3}; \quad degr \in \mathbb{R}^+ \ \wedge \ 0 < degr \leq 1 \tag{2.35}$$

Donde:

$degr$	Degradación del activo por cierta amenaza
$degr_C$	Estimación de degradación en la confidencialidad
$degr_I$	Estimación de degradación en la integridad
$degr_D$	Estimación de degradación en la disponibilidad

Continuando con el ejemplo de la Figura 2.10, para el activo E se han calculado los valores de degradación que una amenaza en particular puede causarle en integridad (I) y disponibilidad (D), en la Tabla 2.45, suponiendo que el análisis de esta amenaza no incide en la confidencialidad (C):

Tabla 2.45. Ejemplo de estimación del nivel de degradación [Elaboración propia]

DEGRADACIÓN		
C	I	D
	90%	100%

Usando la Ecuación 2.32, el valor de degradación del activo E, causado por dicha amenaza como se indica en al Tabla 2.45, es el mostrado en la Ecuación 2.36.

$$degr_E = \frac{degr_C + degr_I + degr_D}{3} = \frac{0 + 90\% + 100\%}{3} = \frac{190\%}{3} = 63.\overline{3}\,\% \qquad (2.36)$$

2.2.4.2 Cálculo del impacto acumulado

El impacto acumulado que una amenaza causa sobre un activo se calcula como el producto del valor acumulado del activo en cuestión y el valor de degradación (total) que le puede provocar dicha amenaza, como se indica en la Ecuación 2.37.

$$IA = VA \times degr; \quad IA \in \mathbb{R}^+ \qquad (2.37)$$

Donde:
- IA Impacto acumulado de cierta amenaza sobre el activo
- VA Valor acumulado del activo
- $degr$ Degradación del activo por dicha amenaza

Continuando con el ejemplo, con el valor acumulado del activo E calculado en la Ecuación 2.34, de la sección 2.2.2.3, y con el valor de degradación calculado en la Ecuación 2.36 causado por la amenaza, en la sección 2.2.4.1, el valor del impacto acumulado del activo E es el que se muestra en la Ecuación 2.38, resultado de la aplicación de la Ecuación 2.37:

$$IA_E = VA_E \times degr_E = 64.63 \times 63.\overline{3}\,\% = 64.63 \times 0.6\overline{3} = 40.932\overline{3} \qquad (2.38)$$

Es decir, que el activo E sufriría un impacto acumulado de 40.93 si se materializa dicha amenaza en particular. Este valor debe calcularse por cada amenaza sobre el activo.

Los valores acumulados de los activos se encuentran registrados en la tabla final del Anexo F y sus respectivos cálculos en el Anexo G. Este trabajo se refleja en el Anexo T.

2.2.4.3 Cálculo del impacto repercutido sobre un activo dependiente

El impacto repercutido, por otro lado, es la "anatomía" del impacto acumulado, es decir que, mientras el impacto acumulado se calcula con el nivel de daño que una amenaza causa a un activo *B* con el peso acumulado de todos los activos A_n que dependen de ese activo, el impacto repercutido se encarga de hallar cómo dicha amenaza afecta particularmente a un activo *A* que depende de ese activo *B* al que atacó dicha amenaza.

En otras palabras, una amenaza cuyo ataque se efectúa sobre el activo *B* repercute en todos los activos A_n que dependen de éste, y la acumulación de los impactos repercutidos sobre los activos A_n (y sobre el valor propio del activo *B*) componen el impacto acumulado sobre el activo *B*. La Figura 2.18 ilustra el ejemplo de cómo la amenaza que recae sobre el activo E "repercute" sobre los activos dependientes.

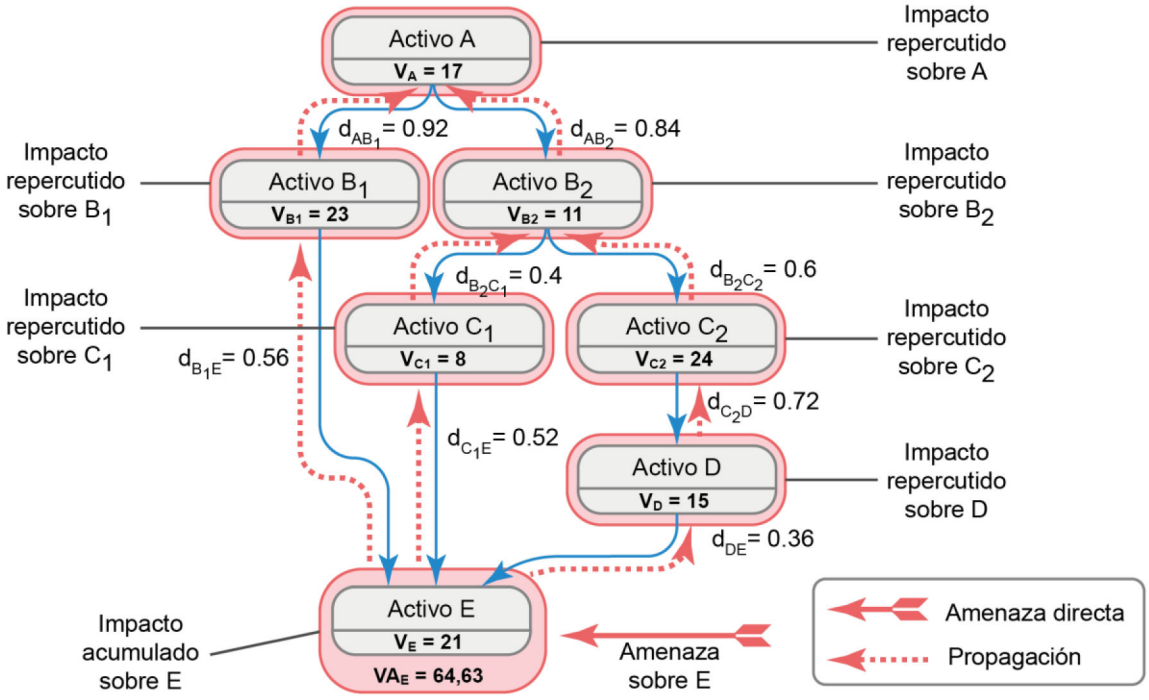


Figura 2.18. Impacto repercutido sobre los activos dependientes de E
[Elaboración propia]

La Figura 2.18 muestra cómo la degradación que una amenaza causa sobre *E* se propaga hacia los demás activos, degradándolos según el grado de dependencia que tengan del activo *E*. El impacto repercutido se calcula sobre un activo dependiente en particular, y no es acumulativo. Para entenderlo mejor, obsérvese la Figura 2.19. Sea *B* el activo sobre el que se efectúa la amenaza, y *A* un activo que depende de éste; el impacto repercutido se analiza sobre *A*, y equivale al producto del nivel de degradación que puede causar una

amenaza X sobre B, por el grado de dependencia del activo *A* de *B*, y por el valor propio de *A*.

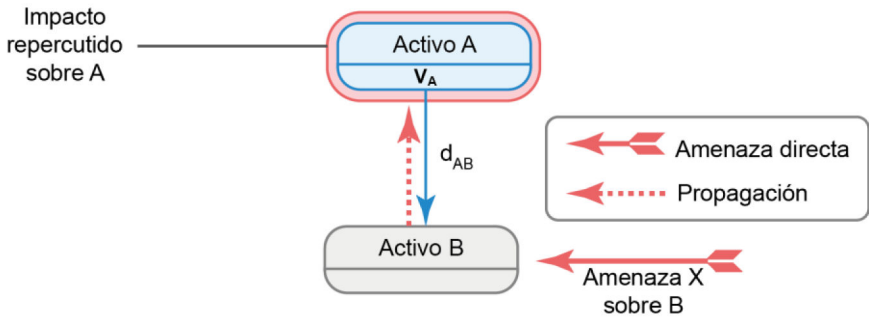


Figura 2.19. Impacto repercutido sobre un activo A, que depende de otro B
[Elaboración propia]

Con la Ecuación 2.39 se calcula el impacto repercutido (no interesa el valor del activo B).

$$IR_A = V_A \times degr_B \times d_{AB}; \quad IR_A \in \mathbb{R}^+ \tag{2.39}$$

Donde:

IR_A	Impacto repercutido sobre A
V_A	Valor propio del activo A
$degr_B$	Nivel de degradación causada por la amenaza X a B
d_{AB}	Grado de dependencia de A hacia B

Siguiendo el ejemplo de la Figura 2.18, suponiendo que se desea calcular el impacto repercutido de la amenaza del activo E sobre el activo C_2, se tendría la situación que se muestra en el ejemplo de la Figura 2.20.

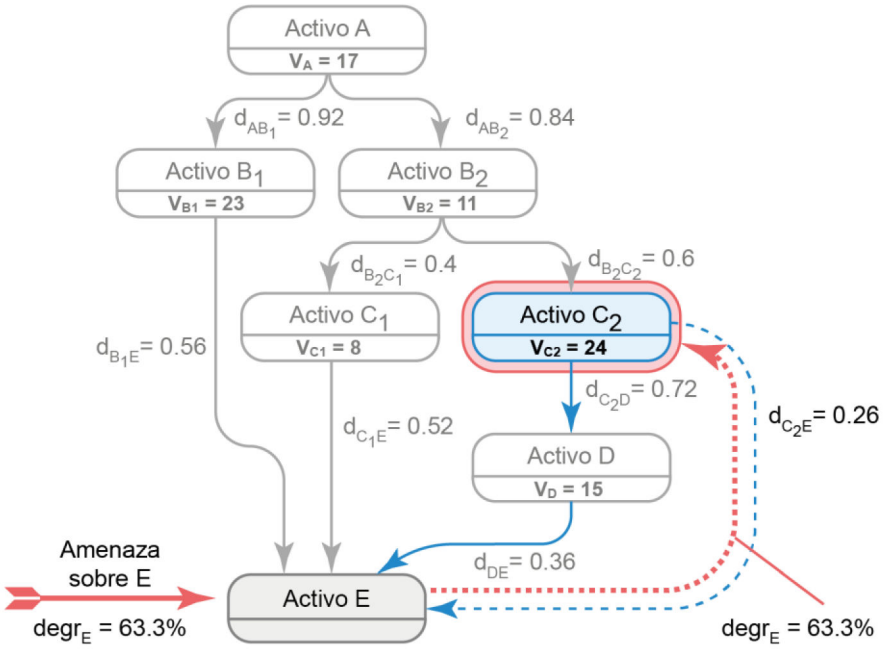


Figura 2.20. Ejemplo de impacto repercutido sobre el activo C_2
[Elaboración propia]

Aplicando la Ecuación 2.39, el cálculo del impacto repercutido sobre C_2 se obtiene como se muestra en la Ecuación 2.40.

$$IR_{C_2} = V_{C_2} \times degr_E \times d_{C_2E} = 24 \times 63.\overline{3}\% \times 0.26 \cong 24 \times 0.63 \times 0.26 = 3.93 \quad (2.40)$$

En donde el valor del activo E no interesa.

2.2.4.3.1 Diagramas de dependencia simplificados para el impacto repercutido

Un activo en cuestión puede tener tantos impactos repercutidos como amenazas haya por cada uno de los activos de los que depende y, como se explicó antes, estos valores son independientes y no son acumulativos. Para analizar los impactos repercutidos sobre un activo, deben considerarse todos los activos de los cuales éste depende (activos inferiores). Los grados de dependencia de un activo hacia los activos inferiores no cambian. Debido a la complejidad que supondría re-diagramar las dependencias inferiores de un activo determinado, es conveniente revisar los diagramas en el que se encuentre el activo en cuestión, y colocar todos los activos de los que depende en un nuevo diagrama simplificado. Por ejemplo, si se quiere analizar el activo *A* de la Figura 2.18, debe considerarse que éste depende de todos y cada uno de los activos que se encuentran debajo, con los grados de dependencia previamente calculados desde A hacia éstos y simplificar el diagrama, como se muestra en el ejemplo de la Figura 2.21.

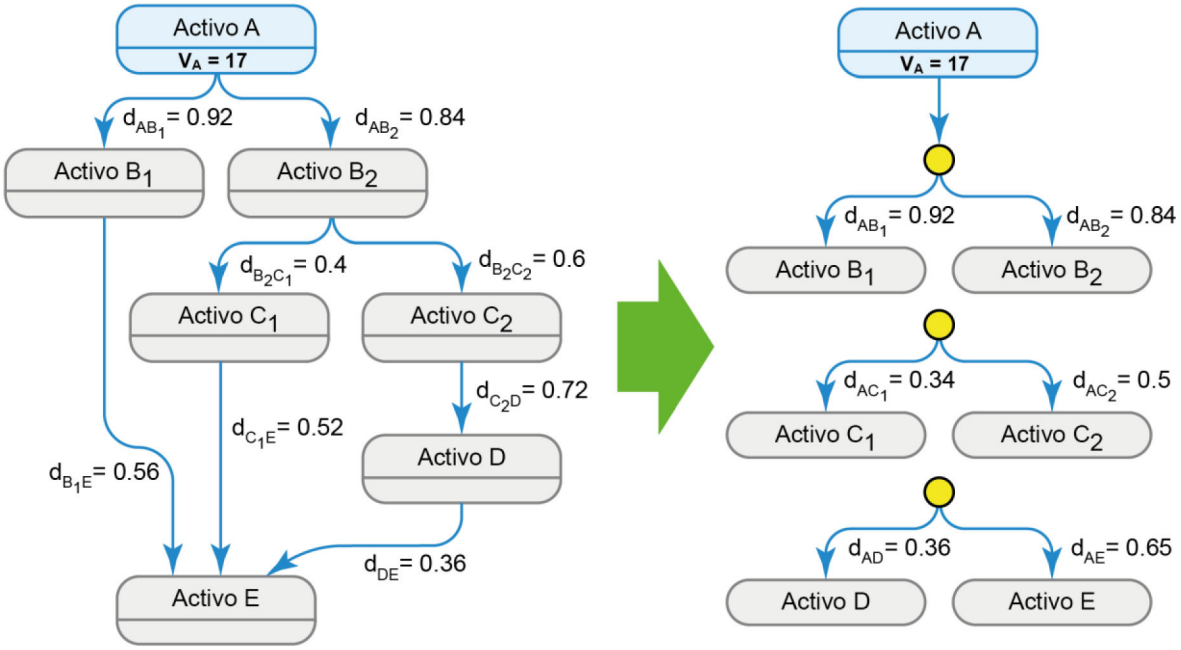


Figura 2.21. Ejemplo de diagrama de dependencias simplificado
[Elaboración propia]

Si al diagrama de la Figura 2.21 se agregan diversas amenazas que puedan recaer sobre los activos inferiores con sus respectivos niveles de degradación, previamente calculados, se tendrá una ilustración como la de la Figura 2.22.

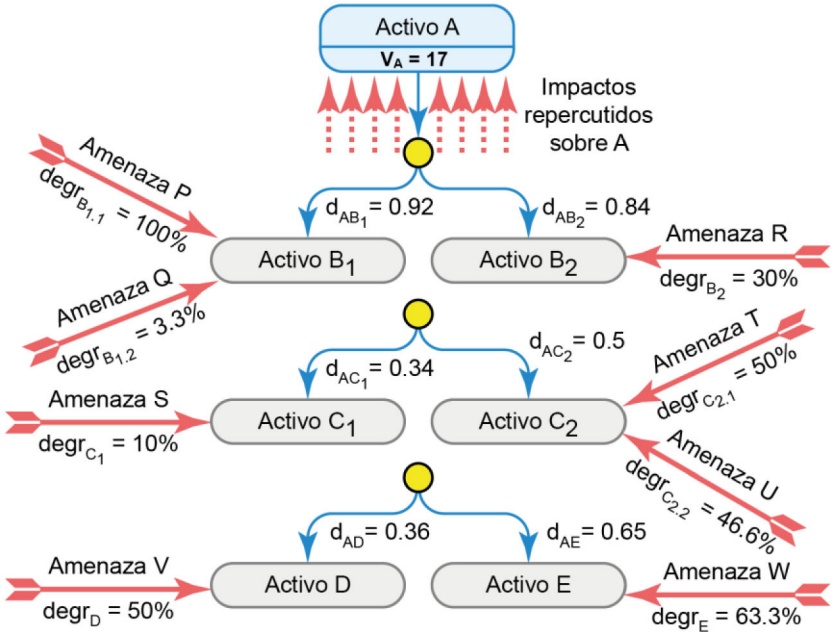


Figura 2.22. Ejemplo de impactos repercutidos sobre el activo A
[Elaboración propia]

Así, todos los impactos repercutidos por las amenazas que atacan directamente a los otros activos, pero que repercuten sobre A, como se muestran en el ejemplo de la Figura 2.22, se calculan aplicando la Ecuación 2.39 para cada caso.

Impacto repercutido de la amenaza P del activo B_1 sobre A (ver Ecuación 2.41).

$$IR_A = V_A \times degr_{B_{1.1}} \times d_{AB_1} = 17 \times 100\% \times 0.92 \equiv 17 \times 1 \times 0.92 = 15.64 \qquad (2.41)$$

Impacto repercutido de la amenaza Q del activo B_1 sobre A (ver Ecuación 2.42).

$$IR_A = V_A \times degr_{B_{1.2}} \times d_{AB_1} = 17 \times 3.3\% \times 0.92 \equiv 17 \times 0.03 \times 0,.2 = 0.47 \qquad (2.42)$$

Impacto repercutido de la amenaza R del activo B_2 sobre A (ver Ecuación 2.43).

$$IR_A = V_A \times degr_{B_2} \times d_{AB_2} = 17 \times 30\% \times 0.84 \equiv 17 \times 0.3 \times 0.84 = 4.28 \qquad (2.43)$$

Impacto repercutido de la amenaza S del activo C_1 sobre A (ver Ecuación 2.44).

$$IR_A = V_A \times degr_{C_1} \times d_{AC_1} = 17 \times 10\% \times 0.34 \equiv 17 \times 0.1 \times 0.92 = 0.58 \qquad (2.44)$$

Impacto repercutido de la amenaza T del activo C_2 sobre A (ver Ecuación 2.45).

$$IR_A = V_A \times degr_{C_{2.1}} \times d_{AC_2} = 17 \times 50\% \times 0.5 \equiv 17 \times 0.5 \times 0.5 = 4.25 \qquad (2.45)$$

Impacto repercutido de la amenaza U del activo C_2 sobre A (ver Ecuación 2.46).

$$IR_A = V_A \times degr_{C_{2.2}} \times d_{AC_2} = 17 \times 46.6\% \times 0.5 \equiv 17 \times 0.47 \times 0.5 = 4 \quad (2.46)$$

Impacto repercutido de la amenaza V del activo D sobre A (ver Ecuación 2.47).

$$IR_A = V_A \times degr_D \times d_{AD} = 17 \times 50\% \times 0.36 \equiv 17 \times 0.5 \times 0.36 = 3.06 \quad (2.47)$$

Impacto repercutido de la amenaza W del activo E sobre A (ver Ecuación 2.48).

$$IR_A = V_A \times degr_E \times d_{AE} = 17 \times 63.3\% \times 0.65 \equiv 17 \times 0.63 \times 0.65 = 6.96 \quad (2.48)$$

Los diagramas de dependencias simplificados para el impacto repercutido se encuentran en el Anexo L, y los valores del impacto repercutido se encuentran el Anexo T.

2.2.5 PROBABILIDAD

Tabla 2.46. Etapa de estimación y cálculo de probabilidad [Elaboración propia]

Entrada	Proceso	Salida
• *Criterios de valoración de probabilidad (sección 2.1.10.4)* • *Anexo K* • *Cuestionario a funcionarios externos de la APCID (Anexo J)*	• Cálculo de las probabilidades según origen natural, accidental o deliberado con la aplicación de fórmulas.	• Columnas de potencialidad y probabilidad en la Matriz de Riesgos (Anexo T)

MEHARI prefiere el término “potencialidad” a “probabilidad”, ya que el primero puede estimarse en una escala semi-cuantitativa, mientras que el segundo implica un valor cuantitativo en un rango continuo de valores [82]. Debido al método de análisis y evaluación de riesgos desarrollado, se usa un modelo cuasi – cuantitativo para la obtención de la probabilidad. Se hace una distinción en el cálculo de probabilidad según 2 fuentes determinadas: si es de origen deliberado, o si es de origen natural - accidental. Estas dos fuentes son mutuamente excluyentes.

La estimación de las potencialidades se realiza mediante las escalas de valor de la sección 2.1.10.4, de acuerdo con su origen, considerando los resultados de los cuestionarios realizados a los funcionarios externos pero relacionados con la institución en el Anexo J, y el estudio de amenazas y vulnerabilidades del Anexo K. A diferencia del impacto, la probabilidad se calcula independientemente del valor propio o acumulado del activo.

2.2.5.1 Probabilidad de una amenaza de origen deliberado

La probabilidad de ocurrencia de una amenaza de origen deliberado se obtiene de los valores estimados de potencialidad de dos factores: interés y facilidad, desde el punto de

vista de un atacante, cuyas escalas de valor se encuentran en la sección 2.1.10.4.1. Para las amenazas de origen deliberado se usa el Anexo J y el estudio del Anexo K. Con los valores estimados de interés y facilidad, se procede a calcular la probabilidad con la Ecuación 2.49.

$$P = P_I \times P_F \tag{2.49}$$

Donde:
- P Probabilidad de ocurrencia de la amenaza
- P_I Potencialidad según el interés del atacante
- P_F Potencialidad según la facilidad de llevar a cabo el ataque

Por ejemplo, el Registro de Bienes Culturales y Patrimoniales guarda información confidencial que puede tener un alto valor para un atacante, y el interés de llevar un determinado tipo de ataque puede ser alto, aunque llevar a cabo tal ataque podría requerir de una mayor experiencia y recursos, por lo que las estimaciones pueden quedar como se indica en el ejemplo de la Tabla 2.47.

Tabla 2.47. Ejemplo de estimación de potencialidad de una amenaza deliberada [Elaboración propia]

POTENCIALIDAD		PROBABILIDAD
Deliberado		
Interés	Facilidad	
100,00%	10,00%	10,00%

La probabilidad se calcula como el producto de las potencialidades estimadas, las cuales se expresan en decimal para el cálculo, como se muestra en la Ecuación 2.50.

$$P = P_I \times P_F = 100\% \times 10\% \equiv 1 \times 0.1 = 0.1 \equiv 10\% \tag{2.50}$$

Estos valores están registrados la Matriz de Riesgos del Anexo T.

2.2.5.2 Probabilidad de una amenaza de origen natural o accidental

La probabilidad de la ocurrencia de una amenaza, sea ésta de origen natural o accidental, comprende los valores estimados de potencialidad de dos factores: susceptibilidad y frecuencia, cuyas escalas de valor se encuentran en la sección 2.1.10.4.2. Para las amenazas de origen natural se usa la versión actual del Atlas de Amenazas naturales y Exposición de Infraestructura del Distrito Metropolitano de Quito (segunda edición) [90]. Para las amenazas accidentales se usa la información del Anexo J. Para ambos casos,

además, se usa el estudio del Anexo K. Con los valores estimados de susceptibilidad y frecuencia, se procede a calcular la probabilidad con la Ecuación 2.51.

$$P = P_S \times P_F \tag{2.51}$$

Donde: P Probabilidad de ocurrencia de la amenaza

P_S Potencialidad según la susceptibilidad

P_F Potencialidad según la frecuencia

Por ejemplo, el sector Mariscal Sucre del D. M. Q., donde se encuentra la Planta Central del MCyP, tiene alta (máximo valor) susceptibilidad a inundaciones, y la frecuencia de las lluvias e inundaciones es varias veces al año, por lo que las estimaciones pueden quedar como se indican en la Tabla 2.48.

Tabla 2.48. Ejemplo de estimación de potencialidad de una amenaza natural o accidental [Elaboración propia]

POTENCIALIDAD		PROBABILIDAD
Natural o accidental		
Susceptibilidad	Frecuencia	
100,00%	10,00%	10,00%

La probabilidad se calcula como el producto de las potencialidades estimadas, aplicando la Ecuación 2.51, las cuales se expresan en decimal para el cálculo, como se indica en la Ecuación 2.52.

$$P = P_S \times P_F = 100\% \times 10\% \equiv 1 \times 0.1 = 0.1 \equiv 10\% \tag{2.52}$$

Estos valores están registrados en la Matriz de Riesgos del Anexo T.

2.2.6 RIESGO

Tabla 2.49. Etapa de estimación y cálculo del riesgo [Elaboración propia]

Entrada	Proceso	Salida
• *Valores de impacto acumulado y repercutido.* • *Probabilidad.* • *Criterios de estimación y clasificación del riesgo.*	• Cálculo del riesgo acumulado y del riesgo repercutido con la aplicación de fórmulas.	• Columnas con valores del riesgo (Anexo T)

El riesgo equivale al producto del impacto que pueda causar una amenaza potencial y la probabilidad de que pueda llegar a efectuarse. En otras palabras, un solo activo puede tener tantos riesgos como amenazas recaigan sobre o se propaguen hacia éste.

El riesgo se analiza en dos aspectos:

a. **Acumulado:** considerando el impacto acumulado de un activo.
b. **Repercutido:** considerando el impacto repercutido sobre un activo.

2.2.6.1 Cálculo del riesgo acumulado

El riesgo acumulado se calcula con el producto del impacto acumulado y la probabilidad de ocurrencia de una amenaza en particular (Ecuación 2.53). Para éste, solo se consideran las amenazas directas sobre el activo en cuestión, y refleja el daño potencial que puede causar a la organización debido a la cantidad de activos que pueden verse afectados.

$$RA = IA \times P; \quad RA \in \mathbb{R}^{+} \tag{2.53}$$

Donde:
- RA Riesgo acumulado por determinada amenaza
- IA Impacto acumulado de la amenaza sobre el activo
- P Probabilidad de ocurrencia de la amenaza sobre el activo

Continuando con el ejemplo anterior, si la amenaza de inundación provoca el impacto acumulado calculado en la Ecuación 2.38, de la sección 2.2.4.2, al activo *E*, y el valor de la probabilidad de ocurrencia de esta amenaza es el calculado en la Ecuación 2.52, de la sección 2.2.5.2, se aplica la Ecuación 2.53 para calcular el riesgo acumulado que corre el activo *E* por dicha amenaza, como se muestra en la Ecuación 2.54.

$$RA_E = IA_E \times P_E = 40.932\overline{3} \times 10\% \equiv 40.932\overline{3} \times 0.1 \cong 4.09323 \tag{2.54}$$

Estos valores están registrados en la Matriz de Riesgos del Anexo T.

2.2.6.2 Cálculo del riesgo repercutido

El riesgo repercutido se calcula con el producto del impacto repercutido y la probabilidad de ocurrencia de una amenaza en particular. Un activo puede correr tantos riesgos repercutidos como amenazas haya sobre los activos de los cuales depende, y refleja el daño potencial que puede causarle al activo como tal. Sea *A* un activo que depende de otro B, si una amenaza se materializa sobre el activo *B*, sus efectos repercuten sobre *A* con la misma probabilidad de ocurrencia, cuyo valor se calcula con la Ecuación 2.55.

$$RR_A = IR_A \times P_B = V_A \times degr_B \times d_{AB} \times P_B; \quad RR \in \mathbb{R}^{+} \tag{2.55}$$

Donde:

RR_A	Riesgo repercutido por determinada amenaza al propagarse hacia el activo A
IR_A	Impacto repercutido de la amenaza al propagarse hacia el activo A
P_B	Probabilidad de ocurrencia de la amenaza sobre el activo B donde se materializó la amenaza
V_A	Valor propio del activo A
$degr_B$	Nivel de degradación causada por la amenaza a B
d_{AB}	Grado de dependencia de A hacia B

Continuando con el ejemplo de la amenaza de inundación sobre el activo *E*, cuya probabilidad es del 10%, en donde sus efectos se propagan hacia el activo C_2, como se ilustra en la Figura 2.20, se toma el valor del impacto repercutido por dicha amenaza sobre C_2, calculado en la Ecuación 2.40 de la sección 2.2.4.3, pero conservando la misma probabilidad de ocurrencia que tiene dicha amenaza sobre el activo *E* (Ecuación 2.52). Así, aplicando la Ecuación 2.55 con estos valores, se obtiene el riesgo repercutido, como se indica en la Ecuación 2.56.

$$RR_{C_2} = IR_{C_2} \times P_E = 3.93 \times 10\% \equiv 3.93 \times 0.1 = 0.39 \quad (2.56)$$

O, considerando la segunda forma de la Ecuación 2.55, obtenemos el mismo resultado, como se indica en la Ecuación 2.57:

$$RR_{C_2} = V_{C_2} \times degr_E \times d_{C_2E} \times P_E = 24 \times 63.3\% \times 0.26 \times 10\% \equiv 0.39 \quad (2.57)$$

Estos valores están registrados en el Anexo T (en los riesgos repercutidos).

2.2.7 SALVAGUARDAS

Tabla 2.50. Etapa de estimación y cálculo de la eficacia de las salvaguardas [Elaboración propia]

Entrada	Proceso	Salida
• *Estudio de amenazas, vulnerabilidades y salvaguardas (Anexo K)* • *Criterios de estimación de eficacia (sección 2.1.10.6)*	• Cálculo del factor de reducción total producido por la eficacia de las salvaguardas con el uso de fórmulas.	• Columnas con valores de eficacia (Anexo T)

Una amenaza determinada puede ser confrontada con múltiples medidas de control. Según su mecanismo de control, las medidas pueden ser correctivas (confrontar el impacto) o

preventivas (confrontar la probabilidad), y la eficacia de una medida de control se mide a través de su factor de reducción.

2.2.7.1 Cálculo de la eficacia total de las medidas de control correctivas

Las escalas de valor de la eficacia de las medidas de control correctivas se encuentran especificadas en la sección 2.1.10.6.1. Estas medidas hacen frente al impacto de una amenaza, tratando de paliar sus efectos a fin de recuperar un activo una vez que la amenaza se ha materializado, como es representada de forma didáctica en la Figura 2.23.

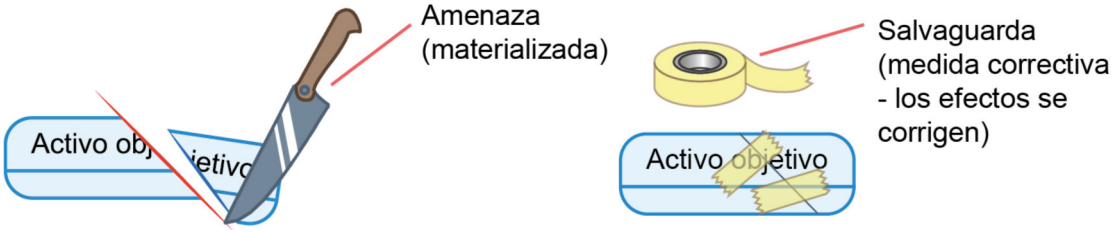


Figura 2.23. Representación del propósito de las medidas correctivas
[Elaboración propia]

La Figura 2.23 es un concepto ideal de una medida correctiva, pues se espera paliar el impacto totalmente, es decir, disminuir a cero los efectos de una amenaza, o recuperar por completo un activo de información, pero lo cierto es que esto puede lograrse solo hasta un cierto nivel.

Para una misma amenaza sobre un determinado activo puede haber un ilimitado número de medidas correctivas, y el factor de reducción total frente al impacto se calcula como el producto de los factores de reducción estimados de todas éstas, como se indica en la Ecuación 2.58.

$$e_I = \prod_{i=1}^{n} em_{C_i} = em_{C_1} \times em_{C_2} \times em_{C_3} \times \cdots \times em_{C_n}; \quad e_I \in \mathbb{R}^+ \tag{2.58}$$

Donde:

e_I	Eficacia total (factor de reducción resultante) de las medidas de control correctivas frente al impacto de determinada amenaza
em_{C_i}	Factor de reducción de la eficacia estimada de cada una de las *n* medidas de control correctivas contra la amenaza
n	Cantidad total de medidas de control correctivas contra dicha amenaza

Por ejemplo, suponiendo que para una amenaza particular se han hallado seis medidas correctivas, cuyos factores de reducción han sido estimados previamente, se las ha organizado en el ejemplo de la Tabla 2.51.

Tabla 2.51. Ejemplo de estimación de eficacia de las medidas correctivas
[Elaboración propia]

AMENAZA	Salvaguarda(s) aplicada(s)	Mecanismo		
		Correctivas		
		De protección o limitación	Paliativa	De recuperación por leyes, garantías o seguros
Amenaza X	Medida de control 01		40%	
	Medida de control 02			16%
	Medida de control 03	6%		
	Medida de control 04	16%		
	Medida de control 05			100%
	Medida de control 06			40%

La eficacia total (factor de reducción resultante) de las medidas correctivas frente al impacto, aplicando la Ecuación 2.58 como se indica en la Ecuación 2.59, es obtenida en la Ecuación 2.60.

$$e_I = 40\% \times 16\% \times 6\% \times 16\% \times 100\% \times 40\% \equiv 0.4 \times 0.16 \times 0.6 \times 0.16 \times 1 \times 0.4 \quad (2.59)$$

$$e_I = 0.0025 \equiv 0.25\% \quad (2.60)$$

2.2.7.2 Cálculo de la eficacia total de las medidas de control preventivas

Las escalas de valor de la eficacia de las medidas de control preventivas se encuentran especificadas en la sección 2.1.10.6.2. Estas medidas hacen frente a la probabilidad de ocurrencia de una amenaza, a fin de evitar que ésta llegue a materializarse. La Figura 2.24 proporciona una representación didáctica del propósito de una medida preventiva.

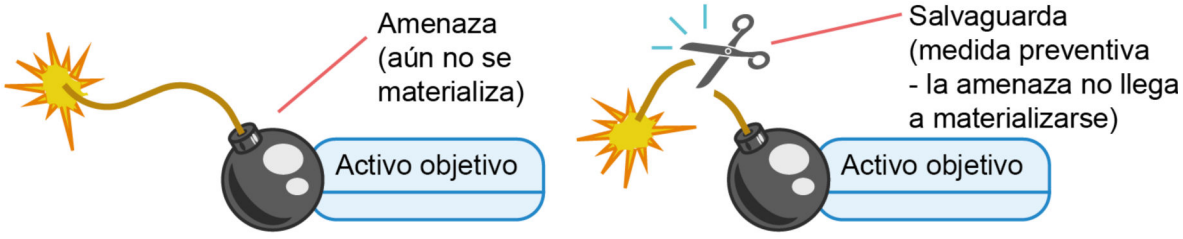


Figura 2.24. Representación del propósito de las medidas preventivas
[Elaboración propia]

La Figura 2.24 es un concepto ideal de una medida preventiva, pues se espera reducir a cero la probabilidad de ocurrencia de una amenaza, pero lo cierto es que esto puede lograrse solo hasta un cierto nivel.

Para una misma amenaza sobre un determinado activo, puede haber un ilimitado número de medidas preventivas, y el factor de reducción total frente a la probabilidad de ocurrencia se calcula como el producto de los factores de reducción estimados de todas éstas. La Ecuación 2.61 permite determinar el factor de reducción total frente a la probabilidad de una amenaza.

$$e_P = \prod_{i=1}^{n} em_{P_i} = em_{P_1} \times em_{P_2} \times em_{P_3} \times \cdots \times em_{P_n}; \quad e_P \in \mathbb{R}^+ \tag{2.61}$$

Donde:

e_P	Eficacia total (factor de reducción resultante) de las medidas de control preventivas frente a la probabilidad de ocurrencia de determinada amenaza
em_{C_P}	Factor de reducción de la eficacia estimada de cada una de las *n* medidas de control preventivas contra la amenaza
n	Cantidad total de medidas de control preventivas contra dicha amenaza

Por ejemplo, suponiendo que para una amenaza particular se han hallado cinco medidas preventivas, cuyos factores de reducción han sido estimados previamente, se las ha organizado en la Tabla 2.52.

Tabla 2.52. Ejemplo de estimación de eficacia de las medidas preventivas
[Elaboración propia]

		Mecanismo	
AMENAZA	Salvaguarda(s) aplicada(s)	Preventivas	
		Disuasiva (Disuasoria)	Preventiva
Amenaza X	Medida de control 07		100%
	Medida de control 08	40%	
	Medida de control 09	40%	
	Medida de control 10		16%
	Medida de control 11	6%	

La eficacia total (factor de reducción resultante) de las medidas preventivas frente al impacto, aplicando la Ecuación 2.61, se calcula como se indica en la Ecuación 2.62, obteniéndose el resultado que muestra la Ecuación 2.63.

$$e_P = 100\% \times 40\% \times 40\% \times 16\% \times 6\% \equiv 1 \times 0.4 \times 0.4 \times 0.16 \times 0.6 \quad (2.62)$$

$$e_P = 0.01536 \equiv 1.54\% \quad (2.63)$$

2.2.8 IMPACTO RESIDUAL

Tabla 2.53. Etapa de cálculo del impacto residual [Elaboración propia]

Entrada	Proceso	Salida
• *Valores de impacto acumulado y repercutido (sección 2.2.4).* • *Eficacia (factor de reducción) de las salvaguardas (sección 2.2.7.1)*	• Cálculo de los impactos acumulado y repercutido residuales con el uso de fórmulas.	• Impacto acumulado residual e impacto repercutido residual (Anexo T)

Impacto residual es el valor del impacto que queda luego de haber sido confrontado por las medidas correctivas.

2.2.8.1 Cálculo del impacto acumulado residual

El impacto acumulado residual se calcula con el producto del impacto acumulado que provoca una amenaza sobre un activo, y la eficacia total (factor de reducción resultante) de las medidas correctivas, como se indica en la Ecuación 2.64.

$$IAr = IA \times e_I; \quad IAr \in \mathbb{R}^+ \quad (2.64)$$

Donde:

IAr	Impacto acumulado residual
IA	Impacto acumulado
e_I	Eficacia total (factor de reducción resultante) de las medidas de control correctivas.

Continuando con el ejemplo, si el impacto acumulado de la amenaza de inundación sobre el activo E, calculado en el ejemplo de la sección 2.2.4.2, en la Ecuación 2.38, es confrontado por las medidas de control correctivas cuyo factor de reducción total fue calculado en el ejemplo de la sección 2.2.7.1, en la Ecuación 2.60, el impacto acumulado quedaría como se indica en la Ecuación 2.65.

$$IAr_E = IA_E \times e_{I_E} = 40.932\overline{3} \times 0.25\% \equiv 40.932\overline{3} \times 0.0025 \cong 0.1023 \quad (2.65)$$

Estos valores están registrados en la Matriz de Riesgos del Anexo T.

2.2.8.2 Cálculo del impacto repercutido residual

Sea B el activo sobre el que se efectúa la amenaza y sobre el que se aplican las medidas de control correctivas, y A el activo hacia el que se propagan los efectos de dicha amenaza; el impacto repercutido residual sobre A se calcula como el producto del impacto repercutido sobre A y la eficacia total (factor de reducción resultante) de las medidas de control correctivas en B, como se indica en la Ecuación 2.66.

$$IRr_A = IR_A \times e_{I_B}; \quad IRr_A \in \mathbb{R}^+ \tag{2.66}$$

Donde:
- IRr_A Impacto repercutido residual sobre A
- IR_A Impacto repercutido de la amenaza del activo B sobre A
- e_{I_B} Eficacia total (factor de reducción resultante) de las medidas de control correctivas aplicadas en B.

Por ejemplo, dado que la amenaza de inundación cayó sobre el activo E, pero sus efectos repercuten con un cierto grado sobre C_2, el impacto repercutido de este último, calculado en el ejemplo de la Ecuación 2.40, de la sección 2.2.4.3, se multiplica por el factor de reducción resultante sobre el impacto hallado en el activo E en la Ecuación 2.60, sección 2.2.7.1, obteniéndose así el impacto repercutido residual sobre C_2, como se indica en la Ecuación 2.67.

$$IRr_{C_2} = IR_{C_2} \times e_{I_E} = 3.93 \times 0.25\% \equiv 3.93 \times 0.0025 \cong 0.0098 \tag{2.67}$$

Estos valores están registrados en la Matriz de Riesgos Anexo T (riesgos repercutidos).

2.2.9 PROBABILIDAD RESIDUAL

Tabla 2.54. Etapa de cálculo de probabilidad residual [Elaboración propia]

Entrada	Proceso	Salida
• *Probabilidad (sección 2.2.5).* • *Eficacia (factor de reducción) de las salvaguardas (sección 2.2.7.2)*	• Cálculo de la probabilidad residual con el uso de fórmula.	• Probabilidad residual (Anexo T)

La probabilidad residual es el resto de la probabilidad de ocurrencia debido a las medidas de control preventivas frente a una amenaza. La probabilidad residual se calcula como el producto de la probabilidad de ocurrencia de una amenaza sin salvaguardas, y la eficacia

total (factor de reducción resultante) de las medidas de control preventivas. La Ecuación 2.68 permite hallar el valor de la probabilidad residual.

$$Pr = P \times e_P; \quad Pr \in \mathbb{R}^+ \tag{2.68}$$

Donde:
- Pr Probabilidad residual
- P Probabilidad de ocurrencia de la amenaza
- e_P Eficacia total (factor de reducción resultante) de las medidas de control preventivas.

A partir del ejemplo de la sección 2.2.5.2, si a la probabilidad de amenaza de inundación calculada en la Ecuación 2.52, se le multiplica la eficacia total (factor de reducción resultante) de las medidas preventivas calculadas en la Ecuación 2.63 de la sección 2.2.7.2, la probabilidad residual sería la que se indica en la Ecuación 2.69.

$$Pr = P \times e_P = 10\% \times 1.54\% \equiv 0.1 \times 0.0154 \equiv 0.154\% \tag{2.69}$$

Estos valores están registrados en la Matriz de Riesgos del Anexo T.

2.2.10 RIESGO RESIDUAL

Tabla 2.55. Etapa de cálculo de riesgo residual [Elaboración propia]

Entrada	Proceso	Salida
• *Valores de impacto acumulado y repercutido (sección 2.2.4), Probabilidad (sección 2.2.5).* • *Riesgo acumulado y riesgo repercutido (sección 2.2.6)* • *Eficacia (factor de reducción) de las salvaguardas (secciones 2.2.7.1 y 2.2.7.2)*	• Cálculo de los riesgos acumulado y repercutido residuales con el uso de fórmulas.	• Riesgo residual (Anexo T)

El riesgo residual es el remanente del riesgo al ser confrontado por las salvaguardas. En la Figura 2.25, el riesgo atraviesa por las salvaguardas, primero a través de las medidas preventivas, las cuales reducen el riesgo generando un primer remanente, y luego por las medidas correctivas, generando el último remanente: el riesgo residual.

Para una amenaza puede haber medidas preventivas, medidas correctivas o ambas. Siempre que atraviese por una salvaguarda con cierto nivel de eficacia, una amenaza representará menos riesgo cada vez.

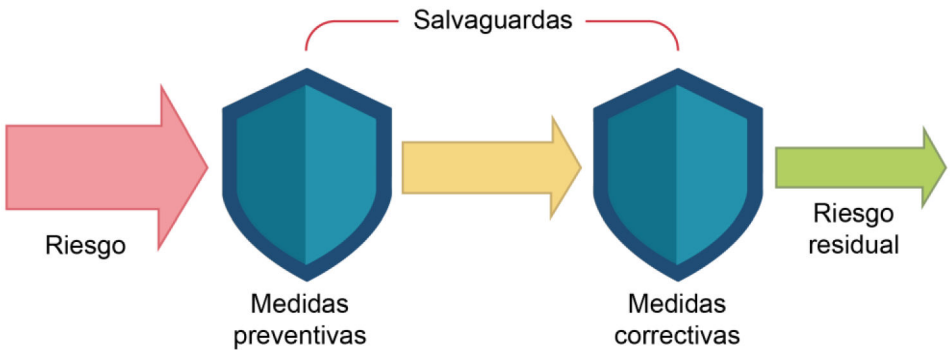


Figura 2.25. Del riesgo original al riesgo residual
[Elaboración propia]

2.2.10.1 Cálculo del riesgo residual acumulado

El riesgo acumulado residual se calcula como el producto del impacto acumulado y probabilidad residuales, como se indica en la Ecuación 2.70, o bien, como el producto del riesgo acumulado y los factores de reducción totales de las medidas correctivas y preventivas, aplicando la Ecuación 2.71. En cualquier caso, el resultado será el mismo.

$$RAr = IAr \times Pr; \quad RAr \in \mathbb{R}^+ \tag{2.70}$$

Donde:
- RAr Riesgo acumulado residual
- IAr Impacto acumulado residual
- Pr Probabilidad residual

O también:

$$RAr = RA \times e_I \times e_P; \quad RAr \in \mathbb{R}^+ \tag{2.71}$$

Donde:
- RAr Riesgo acumulado residual
- RA Riesgo acumulado
- e_I Eficacia total (factor de reducción resultante) de las medidas correctivas
- e_P Eficacia total (factor de reducción resultante) de las medidas preventivas

Siguiendo con el ejemplo, el riesgo residual para la amenaza de inundación del activo E se calcula con el impacto acumulado residual calculado en la Ecuación 2.65, en la sección 2.2.8.1, y la probabilidad residual calculada en la Ecuación 2.69, en la sección 2.2.9, como se indica en la Ecuación 2.72.

$$RAr_E = IAr_E \times Pr = 0.1023 \times 0.154\% \equiv 0.1023 \times 0.00154 \cong 0.00016 \tag{2.72}$$

O aplicando la Ecuación 2.71, con su riesgo acumulado (Ecuación 2.54, sección 2.2.6.1) y la eficacia de sus salvaguardas (Ecuaciones 2.60 y 2.63, de las secciones 2.2.7.1 y 2.2.7.2 respectivamente), como se indica en la Ecuación 2.73, obteniéndose el resultado en la Ecuación 2.74.

$$RAr_E = RA_E \times e_{I_E} \times e_P = 4.0932\overline{3} \times 0.25\% \times 1.54\% \tag{2.73}$$

$$RAr_E \equiv 4.0932\overline{3} \times 0.0025 \times 0.0154 \cong 0.00016 \tag{2.74}$$

Estos valores están registrados en el Anexo T (Riesgos repercutidos).

2.2.10.2 Cálculo del riesgo repercutido residual

El riesgo repercutido residual es el remanente del riesgo repercutido cuando es mitigado por las salvaguardas. Sea A un activo que depende de B, y B el activo sobre el que cae la amenaza, el riesgo repercutido residual se calcula sobre A y equivale al producto del Impacto repercutido residual sobre A y la probabilidad de ocurrencia residual de dicha amenaza, como se indica en la Ecuación 2.75.

$$RRr_A = IRr_A \times Pr_B; \quad RRr_A \in \mathbb{R}^+ \tag{2.75}$$

Donde:

RRr	Riesgo repercutido residual sobre A
IRr	Impacto repercutido residual sobre A
Pr	Probabilidad residual de la amenaza en B

También puede evaluarse como el producto del riesgo repercutido sobre A y la eficacia total (factores de reducción resultantes) de las salvaguardas sobre dicha amenaza, como se muestra en la Ecuación 2.76.

$$RRr_A = RR_A \times e_{I_B} \times e_{P_B}; \quad RRr_A \in \mathbb{R}^+ \tag{2.76}$$

Donde:

RAr	Riesgo repercutido residual sobre A
RA	Riesgo repercutido sobre A
e_{I_B}	Eficacia total (factor de reducción resultante) de las medidas correctivas en B
e_{P_B}	Eficacia total (factor de reducción resultante) de las medidas preventivas en B

Continuando el ejemplo que se ha venido tratando, el riesgo repercutido residual sobre C_2 es el producto del impacto repercutido residual sobre éste, con la Ecuación 2.67, sección

2.2.8.2, y la probabilidad residual sobre el activo E, con la Ecuación 2.69, sección 2.2.9, como se indica en la Ecuación 2.77.

$$RRr_{C_2} = IRr_{C_2} \times Pr_E = 0.0098 \times 0.154\% \equiv 0.0098 \times 0.00154 \cong 0.000015 \quad (2.77)$$

Este valor también puede hallarse aplicando la Ecuación 2.76 con el producto del riesgo repercutido sobre C_2 (Ecuación 2.56, de la sección 2.2.6.2) y la eficacia de las salvaguardas (Ecuaciones 2.60 y 2.63, de las secciones 2.2.7.1 y 2.2.7.2 respectivamente), como se indica en la Ecuación 2.78, cuyo resultado se muestra en la Ecuación 2.79.

$$RRr_{C_2} = RR_{C_2} \times e_{I_E} \times e_{P_E} = 0.39 \times 0.25\% \times 1.54\% \quad (2.78)$$

$$RRr_{C_2} = \equiv 0.39 \times 0.0025 \times 0.0154 \cong 0.00015 \quad (2.79)$$

Estos valores están registrados en el Anexo T (Riesgos repercutidos).

2.2.11 EVALUACIÓN DEL RIESGO

La norma ISO/IEC 27005 [5] establece que los criterios de evaluación del riesgo deben haber sido definidos en el establecimiento del contexto, pero deben revisarse con mayor detenimiento en esta etapa, debido a que se tiene mayor conocimiento de los riesgos identificados.

2.2.11.1 Evaluación del impacto

El impacto calculado según el método de análisis y evaluación de riesgos es evaluado bajo los criterios establecidos en la Tabla 2.18 de la sección 2.1.10.3.2. El impacto máximo posible se alcanza con el valor máximo de degradación (100%) hacia el mayor valor acumulado registrado de todos los valores acumulados de los activos de la Planta Central del MCyP. De acuerdo al Anexo F y al Anexo G, el mayor valor acumulado calculado es el que se indica en la Ecuación 2.80.

$$VA_{(MÁX)} = 1333.86 \quad (2.80)$$

Con esto, el impacto máximo sería el que se indica en la Ecuación 2.81.

$$Impacto_{(MÁX)} = VA_{(MÁX)} \times degr_{(MÁX)} = 1333.86 \times 100\% = 1333.86 \quad (2.81)$$

A partir de esto, tomando como base los umbrales de la Tabla 2.18, se definen rangos de evaluación que se muestran en la Tabla 2.56.

Tabla 2.56. Evaluación del impacto [Elaboración propia]

	RANGO	NIVEL	ABREV.	DESCRIPCIÓN
1333.86	]133.386 – 1333.86]	MUY ALTO	MA	El impacto es vital
133.386	]13.3386 – 133.386]	ALTO	A	El impacto es muy grave
13.3386	]1.33386 – 13.3386]	MEDIO	M	El impacto es grave
1.33386	]0.133386 – 1.33386]	BAJO	B	El impacto es considerable
0.133386	]0 – 0.133386]	MUY BAJO	MB	El impacto es insignificante

2.2.11.2 Evaluación de la probabilidad de origen deliberado

Como se vio en el Método de Análisis y Evaluación de Riesgos, la probabilidad calculada con el producto con los criterios vistos en la sección 2.1.10.4.1, siguiendo el modelo de la Tabla 2.23, se organiza en una matriz de potencialidad (Tabla 2.57) por facilidad e interés para el atacante, en la cual se descartan aquellas combinaciones que estén por debajo del valor 0.01% (gris), por considerarse despreciables.

Tabla 2.57. Evaluación de probabilidad por interés y facilidad para el atacante [Elaboración propia]

FACILIDAD						
F	100%	0.01%	0.1%	1%	10%	100%
M	10%	0.001%	0.01%	0.1%	1%	10%
D	1%	0.0001%	0.001%	0.01%	0.1%	1%
MD	0.1%	0.00001%	0.0001%	0.001%	0.01%	0.1%
ED	0.01%	0.000001%	0.00001%	0.0001%	0.001%	0.01%
		0.01%	0.1%	1%	10%	100%
		SI	EI	MPI	MI	AI
				INTERÉS		

Esto puede organizarse, por tanto, en una tabla de criterios de valoración con casos específicos de facilidad e interés en un activo determinado para que el atacante lleve a cabo un ataque en contra de la seguridad de la información y realice un perjuicio u obtenga un beneficio. Los criterios para los casos específicos pueden verse en la Tabla 2.58.

Tabla 2.58. Casos resultantes de probabilidad de amenaza deliberada
[Elaboración propia]

VALOR	NIVEL	ABREV.	DESCRIPCIÓN (CASOS RESULTANTES)
100%	ALTA PROBABILIDAD	AP	El atacante podría tener un alto interés en el activo y podría llevar a cabo el ataque con gran facilidad.
10%	PROBABLE	P	El atacante podría tener un alto interés en el activo y podría llevar a cabo el ataque con moderada facilidad.
			El atacante podría tener un interés moderado en el activo y podría llevar a cabo el ataque con gran facilidad.
1%	MEDIO	M	El atacante podría tener un alto interés en el activo, pero podría llevar a cabo el ataque con dificultad.
			El atacante podría tener un interés moderado en el activo y podría llevar a cabo el ataque con moderada facilidad.
			El atacante podría tener muy poco interés en el activo, aunque podría llevar a cabo el ataque con gran facilidad.
0.1%	BAJA PROBABILIDAD	BP	El atacante podría tener un alto interés en el activo y podría llevar a cabo el ataque, pero con alta dificultad.
			El atacante podría tener un interés moderado en el activo, pero podría llevar a cabo el ataque con dificultad.
			El atacante podría tener muy poco interés en el activo, aunque podría llevar a cabo el ataque con moderada facilidad.
			El atacante podría tener un escaso interés en el activo, aunque podría llevar a cabo el ataque con gran facilidad.
0.01%	MUY BAJA PROBABILIDAD	MBP	El atacante podría tener un alto interés en el activo, pero podría llevar a cabo el ataque con dificultad extrema.
			El atacante podría tener un interés moderado en el activo y podría llevar a cabo el ataque, pero con alta dificultad.
			El atacante podría tener muy poco interés en el activo, aunque podría llevar a cabo el ataque con dificultad.
			El atacante podría tener un escaso interés en el activo, aunque podría llevar a cabo el ataque con moderada facilidad.
			El atacante podría no tener interés alguno por él activo, aunque podría llevar a cabo el ataque con gran facilidad.

2.2.11.3 Evaluación de la probabilidad de origen natural o accidental

La probabilidad resultante, calculada según lo indicado en el método de análisis y evaluación de riesgos, con los criterios vistos en la sección 2.1.10.4.2, siguiendo el modelo de la Tabla 2.23, se organiza en una matriz de probabilidad (Tabla 2.59) considerando los valores de susceptibilidad y frecuencia. Se ignoran aquellos valores que estén por debajo de 0.01% (gris), por considerarse despreciables.

Los casos resultantes se organizan en la tabla de criterios de valoración con casos específicos de susceptibilidad y frecuencia de ocurrencia de un evento natural o accidental. Los criterios para los casos específicos pueden verse en la Tabla 2.60.

Tabla 2.59. Evaluación de probabilidad por susceptibilidad y frecuencia del evento

[Elaboración propia]

FRECUENCIA							
	MF	100	0.01%	0.1%	1%	10%	100%
	F	10	0.001%	0.01%	0.1%	1%	10%
	N	1	0.0001%	0.001%	0.01%	0.1%	1%
	PF	0.1	0.00001%	0.0001%	0.001%	0.01%	0.1%
	MPF	0.01	0.000001%	0.00001%	0.0001%	0.001%	0.01%
			0.01%	0.1%	1%	10%	100%
			MPS	PS	N	S	MS

SUSCEPTIBILIDAD

Tabla 2.60. Casos resultantes de probabilidad de amenaza natural o accidental

[Elaboración propia]

VALOR	NIVEL	ABREV.	DESCRIPCIÓN (CASOS RESULTANTES)
100%	ALTA PROBABILIDAD	AP	Alta susceptibilidad a que el evento ocurra, y se da a diario o varias veces al mes.
10%	PROBABLE	P	Alta susceptibilidad a que el evento ocurra, pero ocurre mensualmente o varios meses al año.
			Susceptibilidad media a que el evento ocurra, y se da a diario o varias veces al mes.
1%	MEDIO	M	Alta susceptibilidad a que el evento ocurra, pero ocurre solo una vez al año.
			Susceptibilidad media a que el evento ocurra, pero ocurre mensualmente o varios meses al año.
			Susceptibilidad baja a que el evento ocurra, y se da a diario o varias veces al mes.
0.1%	BAJA PROBABILIDAD	BP	Alta susceptibilidad a que el evento ocurra, pero ocurre cada varios años.
			Susceptibilidad media a que el evento ocurra, pero ocurre solo una vez al año.
			Susceptibilidad baja a que el evento ocurra, pero ocurre mensualmente o varios meses al año.
			Susceptibilidad muy baja a que el evento ocurra, y se da a diario o varias veces al mes.
0.01%	MUY BAJA PROBABILIDAD	MBP	Alta susceptibilidad a que el evento ocurra, pero ocurre cada siglo.
			Susceptibilidad media a que el evento ocurra, pero ocurre cada varios años.
			Susceptibilidad baja a que el evento ocurra, pero ocurre solo una vez al año.
			Susceptibilidad muy baja a que el evento ocurra, pero ocurre mensualmente o varios meses al año.
			Susceptibilidad insignificante a que el evento ocurra, y se da a diario o varias veces al mes.

2.2.11.4 Evaluación del riesgo resultante

A partir de la Tabla 2.24, de la sección 2.1.10.5, se desarrolla la cuadrícula de evaluación y aceptación del riesgo de la Figura 2.26, que guarda estrecha afinidad con la Tabla de aceptación del riesgo de MEHARI 2010 en el libro *Conceptos Fundamentales y Especificaciones Funcionales [81]* (Figura 2.27).

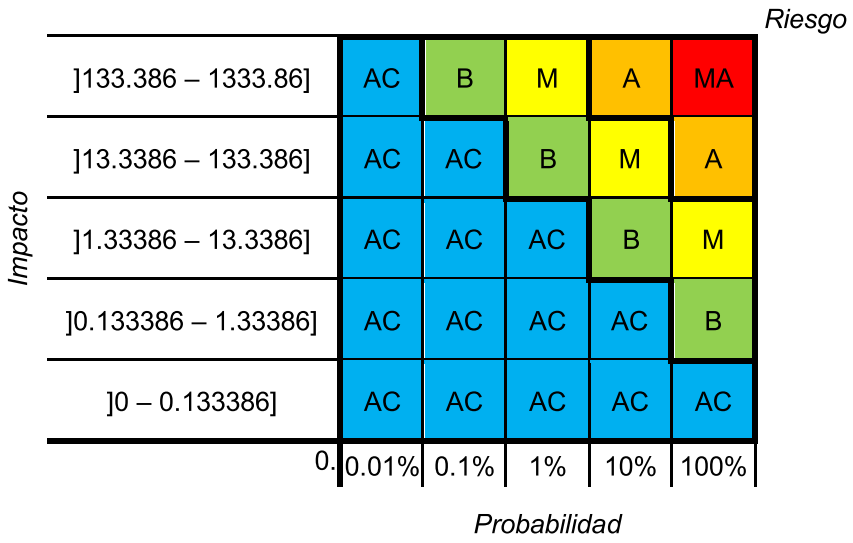


Figura 2.26. Cuadrícula de evaluación y aceptación del riesgo
[Elaboración propia]

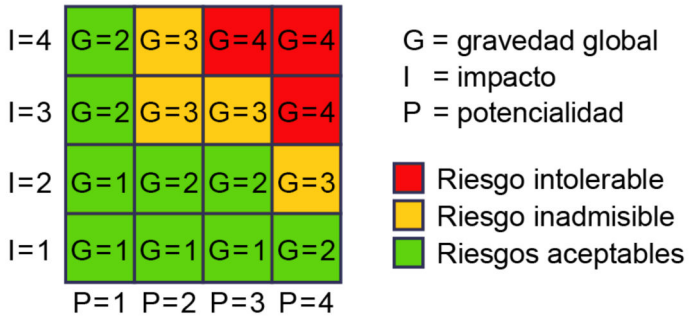


Figura 2.27. Cuadrícula de aceptación del riesgo de MEHARI 2010 [81]

De la avenencia entre la Figura 2.26, resultado de la Metodología de Análisis y Evaluación de Riesgos (MAER) desarrollada en este Trabajo de Titulación, y la Figura 2.27, obtenida de MEHARI 2010 [81], se construye la Tabla 2.61, que proporciona más información a la hora de la toma de decisiones en el tratamiento de riesgos.

Tabla 2.61. Evaluación y aceptación del riesgo [Elaboración propia]

Evaluación MEHARI	Descripción	Evaluación MAER		Abrev.	Descripción
Riesgos intolerables	Requieren medidas de emergencia, fuera de los ciclos presupuestarios normales.	]133.386 – 1333.86]	Muy alto	MA	Muy alto riesgo. Riesgo de atención inmediata (crítico).
		]13.3386 – 133.386]	Alto	A	Alto riesgo. Riesgo de emergencia (emergencia de primer nivel).
Riesgos inadmisibles	Deben reducirse o eliminarse en algún momento, en un ciclo de planificación.	]1.33386 – 13.3386]	Medio	M	Riesgo moderado. Riesgo de urgencia (emergencia de segundo nivel).
		]0.133386 – 1.33386]	Bajo	B	Bajo riesgo. Riesgo de urgencia menor (riesgo estándar).
Riesgos aceptables	Riesgos aceptables.	]0 – 0.133386]	Aceptable	AC	Riesgo aceptable. Riesgo no urgente o descartable.

Los riesgos y su evaluación se encuentran en la Matriz de Riesgos del Anexo T.

2.3 TRATAMIENTO DEL RIESGO

Acorde a la ISO/IEC 27005 [5], existen cuatro opciones para tratar los riesgos: retener, reducir, evitar o transferir los riesgos, y la norma ISO/IEC 27002 [4] proporciona información a detalle de los controles que pueden aplicarse para el tratamiento.

En los siguientes apartados se describe cada opción, pero se advierte que no debe tomarse como una obligación el ponerlas en práctica como se indican, pues la decisión sobre el tratamiento final que se considere oportuno darle a una determinada situación de riesgo será siempre de la autoridad competente, lo que implica que puede haber excepciones en la forma de tratar un riesgo, si así amerita el caso.

2.3.1 ANÁLISIS DE RESTRICCIONES

Idealmente, cualquier control que permita mitigar los riesgos hasta un nivel aceptable debería implementarse, pero en la práctica esto no es así. A la hora de tomar decisiones sobre la selección e implementación de controles, deben considerarse las condiciones que puedan limitar o negar la aplicación de éstos, por lo que realizar un análisis de restricciones resulta importante.

El Anexo E de la norma ISO/IEC 27005 [5] menciona los aspectos generales que pueden restringir la aplicación de un control. La Tabla 2.62 enlista estas restricciones junto con una descripción y ejemplos.

Tabla 2.62. Restricciones para implementación de controles

[Elaboración propia, basada en [5]]

Restricciones	Descripción	Ejemplo(s)
De tiempo	Tiempo disponible para implementar un control determinado. Pueden haber variados tipos de restricción de tiempo.	Vida activa de la información o del sistema. Tiempo aceptable de exposición al riesgo definido por la alta dirección.
Financieras	Cantidad presupuestada para implementar un control determinado. El costo de implementación debe ser menor que el costo del riesgo, salvo en cuestiones de legislación.	Presupuesto definido por la alta dirección. Límite de costo definido según estudio costo-beneficio. Costo incrementa o decrece con la calidad del control, pero se requiere una calidad de control mínima.
Técnicas	Condiciones limitantes de hardware o software para un control determinado.	Compatibilidad. Características técnicas de los equipos. Productividad mínima esperada.
Operativas	Condiciones mínimas de operación a considerar al momento de implementar un control.	Operar 24 horas, 7 días a la semana, y aun así sacar una copia de soporte.
Culturales	Limitaciones de implementación de un control por cuestiones nacionales, sectoriales, de la institución o de un departamento. Este aspecto no puede ignorarse porque muchos activos dependen del activo humano.	Un control culturalmente no aceptable por parte de ciertos individuos o población.
Éticas	Limitaciones de implementación de controles por cuestiones de ética según las normas sociales del país, la región o gobierno.	Privacidad de la información dependiente de la ética regional, como que el explorar el correo electrónico esté prohibido.
Ambientales	Las condiciones del entorno natural limitan la implementación de un control determinado.	Ubicación del *datacenter* fuera del nivel de inundación.
Legales	Condiciones legales que regulan la implementación de un control.	Leyes de protección de datos personales. Códigos criminales para el procesamiento de la información.
De facilidad en el uso	Facilidad requerida de la interfaz tecnología-usuario. Un control de interfaz compleja puede llevar a cometer errores humanos, o a que el usuario busque saltarse el control mientras pueda.	Controles con restricción adaptada a las capacidades de los usuarios.
De personal	Limitaciones en disponibilidad de personal especializado, sueldo de personal especializado en la implementación de controles, capacidad e trasladar a los usuarios fuera de condiciones desfavorables, etc.	Cantidad de personal especializado insuficiente para sustentar un control. Sueldo de personal especializado que no supere el presupuesto.
Integrar controles	Limitaciones de un control determinado por compatibilidad o congruencia con controles existentes.	Incompatibilidad entre sistemas de control de acceso físico.

2.3.2 OPCIONES PARA EL TRATAMIENTO DEL RIESGO

2.3.2.1 Retener el riesgo

Retener el riesgo significa aceptar el riesgo sin tomar acciones para tratarlo. Esto depende de los resultados obtenidos en la evaluación del riesgo, y del análisis de restricciones que lleven a tomar esta decisión. Se han tomado las dos razones que proporciona MEHARI

[81] para aceptar (retener) el riesgo, y se han adaptado a este análisis. Así, la opción de aceptar el riesgo puede ser elegida por estos motivos:

- Los riesgos cuyo valor entra en el rango de aceptación del riesgo en la Tabla 2.61 de evaluación y aceptación del riesgo, aquel marcado como Aceptable (AC), en color azul, de la evaluación MAER. Los riesgos por debajo de este umbral pueden verse en la cuadrícula de evaluación y aceptación del riesgo de la Figura 2.26. Es muy fácil que exista un consenso de aceptación.
- Aquellos riesgos que superen el umbral de aceptación, ubicados típicamente en los niveles Medio (M) y Bajo (B) en la Tabla 2.61, considerados como riesgos inadmisibles, pero que son imposibles de atenuar debido a que la implementación de los controles respectivos sale de las restricciones y no existen otras alternativas. Para este caso se tiene mayor exigencia en la existencia de un consenso de aceptación del riesgo, aceptación que debe ser comunicada.

Como medida alterna, pueden establecerse indicadores de monitoreo a fin de garantizar que se mantengan en el nivel aceptable a largo plazo.

Cuando el riesgo es aceptado, es buena práctica de la institución, además, el reservar fondos para el caso en el que el riesgo llegue a consumarse, a fin de poder afrontar las consecuencias [76].

2.3.2.2 Reducir el riesgo

Reducir el riesgo es menguar el riesgo disminuyendo el impacto (con medidas de control correctivas), la probabilidad (a través de medidas de control preventivas) o ambos, hasta que el riesgo residual sea evaluado como aceptable.

Según MAGERIT [76], la tarea de reducir o mitigar el riesgo puede requerir ampliar el conjunto de controles; por ejemplo, adquiriendo nuevo equipamiento para mejorar la seguridad, mismo que debe ser considerado como un nuevo activo en el SGSI y que, consecuentemente, incluye nuevas amenazas, por lo que resulta ineludible el repetir el análisis de riesgos, de tal forma que el sistema ampliado presente menor riesgo que el sistema original.

MEHARI [81] añade que pueden tomarse medidas de control “estructurales” que modifiquen la naturaleza o el nivel del riesgo, cambiando ciertos aspectos del contexto de la organización. MAGERIT explica algo similar, solo que éste engloba a esta clase de medidas dentro de un tipo de tratamiento al que denomina “mitigación del riesgo”.

La opción de reducir se toma en un principio cuando los riesgos superan el umbral de aceptación (AC) de la Tabla 2.61. Debe considerarse la relación costo-beneficio cuando se seleccionen los controles, así como las restricciones.

Se han agrupado las formas en que las metodologías abordan esta opción:

- Implementar controles de seguridad adecuados, considerando las limitaciones de las restricciones. Se recomienda que estos controles no sean soluciones concretas, porque hacen que la relevancia del control dependa de la evolución tecnológica. [81]
- Implementar "servicios de seguridad" en lugar de controles de seguridad concretos. MEHARI define "servicio" como una función de seguridad con un propósito determinado, independientemente de los mecanismos específicos a emplearse, sea cada uno de éstos un proceso, un algoritmo o una tecnología en particular. Cada servicio puede requerir de "sub-servicios" (servicios complementarios para lograr alcanzar el objetivo de un servicio principal, que a su vez tienen funciones propias y específicas), y éstos, a su vez, pueden valerse de posibles mecanismos de seguridad. Por ejemplo, el servicio "control de acceso físico" puede requerir de los sub-servicios "autenticación", "autorización", "filtrado", etc., y el sub-servicio "autenticación" podría utilizar posibles mecanismos como contraseñas, sistemas biométricos, etc. El rendimiento de un servicio se mide por su eficiencia, robustez y permanencia [82]
- Agregar activos que robustezcan la seguridad, siempre y cuando el riesgo resultante del nuevo sistema (que considera los nuevos activos) sea menor que el riesgo antes de la adición de activos. [76]
- Cambiar una o varias condiciones del contexto. Por ejemplo, mover la institución a otro lugar geográfico en donde los riesgos ambientales sean más favorables. [82]

La implementación de controles que consistan en agregar activos o modificar el contexto requieren de un nuevo análisis de riesgos.

2.3.2.3 Evitar el riesgo

Según la ISO/IEC 27005, evitar el riesgo es evadir la actividad o acción que origina el riesgo, y esto puede lograrse retirando la actividad o cambiando las condiciones en donde se realizan dichas actividades. Según MEHARI, evitar el riesgo es similar a reducir el riesgo a través de medidas de control "estructurales", aquellas que pueden modificar el contexto, pero para que el riesgo deje de existir. MAGERIT, por su parte, explica que pueden

eliminarse fuentes de riesgo, es decir, prescindir de otros componentes no esenciales pero que mantenerlos implican riesgos; a esto denomina “eliminación del riesgo”.

Esta medida se aplica cuando un riesgo no es aceptable. Las formas en que las metodologías abordan esta opción se exponen de la siguiente manera:

- Cambiar cierto tipo de activos por otros. Por ejemplo, cambiar el sistema operativo, optar por otros fabricantes, etc. [76]
- Alterar el valor acumulado de los activos con alto riesgo reordenando el esquema de dependencias. Por ejemplo, distribuir la carga de información de un equipo en varios equipos, separar las redes, aislar lo más valioso de lo que está más expuesto, etc. [76]
- Cambiar o eliminar radicalmente uno o varios aspectos del contexto. Por ejemplo, El desarrollo de cierto plan estratégico podría exponer a la institución a un alto riesgo de divulgación de información extremadamente sensible, riesgo que puede superar por mucho al beneficio que se pueda obtener. En este caso, la solución de evitar el riesgo consiste en no desarrollar dicho plan [82]

Estas decisiones requieren de un nuevo análisis de riesgos.

2.3.2.4 Transferir el riesgo

El riesgo puede transferirse de forma parcial o total. MAGERIT prefiere el término “compartir” porque es más general. Según la norma ISO/IEC 27005, el riesgo debería transferirse a una parte externa que tenga la capacidad de gestionarlo con mayor eficacia, según la evaluación del riesgo. Advierte, además, que es posible compartir la responsabilidad del riesgo, más no así la responsabilidad del impacto, que generalmente será atribuido a fallas de la organización. MAGERIT [76] expone dos formas de:

- Cualitativa, repartiendo hacia partes externas las responsabilidades, por ejemplo, subcontratar un servicio par monitorización del sistema de información. Estas pueden ser de tipo:
    - Técnicas, para quienes operan el componente técnico.
    - Legales: con acuerdos establecidos para la prestación de un servicio.
- Cuantitativa, a través de seguros. En este caso, el asegurador corre con las consecuencias a cambio de una prima.

Al optar por este tratamiento del riesgo, es posible que se generen nuevos riesgos de seguridad, por lo que será necesario un nuevo análisis del riesgo.

2.4 EJEMPLO PRÁCTICO: SISTEMA ANTISPAM

A continuación, para facilitar la comprensión, se proporciona un ejemplo de aplicación de la metodología a un activo real de la Planta central del MCyP, el Sistema Antispam. La información y los valores definidos fueron realizados en sesiones de trabajo con los responsables y con profesionales en la Institución. En el Anexo T se refleja todo el trabajo.

2.4.1 LEVANTAMIENTO DEL SISTEMA ANTISPAM

2.4.1.1 Etapa de depuración

Con la información de los Anexos C, D y E, se resuelve que es un activo importante, por lo que supera la etapa de depuración y entra en el proceso de gestión.

2.4.1.2 Codificación del Sistema Antispam

El Sistema Antispam es categorizado como activo primario (P), importante para la actividad del negocio (AN). Para distinguirlo, se le otorga un número (1). Código resultante: ***PAN001***.

2.4.2 VALORACIÓN DEL SISTEMA ANTISPAM

2.4.2.1 Valor propio (V) del Sistema Antispam

Con la información de los Anexos C, D y E correspondientes al Sistema Antispam, se deliberan los valores en cada criterio y subcriterio tomado de la sección 2.1.10, reflejado en las Tablas 2.63, 2.64, 2.65 y 2.66, y se aplican las fórmulas de la sección 2.2.2.1. El registro puede verse en el Anexo F.

Tabla 2.63. Valoración del Sistema Antispam en la confidencialidad [Elaboración propia]

CRITERIOS						
EFECTO LEGAL		EFECTO PERSONAL	EFECTO INSTITUCIONAL			
Problemas legales y sanciones penales	Acuerdo de Confidencialidad	Exposición de la información personal privada	Exposición de la información institucional confidencial.	Secuestro y fuga de la información crítica	Reputación y confianza de los usuarios	Valor Confidencialidad
1	5	1	1	1	1	2

$$V_C \approx \frac{P_{LSP} + A_C + E_{IPP} + E_{IIC} + S_{FIC} + R_{CU}}{6} = \frac{1+5+1+1+1+1}{6} = \frac{10}{6} = 1.\bar{6} \cong 2 \qquad (2.82)$$

Tabla 2.64. Valoración del Sistema Antispam en la integridad [Elaboración propia]

CRITERIOS						
EFECTO LEGAL	**EFECTO PERSONAL**	**EFECTO INSTITUCIONAL**				
Problemas legales y sanciones penales	**Adulteración personal en el desempeño del activo**	**Problemas en el desempeño del activo**	**Problemas en la actividad normal de la institución**	**Reputación y confianza de los usuarios**	**Afectación a usuarios y terceras partes**	Valor de Integridad
5	1	5	4	1	5	4

$$V_I \approx \frac{P_{LSP} + A_{PDA} + P_{DA} + P_{ANI} + R_{CU} + A_{UTP}}{6} = \frac{5+1+5+4+1+5}{6} = 3.5 \cong 4 \quad (2.83)$$

Tabla 2.65. Valoración del Sistema Antispam en la disponibilidad [Elaboración propia]

CRITERIOS					
EFECTO LEGAL	**EFECTO INSTITUCIONAL**				
Problemas legales y sanciones penales	**Afectación en el desempeño de operación interna**	**Afectación a usuarios y terceras partes**	**Reputación y confianza por parte de los usuarios**	**Nivel de Intolerancia**	Valor Disponibilidad
1	4	4	4	5	4

$$V_D \approx \frac{P_{LSP} + A_{DOI} + A_{UTP} + R_{CU} + N_I}{5} = \frac{1+4+4+4+5}{5} = \frac{18}{5} = 3.6 \cong 4 \quad (2.84)$$

Tabla 2.66. Valoración del Sistema Antispam en costo [Elaboración propia]

CRITERIOS			
INTEGRIDAD	**DISPONIBILIDAD**		
Costo por recuperación de la integridad	**Costos por recuperación de la disponibilidad**	**Pérdida material / financiera**	Costo Total (Valor costo)
5	3	3	4

$$V_{Costo} \approx \frac{C_{RI} + C_{RI} + P_{MF}}{3} = \frac{5+3+3}{3} = \frac{11}{3} = 3.\bar{6} \cong 4 \quad (2.85)$$

Los valores son tabulados en la tabla final del Anexo F (en la que también se ha incluido la columna del valor acumulado, valor que se obtiene en otro proceso). La Tabla 2.67 muestra cómo quedan tabulados los valores del Antispam en cada dimensión, con los que se

obtiene el valor propio, sumando los valores de las Ecuaciones 2.82, 2.83, 2.84 y 2.85, como se ve en la Ecuación 2.86, que se registra en la misma tabla.

Tabla 2.67. Valor propio (V) del Antispam [Elaboración propia]

ACTIVOS			VALORES					
N	Código	Nombre del Activo	Localización	Valor Costo	Valor Confidencialidad	Valor Integridad	Valor Disponibilidad	Valor del Activo (V)
1	PAN001	Sistema Antispam	Storage Hitachi/Data Center	4	2	4	4	14

$$V_{Antispam} = V_C + V_I + V_D + V_{Costo} = 2 + 4 + 4 + 4 = 14 \quad (2.86)$$

2.4.2.2 Valor acumulado (VA) del Sistema Antispam

2.4.2.2.1 Dependencias del Sistema Antispam

Se recurre primero al diagrama correspondiente al Sistema Antispam en el Anexo G, que es el que se muestra en la Figura 2.28. El Sistema Antispam se encuentra en la base del diagrama (activo inferior), y de éste dependen los dos activos que se muestran (activos superiores), cada uno con su valor propio especificado. Los grados de dependencia directa que se ven en la Figura 2.28 se explican a continuación.

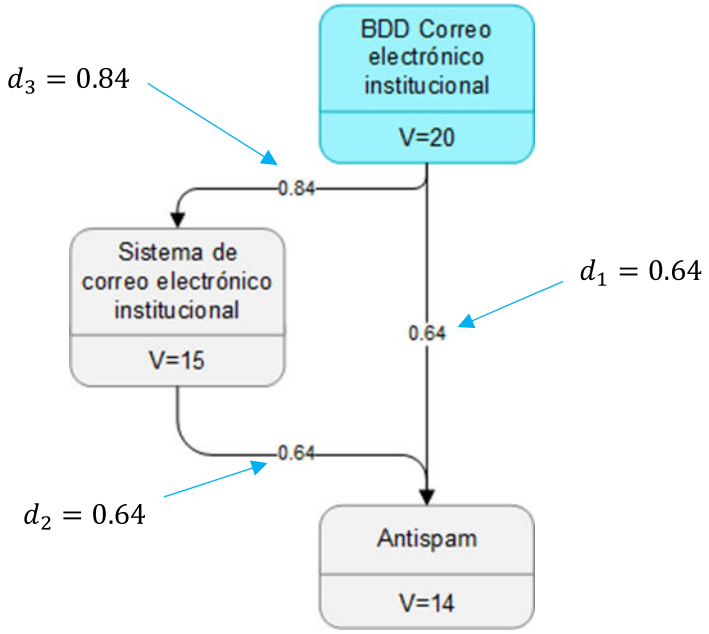


Figura 2.28. Diagrama de dependencias del Sistema Antispam [Elaboración propia]

Las dependencias directas[31] deben calcularse primero. Las dependencias d_1 y d_2 son directas hacia el Sistema Antispam, por lo que se tabulan en el diagrama del Sistema Antispam según los valores que se hayan estimado en cada criterio de valoración de la sección 2.1.10.2, como se muestra en la Tabla 2.68 (ver anexo G), y las dependencias directas resultantes d_1 y d_2 se obtienen aplicando las Ecuación 2.14 (sección 2.2.2.2).

Tabla 2.68. Valoración dependencias directas de los activos superiores al Sistema Antispam [Elaboración propia]

ACTIVOS CON DEPENDENCIA DIRECTA:	CRITERIOS:					DEPENDENCIA RESULTANTE:
	Confidencialidad	Integridad	Disponibilidad	Recursos	Penalización	
BDD Correo electrónico institucional	5	1	5	2	3	0.64
Sistema de correo electrónico institucional	4	3	3	3	3	0.64

$$d_1 = \frac{d_C + d_I + d_D + d_R + d_P}{25} = \frac{5+1+5+2+3}{25} = \frac{16}{25} = 0.64 \quad (2.87)$$

$$d_2 = \frac{d_C + d_I + d_D + d_R + d_P}{25} = \frac{4+3+3+3+3}{25} = \frac{16}{25} = 0.64 \quad (2.88)$$

La dependencia directa d_3 no es directa con respecto al Sistema Antispam, sino con respecto al Sistema de Correo Electrónico Institucional, por lo que debe acudirse al diagrama de dependencias de este último, que es el que se muestra en la Figura 2.29.

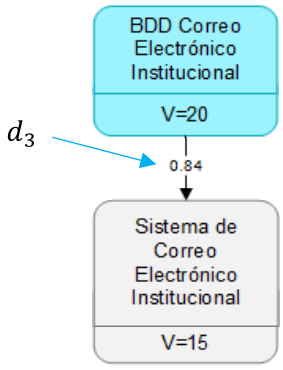


Figura 2.29. Diagrama de dependencias del Sistema de Correo Electrónico Institucional [Elaboración propia]

[31] Los grados de dependencia directa, dados siempre entre dos activos adyacentes, son inmutables en todos los diagramas, es decir, si se ha determinado el grado de dependencia directa entre dos activos definidos, ese valor se mantendrá en todos los diagramas en que aparezcan ambos activos.

En el diagrama del Sistema de Correo Electrónico Institucional del Anexo G se encuentra el cálculo de la dependencia directa para d_3, que se halla de la misma forma que los anteriores.

Se procede a hallar las dependencias finales. Primero se determinan los caminos de cada activo dependiente o superior, con la Ecuación 2.16 de la sección 2.2.2.2, y luego se aplica la Ecuación 2.17 para hallar las dependencias finales de cada activo superior.

Desde el Sistema de Correo Electrónico Institucional al Sistema Antispam hay un solo camino, al que se llamará c_A, con una sola subdependencia (d_2). El valor de dicho camino es el de la Ecuación 2.89. El valor de la dependencia final de este activo ($d_{S.C.E.I.}$) hacia el Sistema Antispam sería el que se muestra en la Ecuación 2.90.

$$c_A = d_2 = 0.64 \tag{2.89}$$

$$d_{S.C.E.I.} = 1 - (1 - c_A) = 1 - (1 - 0.64) = 0.64 \tag{2.90}$$

Desde el activo BDD Correo Electrónico Institucional al Sistema Antispam hay 2 caminos. El primero, al que se llamará $c_{B.1}$, baja por las subdependencias d_3 y d_2. El valor de dicho camino es el de la Ecuación 2.91. El segundo, al que se llamará $c_{B.2}$, baja por una sola subdependencia (d_1). El valor de dicho camino es el de la Ecuación 2.92. El valor de la dependencia final de este activo ($d_{BDD.C.E.I.}$) hacia el Sistema Antispam sería el que se muestra en la Ecuación 2.93.

$$c_{B.1} = d_3 \times d_2 = 0.84 \times 0.64 = 0.5376 \tag{2.91}$$

$$c_{B.2} = d_1 = 0.64 \tag{2.92}$$

$$d_{BDD.C.E.I.} = 1 - (1 - c_{B.1})(1 - c_{B.2}) = 1 - (1 - 0.5376)(1 - 0.64) = 0.833536 \tag{2.93}$$

Finalmente, para hallar el valor acumulado del Sistema Antispam se aplica la Ecuación 2.25 (sección 2.2.2.3), que involucra su valor propio, y la suma de los productos del valor propio de cada activo dependiente (ver Figura 2.28) y sus respectivos grados de dependencias hacia el Sistema Antispam. La aplicación de esto se muestra en la Ecuación 2.94, y el resultado en la Ecuación 2.95.

$$VA_{Antispam} = V_{Antispam} + V_{S.C.E.I.} \times d_{S.C.E.I.} + V_{BDD.S.C.E.i} \times d_{BDD.C.E.I} \tag{2.94}$$

$$VA_{Antispam} = 14 + 15 \times 0.64 + 20 \times 0.833536 = 40.27072 \cong 40.27 \tag{2.95}$$

En la tabla final del Anexo F también consta la columna de valores acumulados. Los cálculos respectivos se encuentran en el Anexo G. Los valores acumulados constan en la Matriz de Riesgos del Anexo T.

2.4.3 IMPACTO ACUMULADO SOBRE EL SISTEMA ANTISPAM

2.4.3.1 Amenazas sobre el Sistema Antispam

Del Anexo T se han seleccionado dos amenazas según su origen para este ejemplo: Errores de administrador, de origen accidental (A) y Denegación de Servicio, de origen deliberado (D). Estas constan en las columnas respectivas de la Matriz de Riesgos del Anexo T. Cada amenaza tiene su propio impacto acumulado sobre el Sistema Antispam.

2.4.3.2 Cálculo de los niveles de degradación e impacto acumulado

En el Anexo T, los valores de la columna "PRIORIDAD" son solo una referencia genérica recomendada por MAGERIT (Libro II, sección *Amenazas*) [77] sobre las dimensiones a las que degrada cierta amenaza, con determinado orden de prioridad (1, 2, o 3), para facilitar el proceso de valoración a discreción de los evaluadores, según la escala de valoración de la Tabla 2.17, de la sección 2.1.10.3. También se registra en el Anexo T. Los valores de impacto acumulado se registran en la columna "IMPACTO".

2.4.3.2.1 Degradación por la amenaza Errores de administrador

Se ha considerado que esta amenaza no tiene influencia en la dimensión de confidencialidad, pero puede provocar degradación *Alta* en la integridad del activo (50%) y *Total* en la disponibilidad (100%). Al aplicar la Ecuación 2.35 (sección 2.2.4.1), se obtiene el valor de la Ecuación 2.96.

$$degr_{Err.Admin.} = \frac{degr_C + degr_I + degr_D}{3} = \frac{0\% + 50\% + 100\%}{3} = 50\% \qquad (2.96)$$

2.4.3.2.2 Impacto acumulado de la amenaza Errores de administrador

Debe aplicarse la Ecuación 2.37 (sección 2.2.4.2), como se muestra en la Ecuación 2.97. El resultado se muestra en la Ecuación 2.98.

$$IA_{Err.Admin.} = VA_{Antispam} \times degr_{Err.Admin.} \qquad (2.97)$$

$$IA_{Err.Admin.} = 40.27 \times 50\% \equiv 40.27 \times 0.5 = 20.135 \cong 20.14 \qquad (2.98)$$

2.4.3.2.3 Degradación por la amenaza Denegación de Servicio

Se ha considerado que esta amenaza no tiene influencia en las dimensiones de confidencialidad e integridad, pero puede provocar degradación *Total* en la disponibilidad

(100%). Al aplicar la Ecuación 2.35 (sección 2.2.4.1), se obtiene el valor de la Ecuación 2.99.

$$degr_{DoS.} = \frac{degr_C + degr_I + degr_D}{3} = \frac{0\% + 0\% + 100\%}{3} = 33.\bar{3}\% \cong 33.33\% \qquad (2.99)$$

2.4.3.2.4 Impacto acumulado de la amenaza Denegación de Servicio

Debe aplicarse la Ecuación 2.37 (sección 2.2.4.2), como se muestra en la Ecuación 2.100.

$$IA_{DoS} = VA_{Antispam} \times degr_{DoS.} = 40.27 \times 33.\bar{3}\% \equiv 40.27 \times 0.\bar{3} = 13.42\bar{3} \qquad (2.100)$$

La Tabla 2.69 es un extracto de la Matriz de Riesgos del Anexo T, de las columnas correspondientes a estas amenazas hacia el Sistema Antispam.

Tabla 2.69. Tabulación de los niveles de degradación e impacto acumulado
[Elaboración propia]

				PRIORIDAD			DEGRADACIÓN				
Nombre del Activo	**Origen**	**Amenaza**	**VALOR ACUMULADO**	**C**	**I**	**D**	**C**	**I**	**D**	**Promedio degradación**	**IMPACTO**
Sistema Antispam	A	Errores de administrador	40.27	3	2	1		50%	100%	50,00%	20,14
	D	Denegación de Servicio				1			100%	33,33%	13,42

2.4.4 PROBABILIDAD (SISTEMA ANTISPAM)

La probabilidad de que una amenaza se materialice tomar mayor consideración cuando existen vulnerabilidades. Parte de las vulnerabilidades asociadas a las amenazas anteriores se muestran en la Tabla 2.70, extracto de la Matriz de Riesgos del Anexo T. Se toma en cuenta la información del Anexo K y la experiencia de las instituciones relacionadas registradas en los cuestionarios del Anexo J, según recomiendan las metodologías. Los valores de probabilidad resultante se registran en el Anexo T, en la columna “PROBABILIDAD”.

2.4.4.1 Cálculo de las probabilidades de ocurrencia de las amenazas

2.4.4.1.1 Probabilidad de ocurrencia de la amenaza Errores de administrador

Por ser de origen accidental, se toman los criterios de la sección 2.1.10.4.2. Se ha estimado que el factor humano es *Muy Susceptible* a cometer errores, por lo que el valor de

potencialidad en este aspecto, según la Tabla 2.21, es del 100%. Se ha determinado que esta amenaza es *Frecuente*, otorgándosele un valor de 10% según la Tabla 2.22. La probabilidad resultante se calcula con la Ecuación 2.51, obteniéndose el valor de la Ecuación 2.101.

$$P_{Err.Admin.} = P_S \times P_F = 100\% \times 10\% \equiv 1 \times 0.1 = 0.1 \equiv 10\% \quad (2.101)$$

2.4.4.1.2 Probabilidad de ocurrencia de la amenaza Denegación de Servicio

Por ser de origen deliberado, se toman los criterios de la sección 2.1.10.4.1. Se ha estimado que es *Fácil* llevar a cabo este ataque en el MCyP, por lo que el valor de potencialidad en este aspecto, según la Tabla 2.19, es del 100%. Se ha estimado que puede haber un *Alto interés* por realizar este ataque, con un valor del 100% según la Tabla 2.20. La probabilidad resultante se calcula con la Ecuación 2.49, obteniéndose el valor de la Ecuación 2.102.

$$P_{DoS} = P_I \times P_F = 100\% \times 100\% \equiv 1 \times 1 = 1 \equiv 100\% \quad (2.102)$$

La Tabla 2.70 es otro extracto de la Matriz de Riesgos del Anexo T, de las columnas correspondientes a las amenazas y sus probabilidades para el Sistema Antispam.

Tabla 2.70. Tabulación de las potencialidades y la probabilidad resultante
[Elaboración propia]

					Suscept.x.Frecuenci.		Interés.x.Facilidad		
					Natural o accidental		Deliberado		
Nombre del Activo	**Origen**	**Amenaza**	**…**	**Vulnerabilidad**	**Susceptibilidad**	**Frecuencia**	**Interés**	**Facilidad**	**PROBABILIDAD**
Sistema Antispam	A	Errores de administrador	…	Falta de capacitación …	100,00%	10,00%			10%
	D	Denegación de Servicio		Falla de antivirus …			100,00%	100,00%	100%

2.4.5 RIESGO ACUMULADO SOBRE EL SISTEMA ANTISPAM

Cada amenaza representa un riesgo acumulado, que se calcula con la Ecuación 2.53 de la sección 2.2.6.1. La tabulación de los riesgos acumulados puede verse en la Tabla 2.71, extracto de la Matriz de Riesgos del Anexo T.

El riesgo acumulado de la amenaza Errores de administrador es el de la Ecuación 2.103, tomando el valor exacto de la Ecuación 2.98, el de la Ecuación 2.101.

$$RA_{Err.Admin.} = IA_{Err.Admin.} \times P_{Err.Admin.} \cong 20.135 \times 10\% \equiv 2.0135 \quad (2.103)$$

El riesgo acumulado de la amenaza Denegación de Servicio es el de la Ecuación 2.104, tomando el valor exacto de la Ecuación 2.100, el de la Ecuación 2.102.

$$RA_{DoS} = IA_{DoS} \times P_{DoS} = 13.42\overline{3} \times 100\% \equiv 13.42\overline{3} \times 1 \cong 13.423 \quad (2.104)$$

Tabla 2.71. Tabulación de los riesgos acumulados en el Sistema Antispam
[Elaboración propia]

Nombre del Activo	Origen	Amenaza	VALOR ACUMULADO	…	IMPACTO	Vulnerabilidad	…	PROBABILIDAD	RIESGO
Sistema Antispam	A	Errores de administrador	40.27	…	20,14	Falta de capacitación …	…	10%	2.0135
	D	Denegación de Servicio			13,42	Falla de antivirus …		100%	13.4233

2.4.6 SALVAGUARDAS APLICADAS EN EL SISTEMA ANTISPAM

2.4.6.1 Eficacia de las salvaguardas sobre el Sistema Antispam

Se valora la eficacia de las salvaguardas según la Tabla 2.25 de la sección 2.1.10.6.

2.4.6.1.1 Eficacia frente a la amenaza Errores de Administrador

Se determinaron 2 salvaguardas preventivas, por lo que hacen frente a la probabilidad, que puede verse en la Tabla 2.72, extracto del Anexo T. Sus factores de reducción fueron estimados en *Baja* (40%) y *Media* (16%) eficacias. Se usa la Ecuación 2.61 de la sección 2.2.7.2, obteniéndose el valor de la Ecuación 2.105. Al no haber salvaguardas frente al impacto, el factor de reducción corresponde a *Nulo* (100%), como muestra la Ecuación 2.106.

$$e_{P_{Err.Admin.}} = 40\% \times 16\% \equiv 0.4 \times 0.16 = 0.064 \equiv 6.4\% \quad (2.105)$$

$$e_{I_{Err.Admin.}} = 100\% \equiv 1 \equiv 100\% \quad (2.106)$$

2.4.6.1.2 Eficacia frente a la amenaza Denegación de Servicio

Se determinó 1 salvaguarda frente a la probabilidad (Ver Tabla 2.72). Su factor de reducción fue estimado en *Baja* (40%) eficacia. Se usa la Ecuación 2.61 de la sección

2.2.7.2, obteniéndose el valor de la Ecuación 2.107. Tampoco se definieron salvaguardas correctivas (Ecuación 2.108).

$$e_{P_{DoS}} = 40\% \equiv 0.4 = 40\% \quad (2.107)$$

$$e_{I_{DoS}} = 100\% \equiv 1 \equiv 100\% \quad (2.108)$$

2.4.7 RIESGO ACUMULADO RESIDUAL EN EL SISTEMA ANTISPAM

2.4.7.1 Impacto acumulado residual sobre el Sistema Antispam

Se aplica la Ecuación 2.64 (sección 2.2.8.1). Como no se registraron salvaguardas frente al impacto de ninguna de las amenazas, el impacto acumulado residual es el mismo que el impacto acumulado (ver Tabla 2.72).

2.4.7.1.1 Impacto acumulado residual de la amenaza Errores de administrador

$$IAr_{Err.Admin.} = IR_{Err.Admin} \times e_{I_{Err.Admin}} = 20.135 \times 100\% \equiv 20.135 \times 1 = 20.135 \quad (2.109)$$

2.4.7.1.2 Impacto acumulado residual de la amenaza Denegación de Servicio

$$IAr_{DoS} = IR_{DoS} \times e_{I_{DoS}} = 13.42\overline{3} \times 100\% \equiv 13.42\overline{3} \times 1 = 13.42\overline{3} \quad (2.109)$$

2.4.7.2 Probabilidad residual sobre el Sistema Antispam

Se aplica la Ecuación 2.68 (sección 2.2.9). en ambas amenazas (ver Tabla 2.72)

2.4.7.2.1 Probabilidad residual de la amenaza Errores de administrador

$$Pr_{Err.Admin.} = P_{Err.Admin} \times e_{P_{Err.Admin}} = 10\% \times 6.4\% \equiv 0.1 \times 0.064 = 0.0064 \equiv 0.64\% \quad (2.109)$$

2.4.7.2.2 Probabilidad residual de la amenaza Denegación de Servicio

$$Pr_{DoS} = P_{DoS} \times e_{P_{DoS}} = 100\% \times 40\% \equiv 1 \times 0.4 = 0.4 \equiv 40\% \quad (2.109)$$

2.4.7.3 Riesgo residual resultante sobre el Sistema Antispam

Se aplica la Ecuación 2.70 (sección 2.2.10.1). en ambas amenazas (ver Tabla 2.72)

2.4.7.3.1 Riesgo acumulado residual de la amenaza Errores de administrador

$$RAr_{Err.Admin} = IAr_{Err.Admin} \times Pr_{Err.Admin} = 20.135 \times 0.0064 \cong 0.1289 \quad (2.110)$$

2.4.7.3.2 Riesgo acumulado residual de la amenaza Denegación de Servicio

$$RAr_{DoS} = IAr_{DoS} \times Pr_{DoS} = 13.42\overline{3} \times 0.4 \cong 5.3693 \quad (2.111)$$

Los valores son tabulados en la Tabla 2.72, que es un extracto de la Matriz de Riesgos del Anexo T.

Tabla 2.72. Matriz de Riesgos (Acumulados) principal del Anexo T (fragmento) [Elaboración propia]

							Mecanismo							
							Correctiv.			Preven.				
Amenaza	**…**	**IMPACTO**	**…**	**PROBABILIDAD**	**RIESGO**	**Salvaguardas**	**De protección o limitación**	**Paliativa**	**De recuperación por …**	**Disuasiva (Disuasoria)**	**Preventiva**	**IMPACTO**	**PROBABILIDAD**	**RIESGO RESIDUAL**
Errores de administ…	…	20,14	…	10%	2.0135	Manual de descripción…					40%	20,1350	0,64%	0,1289
						Soporte del proveedor					16%			
Denegación de Servicio		13,42		100%	13.4233	Firewall					40%	13,4233	40%	5,3693

2.4.8 RIESGOS REPERCUTIDOS DEL SISTEMA ANTISPAM

2.4.8.1 Diagrama de dependencia simplificado

El riesgo repercutido se calcula con los activos de los cuales depende el Sistema Antispam, es decir, con los activos inferiores. Para ello se requiere del diagrama de dependencia simplificado correspondiente (Anexo L), que se construye a partir de las dependencias calculadas desde el Sistema Antispam hacia todos los activos inferiores de los cuales depende. Los valores se extraen de cada diagrama de dependencia para valor acumulado del Anexo G de cada activo inferior en donde se encuentra el Sistema Antispam. La Figura 2.30 muestra el Sistema Antispam y todos los activos inferiores de los que depende, con los respectivos grados de dependencia hacia dichos activos.

El Sistema Antispam “absorberá” todas las amenazas de todos los activos inferiores, según los grados de dependencia que tenga de éstos. Esto hace que se genere una nueva matriz: la Matriz de Riesgos Repercutidos exclusiva para el Sistema Antispam, que se identifica por su código (Anexo T, Matrices de Riesgos Repercutidos > PAN.xlsx > pestaña PAN001).

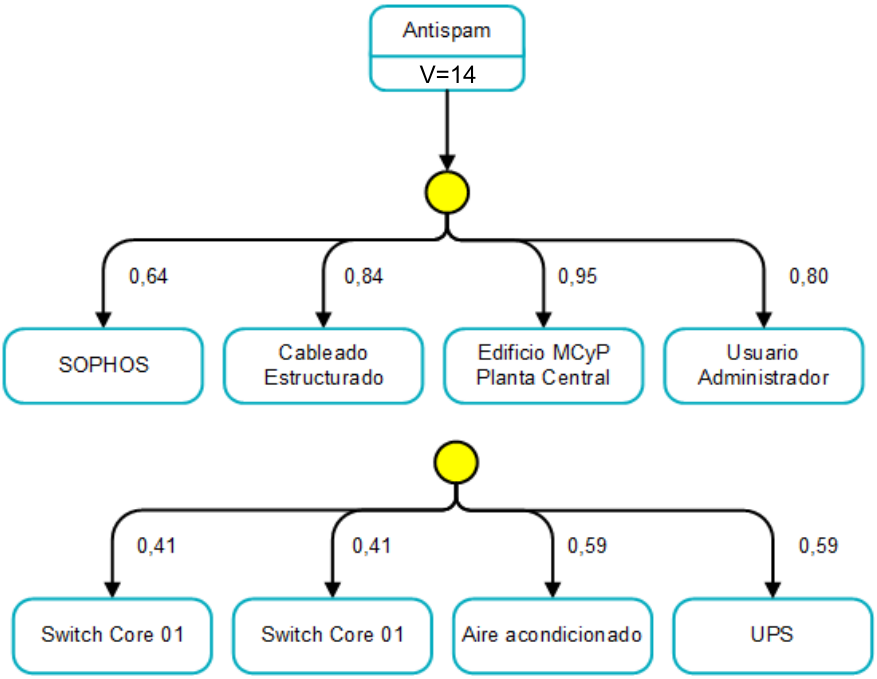


Figura 2.30. Diagrama de dependencias simplificado para el Sistema Antispam

Como el análisis se realiza sobre su Valor Propio con los grados de dependencia hacia los activos inferiores, la columna de la Matriz de Riesgos Repercutidos para el Sistema Antispam cambia la columna "VALOR ACUMULADO" por "VALOR PROPIO", se agrega la columna "GRADO DEPENDENCIA", se identifica el activo inferior en la columna "ACTIVOS INFERIORES", y la columna "V*dep" (producto del Valor Propio y la dependencia), que es el valor con el que se realizarán las operaciones, como se muestra en la Tabla 2.73.

No intervienen los Valores Propios ni los Valores Acumulados de los activos inferiores. Los valores de degradación, de probabilidad y de las salvaguardas son los mismos que tiene el activo inferior en la Matriz de Riesgos (Acumulados) principal del Anexo T, y se operan de la misma manera, pero sobre el Valor Propio del Sistema Antispam y el grado de dependencia. Para esclarecerlo, puede acudirse a las secciones 2.2.4.3, 2.2.6.2, 2.2.8.2 y 2.2.10.2. Por ejemplo, todos los cálculos del activo de soporte (físico) SOPHOS Antispam, impacto, probabilidad, etc., se efectúan con la columna V*dep (Ecuación 2.112).

$$[V * dep] = V_{Antispam} \times dep_{SOPHOS} = 14 \times 0.64 = 8.96 \qquad (2.112)$$

El impacto repercutido por inundación se calcularía como en la Ecuación 2.113.

$$IR_{SOPHOS/Antispam} = [V * dep] \times degr_{SOPHOS_{inundación}} = 8.96 \times 33.33\% \cong 2.99 \qquad (2.113)$$

Tabla 2.73. Matriz de Riesgos Repercutidos del Sistema Antispam PAN001 (fragmento) *[Elaboración propia]*

								PRIOR			DEGRAD.							Accidental		Deliberado					Correct.		Prev.					
CÓD	ACTIVO	VALOR PROPIO	GRADO DEPENDENCIA	ACTIVOS INFERIORES	Origen	Amenaza	V*dep	C	I	D	C	I	D	Promedio degradación	IMPACTO	Vulnerabilidad	Suscept.	Frecuencia	Interés	Facilidad	PROBABILIDAD	RIESGO	Salvaguarda	De protección	Paliativa	De recuperación por…	Disuasoria (disuasiva)	Preventiva	IMPACTO RESIDUAL	PROBABILIDAD RESID.	RIESGO RESIDUAL
PAN 001	Sistema Antispam	14	0,64	SOPHOS Antispam	N	Inundac..	8,96			1			100%	33,33%	2,99	Ubic.	100%	10%			10%	0,2987	N/E						2,9867	10%	0,2987
					N	Plaga…				1			100%	33,33%	2,99	Falta...	100%	10%			10%	0,2987	Servi					40%	2,9867	0,04%	0,0012
					[… Resto de amenazas de SOPHOS Antispam…]																											
			0,84	Cablead. Estruct.	I,A	Fuego	11,76			1			100%	33,33%	3,92	Falta..	100%	0,10%			10%	0,0039	Extin	40%					0,6272	0,10%	0,0006
																							Sist	40%							
					I,D	Fuego				1			100%	33,33%	3,92	Falta..			0,10%	100%	10%	0,0039	Extin	40%					0,6272	0,04%	0,0003
																							Cám				40%				
																							Sist	40%							
																							PRO					100%			
					[… Resto de amenazas de Cableado Estructurado …]																											
			0,95	Edificio	I,A	Fuego	13,30			1			100%	33,33%	4.43	Falta..	10%	0,01%			0,00%	0,0000	Extin	40%					0,7093	0,00%	0,0000
																							Sist	40%							
					I,D	Fuego				1			100%	33,33%	4.43	Falta..			0,01%	1%	0,00%	0,0000	Extin	40%					0,7093	0,00%	0,0000
																							Cám				40%				
																							Sist	40%							
																							PRO					100%			
					[… Resto de amenazas de Edificio…]																											
			0,80	Usuarios Admin.	A	Deficien	11,20			1			100%	33,33%	3,73	Falta..	100%	100%			100%	3,7333	N/E						3,7333	100%	3,7333
					A	Fugas		1			100%			33,33%	3,73	Falta..	100%	100%			100%	3,7333	Acue				100%		3,7333	100%	3,7333
					[… Resto de amenazas de Usuarios Administradores…]																											
			0,41	SW CORE 01	⋮ [… Resto de amenazas de los demás activos…] ⋮																											
			⋮	⋮																											

2.4.9 EVALUACIÓN DE LOS RIESGOS DEL SISTEMA ANTISPAM

Se observa la información de la Matriz de Riesgos del Anexo T. Por ahora, para el activo del ejemplo, basta observar la Tabla 2.72. Según la escala de evaluación de impacto de Tabla 2.56 de la sección 2.2.11.1, el impacto residual de la amenaza Errores de Administrador es *ALTO*, pero debido a los factores de reducción de probabilidad, el riesgo residual de éste ha sido reducido al nivel *Aceptable (AC)*, según la Figura 2.26 y la Tabla 2.61 de la sección 2.2.11.4.

Evaluando con las mismas tablas, el impacto residual de la amenaza Denegación de Servicio también es *ALTO*, pero las medidas preventivas han disminuido el riesgo residual a un valor *Medio (M)*, es decir, que es un riesgo urgente, dentro de la categoría de riesgos inadmisibles.

2.4.10 TRATAMIENTO DE LOS RIESGOS DEL SISTEMA ANTISPAM

Primero deben analizarse las restricciones que pueden influenciar en la toma de decisiones sobre las opciones de tratamiento del riesgo. Toda decisión sobre el riesgo está a cargo de la alta Dirección con el debido asesoramiento.

Por ejemplo, debido a que la amenaza de Errores de Administrador ha sido reducida a *Aceptable (AC)*, puede *retenerse* el riesgo, y tomar las recomendaciones de los párrafos finales de la sección 2.3.2.1.

En cuanto a la amenaza de Denegación de Servicio, no es de atención inmediata, pero debe ser tomada con mucha seriedad, pues debe eliminarse o reducirse en algún momento dentro de un ciclo de planificación. El riesgo podría *reducirse, transferirse* o, incluso, *retenerse* en el peor de los casos, si se presenta el escenario del segundo motivo descrito en la sección 2.3.2.1.

3 POLÍTICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Figura 3.1 muestra la que sería la portada de la Política de Seguridad de la Información.

Figura 3.1. Portada de la Política de Seguridad de la Información [Elaboración propia]

3.1.1 ANTECEDENTES

En el Ecuador, al ser un estado plurinacional e intercultural, se ha visto la necesidad de crear una entidad regente que busque y garantice la diversidad de expresiones culturales y la conservación del patrimonio nacional; por tal razón, el 15 de enero del año 2007, mediante el Decreto Ejecutivo 5, se crea el Ministerio de Cultura y Patrimonio.

El Ministerio de Cultura y Patrimonio es la entidad rectora en el ámbito cultural y patrimonial, responsable del cumplimiento de los derechos culturales, ejerciendo la rectoría de las políticas públicas culturales y del Sistema Nacional de Cultura, incidiendo en la integración simbólica del Ecuador y en el cambio cultural de la sociedad. Esta Cartera de Estado fue creada para fortalecer la identidad nacional y la interculturalidad, salvaguardar la memoria social y el patrimonio cultural del Ecuador. Incentiva la libre creación artística, la producción, difusión, distribución y disfrute de bienes y servicios culturales. [95]

3.1.2 DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD

Se establece la siguiente política que permitirá regular el manejo y protección de la información confidencial, pública e interna del Ministerio de Cultura y Patrimonio, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia de esta Cartera de Estado; así como garantizar el acceso a la información en conformidad con la Constitución, las leyes, y demás normas jurídicas, además de asegurar la continuidad de los servicios propios que permiten a la institución cumplir con la misión y visión y el cumplimiento de la normativa vigente a la que deben someterse las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID), incluyendo esta Cartera de Estado [96]

La máxima autoridad de la Institución, el Comité de Seguridad de la Información (CSI) y el Oficial de Seguridad de la Información (OSI), entendiendo la importancia de una adecuada gestión de la información, se han comprometido a implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI).

El SGSI permitirá lograr niveles adecuados de seguridad para todos los activos de información institucional considerados relevantes, de tal manera que garantice que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y

las tecnologías [97], buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos.

3.1.3 OBJETIVOS

Proporcionar directrices, principios, roles y reglas básicas para la gestión de seguridad de la información con la finalidad de salvaguardar la integridad, confidencialidad y disponibilidad de la información albergada o generada en el Ministerio de Cultura y Patrimonio en cualquiera de sus estados, durante todo el ciclo de vida de la información, desde la creación, recepción y/o modificación, distribución, archivo, conservación, custodia, hasta la transferencia o destrucción de la información [98].

Garantizar que las operaciones de la institución se realicen de forma ininterrumpida, segura y confiable.

Enfocar a las personas como el activo más sensible de la institución en materia de seguridad de la información, generando así una cultura tecnológica amplia que minimice los riesgos de la información.

Realizar un correcto análisis de los activos fundamentales para el cumplimiento de la misión, visión y objetivos de la institución, con la finalidad de aplicar los controles adecuados para mitigar los riesgos.

Salvaguardar la información acerca de la memoria social del país de manera íntegra y asegurar su disponibilidad cuando sea necesaria.

3.1.4 ROLES

Según se dispone en el EGSI v2.0:

La Máxima Autoridad: designará al interior de su Institución un Comité de Seguridad de la Información (CSI) que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información y Unidades Agregadores de Valor; el Área Jurídica participará como asesor.

El Comité de Seguridad de la Información: tiene como objetivo garantizar y facilitar la implementación de las iniciativas de seguridad de la información de la institución.

Los Comités, en la primera convocatoria, definirán su agenda y su reglamento interno. El Comité de Seguridad de la Información, tendrá las siguientes responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel alto de impacto.
d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
e) Promover la difusión de la seguridad de la información dentro de la institución.
f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
g) El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten; se deberán llevar registros y actas de reuniones.
h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).

El Oficial de Seguridad de la Información: debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos. Podrá ser, si existiere, el responsable de la Unidad de Seguridad de la Información. Se recomienda que no pertenezca al área de Tecnologías de la Información.

El Oficial de Seguridad tendrá las siguientes responsabilidades:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información.

c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
d) Elaborar el Plan de concienciación de Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información.
e) Elaborar un plan de seguimiento y control de implementación de las medidas de mejora o acciones correctivas.
f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.
h) Coordinar la gestión de incidentes de seguridad con nivel alto de impacto a través de otras instituciones.
i) Mantener la documentación de la implementación del EGSI debidamente organizada.
j) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucional establecidos.
k) Informar el Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información, así como las alertas que impidan su implementación.
l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad; en caso de ausencia, al Comité de Seguridad de la Información.

3.1.5 ALCANCE

Esta política es de cumplimiento y aplicación obligatoria, según corresponda, para:

- Todos los funcionarios del Ministerio de Cultura y Patrimonio, entidades que almacenen información en el Centro de Datos o que utilicen servicios a través de esta Cartera de Estado.
- Proveedores, colaboradores, consultores, contratistas y terceras partes que accedan a los activos de información de la Institución, durante y después de terminar su relación contractual con el Ministerio de Cultura y Patrimonio, de acuerdo con lo pactado entre ambas partes.
- Todo activo de información que la institución posea actualmente o sea adquirido en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger estos activos de información.

Esta política salvaguarda toda la información concerniente a la institución, sea esta pública, interna o confidencial, en cualquiera de sus estados: impresa, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas, hablada en una conversación, etc.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso de gestión deberá ser aplicado a todos los procesos adjetivos o sustantivos del Ministerio de Cultura y Patrimonio.

En caso de que los procesos se encuentren siendo modificados, se debe aplicar el análisis y evaluación de riesgos a los activos que estén involucrados en el cumplimiento de la misión y visión de esta Cartera de Estado. Así también, como apoyo a esta política general, de acuerdo con la realidad institucional del MCyP, en base a la norma ISO 27001 y el EGSI V2.0, deben determinarse políticas que permitan establecer controles para mitigar el riesgo de los activos de la institución, y actualizar, agregar o suprimir políticas de manera periódica o cuando sea necesario según la realidad institucional actual.

3.1.6 NORMAS GENERALES

- Los miembros del Comité de Seguridad de la Información deben trabajar conjuntamente en la implementación del Sistema de Gestión de Seguridad de la información, el cual debe ser revisado y actualizado periódicamente o cuando sea necesario, alineándose a la realidad institucional.
- La información institucional se gestionará y clasificará dentro de cada área perteneciente al Ministerio de Cultura y Patrimonio como información confidencial, interna y pública; siendo cada una de las áreas las responsables de su clasificación, custodia y respaldos.
- Todos los funcionarios del Ministerio de Cultura y Patrimonio, proveedores, colaboradores, consultores, contratistas y terceras partes que accedan a los activos de información de la Institución, deben firmar un acuerdo de confidencialidad.
- Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo. Es deber del Oficial de Seguridad de la Información, en conjunto con las direcciones de Tecnologías de la Información y Comunicación, Comunicación Social y el Comité de Seguridad de la Información, capacitar y difundir temas relacionados con la Seguridad de la

Información periódicamente, los cuales deben ser dirigidos al personal del Ministerio de Cultura y Patrimonio.

- En el caso en que algún servidor cometiese algún tipo violación de seguridad de la información que incurra en afecciones directas a la imagen institucional del Ministerio de Cultura y Patrimonio, y a lo que éste representa, se requerirá un proceso disciplinario contra el o los implicados.
- Todos los empleados y servidores del Ministerio de Cultura y Patrimonio aceptan y reconocen su responsabilidad de salvaguardar la seguridad de la información pública, interna y confidencial de esta Cartera de Estado, durante su relación contractual y luego del término de la misma.
- Todo servidor de esta Cartera de Estado hará buen uso de los activos de información, y una vez terminada la relación contractual con el MCyP, el funcionario está en el deber de entregar la información generada a su jefe inmediato.
- Es deber tanto de servidores públicos de la institución, como del personal externo autorizado por el Ministerio de Cultura y Patrimonio, entregar de manera oportuna la información requerida en procesos de control y monitoreo.
- Toda información que sea cedida por parte del Ministerio de Cultura y Patrimonio a otras Instituciones, tanto Públicas como Privadas, y a personal externo a esta Cartera del Estado, estará regulada según los convenios de cada solicitante, los cuales tendrán lineamientos establecidos para el uso apropiado de la información, protección de la confidencialidad, causales para la terminación unilateral de los convenios, etc. Todo lo mencionado debe estar acompañado de un acuerdo de confidencialidad.
- Las directrices de Seguridad de la Información están dirigidas al establecimiento y la consolidación de la cultura en materia de seguridad de información entre todos quienes tienen relación directa o indirecta con el Ministerio de Cultura y Patrimonio. En caso de trasgresión a las Políticas de Seguridad de la Información, acuerdos de confidencialidad, procedimientos o normativa legal, estarán sujetos a imposiciones legales según el grado de afección a la entidad.
- Todas las características y especificaciones que no se encuentren de manera expresa en el presente documento serán integrados o reemplazados según el caso, por las regulaciones del marco normativo vigente.

3.1.7 COMUNICACIÓN DE LA POLÍTICA

La presente Política de Seguridad de la Información se encontrará alojada en la página web e intranet del Ministerio de Cultura y Patrimonio.

Se enviarán informativos, en los cuales se sociabilizará la información sobre cada uno de los puntos de esta normativa y sobre la actualización, supresión o creación de nuevas políticas.

3.1.8 DOCUMENTOS DE REFERENCIA

- Acuerdo Ministerial 025-2019.
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0).
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, 27002 y 27005.
- MAGERIT v3.0.
- Alcance del Esquema Gubernamental de Seguridad de la Información.
- Matriz de Riesgos.

3.1.9 TERMINOLOGÍA

Política de Seguridad: es un conjunto de normas, protocolos y reglas que custodian la seguridad informática de la institución, cuyo objetivo es mitigar y prevenir los riesgos a los que un activo se encuentra expuesto. [99]

Información: Se entiende como información todo conjunto de datos que se encuentran organizados, procesados y bajo el control de una entidad que le atribuye un valor a la misma, independientemente de la forma en que ésta esté presentada, almacenada o sea transmitida (ya sea en forma escrita, oral, grabada en imágenes, audios o videos, impresa en papel, almacenada de forma electrónica, proyectada, enviada y/o recibida por correo convencional, correo electrónico o por fax, transmitida por conversaciones directas o por vía telefónica, en reuniones, conferencias o videoconferencias, etc.), de la fuente (sea originada por la propia institución o fuera de ella) o de su fecha de elaboración o expedición. [100]

Confidencialidad: Mantenimiento de la privacidad de los recursos, datos e información, a los cuales únicamente puede acceder el personal autorizado. [101] - [103]

Integridad: La información únicamente puede ser modificada por personal autorizado y de la forma autorizada cuando esto sea necesario. [101] - [103]

Disponibilidad: Los recursos, datos e información del sistema deben permanecer accesibles a las personas autorizadas en el momento que lo requieran. [101] - [103]

Seguridad de la Información: Conjunto de técnicas y medidas que aseguran la información de la institución independiente del estado en que ésta se encuentre, ya sea físico o digital, dentro o fuera de un sistema informático, a fin de que ésta sea utilizada para lo que ha sido establecida, protegiéndola de la divulgación y modificación por parte de personal no autorizado. La seguridad de la información no se centra en la protección de las TIC, sino de todos los activos de información con valor para la institución. [104] - [106]

Activo: Cualquier recurso de la empresa necesario para que ésta pueda desempeñar sus actividades y funciones, o que tiene algún valor para la Organización, cuya indisponibilidad o deterioro supone un costo para la empresa.

3.2 CONTROL: POLÍTICA PARA PLANES DE CAPACITACIÓN

3.2.1 LINEAMIENTOS PARA EL PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE CULTURA Y PATRIMONIO

3.2.1.1 Misión

Nota: Esta sección debe ir en el entregable de la correspondiente política al MCyP. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad (ver capítulo 2, sección 2.1.1.1) de este Trabajo de Titulación.

3.2.1.2 Objetivo del Plan de Capacitación de Seguridad de la Información

Establecer los lineamientos para el diseño, desarrollo, implementación y mantenimiento del plan de capacitación de seguridad de la información, en base al Esquema Gubernamental de Seguridad de la Información, versión 2.0.

3.2.1.3 Descripción del Plan de Capacitación de Seguridad de la Información

El Plan de Capacitación debe estar enfocado en mejorar la cultura tecnológica e incentivar el buen uso de los activos de información de esta Cartera de Estado. Además, permitirá que los funcionarios del MCyP conozcan acerca de las políticas y controles implementados en la institución. Incentiva a la aplicación de buenas prácticas de seguridad de la

información que permitirán salvaguardar la confidencialidad, integridad y disponibilidad de la información interna, pública y confidencial de la información.

Incentivará a que los funcionarios de esta Cartera de Estado participen activamente del Plan de Capacitación de Seguridad de la Información, proponiendo para versiones futuras temas de su interés.

3.2.2 PROCESO DEL PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.2.2.1 Diseño del Plan de Capacitación

El Oficial de Seguridad en conjunto con el Comité de Seguridad de la Información deberán evaluar el Plan de Capacitación de Seguridad de la Información que será desarrollado o actualizado, para proseguir con su aprobación. Es importante que el Plan de Capacitación de Seguridad de la Información se adapte a la realidad institucional, y esté basado en el Esquema Gubernamental de Seguridad de la Información v2.0.

El Diseño del Plan de Seguridad de la Información se encuentra compuesto por los siguientes puntos.

3.2.2.1.1 Estructuración de un área de concientización y entrenamiento

Totalmente Descentralizada: El Plan de Capacitación de Seguridad de la Información debe ser elaborado por el Comité de Seguridad de la Información y el Oficial de Seguridad el mismo debe estar actualizado conforme a la realidad institucional; debe ser aplicado de manera continua y difundido a todos los funcionarios de esta Cartera de Estado.

3.2.2.1.2 Evaluación de necesidades

- La evaluación de necesidades del Ministerio de Cultura y Patrimonio se llevará a cabo a través de una evaluación de diagnóstico. Ésta estará basada en conceptos fundamentales sobre seguridad de la información y del Esquema Gubernamental de Seguridad de la Información.
- Además, se llevarán a cabo entrevistas con los responsables de los sistemas, con el fin de conocer acerca de la información que se alberga en los servidores del MCyP, para salvaguardar esta información conforme a las necesidades de ésta; también con la finalidad de desactivar y reasignar los recursos que no se estén utilizando.

- Se debe verificar el comportamiento general de los funcionarios de esta Cartera de Estado con respecto a seguridad de la información, en el que se observará, por ejemplo, cómo se lleva la confidencialidad de contraseñas, escritorios limpios, sesiones abiertas cuando el funcionario no se encuentre en su lugar de trabajo, ingresos a páginas que no estén relacionadas con sus funciones, no portabilidad de la credencial del MCyP, mal uso de los activos que albergan información, etc.
- Se debe verificar los incidentes de seguridad de la información que se hayan suscitado en esta Cartera de Estado, además de soportes técnicos que estén relacionados con la seguridad de la información, mismos que deben ser debidamente documentados.
- Se debe analizar la documentación de eventos registrados por los dispositivos de seguridad (*firewall*, *CheckPoint*, antispam, antivirus, etc.), o intrusiones en los sistemas del Ministerio de Cultura y Patrimonio.

3.2.3 PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Plan de Capacitación de Seguridad de la Información debe estar basado en la etapa del Diseño del Plan de Capacitación, donde se evidencia las falencias del Ministerio de Cultura y Patrimonio con el fin de solventar y mejorar la cultura tecnológica en seguridad de la información. A continuación, se detallan los puntos que conforman el plan de capacitación.

3.2.3.1 Alcance del Plan

Es deber del Oficial de Seguridad (OSI) y el Comité de Seguridad de la Información (CSI), determinar el alcance de cada Plan de Capacitación de Seguridad de la Información. Este puede estar dirigido para una Dirección, Coordinación, funcionarios que se incorporan al MCyP, a las instituciones adscritas que usen los activos de información del Ministerio de Cultura y Patrimonio o a toda esta Cartera de Estado.

3.2.3.2 Objetivos del Plan

Es deber del OSI y el CSI determinar los objetivos del Plan de Capacitación de Seguridad de la Información acorde al alcance. Debe incluirse la necesidad de protección de la información en las dimensiones canónicas de seguridad de la información (confidencialidad, integridad y disponibilidad), pudiendo extenderlo a las dimensiones derivadas (autenticidad, confiabilidad, no repudio y responsabilidad), basado en el Esquema Gubernamental de Seguridad de la Información vigente.

3.2.3.3 Roles y Responsabilidades

Los roles y responsabilidades estarán definidos de acuerdo con el alcance establecido en el Plan.

El presente Plan de Capacitación de Seguridad de la Información involucra a todos los funcionarios pertenecientes a esta Cartera de Estado, debido a que se considera que el eslabón más débil, en lo que a seguridad de la información respecta, es el personal implicado en las actividades laborales que permiten dar cumplimiento a la misión y visión del Ministerio de Cultura y Patrimonio.

3.2.3.3.1 Nivel Jerárquico Superior

Los niveles directivos del Ministerio de Cultura y Patrimonio apoyarán el Plan de Capacitación de Seguridad de la Información mediante acciones como:

- Motivar y participar junto con su equipo de trabajo en las capacitaciones de seguridad de la información que se desarrollen durante la vigencia del Plan de Capacitación de Seguridad de la Información.
- Garantizar que se lleven a cabo las instrucciones divulgadas en el Plan en el área a su cargo.
- Concientizar al personal sobre la importancia de la seguridad de la información.
- Garantizar el cumplimiento del párrafo tres de la sección 3.2.2.1.2, *Evaluación de necesidades*.

3.2.3.3.2 Oficial de Seguridad de la Información (OSI)

El OSI debe elaborar los planes de concientización en materia de Seguridad de la Información, acorde a los establecido en el EGSI. Sus actividades deben cubrir:

- Preparar el plan de concientización que formará a los funcionarios en lo que a Seguridad de Información respecta, incluyendo información sobre el EGSI y su cumplimiento.
- Dar continuidad a la concientización a través de actividades relacionadas.
- Elaborar planes de formación y charlas para los nuevos funcionarios en materia de Seguridad de la información.
- Elaborar planes de medidas disciplinarias que regulen toda actividad que comprometa la Seguridad de la Información.

3.2.3.3.3 Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información debe:

- Garantizar la promoción de la Seguridad de la Información en toda la institución.
- Coordinar e incentivar la participación de los funcionarios de esta Cartera de Estado en las actividades del Plan de Capacitación de Seguridad de la Información.
- Dar continuidad y seguimiento al Plan de Capacitación de Seguridad de la Información.
- Velar que en las actividades pertenecientes a su área se apliquen las recomendaciones generadas en el presente plan.

3.2.3.3.4 Funcionarios del Ministerio de Cultura y Patrimonio

Es deber de los funcionarios pertenecientes al MCyP:

- Precautelar, durante y después de su relación contractual, la disponibilidad, confidencialidad e integridad de la información.
- Participar en las actividades relacionadas con el Plan de Capacitación de Seguridad de la Información.
- Aplicar en sus actividades diarias recomendaciones y buenas prácticas del presente Plan.
- Participar de forma activa en las etapas de evaluación del Plan de Concientización en Seguridad de la Información, correspondientes a la calidad, impacto y efectividad que el Plan haya generado.
- Proponer actividades y temas para futuros planes de capacitación de seguridad de la información.

3.2.3.4 A quién va dirigido

El Oficial de Seguridad de la Información y el Comité de Seguridad de la Información, basados en el alcance del presente plan, determinarán las áreas o funcionarios a los que será dirigido el presente plan.

3.2.3.5 Temas a ver en cada sesión

Los temas serán determinados según los resultados en la etapa de Evaluación de Necesidades del Diseño del Plan de Capacitación de Seguridad de la Información, y deben ser listados de forma corta, clara y concisa.

3.2.3.6 Frecuencia de las capacitaciones

Las capacitaciones estarán dirigidas a los funcionarios del Ministerio de Cultura y Patrimonio, y se realizarán vía *online* o de forma presencial, según las condiciones del entorno, semestralmente y cuando se considere oportuno.

Se deben realizar pequeñas capacitaciones a los funcionarios que ingresen a la institución, dentro del proceso de inducción.

3.2.3.7 Establecimiento de prioridades

Debe definirse un cronograma que incluya las etapas de la capacitación y las actividades que se realizarán para dar cumplimiento a cada etapa.

3.2.3.8 Evaluación y renovación del material creado

Se deben realizar evaluaciones al inicio y al final de cada una de las capacitaciones. El material utilizado para las capacitaciones deberá ser revisado, renovado, actualizado y mejorado de acuerdo con los resultados obtenidos, cuando éstos sean insuficientes, cuando se requiera reforzar las capacidades, cuando haya cambios en la política interna, controles o procesos, y con la aparición de nuevas tecnologías y sus amenazas asociadas. Se debe tomar en cuenta los temas solicitados por los funcionarios de esta Cartera de Estado.

3.2.3.9 Elección del material en función del personal

El material de capacitación debe ser desarrollado acorde a la realidad institucional, alineado al alcance del plan, utilizando un lenguaje adecuado, adaptado al personal al que va dirigido, utilizando recursos que mejoren la comprensión de los temas tratados, tales como audiovisuales, diapositivas, etc.

3.2.3.10 Financiamiento del Plan de Capacitación de Seguridad de la Información

Luego de determinar la estructura del Plan de Capacitación de Seguridad de la Información se debe realizar el estimado de los recursos financieros y de personal necesarios para el desarrollo del presente plan. La Alta Dirección debe destinar un presupuesto para las capacitaciones de Seguridad de la Información.

3.2.4 DESARROLLO

3.2.4.1 Desarrollo del Material para el Plan de Capacitación de Seguridad de la Información

Se debe especificar el material que se utilizará para la capacitación de seguridad de la información, el mismo que debe ser detallado de forma clara y concisa, especificar un objetivo que se desee alcanzar con el material de capacitación, determinando el desarrollo del material.

El material debe incluir:

- Nombre del material.
- Objetivo.
- Desarrollo.

3.2.5 IMPLEMENTACIÓN

3.2.5.1 Implementación del Plan de Capacitación de Seguridad de la Información

Para la implementación del Plan de Capacitación de Seguridad de la Información, como primera medida se debe sociabilizar el mismo con el Nivel Jerárquico Superior, para garantizar el apoyo y los recursos necesarios e iniciar la implementación.

El material desarrollado se puede difundir a través de informativos o de las pantallas informativas.

Luego de la implementación se debe realizar una evaluación, para determinar el conocimiento adquirido de los funcionarios del MCyP.

Finalizada la implementación se debe generar un informe del Plan de Capacitación de Seguridad de la Información.

3.2.6 MANTENIMIENTO DEL PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información y el Comité de Seguridad de la Información deben dar continuidad al Plan de Capacitación, actualizando la información que se impartirá de acuerdo con la evaluación de necesidades realizadas previamente.

3.3 CONTROL: POLÍTICA DE CONTRASEÑAS

3.3.1 GENERALIDADES

Se define a la política de contraseñas como un conjunto de normas que permiten salvaguardar la seguridad de la información, alentando a los usuarios a utilizar contraseñas robustas que cumplan con los parámetros de seguridad y a que sean utilizadas de manera correcta. [107]

Las contraseñas o *passwords* son las llaves de acceso que constituyen el mecanismo básico que se emplea para la autenticación de los funcionarios de esta Cartera de Estado, y permiten el acceso a los servicios, dispositivos, información interna y confidencial que se manejan en el MCyP. La fortaleza del mecanismo de autenticación basado en contraseña se fundamenta en dos principios básicos:

- Primero, los funcionarios de la institución deben mantener la confidencialidad de la contraseña, es decir, solo debe ser conocida por el usuario que es responsable de su custodia y en ningún caso debe ser transferible sin considerar los protocolos establecidos en esta política; tampoco se deben exponer las contraseñas públicamente por ningún motivo.
- En segundo lugar, la contraseña debe ser robusta; esto quiere decir que la contraseña no debería averiguarse de forma fácil: no debe ser predecible ni deducible a partir de información disponible de forma pública o de interés personal.

Si alguna de las dos condiciones anteriores no se cumple, se puede comprometer no sólo la seguridad del usuario, sino de todo el Ministerio de Cultura y Patrimonio ya que podría generarse eventos como suplantación de identidad e intrusión no autorizada en los sistemas institucionales, en cuentas de correo electrónico y computadoras de la institución, además del sistema de gestión documental Quipux. Los servidores públicos del Ministerio de Cultura y Patrimonio se expondrían a que terceras personas publiquen, modifiquen o eliminen información en su nombre, lean y contesten correos electrónicos o Quipux, afectando a la confidencialidad, disponibilidad e integridad de la información.

Es necesario tener en cuenta que todo ingreso a un servicio será reconocido y registrado ante los servicios y aplicaciones del Ministerio de Cultura y Patrimonio; por tanto, todos los usuarios serán responsables de sus contraseñas de acceso a servicios, aplicaciones y de los accesos que se produzcan haciendo uso de esas contraseñas [108]. Esta política es parte de la normativa del Ministerio de Cultura y Patrimonio.

3.3.2 OBJETIVOS

El Objetivo de esta política es establecer reglas para garantizar la gestión y el buen uso de las contraseñas que permitan proteger la información del Ministerio de Cultura y Patrimonio y garanticen su confidencialidad, disponibilidad e integridad.

Determinar los procedimientos para la asignación, cambio y *reseteo*[32] de contraseñas.

3.3.3 ROLES

- **Oficial de Seguridad:** Velará por el cumplimiento de esta política. Promoverá entre los usuarios la importancia de la seguridad de las contraseñas, y los capacitará en el tema.
- **Dirección de Tecnología de la Información y Comunicación:** Proveerá a los usuarios un sistema que les permita cambiar y *resetear* de manera segura su contraseña, además de la sociabilizar este sistema en la Institución.
- **Dirección de Talento Humano:** Trabajará juntamente con el Oficial de Seguridad y con la Dirección de Tecnologías de la Información y Comunicación realizando capacitaciones y concientizando a los usuarios sobre el uso de contraseñas en la Institución. Incluirá en los acuerdos de confidencialidad el adecuado manejo de las contraseñas.
- **Responsables de los sistemas:** Protegerán las claves de los sistemas de los cuales son responsables, creando claves robustas, y velando porque proceso de transferencia se lleve a cabo acorde a lo establecido en esta política.
- **Usuarios:** Guardarán confidencialmente sus contraseñas. los usuarios de esta Cartera de Estado son responsables del uso adecuado de sus claves.

3.3.4 ALCANCE

El alcance de esta política es el mismo que se especifica en los tres primeros párrafos de la sección 3.1.2.4 de la Política de Seguridad de la Información, agregándose lo siguiente:

La gestión de la Seguridad de la Información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización, en base a metodologías de

---

[32] Proceso de cambio de contraseña cuando ha sido olvidada la anterior.

mejoramiento continuo, el cual deberá ser aplicado a todos los funcionarios de esta Cartera de Estado sin excepción.

3.3.5 NORMAS GENERALES

3.3.5.1 Oficial de Seguridad

El OSI deberá:

- Velar por el cumplimiento de esta política por parte de todos los funcionarios de esta Cartera de Estado e instituciones adscritas que ingresen o utilicen el servidor de correo electrónico del Ministerio de Cultura y Patrimonio, o los sistemas que estén alojados en el MCyP, o equipos de usuario final que se encuentren en la red local.
- Difundir la política de contraseñas en esta Cartera de Estado.
- Generar un proceso y normativa de administración y custodia de la contraseña.

3.3.5.2 Dirección de Tecnología de la Información y Comunicación

La Dirección de Tecnologías de la Información y Comunicación proveerá un sistema que permita a los usuarios escoger y cambiar sus propias contraseñas, de acuerdo con parámetros de seguridad de contraseña robusta, de igual o mayor restricción que los parámetros mínimos para contraseñas. Además, debe llevar a cabo el cumplimiento de los parámetros mínimos para el control de contraseñas.

3.3.5.2.1 Parámetros mínimos para contraseñas

Las contraseñas deben constar con:

- Más de ocho caracteres.
- Al menos una mayúscula.
- Al menos una minúscula.
- Al menos un número.
- Al menos un caracter especial.

3.3.5.2.2 Parámetros mínimos para control de contraseñas

- El sistema en cuestión debe:
    - Forzar a los usuarios al cambio de contraseña en la primera entrada. La clave generada por defecto para el usuario debe ser su número de cédula,

La clave debe ser cambiada con el primer ingreso al sistema por parte del usuario.
    - Forzar al usuario al cambio periódico de contraseñas, y evitar la reutilización de las ultimas diez (10) contraseñas.
- Las contraseñas deben estar cifradas, sin excepción, para todos los sistemas que requieran o soliciten las mismas.
- Las contraseñas deben estar almacenadas en una base de datos, cifradas de forma irreversible, pudiendo usarse para el efecto algoritmos de cifrado como las funciones *hash* actualizadas y más robustas.
- La asignación de contraseñas a los responsables de los sistemas albergados en esta Cartera de Estado debe estar bajo un acuerdo de confidencialidad firmado, donde se establezcan el adecuado uso de éstas, y el adecuado manejo de la confidencialidad. En caso de que una contraseña sea entregada de forma física, debe transferirse en un sobre sellado, por parte del Director de TICs, o un delegado de DTICs, al responsable.
- Debe registrarse y llevar un control de los accesos a través de contraseñas en los sistemas.
- Debe desactivarse de manera inmediata la contraseña del funcionario que ha sido desvinculado.
- No deben realizarse cambios de contraseña que hayan sido pedidos a través de correo electrónico, mensajes de texto o través de llamadas telefónicas, bajo ningún concepto.

Los funcionarios de la esta dirección deben firmar un acuerdo de confidencialidad donde se especifique la confidencialidad de la base de los sistemas que contengan contraseñas, sean de funcionarios públicos o no.

3.3.5.3 Usuarios

Es responsabilidad de los usuarios el buen uso de las contraseñas y velar por la confidencialidad de éstas.

La contraseña es intransferible, confidencial, de uso personal, y en ningún caso debe ser divulgada, ya sea de forma accidental o deliberada.

Los custodios de las contraseñas serán responsables de los daños que haya causado el mal uso de éstas, a menos que estos daños sean causados por terceras personas y haya sido evidenciado.

La política de contraseñas hace referencia a la Política de Protección de Datos Personales establecida en el Ministerio de Cultura y Patrimonio.

Su incumplimiento estará asociado a acciones penales de acuerdo con lo estipulado en el Código Orgánico Integral Penal (COIP).

De incumplirse esta Política de Seguridad de Contraseñas, y de acuerdo con la gravedad del evento suscitado, se realizará la acción administrativa pertinente, que puede ir desde una amonestación verbal hasta el cese de funciones por parte de los funcionarios de esta Cartera de Estado.

3.3.6 PROCEDIMIENTO DE CAMBIO O *RESETEO* DE CONTRASEÑA

El procedimiento para el cambio o *reseteo* de contraseñas se ilustra en el diagrama de la Figura 3.2, seguido de la explicación del procedimiento.

Para el cambio de contraseña, los funcionarios del Ministerio de Cultura y Patrimonio deben llenar el formulario que se encuentra en el siguiente enlace:

https://sistemas.culturaypatrimonio.gob.ec/formulario/modules/form_builder/published/actualizacion_datos.php

Para realizar el cambio y *reseteo* de contraseñas se debe ingresar en el siguiente enlace:

https://sistemas.culturaypatrimonio.gob.ec/password/

3.3.7 COMUNICACIÓN DE LA POLÍTICA

La difusión de la presente política se realizará como se especifica en la sección 3.1.2.6 de la Política de Seguridad de la Información.

3.3.8 DOCUMENTOS DE REFERENCIA

Los documentos de referencia utilizados para la presente política son los que se mencionan en la sección 3.1.3 de la Política de Seguridad de la Información. Adicionalmente, se utiliza la Política de Datos Personales del Ministerio de Cultura y Patrimonio.

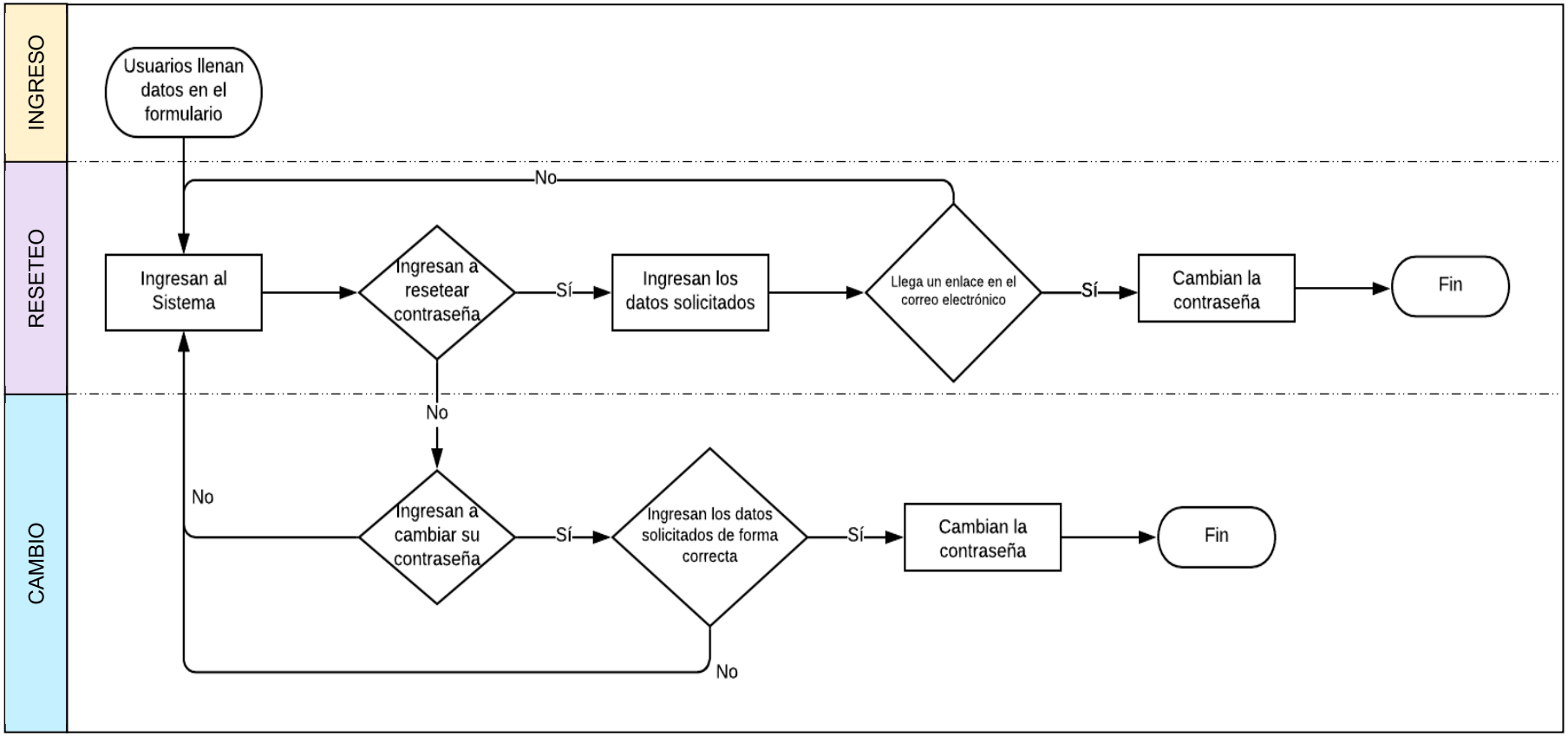


Figura 3.2. Procedimiento de cambio o *reseteo* de contraseñas [Elaboración propia]

3.3.9 TERMINOLOGÍA

Política de Contraseñas: Es un conjunto de normas, protocolos y reglas que custodian la seguridad de las contraseñas que se maneja en la institución, cuyo objetivo es mitigar y prevenir los riesgos a los que un activo se encuentra expuesto.

En el entregable de la Política de Contraseñas se debe agregar la terminología utilizada en la Política de Seguridad de la Información sección 3.1.4.

3.4 POLÍTICA DE *BACKUPS*

3.4.1 GENERALIDADES

Se define a la Política de *Backups* (respaldos) de Sistemas del MCyP, como un conjunto de normas que salvaguardan la disponibilidad de los sistemas del Ministerio de Cultura y Patrimonio, permitiendo que éste cumpla con su misión, visión y objetivos establecidos. Los servidores de esta Cartera de Estado contienen el activo más preciado que es la información. Estos dispositivos pueden verse involucrados en robo o daños accidentales o deliberados, trayendo como consecuencia la falta de disponibilidad de los servicios, afectando así a la continuidad de negocio del Ministerio de Cultura y Patrimonio.

El MCyP, con el acompañamiento del Oficial de Seguridad de la Información, debe realizar una clasificación de la información en pública, confidencial e interna. Los responsables de esta información serán los encargados de realizar copias de respaldo; los mismos criterios de esta política de seguridad serán aplicables en caso de hacer copias en la nube o en proveedores externos [109].

3.4.2 OBJETIVOS

Mantener disponibles la información pública, interna y confidencial de la institución, dando así cumplimiento a uno de los pilares de Seguridad de la Información, la disponibilidad.

Evitar que el cese de funciones por destrucción o falta de acceso a la información afecte a la continuidad de negocio del Ministerio de Cultura y Patrimonio.

3.4.3 ROLES

- **Oficial de Seguridad de Información:** Velará por el cumplimiento de esta política. Incentivará y capacitará a los usuarios acerca de la importancia de los respaldos de

la información. Ayudará en el proceso de clasificación de la información a cada una de las áreas del Ministerio de Cultura y Patrimonio.

- **Dirección de Tecnologías de la Información y Comunicación:** La Dirección de Tecnologías de la Información y Comunicación dará asesoramiento para el proceso de respaldos de la información.
- **Responsables de los sistemas:** Velarán por el correcto respaldo de la información del sistema del cual son custodios.
- **Usuarios:** Respaldarán y cooperarán con sus jefes inmediatos en el respaldo de la información de su área.

3.4.4 ALCANCE

Esta política es de cumplimiento y aplicación obligatoria, según corresponda, para todas las áreas del Ministerio de Cultura y Patrimonio y entidades adscritas[33] que utilicen servicios a través de esta Cartera de Estado. Esta política salvaguarda todos los activos que alberguen información pública, interna o confidencial.

La gestión de respaldos de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización, en base a metodologías de mejoramiento continuo, el cual deberá ser aplicado a todos los funcionarios de esta Cartera de Estado sin excepción.

3.4.5 NORMAS GENERALES

3.4.5.1 Clasificación de la Información

El Oficial de Seguridad de la Información, en conjunto con las áreas pertinentes, deberán clasificar la información del Ministerio de Cultura y Patrimonio en confidencial, pública e interna, misma que será protegida de acuerdo con la normativa vigente. El custodio de la información y encargado de respaldar la información será el jefe inmediato o, a su vez, un delegado del área; sea cual fuere el caso, deberá firmar un acuerdo de confidencialidad acorde con la criticidad de la información que se respalda, si ésta ha sido clasificada como confidencial. Este acuerdo de confidencialidad será determinado por el OSI[34] en conjunto con la Coordinación jurídica.

---

[33] Entidades adscritas son, actualmente, Coordinaciones zonales (EODs)
[34] OSI. Oficial de Seguridad de la Información

3.4.5.2 Respaldos de sistemas

El responsable de la Dirección de Tecnología de Información y Comunicación o, a su vez, la o el encargado del Área de Infraestructura, deberá realizar un respaldo de bases y sistemas de manera periódica. La periodicidad del respaldo estará determinada por el nivel de riesgo valorado de las bases o sistemas**.** Se llenará una bitácora que debe contener el nombre del sistema, el nombre del respaldo, fecha de respaldo, ubicación física, nombre del servidor, *path*[35], periodicidad (semanal, mensual, semestral, anual), fecha de los respaldos, tamaño del archivo, usuario responsable y firma del responsable.

3.4.5.3 Respaldos de información confidencial

Los jefes de cada área o usuarios delegados deberán respaldar el primer y último día de la semana la información confidencial, y documentar este proceso de acuerdo con el formato de esta actividad, especificado en la sección "Bitácora de *backups"* más adelante.

3.4.5.4 Respaldos de la información pública e interna

Los jefes de cada área o usuarios delegados deberán respaldar la información en un periodo establecido de acuerdo con la criticidad o importancia de la información catalogada como pública e interna.

3.4.6 COMUNICACIÓN DE LA POLÍTICA

Nota: Esta sección debe ir en el entregable de la correspondiente política al MCyP. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad ya que deberán realizarse las mismas acciones determinadas en la sección 3.1.2.6 para la Política de Seguridad de la Información.

3.4.7 DOCUMENTOS DE REFERENCIA

Se toman como referencia los documentos especificados en la sección 3.3.8, perteneciente a la Política de Contraseñas.

3.4.7.1 Bitácora de Backups

El formato para la Bitácora de *backups* se encuentra en la Tabla 3.1.

---

[35] Directorio (variable de entorno del S.O. en el que se especifica la ruta del respaldo)

Tabla 3.1. Bitácora para registrar los *backups* [Elaboración propia]

Nombre del Servicio	Nombre del Respaldo	Fecha del Respaldo	Ubicación Física	Nombre del Servidor	PATH	Periodicidad				Fecha de prueba del Respaldo	Tamaño del Archivo	Usuario responsable	Firma
						semanal	mensual	semestral	anual				

Los documentos generados con el uso de este formato son considerados de carácter confidencial.

3.4.8 TERMINOLOGÍA

Nota: Esta sección debe ir en el entregable de la correspondiente política al MCyP. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad en el Trabajo de Titulación. Los conceptos de información, confidencialidad, integridad, disponibilidad, seguridad de la información, y activo a especificarse aquí se toman de la sección 3.1.4, del capítulo 3.

3.5 POLÍTICA PARA EL TÉRMINO DE UN SISTEMA

3.5.1 GENERALIDADES

Se define a la Política de Término de un Sistema como un conjunto de normas que permiten salvaguardar los recursos del Ministerio de Cultura y Patrimonio, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información en el proceso de término de un sistema.

3.5.2 OBJETIVO

Establecer un proceso que permita el término de los sistemas del Ministerio de Cultura y Patrimonio de forma segura, cuando éstos hayan cumplido su función.

3.5.3 ROLES

Oficial de Seguridad: El Oficial de Seguridad velará por el cumplimiento de esta política. Se encargará de incentivar y capacitar a los usuarios acerca de la asignación de un responsable de los sistemas, y velará por el correcto desarrollo de las normativas establecidas en este documento. Además, participará de forma activa en los cambios y actividades en el término del sistema, que impliquen criterios de seguridad de la información.

Responsable del sistema: Usuario encargado de determinar las directrices sobre el sistema. Por ejemplo: puede solicitar la terminación del sistema.

Jefe inmediato del área requirente: Persona del Nivel Jerárquico Superior que puede designar al responsable del Sistema o dar directrices directas sobre el sistema.

Director de la Dirección de Tecnologías de la Información: Persona encargada de la autorización de los procedimientos sobre los sistemas informáticos, asignar y dar seguimiento a los procesos.

Administrador de la Red del Ministerio de Cultura y Patrimonio: Funcionario de la Dirección de Tecnologías del área de infraestructura encargado de configurar, poner en marcha o dar de baja a un sistema y verificar la capacidad de los equipos y sus características para un buen desempeño de la red.

Desarrolladores: Servidores públicos capacitados para el desarrollo de los sistemas.

3.5.4 ALCANCE

Esta política es de cumplimiento y aplicación obligatoria, según corresponda, para:

- Todos los funcionarios del Ministerio de Cultura y Patrimonio y entidades que utilicen servicios a través de esta Cartera de Estado que requieran la terminación de un sistema.
- También se aplica a los responsables de cada sistema siempre y cuando exista una asignación formal informada a la Dirección de Tecnologías de la Información y Comunicación. En el caso en que no exista un responsable designado formalmente, este documento se aplica a los jefes inmediatos del área requirente, durante su relación contractual con el Ministerio de Cultura y Patrimonio.

3.5.5 DESCRIPCIÓN DEL PROCEDIMIENTO PARA DAR DE BAJA UN SISTEMA

3.5.5.1 Solicitud para dar de baja al Sistema

- **Actividad:** El responsable del sistema o el jefe inmediato del área requirente debe realizar una solicitud formal dirigida al director de la Dirección de Tecnologías de la Información y Comunicación, adjuntando la designación formal firmada por el jefe inmediato del área requirente.
- **Actor:** Responsable del Sistema, Jefe Inmediato de la Unidad Requirente.

3.5.5.2 Asignación al Administrador de Red

- **Actividad:** El Director de la Dirección de Tecnologías de la Información y Comunicación recibe la solicitud y asigna al Administrador de red la tarea de dar de baja al sistema e informa de este proceso al Oficial de Seguridad de la Información.
- **Actor:** Director de la DTICs, Administrador de Red, Oficial de Seguridad de la Información.

3.5.5.3 Respaldo del Sistema

- **Actividad:** El Administrador de red realiza el respaldo del sistema dentro de un plazo máximo de tres (3) días laborables. El respaldo debe ser almacenado en un servidor de respaldos o en un disco externo, cuyas prestaciones sean adecuadas para salvaguardar dicha información.
- **Actor:** Administrador de Red.

3.5.5.4 Elaboración del Acta de Respaldo e Informe de Levantamiento

- **Actividad:** El Administrador de Red elabora y emite un acta de información (de carácter confidencial) luego del respaldo realizado, en el cual debe constar el nombre del respaldo, fecha, lugar de almacenamiento, *path* con la ubicación exacta, clave (en caso de que se haya añadido una clave de seguridad para proteger el respaldo), roles sobre el sistema con sus respectivas claves, y un informe en el que se debe especificar el procedimiento para levantar nuevamente el sistema para futuros requerimientos, dirigido de manera formal al Director de Tecnologías de la Información y Comunicación y al Oficial de Seguridad de la Información, en un plazo de dos (2) días laborables.
- **Actor:** Director TICs, Administrador de Red, Oficial de Seguridad de Información.

3.5.5.5 Verificación de los Documentos

- **Actividad:** El Director de Tecnologías de la Información y Comunicación y el Responsable de Seguridad de la Información verifican el informe en un plazo máximo de dos (2) días laborables. Si el informe es aprobado, pasa al punto 3.5.5.6, caso contrario, regresa al punto 3.5.5.4.
- **Actor:** Director de la DTICs, Oficial de Seguridad de la Información.

3.5.5.6 Baja del Sistema

- **Actividad:** El Administrador de red da de baja el sistema.
- **Actor:** Administrador de Red.

3.5.5.7 Notificación del Proceso

- **Actividad:** El Administrador de Red de la Información comunica del proceso realizado al Director de Tecnologías y al Oficial de Seguridad de manera formal

adjuntando el acta de respaldos (las claves no deben constar en dicho informe) en un plazo máximo de dos (2) días laborables.

El Director de Tecnologías notifica al responsable o al jefe inmediato del área requirente del proceso realizado.

- **Actor:** Director de la DTICs, Oficial de Seguridad de la Información y Administrador de Red.

En la Figura 3.3 se ilustra el proceso para dar de baja un sistema siguiendo los pasos especificados anteriormente.

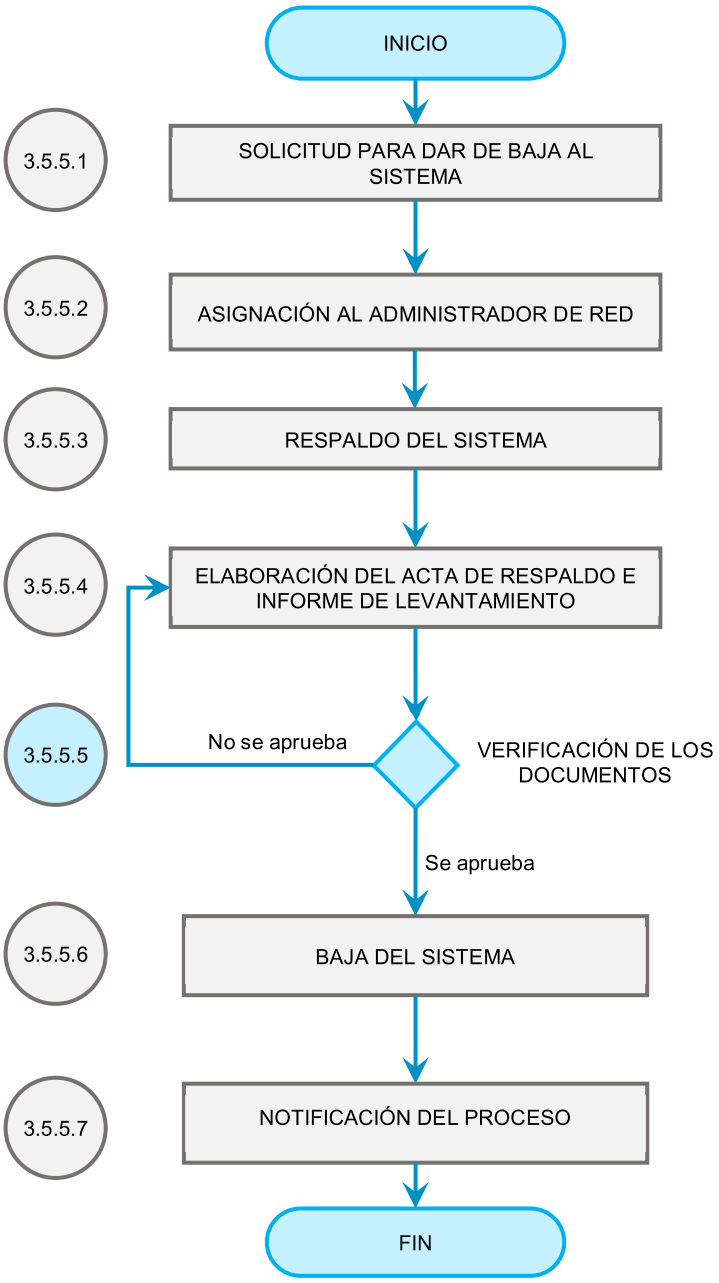


Figura 3.3. Procedimiento para dar de baja un sistema [Elaboración propia]

3.5.6 PROCEDIMIENTO PARA SOLICITAR LA BAJA DE UN SISTEMA, SI SE ENCUENTRA INOPERATIVO

3.5.6.1 Monitoreo de las Actividades de los sistemas

- **Actividad:** El Oficial de Seguridad de la Información, maneja un listado de los sistemas actuales de la institución y monitorea su actividad, cambios de responsables, creación de nuevos usuarios y roles, y actualizaciones.
- **Actores:** Oficial de Seguridad de la Información.

3.5.6.2 Detección de inoperabilidad

- **Actividad:** Si el Oficial de Seguridad de la Información detecta que el sistema no ha sido actualizado, ni utilizado en un periodo de tres (3) meses, pasa al punto 3.5.6.3. Caso contrario, pasa al punto 3.5.6.1.
- **Actores:** Oficial de Seguridad de la Información.

3.5.6.3 Notificación Inoperabilidad del Sistema

- **Actividad:** El Oficial de Seguridad de la Información notifica a los responsables del sistema o al jefe inmediato del área requirente vía Quipux solicitando se justifique la falta de uso del sistema, con copia al Director de la Dirección de Tecnologías de Información y Comunicación.
- **Actores:** Oficial de Seguridad de la Información.

3.5.6.4 Justificación Inoperabilidad del Sistema

- **Actividad:** Si el responsable del sistema justifica la inoperatividad vía Quipux al Oficial de Seguridad de la Información con copia al director de la Dirección de Tecnologías de Información y Comunicación en el período de tres (3) días laborables, regresa al punto 3.5.6.1, caso contrario se dirige al punto 3.5.6.5.
- **Actores:** Oficial de Seguridad de la Información, jefe del área requirente.

3.5.6.5 Solicitud para de dar de baja al sistema inoperativo

- **Actividad**: El Oficial de Seguridad de la Información solicita vía Quipux al Director de Tecnologías que se dé de baja al sistema debido a la inoperatividad de éste y el consumo de recursos.
- **Actores:** Oficial de Seguridad de la Información.

3.5.6.6 Terminación del sistema inoperativo

- **Actividad:** Se realizan las actividades del 3.5.5.2 al 3.5.5.7 del procedimiento para solicitar la baja de un sistema.
- **Actores:** DTICs.

La Figura 3.4. ilustra el proceso para solicitar la dada de baja de un sistema inoperativo.

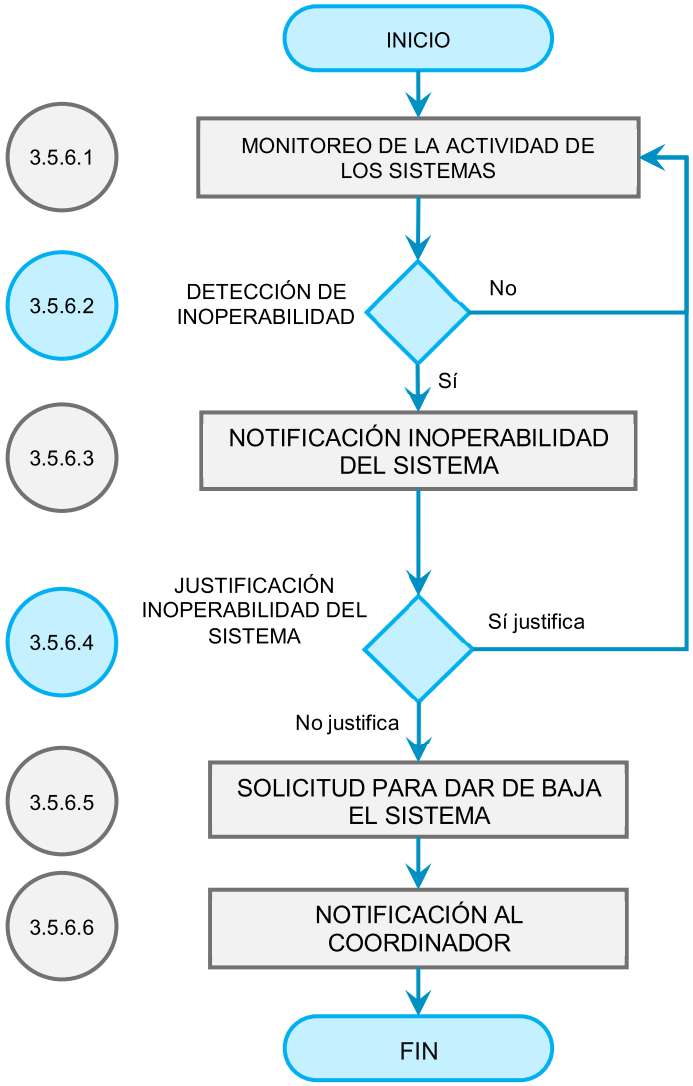


Figura 3.4. Procedimiento para solicitar la dada de baja de un sistema inoperativo [Elaboración propia]

En el caso de que no exista responsable, ni se identifique el jefe inmediato del área requirente, al detectar la inoperatividad y el no uso del sistema, es deber del Oficial de Seguridad y del Director de la Dirección de Tecnologías de la Información y Comunicación proseguir con el paso 3.5.6.2 al 3.5.6.6 del Proceso para dar de baja a un sistema, si se encuentra inoperativo.

3.5.7 COMUNICACIÓN DE LA POLÍTICA

Se difundirá de la misma forma que las políticas mencionadas anteriormente.

3.5.8 DOCUMENTOS DE REFERENCIA

Se utiliza como base los documentos de referencia utilizados en la Política de Seguridad de la Información (sección 3.3.8). Adicionalmente, se utilizan la Política de Contraseñas y la Política de *Backups*.

3.5.9 TERMINOLOGÍA

Seguridad de la información: Conjunto de medidas y técnicas para asegurar la confidencialidad, integridad y disponibilidad de la información, identificando, valorando y gestionando los activos de información y sus riesgos.

Seguridad informática: Conjunto de medidas y técnicas relacionadas con el área de informática y telemática. Se enfoca en la protección de la infraestructura de red. Es también conocida como Ciberseguridad.

Sistema: Conjunto de funciones interrelacionadas, hardware, software y de recursos humanos que hace posible el tratamiento automático de la información.

3.6 POLÍTICA PARA EL LEVANTAMIENTO DE UN SISTEMA

3.6.1 GENERALIDADES

Se define a la Política de Levantamiento de Sistemas como un conjunto de normas que permiten salvaguardar los recursos del Ministerio de Cultura y Patrimonio, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Los textos correspondientes a los apartados con el nombre “Obligaciones” han sido tomados textualmente de lo establecido en el EGSI v1.0 puesto que las recomendaciones y directrices que éste proporciona son vigentes en lo que a materia de seguridad respecta, y el EGSI v2.0 no especifica lineamientos pertinentes.

Las “Obligaciones” se aplican a los actores de las etapas correspondientes. Las etapas también siguen los lineamientos del EGSI v1.0, que están correlacionados con las actividades y etapas de esta política de seguridad (ver Anexo Q).

3.6.2 OBJETIVOS

Establecer un proceso que permita la creación de un sistema que se ajuste a las necesidades del Ministerio de Cultura y Patrimonio, a través de procedimientos de calidad en los sistemas, evaluando métricas e indicadores, y controlando la calidad del *software* producido y velando por la seguridad de la información en el proceso.

Definir la documentación necesaria que demuestre la viabilidad técnico-económica del sistema, a fin de que no consuma recursos innecesariamente, afectando al resto de servicios que provee el Ministerio de Cultura.

3.6.3 ROLES

Nota: Esta sección debe ir en el entregable de la política correspondiente al MCyP. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad (ver capítulo 3, sección 3.5.3) de este Trabajo de Titulación.

3.6.4 ALCANCE

Se considera el mismo alcance que se encuentra en la Política para el Término de un Sistema (ver sección 3.5.4).

3.6.5 DESCRIPCIÓN DEL PROCESO

3.6.5.1 Fase I: Requerimiento

- **Descripción:** En esta fase se recopila, analiza y verifica las necesidades del área requirente para el desarrollo de un sistema.
- **Objetivo:** Especificar de forma clara y detallada las funcionalidades del software que se quiere desarrollar.

3.6.5.1.1 Procedimiento: Requerimiento formal

- **Actores:** Jefe área requirente
- **Actividad:**
    - Designa un responsable del Sistema a través de un documento formal.
    - El jefe del Área Requirente envía una solicitud formal para la creación de un nuevo sistema vía Quipux adjuntando el documento DTICS-EGSI-FR-001 dirigida al Director de Tecnologías de la Información y Comunicación, donde

adicionalmente se solicita una reunión con el equipo de desarrollo y el Oficial de Seguridad de la Información.

- **Obligaciones:**
  - Designar un responsable del Sistema.
  - Realizar la solicitud formal para el desarrollo del sistema adjuntando el formulario DTICS-EGSI-FR-001.

3.6.5.1.2 Procedimiento: Recepción de Solicitud

- **Actores:** Director de DTICs y Oficial de Seguridad de la Información.

3.6.5.1.3 Procedimiento: Acuerdo de Reunión

3.6.5.1.4 Procedimiento: Reunión

- **Actores:** Jefe área requirente, Director de DTICs, responsable del Sistema, Desarrolladores.
- **Actividad:**
  - Se realiza una reunión con el jefe del Área Requirente, el responsable del Sistema, el Director del área de Tecnologías, Desarrolladores y el Oficial de Seguridad de la Información en donde se determinarán:
    - Historias del usuario.
    - Prioridad de las Historias del Usuario.
    - Requerimiento del tiempo de entrega del proyecto.
- **Obligaciones:**
  - Determinar la fecha de reunión entre la DTICs y el área requirente.
  - Completar y firmar el acta de reunión con la información solicitada DTICS-EGSI-AR.

3.6.5.2 Fase II: Análisis

- **Descripción:** En esta fase se realiza un informe de factibilidad, para saber si el sistema a implementarse es viable para el Ministerio de Cultura y Patrimonio, se realizan reuniones para establecer los requerimientos.
- **Objetivo:** Determinar la factibilidad del Sistema.

3.6.5.2.1 Procedimiento: Análisis de Factibilidad

- **Actores:** Desarrollares, Oficial de Seguridad de la Información.

- **Actividad:**
    - Generan un informe de factibilidad en el cual se determine:
        - Historias de Usuario.
        - Lenguaje, Sistema Operativo, Tipo de Base de Datos, Criptografía, Certificados de Seguridad.
        - Capacidad de equipos tecnológicos (Espacio de Disco, Memoria RAM), *firewall*, antispam.
        - Identificación y comparación de sistemas con funcionalidades similares.
        - Personal requerido.
        - Estimación del Tiempo.
        - Determinar si existen los recursos necesarios.
        - Especificación de supuestos daños en caso de afectar la disponibilidad, confidencialidad e integridad.
        - Conclusión: Si es favorable se sigue con el siguiente paso del proceso, si no es favorable deben proporcionarse recomendaciones en las que se incluyan los requisitos de seguridad que debe cumplir el proveedor del sistema.
- **Obligaciones:** Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.
- **Plazo máximo:** 5 días laborables.

3.6.5.2.2 Procedimiento: Resultados del análisis positivo

- **Actores:** Desarrollares, Oficial de Seguridad de la Información.
- **Actividad:** Se establece la fecha para la reunión de planificación.

3.6.5.2.3 Procedimiento: Resultados del análisis negativo

- **Actores:** Jefe del Área Requirente.
- **Actividad:**
    - En el caso de que el Informe de Factibilidad sea desfavorable para el desarrollo del sistema, el área requirente tiene 10 días laborables para realizar cambios y/o modificaciones para que sean analizadas por DTICs; estos cambios solo se pueden realizar una vez, caso contrario se finaliza el proceso. Si no existe pronunciamiento alguno por parte del área requirente, se procederá a finalizar el proceso.

- **Plazo máximo:** 10 días laborables.

3.6.5.3 Fase III: Planificación

3.6.5.3.1 Proceso: Reunión de Planificación

- **Descripción:** En esta etapa se realiza la planificación del proyecto, en donde se determinan fechas de entrega.
- **Objetivo:** Determinar cuáles son los requerimientos y fechas de entrega de los proyectos.
- **Actores:** Jefe área requirente, Director de DTICs, responsable del Sistema, Desarrolladores, Oficial de Seguridad y Administrador de Red.
- **Actividad:** Se establece una reunión con el Jefe del Área Requirente, el responsable del Sistema, el Director del área de Tecnologías, Desarrolladores y el Oficial de Seguridad de la Información en donde se determinarán:
    - En caso de que sea la primera reunión:
        - Establecer la prioridad de las historias de usuarios.
        - Establecer un cronograma de actividades y del periodo de entregables.
        - Establecer la fecha de la primera reunión para la revisión del primer entregable.
        - Firma de acuerdos de confidencialidad donde se detalle el uso y traspaso de las claves de los involucrados en el sistema.
    - En caso de que no sea la primera reunión:
        - Establecer la prioridad de las historias de usuarios.
        - Establecer plazo de entregable.
- **Actores:** Administrador de Red.
- **Obligaciones:**
    - Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se puedan definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.
    - Aislar los ambientes de desarrollo, pruebas, capacitación y producción.
    - Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
- **Actores:** Director de DTICs, desarrolladores, Oficial de Seguridad de Información, Administrador de Red.

- **Obligaciones:**
    - Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.
- **Actores:** Oficial de Seguridad, Director DTICs, Administrador de Red.
- **Obligaciones:**
    - Evitar que la función de Administrador de programas fuentes sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.
    - Prohibir el almacenamiento de programas fuentes históricos (que no sean correspondientes a los programas operativos) en el ambiente de producción.
    - Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
    - El código fuente de programas y las bibliotecas fuente de programas se deberán gestionar de acuerdo con los procedimientos establecidos.
    - El personal de soporte no debe tener acceso al código fuente de programas.
    - El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios.
    - Restringir el envío de información a correos externos no institucionales.
    - Controlar el acceso y las modificaciones al código instalado.
- **Plazo máximo:** A determinar.

3.6.5.4 Fase IV: Diseño

- **Descripción:** En esta etapa se realiza el diseño del sistema y se determina el cifrado a utilizarse.
- **Objetivo:** Diseñar el sistema solicitado.

3.6.5.4.1 Proceso: Diseño

- **Actores:** Jefe área requirente, Director de DTICs, Responsable del Sistema, Desarrolladores, Oficial de Seguridad de Información, Administrador de Red.
- **Actividad:** Elaborar el diseño del sistema solicitado (incluir el algoritmo de cifrado).
- **Plazo máximo:** Por definir.
- **Actores:** Director de DTICs, Desarrolladores, Oficial de Seguridad de Información, Administrador de Red.

- **Obligaciones:**
    - Utilizar herramientas para la protección contra la infección del software con código malicioso.
- **Plazo máximo:** Por definir.

3.6.5.5 Fase V: Desarrollo

- **Descripción:** Se establecen los criterios para el desarrollo del sistema.
- **Objetivo:** Desarrollar un sistema que cumpla con los requerimientos establecidos.

3.6.5.5.1 Procedimiento: Desarrollo

- **Actores:** Jefe área requirente, Director de DTICs, responsable del Sistema, Desarrolladores, Oficial de Seguridad de Información, Administrador de Red.
- **Actividad:**
    - Establecer las pruebas a cumplir.
    - Crear un registro de actividades.
    - Asegurar datos ingresados.
    - Encriptación de claves.
- **Obligaciones:** Utilizar herramientas para la protección contra la infección del software con código malicioso.
- **Actores:** Director de DTICs, desarrolladores, Responsable de Seguridad de Información, Administrador de Red.

3.6.5.5.2 Procesos: Cambios

- **Actores:** jefe del área requirente, responsable del Sistema.
- **Actividad:** Solicitud de Cambios.
- **Actores:** Oficial de Seguridad.
- **Actividad:**
    - Análisis de Seguridad. Si el análisis es favorable, se realiza el cambio, si no, no se realiza y se sigue con el proceso.
- **Obligaciones:**
    - Se debe realizar una solicitud formal del cambio.
    - Se debe realizar el análisis de seguridad.

3.6.5.6 Fase VI: Pruebas

- **Descripción:** Se establecen las pruebas para el funcionamiento del sistema.
- **Objetivo:** Realizar pruebas que determinen el correcto funcionamiento del sistema.

3.6.5.6.1 Procedimiento: Pruebas de Funcionalidad

- **Actores:** Desarrolladores, responsable del Sistema.
- **Actividades:**
    - Paso al ambiente de pruebas.
    - Informe ambiente de pruebas.
    - Si cumple con las pruebas pasa al siguiente módulo, si es el módulo final se pasa a la siguiente fase del proceso.
- **Obligaciones:**
    - Se debe realizar el informe de pruebas.
    - Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.
    - Crear un registro de las actividades del proceso de validación de la salida de datos.

3.6.5.7 Fase VII: Entrega del Proyecto

- **Descripción:** En esta fase se entrega el proyecto.
- **Objetivo:** Entregar el proyecto.

3.6.5.7.1 Procedimiento: Entrega del proyecto

- **Autores**: Jefe área requirente, Director de DTICs, responsable del Sistema, Desarrolladores, Oficial de Seguridad.
- **Actividad:**
    - Entrega de claves de administración.
    - Establecer el período de respaldos.
- **Plazo máximo:** por determinar.

3.6.5.8 Fase VIII: Implementación

- **Descripción:** En esta fase el sistema una vez ya listo pasa al ambiente de producción.

- **Objetivo:** Implementar el sistema en el ambiente de producción.

3.6.5.8.1 Procedimiento: Implementación

- **Actividad:**
  - Paso al ambiente de implementación.
  - Levantamiento del sistema.
  - Plan de contingencia.
- **Actores:** Desarrolladores, Oficial de Seguridad, Infraestructura.
- **Obligaciones:**
  - Prevenir y restringir el acceso no autorizado a la red.
  - Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

3.6.5.9 Fase IX: Entrega de Documentación

- **Descripción:** En esta fase se entrega la documentación.
- **Objetivos:** Entregar el proyecto.

3.6.5.9.1 Procedimiento: Entrega del proyecto

- **Actores:** Administrador de Red, Desarrolladores, Oficial de Seguridad.
- **Actividad:**
  - Manuales técnicos y manuales de usuario.
- **Obligaciones:**
  - Entrega de documentación al área requirente.
  - Generación de portafolio del sistema desarrollado almacenado en el repositorio de la Dirección de Tecnología.
- **Plazo máximo:** Por definir.

La Figura 3.5 (partes 1 y 2) presenta el procedimiento para el levantamiento de un sistema, y en la Tabla 3.2 se encuentran especificados los documentos requeridos.

Nota: De los documentos que se especifican en la Tabla 3.2, solo se han diseñado los documentos DTICS-EGSI-FR-001 - *Formulario de requerimiento de implementación del sistema*, DTICS-EGSI-AR – *Acta de reunión,* en este Proyecto como propuesta para la institución. El resto de los documentos deberán ser creados por el Ministerio de Cultura y Patrimonio.

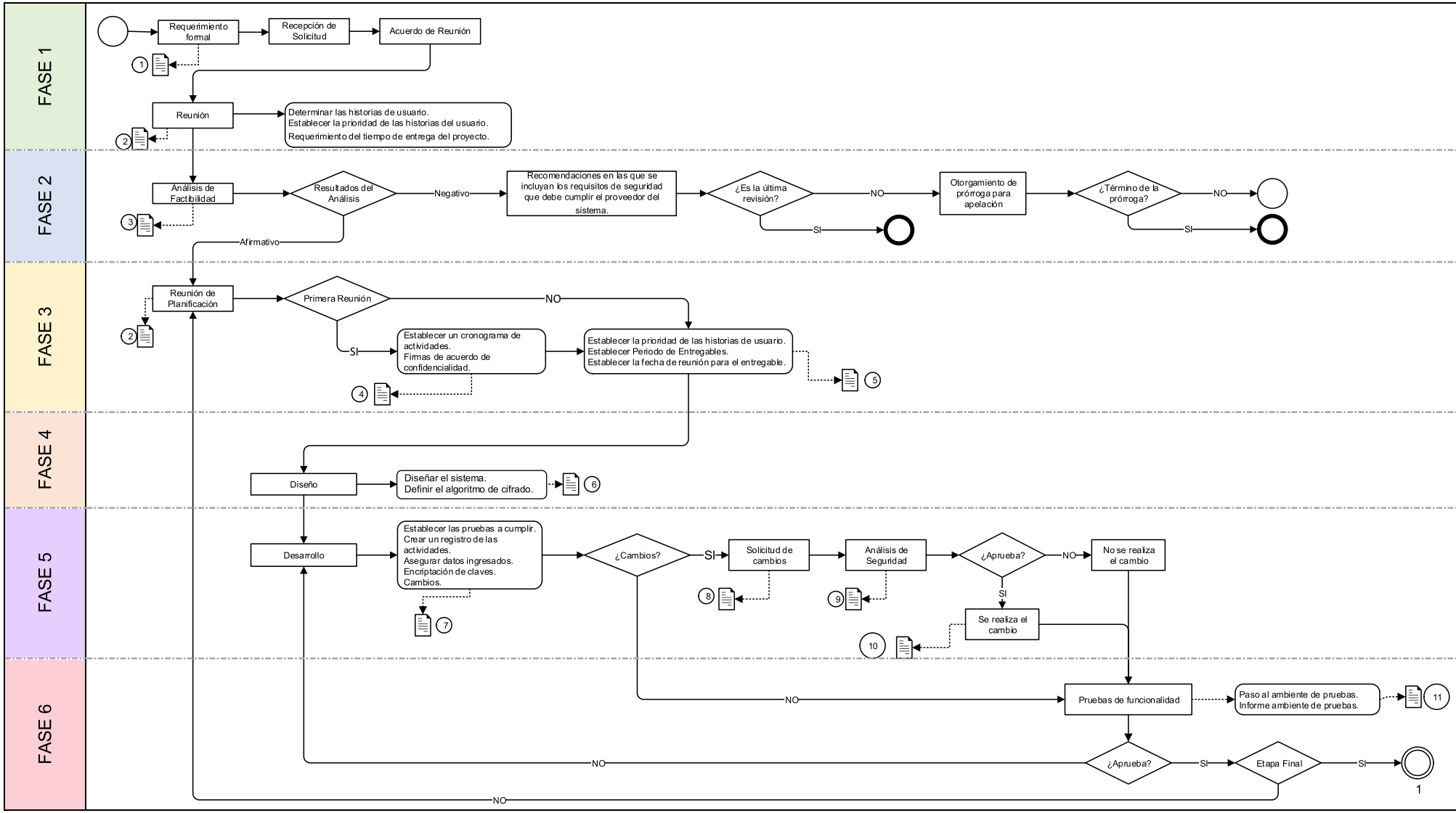


Figura 3.5. Procedimiento para el levantamiento de sistemas (parte 1 de 2)

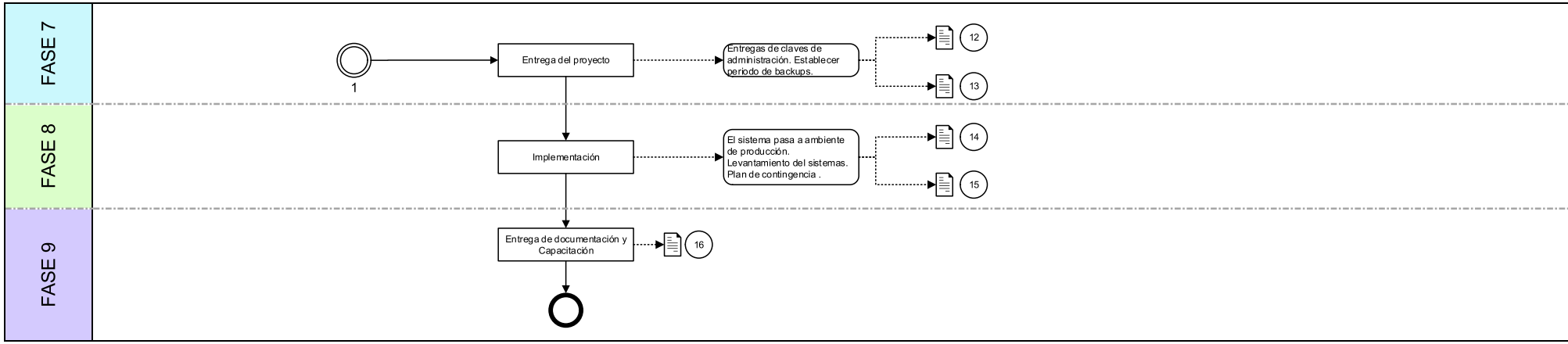


Figura 3.5. Procedimiento para el levantamiento de sistemas (parte 2 de 2) [Elaboración propia]

Tabla 3.2. Documentos requeridos en el proceso [Elaboración propia]

No. DOCUMENTO	CÓDIGO	NOMBRE
1	DTICS-EGSI-FR-001	FORMULARIO DE REQUERIMIENTO DE IMPLEMENTACIÓN DE SISTEMA
2	DTICS-EGSI-AR	ACTA DE REUNIÓN
3	DTICS-EGSI-IF	INFORME DE FACTIBILIDAD
4	DTICS-EGSI-AC	ACUERDO DE CONFIDENCIALIDAD
5	DTICS-EGSI-HU	TARJETA DE HISTORIA DE USUARIO
6	DTICS-EGSI-DD	DOCUMENTACIÓN DE DISEÑO
7	DTICS-RP	REGISTRO DE PRUEBAS Y ACTIVIDADES
8	DTICS-EGSI-FR-002	FORMULARIO DE REQUERIMIENTO DE CAMBIOS
9	DTICS-EGSI-FR	INFORME DE ANÁLISIS DE SEGURIDAD
10	DTICS-EGSI-RC	REGISTRO DE CAMBIOS
11	DTICS-EGSI-IF	INFORME DE PRUEBAS DE FUNCIONALIDAD
12	DTICS-EGSI-EC	DOCUMENTOS DE ENTREGAS DE CLAVES
13	DTICS-EGSI-RB	REGISTRO DE BACKUPS
14	DTICS-EGSI-IL	INFORME DE LEVANTAMIENTO
15	DTICS-EGSI-M	MANUALES

MINISTERIO DE CULTURA Y PATRIMONIO	**INFORMACIÓN QUE RESPALDA LA SOLICITUD DE LEVANTAMIENTO DEL SISTEMA INSTITUCIONAL**	**DTICS-EGSI-FR-001**
	Elaborado por Johan Marcelo Montenegro Zambrano y María Cristina Vivar Herrera	**Página 1 de 1**

NOMBRE DEL SISTEMA:		
NOMBRE DE LA PERSONA RESPONSABLE:		
PERÍODO DE VIGENCIA QUE TENDRÁ EL SISTEMA:		
OBJETIVO PRINCIPAL DEL SISTEMA:		
FUNCIONES DEL SISTEMA: **Enumere y describa las funciones que realizará el sistema:**		
DESCRIPCIÓN DEL SISTEMA: **Redacte una breve descripción del sistema, en la que conste una visión general del mismo.**		
RELACIÓN COSTO-BENEFICIO: **Indique el costo estimado y justifique.**		
RELACIÓN MISIONAL: **Marque con una "X" en el (o los) recuadro(s) correspondiente(s) a los objetivos de la Misión institucional que cumpliría el sistema solicitado.**	**OBJETIVO:**	**SELECCIÓN:**
	Proteger y promover la diversidad de expresiones culturales.	
	Incentivar la creación artística y la producción, difusión y disfrute	
	Salvaguardar la memoria social y el patrimonio cultural, garantizando el ejercicio pleno de los derechos culturales a partir de la descolonización del saber y del poder.	
	NO APLICA.	
TIPO DE INFORMACIÓN: **Marque con una "X" en el recuadro el (o los) tipo(s) de información que manejará el sistema.**	**TIPO:**	**SELECCIÓN:**
	Confidencial	
	Pública	
OBSERVACIONES:		

FIRMA DE LOS SOLICITANTES:	
Firma del Jefe del área requirente:	**Firma de la persona responsable:**
Nombre del Jefe del área requirente:	**Nombre de la persona responsable:**

MINISTERIO DE CULTURA Y PATRIMONIO	ACTA DE REUNIÓN	DTICS-EGSI-AÑO-MES-DIA
	IMPLEMENTACIÓN DE SISTEMAS	Página 1 de 2
	Elaborado por Johan Marcelo Montenegro Zambrano y María Cristina Vivar Herrera	

FECHA:		HORA INICIO:		HORA FIN:	
LUGAR:		CONVOCADO POR:			

NOMBRE DEL SISTEMA:		FECHA DE ENTREGA	

TEMA:	

TIPO: Marque con una "X" en la casilla que corresponda	REQUERIMIENTO:	
	AVANCES:	
	CAMBIOS:	
	ENTREGABLES:	

No. DE REUNIÓN:	

AGENDA:

REQUERIMIENTOS:

COMENTARIOS / OBSERVACIONES:

Nombre del Responsable:	Nombre del Jefe inmediato del área requirente:
Firma:	Firma:

COMPROMISOS			
Actividad	Responsable Unidad de Ejecución	Fecha de entrega	Firma de aceptación

ASISTENTES					
INSTITUCIÓN	NOMBRES Y APELLIDOS	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA

3.6.6 COMUNICACIÓN DE LA POLÍTICA

Se debe incluir esta sección en el entregable de la política al Ministerio. La comunicación se realizará de la misma forma de las políticas anteriores.

3.6.7 DOCUMENTOS DE REFERENCIA

Los documentos de referencia para la presente política son los indicados en la sección 3.3.8.

Debe agregarse a la lista la Política de Contraseñas.

3.6.8 TERMINOLOGÍA

Amenaza: Agente que puede atentar contra la seguridad de la información aprovechando una vulnerabilidad. Puede ser una acción o un elemento.

Ejecutable: Archivo que contiene y ejecuta instrucciones de un sistema, de forma transparente al usuario.

Entregable: Bloque de construcción, tangible o intangible, que actúa como resultado de un proyecto, parcial o total.

Historia de Usuario: Documento que contiene una breve descripción de una funcionalidad del sistema, descrito en forma breve, simple y concisa, por parte del usuario requirente. Puede ser adoptada, cambiada o eliminada según la necesidad de desarrollo, y debe ser validada acorde a los criterios de aceptación determinados para la misma.

Informe de factibilidad: Documento que sirve para evaluar de manera objetiva si se debe o no proceder con un proyecto propuesto.

Iteración: Repetición de un proceso dentro del proyecto solicitado.

Vulnerabilidad: Debilidad en sistema de información, misma que compromete la seguridad de la información, y genera el riesgo de ser explotada por una amenaza, lo que representa un nivel de impacto en el desempeño de la institución.

El resto de la terminología que deberá ir en el entregable de esta política incluye los conceptos de la sección 3.5.9.

3.7 POLÍTICA DE CONTROL DE ACCESO

3.7.1 GENERALIDADES

El Ministerio de Cultura y Patrimonio es la entidad rectora en el ámbito cultural y patrimonial, que garantiza el ejercicio de los derechos culturales, ejerciendo la rectoría de las políticas públicas culturales y del Sistema Nacional de Cultura, incidiendo en la integración simbólica del Ecuador y en el cambio cultural de la sociedad. Esta Cartera de Estado fue creada para fortalecer la identidad nacional y la interculturalidad, salvaguardar la memoria social y el patrimonio cultural del Ecuador. Incentiva la libre creación artística, la producción, difusión, distribución y disfrute de bienes y servicios culturales [95].

La Política de Control de Accesos es importante, ya que permite salvaguardar la integridad, confidencialidad y disponibilidad de la información de los efectos que puedan suscitarse por accesos no autorizados. La información es considerada como el activo más importante, pues permite dar cumplimiento a la misión, visión y valores del Ministerio de Cultura y Patrimonio.

Debido a la existencia de amenazas que pueden presentarse de forma deliberada o accidental, es importante mantener mecanismos de control de acceso físico, dando prioridad y relevancia a las áreas críticas de esta Cartera de Estado, y controles de acceso lógico para la información que se desea proteger.

Los mecanismos de control físico detienen o previenen del acceso mal intencionado por personas no autorizadas a la institución; son importantes ya que, si una persona con intenciones maliciosas accede a esta Cartera de Estado o a sus áreas críticas, sin ninguna supervisión, el resto de las medidas de seguridad de la información serían inútiles.

3.7.2 DESCRIPCIÓN DE LA POLÍTICA DE CONTROL DE ACCESOS

La presente política propone el control de accesos a las diferentes áreas del Ministerio de Cultura y Patrimonio, precautelando la protección de la información que ha sido catalogada como pública, confidencial e interna.

3.7.3 OBJETIVOS

Esta política tiene el propósito salvaguardar la información del Ministerio de Cultura y Patrimonio, misma que puede encontrarse de forma física o digital.

3.7.4 ROLES

Oficial de Seguridad de la Información: Encargado de salvaguardar la integridad, disponibilidad y confidencialidad de la información del Ministerio de Cultura y Patrimonio.

Director de la Dirección de Tecnologías de la Información y Comunicación: Director del área encargada del manejo del sistema de accesos y del acceso autorizado al Centro de Datos.

Funcionarios públicos del Ministerio de Cultura y Patrimonio: Encargados de velar por la confidencialidad, integridad y disponibilidad de la información del MCyP.

3.7.5 ALCANCE

Nota: Esta sección debe ir en el entregable de la correspondiente política al MCyP. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad (ver capítulo 3, sección 3.1.2.4) de este Trabajo de Titulación. Se extiende el alcance a toda persona natural que no forme parte de la institución.

3.7.6 NORMAS GENERALES

Es deber del Oficial de Seguridad de la Información clasificar las áreas del Ministerio de Cultura y Patrimonio en áreas de libre acceso y áreas de acceso crítico, dentro de la Planta Central del MCyP. Deben excluirse de esta clasificación el Centro de Datos, Cuartos de Telecomunicaciones y Área de Desarrollo, ya que éstos requieren un tratamiento especial.

3.7.6.1 Ingreso al Edificio del Ministerio de Cultura y Patrimonio

Toda persona natural que no forme parte de esta Cartera de Estado debe registrar su ingreso al Ministerio de Cultura, y debe proveérsele una tarjeta de visitante. En el caso en que ésta requiera ingresar a una de las áreas críticas, debe estar custodiado por al menos uno de los guardias de seguridad, según el requerimiento de seguridad física que se considere necesario.

La Dirección de Talento Humano enviará las credenciales de ingreso a la Dirección de Tecnologías de la Información y Comunicación para su activación.

La Dirección de Talento Humano entregará a los funcionarios sus correspondientes credenciales magnéticas.

Es deber de la Dirección de Tecnología de la Información y Comunicación establecer la configuración correcta de las credenciales, en las que solo se activarán los accesos al edificio y al piso correspondiente del funcionario.

Todos los funcionarios de esta Cartera de Estado están en la obligación de portar sus credenciales durante su jornada laboral; ésta debe permitir a los funcionarios abrir las puertas magnéticas únicamente de las áreas que les competen.

En el caso en que estas tarjetas presenten avería, es deber de los usuarios solicitar a la Dirección de Talento Humano el cambio o arreglo de éstas inmediatamente.

Las credenciales son intransferibles.

3.7.6.2 Requerimientos mínimos del registro de ingreso/egreso:

- Nombres completos (nombres y apellidos).
- Cédula de identidad.
- Institución de la que proviene (si aplica).
- Área, departamento o dependencia a la que se dirige.
- Hora de ingreso (hora y minuto del día). El formato puede ser de 12 horas (incluir si es A.M. o P.M.) o de 24 horas.
- Fecha de ingreso. Debe registrarse con claridad, sin que pueda presentar ambigüedad.
- Firma.

3.7.6.3 Ingreso a Áreas Críticas

El acceso a las Áreas Críticas está restringido para personas que no tengan una relación contractual con el Ministerio de Cultura y Patrimonio. Se permitirá el acceso, únicamente con la autorización previa de los funcionarios del área restringida y en compañía de un guardia de seguridad. Dichas personas deben portar las credenciales de visita, durante todo el tiempo que se encuentren dentro de la institución.

Cada ingreso y egreso de éstas a la Institución debe ser debidamente registrado, y el personal de guardianía deberá garantizar que cada ingreso y egreso sea registrado en el momento en que se efectúan, cumpliendo los requerimientos mínimos del registro establecidos, presentando su cédula de identidad o pasaporte.

3.7.6.4 Ingreso a Áreas de Libre Acceso

Para ingresar a las Áreas de Libre Acceso, las personas que no tengan una relación contractual con el MCyP deben estar autorizadas por el área que requieren visitar, además deberán portar la credencial de visitante durante todo el tiempo de visita.

Se debe estimar en el ingreso, el tiempo que estas personas permanecerán en la institución y realizar un control de éstas.

Cada ingreso y egreso a la institución debe ser debidamente registrado, y el personal de guardianía deberá garantizar que cada ingreso y egreso sea registrado en el momento en que se efectúan, cumpliendo los requerimientos mínimos del registro establecidos, presentando su cédula de identidad o pasaporte.

Se deben registrar maletas, bolsos y carteras de las personas que ingresan al Ministerio de Cultura y Patrimonio, y llevar un registro de ingreso de equipos tecnológicos que deben incluir sus características básicas.

3.7.6.5 Ingreso al *Data Center* y Cuarto de *Racks*

El acceso al Centro de Datos únicamente está permitido para el Director de Tecnologías de la Información, el Oficial de Seguridad, el Administrador del *Data Center* y el equipo de la Dirección de Tecnologías de la Información en el caso de que se requiera.

Se debe registrar los ingresos al Centro de Datos, en donde debe constar el Nombre del Usuario, la fecha y hora de ingreso y de salida, y el motivo de ingreso al Centro de Datos. Esto también debe aplicarse a los ingresos a los cuartos donde se encuentran los *racks* de esta Cartera de Estado.

3.7.6.6 Acceso a las computadoras y *laptops* de los funcionarios

Esta política incluye el control de acceso a través de contraseñas (véase Política de Contraseñas).

Las computadoras y equipos portátiles deben permanecer en modo hibernación o suspensión cuando los funcionarios no se encuentran en sus puestos de trabajo.

Los escritorios de sus computadoras y *laptops* deben estar limpios, y no contener la información en ellos.

3.7.7 COMUNICACIÓN DE LA POLÍTICA

Se difundirá esta Política de la misma forma que las demás.

3.7.8 DOCUMENTOS DE REFERENCIA

Los documentos de referencia son los mismos de la Política para el Levantamiento de Sistemas, expuestos en la sección 3.6.7.

3.7.9 TERMINOLOGÍA

En el entregable de esa política se deben añadir los conceptos de la sección 3.1.4.

3.8 POLÍTICA DE REUBICACIÓN DEL *DATACENTER*

3.8.1 GENERALIDADES

Esta sección debe incluirse en el entregable de la correspondiente política. El contenido respectivo se ha omitido intencionalmente para evitar duplicidad (ver capítulo 2, sección 2.1.1.1) de este Trabajo de Titulación.

La Planta Central del Ministerio de Cultura y Patrimonio alberga el *Data Center,* que concentra la información del MCyP que permite dar continuidad de negocio a esta Cartera de Estado.

3.8.2 DESCRIPCIÓN DE LA POLÍTICA DE REUBICACIÓN DE *DATA CENTER*

La presente política propone la reubicación del *Data Center*.

3.8.3 OBJETIVO

Salvaguardar la confidencialidad, integridad y disponibilidad de la información albergada en el *Data Center* de esta Cartera de Estado.

3.8.4 ROLES

Máxima Autoridad: Encargada de la aprobación de la reubicación del *Data Center*.

Oficial de Seguridad de la Información: Encargado de salvaguardar la integridad, disponibilidad y confidencialidad de la información del Ministerio de Cultura y Patrimonio.

Director de la Dirección de Tecnologías de la Información y Comunicación: Director del área encargada del monitoreo y mantenimiento del *Data Center*. Realizará el estudio de viabilidad para la reubicación del *Data Center*.

3.8.5 NORMAS GENERALES

3.8.5.1 Centro de Datos

El Oficial de Seguridad de la Información en conjunto con la Dirección de Tecnologías de la Información y Comunicación deben realizar un informe de viabilidad de la ubicación del Centro de Datos, en el que se deben incluir eventos suscitados (o potenciales), accidentales o deliberados, que hayan afectado (o puedan afectar) su buen funcionamiento, acompañado del estudio acerca del estado del edificio de Planta Central que incluya los riesgos asociados.

Este informe, más el estudio de riesgos de los activos de información o de software que se encuentren alojados en el *Data Center*, proporcionarán la información necesaria para considerar la reubicación del Centro de Datos del MCyP o la migración de la información más relevante para la continuidad del negocio a la nube. En este análisis se debe considerar si:

- El *Data Center* cumple con las normas establecidas de un centro de Datos.
- Considerar si los equipos, cables y puertos se encuentran etiquetados de forma adecuada.
- Considerar si el control de accesos es adecuado para el Centro de Datos.

Debe realizarse un esquema del Centro de Datos; esta tarea será llevada a cabo por la Dirección de Tecnologías de la Información y Comunicación.

Se debe documentar todo evento deliberado o accidental que haya afectado el funcionamiento del *Data Center*.

3.8.5.2 *Racks* en cada piso

Referente a los *Racks* que se encuentran en los pisos del Ministerio de Cultura y Patrimonio se debe:

- Mejorar el control de los Accesos.

- Reubicar éstos alejados de tuberías de agua, o a su vez llevar un control periódico de su estado.

3.8.5.3 Plan de Migración

Como institución perteneciente a la APCID, esta Cartera de Estado debe dar cumplimiento a las fases del plan de migración vigente normados por el MINTEL [110], mismo que ha sido ajustado a esta institución, como se expone a continuación:

- **Fase Preparatoria**
    - Debe incluir los siguientes entregables:
        - Inventario detallado de equipos, aplicaciones y arquitecturas, enlaces de datos, conexión a internet.
        - Listados de:
            - Contratos de servicios y mantenimiento de los sistemas de información.
            - Administradores funcionales de los sistemas de información y de usuarios de impacto.
            - Instituciones o áreas de la misma entidad, sean proveedoras y/o consumidoras de información. Debe darse a conocer a éstas sobre el proceso de la migración, con el propósito de evitar afecciones en el servicio que prestan.
- **Fase de Evaluación de riesgos**
    - Debe incluir los siguientes entregables:
        - Evaluación de riesgos de la migración asociados a la seguridad de la información de los activos identificados, acorde a lo señalado en el EGSI v2.0. Esta tarea debe ser ejecutada por el Oficial de Seguridad.
        - Plan de tratamiento de riesgos como resultado de dicha evaluación, orientada a la prevalencia de la disponibilidad de los sistemas adecuados durante y después del proceso de migración. Este proceso debe garantizar la integridad y totalidad de los datos.
        - Ejecución del plan de tratamiento de los riesgos por parte del Oficial de Seguridad y del ejecutor del plan en cuestión.
        - Matriz de riesgos como parte del plan de migración institucional, misma que debe ser remitida a la máxima autoridad del MINTEL.

- **Fase de Planificación**
    - Debe incluir los siguientes entregables:
        - Cronograma de migración.
        - Matriz de riesgos.
        - Plan de contingencia (debe garantizarse la disponibilidad de los sistemas adecuados).
        - Procedimiento de retorno (*rollback*).
        - Plan de pruebas a ejecutarse antes y después de la migración.
        - Elaboración de pliegos, publicación del proceso, adjudicación y firma de contrato.
- **Fase de Implementación**
    - Debe llevarse a cabo:
        - Ejecución del Plan de pruebas, definido en la Fase de Planificación.
        - Si la migración será realizada hacia un Centro de Datos Virtual, el proceso de migración se ejecutará en coordinación con la entidad que albergará los datos, en un período determinado de 42 días, a partir de la subscripción del contrato.

3.8.6 COMUNICACIÓN DE LA POLÍTICA

La difusión de esta política se la realizará de manera similar a la de las políticas anteriores. Dicha información debe ser incluida en el entregable del MCyP.

3.8.7 DOCUMENTOS DE REFERENCIA

Se utiliza la documentación de referencia de la Política de Seguridad de la Información (sección 3.1.3).

3.8.8 TERMINOLOGÍA

Se incluye la terminología sobre los conceptos de Información, confidencialidad, integridad, disponibilidad, seguridad de la información y activo, que se indica en la sección 3.1.4.

3.9 PRUEBAS Y RESULTADOS DE LOS CONTROLES

En esta sección se indican los resultados obtenidos al verificar los controles:

- Control administrativo – preventivo: Capacitación a los usuarios.
- Control técnico – preventivo: *Backups* de sistemas del MCyP.

Estos resultados permitieron verificar la eficacia de los controles aplicados, que fueron determinados después de la estimación del riesgo y son detallados a continuación.

3.9.1 CONTROL ADMINISTRATIVO- PREVENTIVO: CAPACITACIÓN A LOS USUARIOS

De acuerdo con los resultados obtenidos en la evaluación realizada por el Ministerio de Telecomunicaciones, donde se indica que los funcionarios del Ministerio de Cultura y Patrimonio no poseen una cultura tecnológica, y enfocando a los usuarios como el eslabón más débil en un sistema de seguridad de la información, se aplica el control de capacitación a los usuarios evidenciados en los Anexos M y O, donde se indica lo siguiente:

De acuerdo con lo planificado en el Plan de Capacitación, el Seminario Web con el tema Seguridad de la Información fue llevado a cabo el lunes 31 de agosto de 2020 desde las 12:00 hasta 13:15 p.m.[36], en el cual se trataron los temas:

- Seguridad de la Información.
- Pilares de la Seguridad de la Información.
- *Phishing, vishing, ransomware, spam.*
- Recomendaciones sobre sitios fraudulentos.
- EGSI v2.0.
- Estructura del EGSI v2.0.
- Comité de Seguridad de la Información: estructura y resumen de funciones.
- Oficial de Seguridad de la Información: responsable y resumen de funciones.
- Responsabilidades de las áreas de la Institución en la Gestión de Seguridad de la Información.
- *Grooming* (ciberacoso por redes sociales).
- Violaciones de seguridad de la información en Ecuador: casos.
- Leyes ecuatorianas sobre seguridad de la información.
- Capacitación para recuperar correos spams.
- Capacitación para *reseteo* y cambio de contraseñas.

La capacitación a través del Seminario web acogió un total de 55 participantes de todo el Ministerio de Cultura y Patrimonio. Se realiza evaluaciones a los funcionarios de esta

---

[36] La capacitación vía Seminario web estuvo programada en un principio a las 11h00, pero debido a la falta de organización, la programación fue cambiada a última hora a las 12h00 por cruce de horarios con otro evento de Comunicación Social.

Cartera de Estado pre y post capacitación, los resultados de estas evaluaciones pueden verse en el Anexo M.

3.9.1.1 Comparativa pre-capacitación y post-capacitación

Los resultados de la Tabla 3.3 muestran una comparación entre los resultados de la encuesta inicial realizada antes de la capacitación (ver el Anexo M), con la encuesta realizada después de la capacitación. Ambas encuestas fueron realizadas a través de *Google Forms*.

Puede evidenciarse un aumento en el rendimiento de la evaluación. Es necesario acotar que en la encuesta pre-capacitación participaron 118 personas, y en la encuesta post-capacitación participaron 38 personas. Esto evidencia que hay una deficiencia en el compromiso que debe haber en la Institución sobre este tema.

Tabla 3.3. Comparativa pre y post capacitación
[Elaboración propia]

	PRE – CAPACITACIÓN (ver Anexo M)			**POST – CAPACITACIÓN (Ver Anexo M)**		
Número de personas Evaluadas	**118 personas**			**38 personas**		
Preguntas	**# total**	**Porcentaje**		**# total**	**Porcentaje**	
	Contestaron	**Sí / Correcto**	**No / Incorrecto**	**Contestaron**	**Sí / Correcto**	**No / Incorrecto**
¿Conoce Ud. cuáles son los pilares de la Seguridad de la Información?	118	37,3%	62,70%	38	89,50%	10,5%
Seleccione los pilares de la Seguridad de la Información:	44	79,5%	20,50%	34	91,20%	8,8%
¿Cuál de estas afirmaciones describe de mejor manera el concepto de Seguridad de la Información?	118	14,4%	85,6%	38	44,7%	55,3%
¿Sabe usted que es el EGSI?	118	28,8%	71,2%	38	92,1%	7,9%
¿Sabe usted de qué trata el Esquema Gubernamental de Seguridad de la Información (EGSI)?	34	14,7%	85,3%	35	91,40%	8,6%
¿Conoce si el Ministerio de Cultura y Patrimonio cuenta con un Oficial de Seguridad?	118	30,5%	69,5%	38	86,8%	13,2%
¿Quién es el Oficial de Seguridad?	36	83,3%	16,7%	33	100%	0,0%

	PRE – CAPACITACIÓN (ver Anexo M)			POST – CAPACITACIÓN (Ver Anexo M)		
Número de personas Evaluadas	**118 personas**			**38 personas**		
Preguntas	**# total**	**Porcentaje**		**# total**	**Porcentaje**	
	Contestaron	**Sí / Correcto**	**No / Incorrecto**	**Contestaron**	**Sí / Correcto**	**No / Incorrecto**
¿Conoce las funciones del Oficial de Seguridad de la Información dentro de su Institución?	36	55,6%	44,4%	33	87,9%	12,1%
¿Sabe si existe política de Seguridad de la Información en el MCyP?	118	41,5%	58,5%	38	86,8%	13,2%
¿Conoce usted la política de Seguridad de la Información de su Entidad?	49	36,7%	63,3%	33	84,8%	15,2%
¿Conoce cómo se manejan los procesos de su institución?	118	53,4%	46,6%	38	89,5%	10,5%
¿Ha recibido o recibe información acerca de la importancia de la seguridad de la información dentro de la institución?	118	52,5%	47,50%	38	89,50%	10,5%
¿Si existe un incidente de seguridad de la información, sabe cuál es el protocolo que debe seguir?	118	20,3%	79,70%	38	89,50%	10,5%
¿Conoce si la información que usted maneja es catalogada como confidencial, pública e interna?	118	53,4%	46,60%	38	81,60%	18,4%
¿Sabe dónde encontrar la Política de Seguridad, procedimientos, procesos o normas de su institución?	118	24,6%	75,40%	38	65,80%	34,2%
¿Ha respaldado su contraseña con alguien de su confianza?	118	13,6%	86,40%	38	84,20%	15,8%
¿Comparte información personal (fechas importantes, hobbies, artistas favoritos, gustos musicales, claves, lugares favoritos u otros) con personas de su confianza?	118	16,9%	83,10%	38	84,20%	15,8%
¿Conoce usted el sistema para recuperar la contraseña?	118	34,7%	65,30%	38	89,50%	10,5%

	PRE – CAPACITACIÓN (ver Anexo M)			POST – CAPACITACIÓN (Ver Anexo M)		
Número de personas Evaluadas	**118 personas**			**38 personas**		
Preguntas	**# total**	**Porcentaje**		**# total**	**Porcentaje**	
	Contestaron	**Sí / Correcto**	**No / Incorrecto**	**Contestaron**	**Sí / Correcto**	**No / Incorrecto**
¿Conoce qué parámetros debe tener una contraseña para que sea muy robusta?	118	73,7%	26,30%	38	86,80%	13,2%
¿Sabe qué es la INGENIERÍA SOCIAL?	118	24,6%	75,40%	38	73,70%	26,3%
¿Sabe qué es un RANSOMWARE?	118	16,9%	83,10%	38	84,20%	15,8%
¿Sabe qué es un correo SPAM?	118	94,1%	5,90%	38	97,40%	2,6%
¿Sabe usted que es PHISHING?	118	45,8%	54,20%	38	92,10%	7,9%

Durante la capacitación, los funcionarios asistentes publicaron preguntas sobre el tema, lo que indica el interés que se generó en el tema de Seguridad de la Información. Además, cerca de finalizar, los asistentes publicaron mensajes de retroalimentación positiva sobre la capacitación recibida, en los que constaban su apoyo a la continuidad de este tema. Esto quedó evidenciado en una pregunta adicional sobre si consideran que las capacitaciones sobre Seguridad de la Información son importantes. En la Figura 3.6 se puede observar la captura del porcentaje de respuestas afirmativas a esta cuestión, cuyo valor es del 100%.

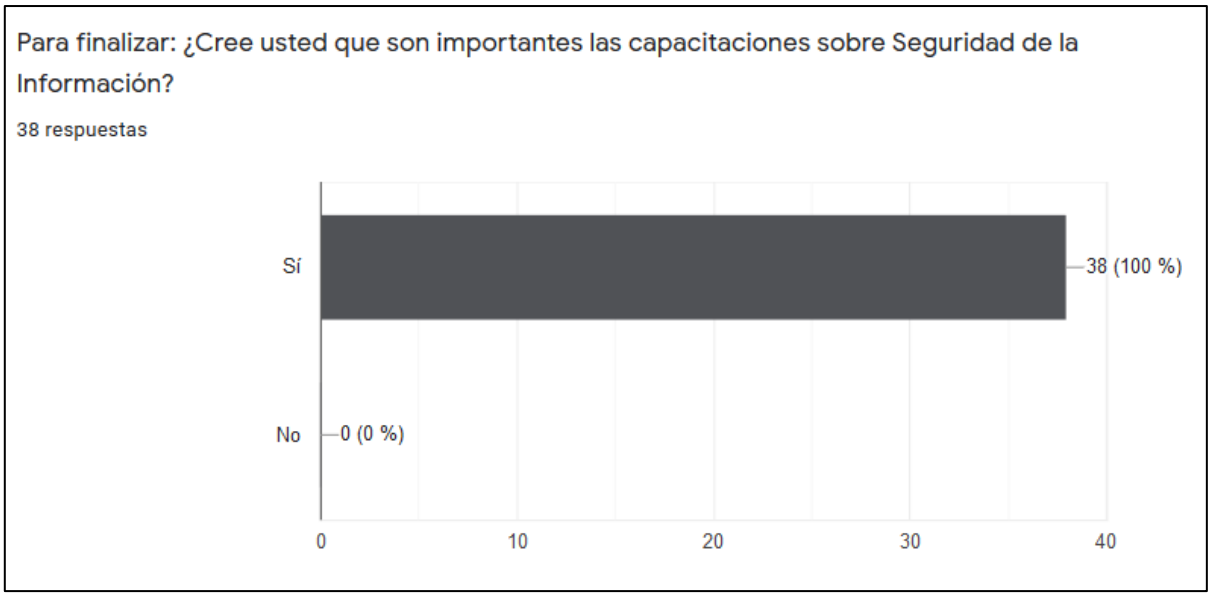


Figura 3.6. Porcentaje de aceptación sobre la importancia de las capacitaciones sobre Seguridad de la Información

3.9.1.2 Conclusiones sobre los resultados

Los resultados son favorables, a pesar de tener una asistencia de alrededor del 50% de personas en comparación con las que llenaron la encuesta la primera vez. Es la primera vez que se realiza un seminario de Seguridad de la Información en el Ministerio de Cultura y Patrimonio, y el desconocimiento de la importancia de este tema todavía es un problema que debe afrontarse, sobre todo desde la cabeza de la institución.

Debido a la falta del compromiso de los funcionarios de Nivel Jerárquico Superior, no se efectuó la difusión esperada sobre el Seminario web, además del problema de coordinación de la hora de la capacitación.

Las personas que asistieron a la capacitación mencionaron, no formalmente, que la capacitación resultó de gran ayuda al comprender la responsabilidad que se tiene en materia de Seguridad de la Información. En la encuesta respondieron que es importante que este tema se difunda en la institución. En base a esto, se espera que incremente el interés, conocimiento, cultura y compromiso por toda la institución en esta área.

3.9.2 CONTROL TÉCNICO – PREVENTIVO: *BACKUPS* DE SISTEMAS

Debido a los eventos suscitados en el Ministerio de Cultura y Patrimonio durante los últimos años, donde se ha vulnerado la disponibilidad e integridad de la información como resultado de las desfavorables condiciones en las que se encuentra el Centro de Datos, se procede a la aplicación del control técnico-preventivo: *backups* de sistemas del MCyP, del que se destacan los resultados que se exponen a continuación.

La Política de *Backups*[37] ha sido aplicada únicamente a los sistemas y bases de datos, ya que no se ha realizado aun el acompañamiento en la clasificación de la información en confidencial, pública e interna por parte de cada área debido a la emergencia sanitaria por la pandemia de SARS-CoV-2 (COVID-19) durante el último año, y a la consecuente imposición del teletrabajo desde el 16 de marzo del 2020. Dicho control ha sido registrado en la Bitácora de *backups* usando el formato especificado en la Tabla 3.1 del capítulo anterior, y que puede verse en el Anexo P. Las firmas de los responsables y del supervisor fueron realizadas a través de firma digital. Esto consta como un primer registro formal en que se han de llevar los respaldos.

---

[37] Respaldos de la información

3.9.2.1 Resultados

La Política de *Backups,* con la aplicación del formato de Bitácora de *backups* de la Tabla 3.1, ha permitido que:

- Se tenga documentación organizada acerca del estado de los respaldos, como el nombre del servicio, el nombre del respaldo, fecha del respaldo, ubicación física, nombre del servidor, *path*, periodicidad, fecha de prueba de respaldo, tamaño del archivo, usuario responsable y firma, de acuerdo con la bitácora diseñada.
- Se generen respaldos de los sistemas de forma periódica, de acuerdo con la importancia del sistema o base de datos, que ha sido determinada por el riesgo presentado en la matriz.

Los discos externos con los respaldos que debían trasladarse a Fábrica Imbabura aún se encuentran en la Dirección de Tecnología de la Información y Comunicación en Planta Central, debido al teletrabajo. Los discos externos, apenas se permita el retorno, serán llevados a la ciudad de Ibarra, para asegurar de mejor forma los respaldos.

En el registro de la Bitácora de *backups* (Anexo P) se especifica que no se realizan pruebas de los *backups*, a pesar de que ésta es importante, ya que, si el respaldo no funciona, en caso de un evento fortuito de pérdida de información, sería inútil efectuar una restauración, a pesar de las sugerencias realizadas. Esto se debe a la escasez de personal en la Dirección de Tecnología de Información y Comunicación, a la reducción de horas laborables y al aumento de trabajo en esta área.

3.9.2.2 Conclusiones sobre los resultados

El uso de la política de respaldos ha permitido llevar a cabo registros de los *backups* de manera formal. Así mismo, faculta el regular la frecuencia con la que éstos se harán, a fin de que existan puntos de restauración que permitan recuperar la información al máximo posible.

A pesar de lo anterior, no se ha garantizado la fiabilidad al no haberse realizado las pruebas respectivas sobre el funcionamiento de los respaldos; sin embargo, el hecho de que esto también quede registrado, es decir, que haya constancia de que no se han hecho pruebas, es positivo debido a que alerta al administrador para que comprenda los riesgos que pueden existir y pueda adelantarse a tomar acciones al respecto, por ejemplo, programando las pruebas cuando sea factible. Para un mejor trabajo, hace falta más personal en el área de la Dirección de Tecnologías de la Información y Comunicación.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Se diseñó un Sistema de Gestión de Seguridad de la Información para la Planta Central del Ministerio de Cultura y Patrimonio del MCyP, en base a las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, en aras del interés nacional de incrementar la seguridad de la información en las instituciones públicas.
- Se analizó la documentación asociada a la evaluación de riesgos de seguridad de la información, que incluye las normas base mencionadas en el párrafo anterior, la normativa regente por disposición gubernamental, como el Acuerdo Ministerial 025-2019 “Esquema Gubernamental de Seguridad de la Información” (EGSI v2.0), y las metodologías MAGERIT y MEHARI.
- Se evaluaron los riesgos de seguridad de la información. A fin de conseguirlo, se desarrolló una Metodología para este Trabajo de Titulación que incluye un Método de Análisis y Evaluación de Riesgos, basada en las normas ISO/IEC especificadas, y con elementos de las metodologías ya mencionadas. Con esto, se determinó el contexto de la Institución, se identificaron los activos de información, se valoraron acorde a los criterios establecidos, se determinaron amenazas, y se definieron valores de impacto, probabilidad y riesgo acumulados y repercutidos.
- El uso de metodologías facilita la comprensión de las directrices de las normas, puesto que éstas se encuentran definidas genéricamente (es decir, se especifica el qué, pero no el cómo). Además, las metodologías proveen técnicas, herramientas y fórmulas para llevar a cabo los procesos. Está claro que las metodologías a aplicarse deben ser compatibles con las normativas a usarse como base.
- El uso combinado de las metodologías permitió mayor flexibilidad a la hora de desarrollar la solución adaptada a los requerimientos y necesidades de la institución.
- Debido a que no están definidos aún los procesos sustantivos de la institución, se usó un enfoque global de análisis y evaluación de riesgos, es decir, que no se realizó el análisis por procesos. Tal enfoque requirió un mayor esfuerzo, puesto que aumentó la complejidad del análisis en etapas como, por ejemplo, las relaciones de dependencia entre activos, el cálculo del valor acumulado, entre otros.
- El desarrollo del programa de cómputo en este Trabajo agilizó el cálculo del que resultó uno de los factores más complejos: el valor acumulado. El tiempo invertido

en el desarrollo del programa se vio compensado al aplicarlo durante el análisis, reflejándose en un ahorro sustancial de tiempo.

- Se desarrollaron las propuestas de opciones para el Tratamiento de Riesgos, resultado de la avenencia de las metodologías mencionadas, ajustándolas a las normas ISO/IEC en las que está fundamentado diseño del SGSI.
- Se definieron controles de seguridad de la información, a través de Políticas de Seguridad, como propuesta para esta Cartera de Estado.
- Se validaron los controles de seguridad, mismos que reflejan una mejora en la seguridad de la información en la institución. Por ejemplo, la capacitación de usuarios es un factor determinante en el SGSI, pues se evidenció en la Institución que gran parte de las brechas de seguridad se deben a las malas prácticas de sus funcionarios por falta de conocimiento, interés y compromiso. Los resultados post-capacitación reflejan una mejora en el conocimiento y concientización sobre el tema en los usuarios.
- La inestabilidad en los puestos de la alta Dirección y en los puestos de los responsables de la toma de decisiones constituyen, según la experiencia durante el desarrollo del presente Trabajo, un considerable aumento en la dificultad del Trabajo. El continuo cambio de Directores, Coordinadores, el OSI y los miembros del CSI, requirió el tener que repetir la capacitación a cada ocupante de turno (lo que generaba un gasto considerable del tiempo) quien, acorde a sus percepciones, facilitaba o dificultaba el trabajo, entorpeciendo la continuidad en el diseño del SGSI.

4.2 RECOMENDACIONES

- Se recomienda el uso de un análisis y evaluación de riesgos enfocado a procesos, cuando éstos se encuentren definidos en la institución.
- Se recomienda la lectura a conciencia y estudio profundo de las normas de la familia ISO/IEC 27000, sobre todo las utilizadas en este Trabajo de Titulación (ISO/IEC 27001, 27002 y 27005), a fin de esclarecer la forma en que se abordará el diseño de un SGSI. Se sugiere que se realice la lectura al menos dos veces.
- Se recomienda complementar el análisis en la etapa de establecimiento del contexto revisando las directrices de las secciones correspondientes al contexto interno y externo de la organización, descritos en la norma ISO 31000.
- Se recomienda el uso de las metodologías MAGERIT y MEHARI, que proporcionan técnicas, catálogos, fórmulas y herramientas para llevar a cabo el diseño de un SGSI.

- Se recomienda de forma especial cerciorarse del nivel de compromiso que tiene la institución con respecto al tema. Se ha encontrado que cuando no existe compromiso o hay resistencia, el trabajo se vuelve muy difícil y el esfuerzo se multiplica considerablemente.
- Se recomienda la participación en seminarios, webinarios, y conferencias de expertos. Las respuestas obtenidas resultan sumamente útiles cuando el trabajo se estanca debido al surgimiento de dudas o ambigüedades.
- Se recomienda consultar con expertos en el área continuamente.
- Se recomienda la revisión de trabajos relacionados.
- Para agilizar la labor, se recomienda la conformación de un equipo de trabajo.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] "WikiLeaks - Brutal Kangaroo -- Drifting Deadline v1.2 - User Guide", *Wikileaks.org*, 2017. [En línea]. Disponible en: https://bit.ly/2EsJyXd [Accedido el 16 de agosto de 2020].

[2] "Glosario. TEMPEST.", *Ccn-cert.cni.es*, 2020. [En Línea]. Disponible en: https://bit.ly/31VcsXY [Accedido el 16 de agosto de 2020].

[3] Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2013. (2017). Tecnologías de la Información — Técnicas de Seguridad — Sistemas de Gestión de Seguridad de la Información – Requisitos (ISO/IEC 27001:2013+Cor.1:2014+ Cor. 2:2015, Idt), NTE INEN-ISO/IEC 27001. Quito,2013.

[4] Norma Técnica Ecuatoriana NTE INEN ISO / IEC 27002:2013. Tecnologías de La Información ─ Técnicas de Seguridad ─ Código de Práctica para los Controles de Seguridad de la Información (ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015, Idt), NTE INEN ISO / IEC 27002, 2da ed., Quito, 2017.

[5] Norma Técnica NTE INEN ISO / IEC 27005:2012. Tecnología de la Información - Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la Información, NTE INEN ISO / IEC 27005, Quito, 2012.

[6] Ministerio de Telecomunicaciones y de la Sociedad de la Información, *Acuerdo Ministerial No. 025-2019 Esquema Gubernamental de Seguridad de la Información,* 2da edición. Quito, 2019.

[7] Norma Técnica Ecuatoriana NTE INEN ISO / IEC 27000:2016. Tecnologías de la Información — Técnicas de Seguridad — Sistemas de Gestión de Seguridad de la Información — Descripción General y Vocabulario (ISO/IEC 27000:2016, Idt), NTE INEN ISO / IEC 27000, 4ta ed., Quito, 2016.

[8] J. C. Najar Pacheco y N. E. Suárez Suárez, “La seguridad de la información: un activo valioso de la organización”, *Vínculos*, vol. 12, no. 1, pp. 89-97, jun., 2016. [En línea]. Disponible en: https://bit.ly/3kLXVX8

[9] C. Parra, "Seguridad informática y seguridad de la información en el mundo, como factor de enseñanza en Colombia,” Repositorio Institucional Universidad Piloto de Colombia, jul.,2015. [En línea]. Disponible en: https://bit.ly/3h2LyDU

[10] D. G. Zambrano *La falta de conciencia, una vulnerabilidad latente para la seguridad de la información*. [En línea]. Disponible en: http://hdl.handle.net/10654/35135.

[11] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, T. Herawan. “Information security conscious care behaviour formation in

organizations," *Computers & Security*, V. *53*, sep., 2015, pp. 65-78. [En línea]. Recuperado de: https://doi.org/10.1016/j.cose.2015.05.012

[12] H. NguegangTewamba, J. R. Kala Kamdjoug, G. Bell Bitjoka, S. FossoWamba y N. Nkondock Mi Bahanag, "Effects of Information Security Management Systems on Firm Performance," *American Journal of Operations Management and Information Systems*. vol. 4, no. 3, pp. 99-108, 2019. [En línea]. Recuperado de: https://bit.ly/2DZkas3

[13] J. Flyktman, "Implementing Information Security Management System as a part of business processes: Where to gain competitive advantage for ISMS?" Tesis M. Sc., Dpto. Technology, ICT. Univ.JAMK University of Applied Sciences, 2016.

[14] E. I. Chilán-Santana y W. F. Pionce-Pico, "Apuntes teóricos introductorios sobre la seguridad de la información," *Dominio de las Ciencias*, vol. 3*,* no*.* 4, pp. 284-295, 2017. [En línea]. Recuperado de: http://dx.doi.org/10.23857/dc.v3i4.686

[15] M. G. Hernández Pinto, "Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial." Tesis de Grado, Univ. Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador, 2006. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/retrieve/94448/D-71165.pdf

[16] M. D. Flores Loayza, "ESTUDIO COMPARATIVO SOBRE EL ENTENDIMIENTO DE LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN USUARIOS DE TI MAYORES A 45 AÑOS DE LOS ESTRATOS SOCIALES C, DYE DE SUDAMÉRICA. "Tesis M. Sc., Univ. Espíritu Santo, Samborondón, Ecuador,2018. [En línea]. Recuperado de: https://bit.ly/3atupQZ

[17] K. M. Terán Valenzuela, "Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador," Tesis M. Sc., Univ. ESPE Universidad de las Fuerzas Armadas, Sangolquí, Ecuador,2018. [En línea]. Recuperado de: https://bit.ly/343fETX

[18] L.F. Molina Batallas, "Diseño de un sistema de gestión de seguridad de la información para la corporación nacional de telecomunicaciones CNT EP, agencia doral," Trabajo de Titulación, Fac. Ingeniería y Ciencias Agropecuarias, Univ. Universidad de las Américas, Quito, Ecuador, 2016. [En línea]. Recuperado de: https://bit.ly/3as589Y

[19] P.P. Guamán Yucaza y N.R. Moncayo Zambrano. "Desarrollo de un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) basado en las mejores prácticas de seguridad informática para la Agencia de Regulación y Control Hidrocarburífero", Trabajo de Titulación, Univ. ESPE Universidad de las Fuerzas

Armadas, Sangolquí, Ecuador,2016. [En línea]. Recuperado de: https://bit.ly/3as589Y

[20] F. Y. Holguín García y L. M. Lema Moreta, “Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas,” Navieras. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, no. 31, pp. 1-17, 2019. [En línea]. Recuperado de: https://dx.doi.org/10.17013/risti.31.1-17

[21] R. Prada, “Epistemología del dato,” *Revista Mexicana de Sociología*, vol. 49, no.1, pp. 307-334. [En línea]. Disponible en: https://bit.ly/36pE5MH

[22] R. Stair y G. Reynolds, *Principios de sistemas de información: Un enfoque administrativo*, 9na ed.,2000. [En línea]. Disponible en: http://docshare04.docshare.tips/files/24101/241015829.pdf

[23] G. P. Abritta, “Noción y estructura del dato.” ,1999. [En línea]. Disponible en: https://bit.ly/3nbCn7h

[24] A. C. Nieves, “Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013,” Univ. Institución Universitaria Politécnico Grancolombiano, 2017.

[25] Prieto, A. Lloris, A. y J.C. Torres, “Introducción,” *Introducción a la Informática*, 3ra ed. España,2006, cap.1, pp.1-35.

[26] Á. G. Vieites, *Enciclopedia de la seguridad informática*: Grupo Editorial RA-MA,2011.

[27] M. I. Romero Castro, G. L. Figueroa Morán, D. S. Vera Navarrete, J. E. Álava Cruzatty, G. R. Parrales Anzúles, C. J. Álava Mero, Á. L. Murillo Quimiz, M. A. Castillo Merino, *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES,* 1era. ed. Alicante: Editorial Área de Innovación y Desarrollo, S.L., 2018.

[28] K. G. Bermúdez Molina, E. R. Bailón Sánchez, “ANÁLISIS EN SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001- SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIRIGIDO A UNA EMPRESA DE SERVICIOS FINANCIEROS,” Trabajo de Grado, Dpto. Ing. Sistemas, Univ. Politécnica Salesiana sede Guayaquil,2015.

[29] J. F. Roa Buendía, *Seguridad Informática,* 1era ed. Madrid: Editorial McGraw-Hill/Interamericana de España, S. L, 2013. [En línea]. Disponible en: https://bit.ly/2LrsynC

[30] National Institute of Standard and Technology, “About NIST.” [En línea]. Disponible en: https://www.nist.gov/about-nist.

[31] National Institute of Standard and Technology, “Cyberspace.” [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/cyberspace

[32] National Institute of Standard and Technology, “Cyber Security.” [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/Cyber_Security.

[33] Consejo Nacional de Política Económica y Social. *Política Nacional de Seguridad Digital*. Bogotá, 2016 [En línea]. Disponible en: https://bit.ly/3hwhqBI

[34] F. J. Valencia Duque, M. Orozco Alzate, “Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,” *RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação*, no.22, pp. 73-88,2017. [En línea]. Disponible en: https://bit.ly/394odyR.

[35] National Institute of Standard and Technology, “Information Security.” [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/information_security.

[36] M. Soriano, *Seguridad en redes y seguridad de la información,* 1era ed: Editorial České vysoké učení technické v Praze. [En línea]. Disponible en: https://bit.ly/3rXqWCF .

[37] V. Măzăreanu, A. Marin y R. Ungureanu, *MEHARI 2007. Concepte şi Mecanisme* [Ebook]. Paris, Francia, 2008

[38] M. A. Mendoza, “Control y objetivos del Control,” *Módulo 1: Conceptos básicos de Seguridad de la información*, Academia ESET, 2015.

[39] Organización Internacional de Normalización, “ABOUT US”. [En línea]. Disponible en: https://www.iso.org/about-us.html

[40] Organización Internacional de Normalización, “STANDARDS”. [En línea]. Disponible en: https://www.iso.org/standards.html

[41] Organización Internacional de Normalización, “MEMBERS”. [En línea]. Disponible en: https://www.iso.org/members.html

[42] Servicio Ecuatoriano Normalización, “Ecuador forma parte de importantes organismos internacionales”. [En línea]. Disponible en: https://bit.ly/2ERSvd5

[43] Organización Internacional de Normalización, “TECHNICAL COMMITTEES”. [En línea]. Disponible en: https://www.iso.org/technical-committees.html

[44] International Electrotechnical Commission, “Who we are”. [En línea]. Disponible en: https://www.iec.ch/about/profile/

[45] International Electrotechnical Commission, “Where we are”. [En línea]. Disponible en: https://www.iec.ch/about/locations/

[46] International Electrotechnical Commission, “Who we are: Members: List of members”. [En línea]. Disponible en: https://www.iec.ch/dyn/www/f?p=103:5:0

[47] International Electrotechnical Commission, “What we do”. [En línea]. Disponible en: https://www.iec.ch/about/activities/

[48] International Electrotechnical Commission, “Who we are: Members: National Committees”. [En línea]. Disponible en: https://bit.ly/2GgLHGw

[49] International Electrotechnical Commission, “Who we are: Experts & delegates”. [En línea]. Disponible en: https://www.iec.ch/about/profile/experts.htm

[50] Organización Internacional de Normalización, “INEN Ecuador”. [En línea]. Disponible en: https://www.iso.org/member/1711.html

[51] Servicio Ecuatoriano Normalización, “Reseña Histórica”. [En línea]. Disponible en: https://www.normalizacion.gob.ec/resena-historica/

[52] Servicio Ecuatoriano Normalización, “Contáctenos”. [En línea]. Disponible en: http://inennormalizacion.blogspot.com/p/contactenos.html

[53] Ministerio de Telecomunicaciones y de la Sociedad de la Información, *Decreto Ejecutivo 8*. Quito, 2009.*”*. [En línea]. Disponible en: https://bit.ly/30rYMUd

[54] Ministerio de Telecomunicaciones y de la Sociedad de la Información, “Valores/ Misión/Visión.” [En línea]. Disponible en: https://bit.ly/2ShdKb9

[55] Ministerio de Telecomunicaciones y de la Sociedad de la Información, “MINTEL cumple 7 años de servir a los ecuatorianos.” [En línea]. Disponible en: https://bit.ly/36oIn6R

[56] Ministerio de Telecomunicaciones y de la Sociedad de la Información, “¿Sabe cuáles son las entidades adscritas y relacionadas al Mintel?” [En línea]. Disponible en: https://bit.ly/3cNlhYE

[57] Asamblea Nacional República del Ecuador, *Ley Orgánica de Telecomunicaciones*. Quito, feb., 2015. [En línea]. Disponible en: https://bit.ly/30spRqn

[58] Presidencia de la Republica del Ecuador, *CREA LA EMPRESA PÚBLICA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT: Decreto Ejecutivo No.128*. Quito, feb., 2010. [En línea]. Disponible en: https://bit.ly/2GhSUpN

[59] Dirección General de Registro Civil, Identificación y Cedulación, “Registro Civil 113 años de historia.” [En línea]. Disponible en: https://bit.ly/2ShefC3

[60] Asamblea Nacional República del Ecuador, *LEY GENERAL DE LOS SERVICIOS POSTALES*. Quito, sep., 2015. [En línea]. Disponible en: https://bit.ly/2SeI5Ho

[61] Correos del Ecuador, “183 AÑOS AL SERVICIO DEL PAÍS”. [En línea]. Disponible en: https://bit.ly/33lXV9t

[62] Presidencia de la República del Ecuador, *Decreto Ejecutivo [1156]*. [En línea]. Disponible en: https://minka.presidencia.gob.ec/portal/usuarios.

[63] Presidencia de la República del Ecuador, *Decreto Ejecutivo [1123]*, 2020 [En línea]. Disponible en: https://minka.presidencia.gob.ec/portal/usuarios.

[64] Ministerio de Telecomunicaciones y de la Sociedad de la Información, *Acuerdo Ministerial No. 025-2019 Esquema Gubernamental de Seguridad de la Información,* 2da edición. Quito, 2019.

[65] Organización Internacional de Normalización, “ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary”. [En línea]. Disponible en: https://www.iso.org/standard/66435.html

[66] Organización Internacional de Normalización, “ISO/IEC 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements”. [En línea]. Disponible en: https://www.iso.org/standard/54534.html

[67] *Iso27000, “Sistema de Gestión de la Seguridad de la Información*.” [En línea]. Disponible en: https://es.scribd.com/document/387823257/doc-sgsi-all-pdf

[68] Organización Internacional de Normalización, “ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls”. [En línea]. Disponible en: https://www.iso.org/standard/54533.html

[69] Organización Internacional de Normalización, “ISO/IEC 27005:2011Information technology — Security techniques — Information security risk management”. [En línea]. Disponible en: https://www.iso.org/standard/56742.html

[70] Ministerio de Telecomunicaciones y de la Sociedad de la Información, *Acuerdo Ministerial No. 166 Esquema Gubernamental de Seguridad de la Información,* 1ra edición. Quito, sep., 2013. [En línea]. Disponible en: https://bit.ly/36sOly6

[71] Presidencia de la República del Ecuador, Decreto Ejecutivo No 5. Quito, may.,2017. [En línea]. Disponible en: https://bit.ly/36kDM5l

[72] Presidencia de la República del Ecuador, *Decreto No. 526*. [En línea]. Disponible en: https://minka.presidencia.gob.ec/portal/usuarios.

[73] GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN, 1ra ed., Ministerio de Telecomunicaciones y de la Sociedad de la Información, Quito, 2020. [En línea]. Disponible en: https://bit.ly/30mH9VS.

[74] R. M. Aguilera Hintelholher, “Identidad y diferenciación entre Método y Metodología,” *Estudios políticos (México),* no. 28, pp.81-103. [En línea]. Recuperado en: https://bit.ly/2G9qiza.

[75] H. Alemán Novoa y C. Rodríguez Barrera, “Metodologías para el análisis de riesgo en los sgsi,” *Publicaciones e Investigación,* vol.9, pp. 73-86, oct., 2015. [En línea]. Disponible en: https://doi.org/10.22490/25394088.1435.

[76] Ministerio de Hacienda y Administraciones Públicas, *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*, Madrid, España, 2012. [En línea]. Disponible en: https://bit.ly/39rlUDd

[77] Ministerio de Hacienda y Administraciones Públicas, *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, Madrid, España, 2012. [En línea]. Disponible en: https://bit.ly/39rlUDd

[78] Ministerio de Hacienda y Administraciones Públicas, *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*, Madrid, España, 2012. [En línea]. Disponible en: https://bit.ly/39rlUDd

[79] CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS, “PRÉSENTATION DE L’ASSOCIATION”. [En línea]. Disponible en: https://clusif.fr/a-propos/.

[80] J. Jouas, J. Roule, D. Buc, O. Corbier, M. Gagné y M. Hazzan, *MEHARI 2010. Introducción*. Paris, Francia, 2010.

[81] J. Jouas y J. Roule, MEHARI *2010. Fundamental concepts and functional specifications*. Paris, Francia, 2010.

[82] V.Măzăreanu, A. Marin y R. Ungureanu. *MEHARI 2007. Concepte şi Mecanisme* [Ebook]. Paris, Francia, 2008

[83] J. Jouas, J. Roule, D. Buc, O. Corbier, M. Gagné y M. Hazzan. et al. *MEHARI 2010. Security stakes analysis and classification guide*. Paris, Francia, 2010.

[84] J. Jouas, J. Roule, D. Buc, O. Corbier, M. Gagné y M. Hazzan. et al. *MEHARI 2010. Guide de l’analyse et du traitement des risques*. Paris, Francia, 2010.

[85] J. Jouas y J, Roule, *MEHARI 2010. Evaluation Guide for security services.* Paris, Francia, 2010.

[86] R. Torres, A. Nina, G. Cisneros, C. Herrera, I. Ron, A. Tobar, R. Pazmiño y G. Calvas, INFORME DE RENDICIÓN DE CUENTAS, Ministerio de Cultura y Patrimonio, Quito, Ecuador, 2018. [En línea]. Disponible en: https://bit.ly/2MF2hml

[87] Ministerio de Cultura y Patrimonio, “Objetivos”. [En línea]. Disponible en: https://www.culturaypatrimonio.gob.ec/objetivos/.

[88] Ministerio de Cultura y Patrimonio, “Literal a1) Estructura orgánica funcional”. [En línea]. Disponible en: https://bit.ly/3jm4rTr.

[89] Ministerio de Cultura y Patrimonio, “Literal a4) Las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos”. [En línea]. Disponible en: https://bit.ly/2Gpzjns.

[90] Municipio de Quito, “*Atlas Amenazas Naturales y Exposición de Infraestructura del DMQ”*. [En línea]. Disponible en: https://bit.ly/3nkzUrw.

[91] Municipio de Quito, *PLAN ESPECIAL “LA MARISCAL”.* Quito, Ecuador, 2017. [En línea]. Disponible en: https://bit.ly/30q5k5Q.

[92] Ministerio de Cultura y Patrimonio, “Literal a2) Base legal que la rige”. [En línea]. Disponible en: https://bit.ly/3cWegF5.

[93] Ministerio de Cultura y Patrimonio, “d) Los servicios que ofrece y las formas de acceder a ellos, horarios de atención y demás indicaciones necesarias, para que la ciudadanía pueda ejercer sus derechos y cumplir sus obligaciones”. [En línea]. Disponible en: https://bit.ly/3jnWixM

[94] PILAR Basic: Análisis y Gestión de Riesgos Ayuda, 7ma ed., Ministerio de Hacienda y Administraciones Públicas., Madrid, España. [En línea]. Disponible en: https://www.pilar-tools.com/doc/help_basic_es_e_74.pdf.

[95] Ministerio de Cultura y Patrimonio, “Valores / Misión / Visión”. [En línea]. Disponible en: https://www.culturaypatrimonio.gob.ec/valores-mision-vision/.

[96] COMISIÓN NACIONAL DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA, *Política General de Seguridad de la Información, 2da ed.* Chile, 2011. [En línea]. Disponible en: https://bit.ly/2GgZuNi

[97] Ministerio de Telecomunicaciones y de la Sociedad de la Información, “FORMATO REFERENCIAL PARA LA ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN(EGSI)”. [En línea]. Disponible en: https://bit.ly/3nik6FN.

[98] Asamblea Nacional, “Política de Seguridad de la Información,” 1ra ed. Sin publicar.

[99] Emprende pyme, “Políticas de seguridad”. [En línea]. Disponible en: https://bit.ly/34kHPfJ.

[100] ISO27000, “Sistema de Gestión de Seguridad de la Información”. [En línea]. Disponible en: https://bit.ly/34wT7h9.

[101] EcuRed, “Seguridad Informática”. [En línea]. Disponible en: https://bit.ly/3jqbxpR.

[102] Universidad Internacional de Valencia, “¿Qué es la seguridad informática y cómo puede ayudarme?”. [En línea]. Disponible enhttps://bit.ly/33lEmOD

[103] V. S. Enríquez Novillo y P. A. Torrez Enríquez. “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA UN DATA CENTER TIER III DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP) TIPO, DE LA CIUDAD DE QUITO”, Proyecto, Univ. Escuela Politécnica Nacional, Quito, Ecuador,2014.

[104] OBS Business School, “Seguridad de la información, un conocimiento imprescindible”. [En línea]. Disponible en: https://bit.ly/36vFoK5

[105] Tecon Soluciones Informáticas, “La Seguridad de la Información”. [En línea]. Disponible en: https://www.tecon.es/la-seguridad-de-la-informacion/.

[106] “Seguridad Informatica”, [En línea]. Disponible en: https://seguridadinformatica233743529.wordpress.com/

[107] Digital Guide IONOS, “Aprenda a crear una contraseña segura”. [En línea]. Disponible en: https://bit.ly/3l7byQ4

[108] Universidad de Alcalá, *Política de contraseñas*. Madrid, España, 2017. [En línea]. Disponible en: https://bit.ly/3io56lK

[109] Instituto Nacional de Ciberseguridad, *Copias de seguridad: Política de seguridad para la pyme.* España. [En línea]. Disponible en: https://bit.ly/3cRFcWl

[110] W. Cifuentes y M. Dávila, PLAN DE MIGRACIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN PÚBLICA CENTRAL INSTITUCIONAL Y QUE DEPENDEN DE LA FUNCIÓN EJECUTIVA A UN CENTRO DE DATOS SEGUROPARA EL MINISTERIO DE CULTURA Y PATRIMONIO, Ministerio de Cultura y Patrimonio, Quito, Ecuador, 2020.

6 ANEXOS