ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

UNIDAD DE TITULACIÓN

EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y GENERACIÓN DEL PLAN DE GESTIÓN DE INCIDENTES. CASO DE ESTUDIO FONDO PARA LA PROTECCIÓN DEL AGUA (FONAG)

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SOFTWARE, MENCIÓN EN SEGURIDAD

PAUL VINICIO CHICAIZA CHABLA

paul.chicaiza@epn.edu.ec

Directora: Lorena Isabel Barona López, PhD.

lorena.barona@epn.edu.ec

Codirectora: Jenny Gabriela Torres Olmedo, PhD.

jenny.torres@epn.edu.ec

Septiembre, 2023

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y GENERACIÓN DEL PLAN DE GESTIÓN DE INCIDENTES. CASO DE ESTUDIO FONDO PARA LA PROTECCIÓN DEL AGUA (FONAG) desarrollado por PAUL VINICIO CHICAIZA CHABLA, estudiante de la MAESTRÍA EN SOFTWARE, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Lorena Isabel Barona López

DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Paul Vinicio Chicaiza Chabla, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Paul Vinicio Chicaiza Chabla

DEDICATORIA

Este proyecto de titulación está dedicado a toda mi familia por el apoyo incondicional que me han brindado en todas las decisiones que he tomado hasta el momento. A mi esposa, por ser la razón que me motiva a mejorar como persona y profesional; así como enfrentar nuevos retos cada día. Al FONAG por la motivación y apoyo económico para poder estudiar la presente maestría y así mejorar mi conocimiento profesional.

AGRADECIMIENTO

Al FONAG por su cooperación y apertura para la realización de este proyecto

A la PhD. Lorena Isabel Barona López por su apoyo, confianza y guía para realizar este proyecto.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

La información es uno de los activos más importantes para una organización y precautelar la seguridad de ésta, se ha convertido en uno de los objetivos de muchas instituciones que buscan reducir los impactos asociados a cualquier amenaza existente o futura. Como parte de las estrategias para asegurar la disponibilidad, integridad y confidencialidad de la información se encuentra la evaluación de riesgos, que permite determinar la probabilidad que una amenaza se materialice y calcular el nivel de impacto que causaría.

El Fondo Protección del Agua (FONAG), como cualquier otra entidad, tiene un riesgo latente de sufrir un ataque a la seguridad de la información en cualquier momento. En el año 2016, tuvo un ataque de ransomware que implicó la pérdida de información vital para el funcionamiento administrativo de la organización. Por ello se propuso ejecutar un caso de estudio que permita identificar, comprender evaluar y mitigar los riesgos a la seguridad de la información; así como generar un plan de gestión de incidencias para anticipar, resolver y documentar los incidentes que puedan presentarse en el futuro.

El presente trabajo de titulación de maestría muestra el proceso que se llevó a cabo para realizar una evaluación de riesgos dentro de la infraestructura informática del FONAG, junto con la generación de un plan de gestión de incidentes a la seguridad de la información. Para llevar a cabo este procedimiento, primero se seleccionó una metodología adecuada para el caso de estudio; segundo, se hizo una exploración del trabajo de la institución y se seleccionó el proceso más importante y crítico dentro de la estructura organizacional. Luego se aplicó las fases de la metodología MAGERIT, que permitió determinar el riesgo actual y residual de los activos de información en cuanto a la adquisición de bienes y servicios en la organización.

En términos generales el nivel de riesgo que existe dentro del proceso seleccionado es bajo, gracias a las salvaguardas que tienen implementadas hasta el momento. Sin embargo, es necesario implementar normativas y ejecutar ciertas actividades para cerrar brechas de seguridad existentes.

Palabras clave: MAGERIT, análisis de riesgos, gestión de incidencias, vulnerabilidad, amenaza, salvaguardas.

ABSTRACT

Information is considered one of the most important assets for an organization. The main objective for some institutions is to reduce the impact associated with any current or future threat. Risk assessment is a strategy to ensure the availability, integrity, and confidentiality of information. Risk assessment is used to determine the probability of a threat becoming a real problem, and to calculate the level of impact it would cause.

The Fondo Protección del Agua (FONAG), like other entities, has a latent risk of suffering an information security attack at any time. In 2016, FONAG suffered from a ransomware attack that implied the loss of vital information. Thus, it affected the administrative operation within the organization. Therefore, a case study was proposed to identify, understand, evaluate, and mitigate information security risks, and an incident management plan was generated to anticipate, resolve, and document incidents that may occur in the future.

This master's degree project shows the procedure carried out to perform a risk assessment within FONAG's IT infrastructure, and the generation of an information security incident management plan. To carry out this procedure, first, an appropriate methodology was selected for the case study; then an exploration of the institution's work was performed, and lastly, the most important and critical process within the organizational structure was selected. Finally, the MAGERIT methodology´s phases were applied, which allowed to determine the current and residual risk of the information assets in terms of the acquisition of goods and services in the organization.

In general terms, the risk level in the selected process is low, thanks to the safeguards that have been implemented so far. Nevertheless, it is necessary to implement regulations and execute certain activities to close existing security vulnerabilities.

Key words: MAGERIT, risk analysis, incident management, vulnerability, threat, safeguards.

CAPÍTULO 1. INTRODUCCIÓN

1.1 Planteamiento del Problema

En la actualidad la información es uno de los activos más importantes que maneja una empresa, tanto que la seguridad de la información determina el nivel de competitividad y productividad de la organización. Al ser la información un recurso tan valioso, cada día los ciberdelincuentes crean nuevas formas de romper las estructuras de seguridad de una organización con el afán de apoderarse de la información o dañar sus recursos tecnológicos.

Según el informe del Banco Interamericano de Desarrollo (BID) [1] , hasta el 2016 América Latina y el Caribe no había invertido la suficiente cantidad de recursos y esfuerzo en precautelar la integridad, confidencialidad y disponibilidad de la información, siendo las instituciones financieras los principales focos de ataque. Para agravar esta problemática, en el año 2020 se desató una pandemia global debido al COVID 19, marcando un antes y un después en muchas de las actividades cotidianas. Por ejemplo, tanto en empresas públicas y privadas adoptaron nuevas tecnologías para que sus empleados y miembros puedan trabajar desde sus hogares [2]. Como consecuencia, el número de usuarios inexpertos en temas de seguridad de la información aumentó vertiginosamente, lo cual propicia un ambiente de riesgos a nivel empresarial [3].

Sin embargo, hay buenas noticias, en la encuesta realizada en el año 2019 por la consultora en seguridad MARSH, el 73% de las organizaciones en Latinoamérica clasificó el riesgo cibernético como una de las cinco principales preocupaciones para su organización, frente al 47% del 2017. Adicionalmente, el 62% de los encuestados menciona que un ataque cibernético sería el principal motivo para incrementar su inversión en seguridad de la información [4].

En este contexto, la revista de tecnología iTahora, junto con la consultora Deloitte y la Asociación Ecuatoriana de Ciberseguridad (AECI), realizaron un sondeo en el 2020 [5], para conocer el estado actual de la Ciberseguridad en el país. La encuesta consistió en 10 preguntas realizadas a 100 empresas, de seis sectores estratégicos: i) Banca y Seguros, ii) Comercio, iii) Manufactura, iv) Servicios y Tecnología, v) Salud/Energía y vi) otros sectores (Educación, Turismo, Telecomunicación, Automotriz y Sector Público). Las áreas que se analizaron en este estudio fueron: estrategia y gobierno, prevención de riesgos, vigilancia del ciber espacio y respuesta ante amenazas. Dentro de la sección de vigilancia, una de las preguntas de la encuesta está enfocada en el monitoreo del ciber-espacio para identificar las amenazas a las que están expuestas las empresas. El

56% de los encuestados realizan un análisis de las amenazas de seguridad existentes, pero solo el 34% cuenta con un plan de gestión de incidentes [5]. Como se puede apreciar hay un porcentaje importante de organizaciones que requieren ayuda para realizar una evaluación de riesgos y generar un plan de gestión de las interrupciones de los servicios de TI y dentro de este grupo se encuentra el Fondo para la Protección del agua (FONAG).

El FONAG es un fideicomiso mercantil ambiental creado el 25 de enero del 2000 con el fin de garantizar agua en calidad y cantidad a más de 2,5 millones de habitantes en el Distrito Metropolitano de Quito. El FONAG se ha caracterizado por ser una organización que adopta e implementa tecnologías constantemente, con la finalidad de agrupar, clasificar y publicar la información que genera periódicamente.

Desde el 2011, el FONAG ha implementado diferentes aplicativos webs y de escritorio que permiten gestionar toda la información que genera la institución y ayudar en el control del presupuesto anual. Sin embargo, en sus inicios no se implementaron mecanismos robustos para salvaguardar la seguridad de la información y como consecuencia en el año 2016, el FONAG sufrió un ataque de ransomware que afectó a varios computadores de los puestos directivos más importantes de la organización. Al no contar con respaldos la pérdida fue significativa e implicó la adopción de medidas inmediatas para prevenir futuros ataques. A raíz de este incidente se implementó un sistema de respaldos y un firewall físico con la intención de precautelar toda la información generada por el personal de la institución. No obstante, es necesario invertir mayores esfuerzos en identificar, comprender, evaluar y mitigar los riesgos a la seguridad de la información. Con este antecedente se busca realizar una evaluación de riesgos de la seguridad de la información y generar un plan para la gestión de incidentes para los servicios de TI con la finalidad de mitigar los impactos asociados a los activos de información, el cual es el principal objetivo de este trabajo de titulación.

1.2 Justificación

Este trabajo de titulación busca evaluar las amenazas y vulnerabilidades a la seguridad de la información del FONAG basado en una metodología de gestión de riesgos. Con el resultado de la evaluación se pretende generar un plan de gestión de incidentes para los servicios de TI.

1.2.1 Justificación Teórica

Dado que el FONAG está adoptando nuevas tecnologías de manera constante, existe la posibilidad de que se generen brechas en la seguridad de la información. Por esto es importante implementar una metodología de evaluación de riesgos con el objetivo de controlar y asegurar la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) dentro del ámbito tecnológico. Dentro del análisis y evaluación de riesgos se pueden encontrar varias metodologías que ayudan a las organizaciones a proteger su información, a recuperarse ante una pérdida de información crítica (afectación en la continuidad del negocio) y/o cumplir con normativas locales. Entre las metodologías que permiten realizar lo mencionado anteriormente están MAGERIT, OCTAVE, NIST SP 800:30 e ISO 27005-IS03001 [6], las cuales se detallan a continuación:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT) ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación [7]. Esta metodología fue desarrollada con el objetivo de conocer el estado de seguridad de los sistemas de información, implementar medidas de seguridad y garantizar que no haya elementos del sistema de gestión de seguridad de la información (SGSI) que se queden fuera del análisis. Adicional, permite prepararse para procesos de auditorías, certificaciones y acreditaciones, complementándose con ISO 27001 [8].
- Evaluación operativa de amenazas, activos y vulnerabilidades (OCTAVE) está centrado en la evaluación de riesgos de seguridad de la información y como producto final se obtiene un plan de mitigación. La metodología equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para tener los insumos necesarios para la toma de decisiones a nivel empresarial [9].
- Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información NIST SP800:30, proporciona las pautas para llevar a cabo cada uno de los pasos del proceso de evaluación de riesgo. Adicionalmente, permite identificar factores de riesgo para realizar un monitoreo constante, lo cual permite determinar si los niveles de riesgo han superado los niveles aceptables y poder ejecutar acciones correctivas [10].
- Gestión del riesgo de seguridad de la información ISO27005 es una norma que describe las directrices para el desarrollo del contexto de evaluación de riesgos, la comunicación y el tratamiento los mismos. Sin embargo, no proporciona una metodología para determinar la naturaleza y el impacto del riesgo real [11].

Una vez que se seleccione la metodología de gestión de riesgos, que se mejor se adapte al caso de estudio, se seguirán las siguientes subfases:

- Identificar la información organizacional
- Crear el perfil de amenazas
- Examinar la infraestructura
- Identificar y analizar los riesgos
- Elaborar la estrategia de protección y planes de mitigación

Las subfases mencionadas se aplican a un modelo de gestión de riesgos orientado a las Pequeñas y Medianas Empresas (PYMES), el cual analiza y considera distintos marcos de trabajo como: la Guía de los Fundamentos para la Dirección de proyectos (PMBoK), ISO 27000, Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT), ISO 31000, NIST entro otros, con la finalidad de simplificar y sistematizar el análisis, identificación y tratamiento de riesgos asociados a los activos de información [12].

1.2.2 Justificación Metodológica

El Estudio de Caso es una metodología de investigación que permite analizar un fenómeno en su contexto real, usando diversas fuentes de evidencia que pueden ser cuantitativas y/o cualitativas [13]. El Estudio de Caso resalta entre las metodologías de tipo cualitativo porque permite medir y registrar la realidad del fenómeno estudiado, mientras que los métodos cuantitativos solo se centran en la información obtenida de las encuestas [14]. En [15] se detalla una guía basada en tres condiciones para determinar cuándo se debe aplicar el Estudio de Caso como metodología de investigación. Estas condiciones son: i) si se busca resolver preguntas del tipo “cómo” o “por qué”, ii) si el investigador tiene poco control sobre el fenómeno y iii) si el tema de estudio está dentro de las tendencias actuales. Por tanto, en el presente trabajo de investigación se utilizará el Estudio de Caso ya que cumple con las tres condiciones mencionadas anteriormente.

1.2.3 Justificación Práctica

El FONAG es una institución que genera información constantemente con la intención de facilitar la toma de decisiones a las personas e instituciones involucradas en la gestión del recurso hídrico. Asegurar la confidencialidad, integridad y disponibilidad de esta data es de vital importancia para mantener el prestigio que ha ganado a lo largo de su historia. Por esta razón, se hace necesario realizar una evaluación de riesgos de

seguridad de la información y elaborar un plan de gestión de incidencias con el fin de mitigar los impactos asociados a los activos de información.

1.3 Objetivo General

Evaluar los riesgos de seguridad de la información y generar el plan de gestión de incidencias para los servicios de TI. Caso de Estudio Fondo para la Protección del Agua (FONAG)

1.4 Objetivos Específicos

- Analizar y comparar las diferentes metodologías de evaluación de riesgos de seguridad de la información para determinar la que mejor se adapta la realidad del FONAG.
- Determinar la situación actual del FONAG para definir el alcance del plan de gestión de riesgos en el cual se estudiará las amenazas, activos de la información, vulnerabilidad y riesgos de la institución.
- Implementar la metodología de evaluación de riesgos enfocado en las necesidades de protección de los activos y la información del FONAG.
- Proveer un plan de gestión de incidencias considerando los recursos disponibles del FONAG, para los servicios de TI existentes.

CAPÍTULO 2. MARCO TEÓRICO

En esta sección se describe la terminología utilizada dentro de este documento para ayudar a la comprensión y entendimiento del presente trabajo de titulación.

2.1 Fundamentos Seguridad de la información

La “seguridad de la información” es un tema complejo, que se centra en la protección de la información de las amenazas existentes, con el objetivo de garantizar la continuidad del negocio, minimizar los riesgos que puedan comprometerla, y maximizar el retorno sobre la inversión. Para lograrlo es necesario la implementación de un conjunto de controles: políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software [11].

Esta definición da introducción a tres conceptos principales dentro de la seguridad de la información: Confidencialidad, Integridad y Autenticidad (CIA) [16].

- Confidencialidad: Establecer mecanismos de acceso para usuarios autorizados y evitar la divulgación de la información, que incluye la privacidad de las personas e información propietaria.
- Integridad: Proteger la información de modificaciones o destrucciones indebidas, esto incluye garantizar su autenticidad y el no repudio.
- Disponibilidad: Garantizar el acceso oportuno y fiable a la información. Evitar la interrupción de acceso o uso de la información.

Si bien el uso de la tríada del CIA sirve para definir los objetivos de la seguridad de la información, algunos consideran que debe complementarse con dos conceptos adicionales: los cuales son [16]:

- Autenticidad: Otorgar validez de una transmisión al garantizar que el emisor y el receptor son quienes dicen ser y cada entrada al sistema provenga de una fuente de confianza.
- Trazabilidad: Tener la capacidad de rastrear una violación de la seguridad hasta una entidad responsable. Es decir, los sistemas deben llevar un registro auditable para un posterior análisis forense.

En la Figura 1 se muestra un diagrama de relación entre las cinco dimensiones de seguridad que se describieron en los párrafos anteriores.

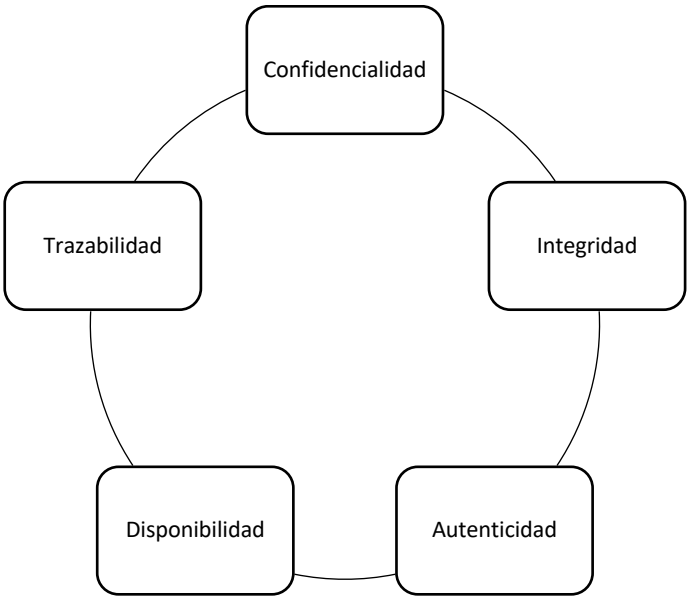

Figura 1. Dimensiones de seguridad. [16]

2.2 Familia de Normas ISO 27000

La serie ISO/IEC 27000, es una familia de normas que brindan una guía para la implementación de un sistema de gestión de la seguridad de la información. Fue propuesta por la International Organization for Standardization (ISO) y la International Electrotechnical Commision (IEC) y contiene las definiciones y términos sobre conceptos técnicos y de gestión, con la finalidad de facilitar la revisión de las demás normas existentes. Se compone de 17 normas clasificadas en cuatro categorías [17] las cuales se detallan a continuación (Figura 2):

Figura 2. Categorías y Normas ISO27000. [17]

De las 17 normas listadas en la Figura 2, cuatro se centran en la implementación de un SGSI, tal como se detalla a continuación [17]:

- ISO/IEC 27001: Establece los requisitos para implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.
- ISO/IEC 27002: Ofrece los controles y evaluaciones relacionados a la seguridad de la información. Se encuentra organizada en 14 dominios, 35 objetivos de control y 114 controles.
- ISO/IEC 27003: Establece las especificaciones y el diseño de un SGSI basado en la ISO/IEC 27001. Además, se detalla el uso del ciclo: Plan, Do, Check, Act (PDCA).
- ISO/IEC 27005: Proporciona directrices de la gestión del riesgo en la seguridad de la información. Es una norma de apoyo a los conceptos generales detallados en la ISO 27001.

2.3 Sistemas de seguridad de la información

Un SGSI permite asegurar el manejo adecuado de los activos de una empresa y evitar las fugas de información.

2.4 Metodologías de Evaluación de Riesgos

Para gestionar los riesgos de seguridad es preciso definir qué es un riesgo, la magnitud (impacto) de los daños causados por la amenaza, las causas o eventos con el potencial de causar daños a la infraestructura tecnológica, y qué hacer ante el riesgo. La evaluación de las amenazas y riesgos constituye un mecanismo para gestionar los riesgos. Otros mecanismos para gestionar los riesgos serían la educación y creación de conciencia, políticas de seguridad, normas operativas y documentación técnica. En la Figura 3 se puede apreciar la relación que existe entre el análisis, el tratamiento y la gestión de riesgos.

Figura 3. Gestión de riesgos. [Elaboración propia]

MAGERIT es una metodología desarrollada con el objetivo de i) conocer el estado de la seguridad de los sistemas de información, ii) implementar medidas de seguridad y iii) garantizar que no haya elementos del SGSI que se queden fuera del análisis. Adicionalmente, MAGERIT permite prepararse para procesos de auditorías, certificaciones y acreditaciones, complementándose con la norma ISO 27001 [8]. Según [7], la metodología MAGERIT abarca cuatro objetivos:

- Concientizar a los responsables de la información dentro de las organizaciones, la existencia de los riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación.

MAGERIT se centra en encontrar las amenazas, vulnerabilidades y calcular en qué nivel afectarían a una organización. MAGERIT ayuda a tener un panorama de las medidas preventivas y correctivas que deben aplicarse en una empresa. Las fases de MAGERIT se pueden apreciar en la Figura 4:

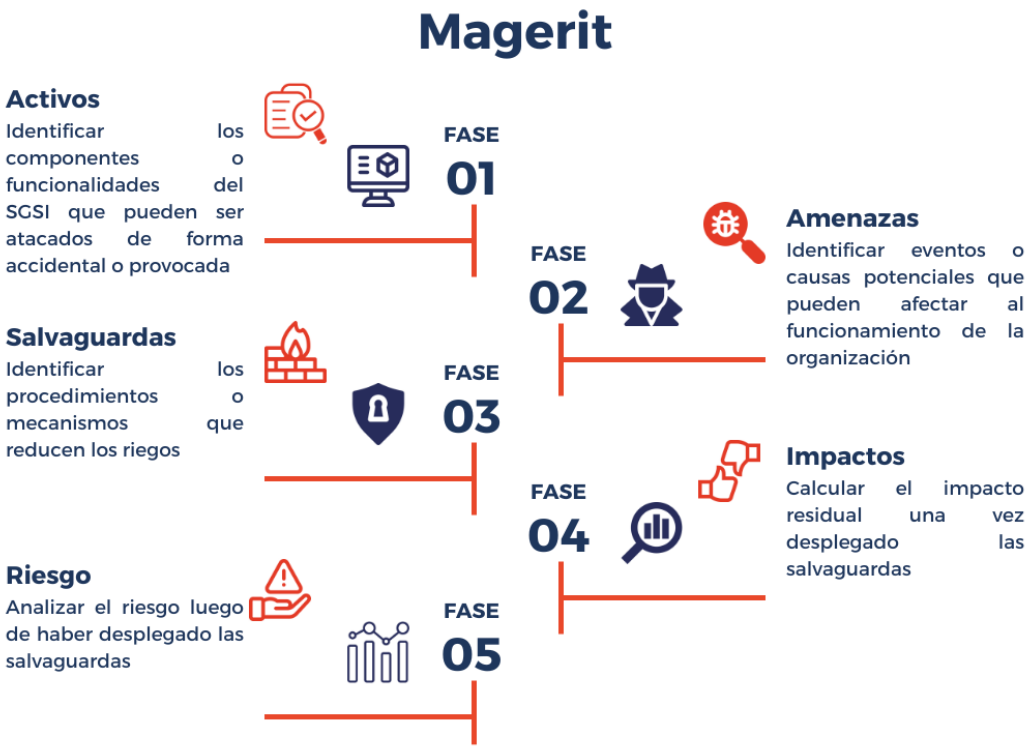

Figura 4. Fases de Magerit. [7]

OCTAVE está centrado en la evaluación de riesgos de seguridad de la información y cómo producto final se obtiene un plan de mitigación. La metodología equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para tener los insumos necesarios para la toma de decisiones a nivel empresarial [9]. La metodología OCTAVE se desarrolló en la Universidad Carnegie Mellon de Pensilvania en los Estados Unidos, específicamente en el Centro de Coordinación del Instituto de Ingeniería de Software. Según [9], la metodología tiene cuatro características principales, las cuales son:

- Identificar información prioritaria acerca de los activos
- Centrar el análisis de riesgos en los activos críticos para la organización
- Considerar las relaciones entre los activos críticos, las amenazas y vulnerabilidades
- Evaluar el riesgo en el contexto operacional
- Crear estrategias de protección basadas en la práctica y planes de mitigación para reducir el riesgo de seguridad a los activos críticos.

La metodología OCTAVE se centra en definir los aspectos de riesgos operativos y las prácticas de seguridad. Esto significa que las decisiones relacionadas a la protección de la información de las empresas y las organizaciones se basan en el análisis a la infraestructura tecnológica con base a las diferentes prácticas de seguridad. La metodología OCTAVE cuenta con tres fases y ocho procesos las cuales se pueden apreciar en la Figura 5.

Figura 5. Fases Metodología Octave. [9]

La **NIST SP800:30** proporciona las pautas para llevar a cabo cada uno de los pasos del proceso de evaluación de riesgo. Adicionalmente, permite identificar factores de riesgo para realizar un monitoreo constante, lo cual permite determinar si los niveles de riesgo han superado los niveles aceptables y poder ejecutar acciones correctivas [10]. La norma define el proceso de gestión de riesgo en cuatro componentes:

- Marco: contar una estrategia de administración de riesgo que describa como: evaluar, responder y monitorear el riesgo
- Evaluación: identificar amenazas, vulnerabilidad (internas y externas), daño potencial y probabilidad de ocurrencia
- Respuesta: proporcionar una respuesta coherente a nivel de toda la organización al riesgo de acuerdo con la estrategia de administración de riesgo.
- Monitoreo: Determinar la eficacia de las respuestas, identificar el impacto ante cambios en sistemas de información y verificar que los requisitos de seguridad se implementen.

Los pasos de la metodología NIST se pueden apreciar en la Figura 6.

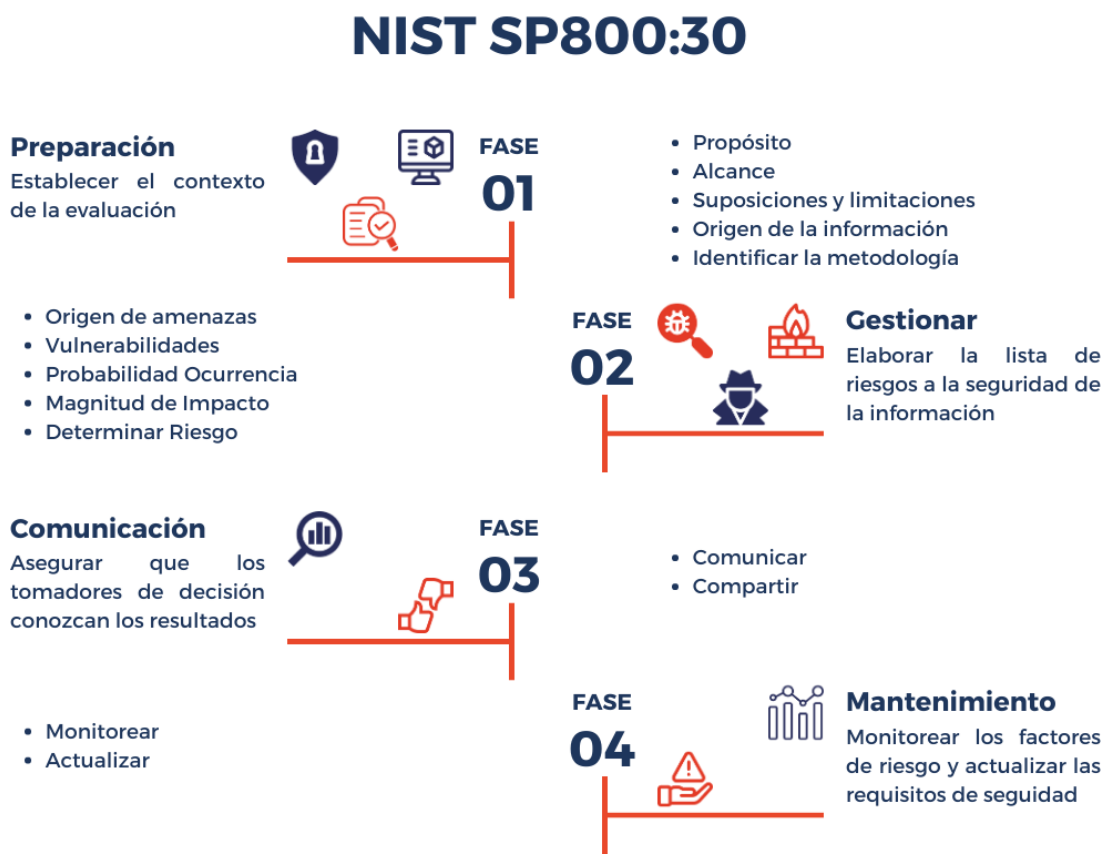

Figura 6. Proceso NIST SP 830. [10]

La **ISO27005** es una norma que describe las directrices para el desarrollo del contexto de evaluación de riesgos, la comunicación y el tratamiento los mismos. Sin embargo, no proporciona una metodología concreta para determinar la naturaleza y el impacto del riesgo real [11] . En su lugar describe, en forma de cláusulas, el proceso que se recomienda seguir para analizar el riesgo. La metodología se puede apreciar de manera gráfica en la Figura 7.

Figura 7. Fases Norma ISO 27005. [11]

La norma ISO 27005 permite establecer los diferentes elementos que debe incluir toda la metodología de análisis de riesgos. La norma incluye 6 anexos diferentes que van desde la A hasta la F, los cuales son de carácter informativo y no normativo. Además, la norma proporciona orientación para realizar la identificación de activos e impactos; ciertos ejemplos de vulnerabilidad y las amenazas que se pueden asociar y diferentes aproximaciones para realizar el análisis de riesgos.

2.5 Comparación de Metodologías

Como parte de este proyecto se hará una breve comparación de las metodologías mencionadas para determinar la que mejor se adapta al proyecto. En [8] hace un estudio comparativo entre OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS Y NIST SP 800-30, al cual se complementará la comparación con ISO 27005.

La comparación se basa en cinco criterios: fases o etapas, tipos de enfoque (cualitativo, cuantitativo y/o mixto), tipo de riesgo (intrínseco, efectivo y/o residual), elementos de análisis (activos, vulnerabilidades, entre otros) y objetivos (autenticidad, integridad, confidencialidad, disponibilidad, responsabilidad).

2.5.1 Fases o etapas de cada metodología

En la Tabla 1 se presentan las fases o pasos que componen cada una de las metodologías mencionadas anteriormente.

Tabla 1. Comparación metodologías/normas por fases o etapas. [Elaboración propia]

MAGERIT	OCTAVE	NIST SP800:30	ISO 27005
Definir el alcance	Identificar el conocimiento de la empresa	Caracterizar el sistema	Establecer el contexto
Identificar los activos	Identificar el conocimiento del área operativa	Identificar amenazas	Evaluar el riesgo
Identificar las amenazas	Identificar el conocimiento del personal	Identificar vulnerabilidades	Tratar el riesgo
Identificar salvaguardas	Crear perfiles de amenaza	Analizar controles	Aceptar el riesgo
Evaluar el riesgo	Identificar componentes clave	Determinar probabilidad	Comunicar el riesgo
Tratar el riesgo	Evaluar componentes	Analizar impacto	Monitorear y revisar el riesgo
	Analizar el riesgo	Determinar el riesgo	
	Desarrollar estrategia de protección	Recomendar controles	
		Documentar Resultados	

En esta comparación se puede apreciar que MAGERIT tiene menos fases para lograr la evaluación y tratamiento de los riesgos, alineados con la ISO 27005 y con la gran ventaja que detalla cómo implementar cada una de ellas.

2.5.2 Tipo de enfoque de cada metodología

La segunda comparación (Tabla 2) se basa en el tipo de enfoque que abordan las metodologías o normas, entre los cuales se definieron tres categorías:

- Cualitativo: Evaluar la probabilidad de los riesgos identificados para determinar su magnitud y prioridad, utilizando escalas de valor (alto, medio, bajo). Este enfoque generalmente se aplica en casos que el tiempo y los recurso son limitados [18].
- Cuantitativo: Asignar valores de ocurrencia a los riesgos identificados. Se considera que este enfoque sucede al análisis cualitativo [19].
- Mixto: Aplicar los dos tipos de análisis de manera separada o simultanea dependiendo el tipo de proyecto.

Tabla 2. Comparación metodologías/normas por tipo de enfoque. [Elaboración propia]

	MAGERIT	**OCTAVE**	**NIST SP800:30**	**ISO 27005**
Cualitativo				
Cuantitativo				
Mixto	X	X	X	X

Todas las metodologías y normas objeto de estudio utilizan un enfoque mixto combinando las técnicas cuantitativas y cualitativas. Por un lado, se manejan técnicas estadísticas para medir los riesgos y por otro lado se utiliza un enfoque basado en la experiencia y juicio de expertos para evaluar los riesgos.

2.5.3 Tipo de riesgo de cada metodología

El tercer punto de comparación fue el tipo de riesgo (Tabla 3) que aborda cada metodología/norma. Para este análisis se utilizaron los siguientes riesgos:

- Riesgo intrínseco: es la probabilidad que una amenaza explote una vulnerabilidad de un sistema de información. Está influenciado por la naturaleza y la magnitud de los riesgos asociados con los recursos, el entorno y la actividad humana.
- Riesgo residual: es el riesgo que queda una vez que se han tomado las medidas de seguridad necesarias(salvaguardas) para mitigar el riesgo intrínseco.
- Riesgo efectivo: es el riesgo resultado de la suma del riesgo intrínseco y el riesgo residual.

Tabla 3. Comparación metodologías/normas por tipo de riesgo. [Elaboración propia]

	MAGERIT	OCTAVE	NIST SP800:30	ISO 27005
Intrínseco	X		X	X
Efectivo	X	X	X	X
Residual	X		X	X

MAGERIT, NIST SP800-30 e ISO 27005 se centra en la gestión de riesgos en general, abarcando la identificación, evaluación y tratamiento de riesgos. Por otro lado, OCTAVE se centra en la evaluación de riesgos efectivos.

2.5.4 Elementos de análisis de cada metodología

En la Tabla 4, se comprarán los principales elementos que intervienen en un análisis de riesgos, entre las diferentes metodologías/normas objeto de estudio.

Tabla 4. Comparación metodologías/normas por elementos de análisis. [Elaboración propia]

	MAGERIT	OCTAVE	NIST SP800:30	ISO 27005
Activos	X	X	X	X
Vulnerabilidades	X	X	X	X
Amenazas	X	X	X	X
Controles	X	X	X	X
Procesos	X			
Alcance			X	
Probabilidad			X	

En términos generales, todas las metodologías/normas objeto de estudio se centran en la identificación y valoración de activos; evaluación de vulnerabilidades; identificación y valoración de amenazas; y el levantamiento de controles para mitigación de controles; pero cada una tiene un enfoque ligeramente diferente y varios niveles de detalle y profundidad. MAGERIT destaca del resto porque tiene un proceso establecido para realizar todas las actividades descritas, esto se puede apreciar en la documentación oficial, donde detalla el método, los elementos y la guía de técnicas que se pueden aplicar para hacer un análisis de riesgos.

2.5.5 Objetivos de cada metodología

En la Tabla 5 se analiza las dimensiones de seguridad(objetivos) que aborda cada norma/metodología dentro del proceso de análisis de riesgos.

Tabla 5. Comparación metodologías/normas por objetivos. [Elaboración propia]

	MAGERIT	**OCTAVE**	**NIST SP800:30**	**ISO 27005**
Autenticidad	X			
Integridad	X	X	X	X
Confidencialidad	X	X	X	X
Disponibilidad	X	X	X	X

En resumen, todas estas metodologías/normas se enfocan en garantizar la autenticidad, integridad, confidencialidad y disponibilidad, pero cada una de ellas tiene un enfoque ligeramente diferente en términos de objetivos específicos.

Como elemento adicional se realizó una comparación de los ámbitos de aplicación de cada metodología/norma (Tabla 6) para ayudar a definir aquella que se ajusta de mejor manera a las necesidades del FONAG. Para este caso de estudio, la institución requiere gestionar la seguridad de la información y como primer paso se quiere hacer el análisis de riesgos.

Tabla 6. Comparación ámbitos de aplicación. [Elaboración propia]

MAGERIT	**OCTAVE**	**NIST SP800:30**	**ISO 27005**
Cualquier organización, grande o pequeña, que necesite **gestionar** la seguridad de la información.	Organizaciones de cualquier tamaño y sector que deseen **evaluar y mejorar** su capacidad de respuesta ante incidentes de seguridad de la información.	Cualquier organización que desee llevar a cabo una **evaluación** de riesgos a la seguridad de la información.	Cualquier organización que desee **mejorar** la **gestión** de la **seguridad** de la información

Es importante mencionar que hasta el momento no se ha realizado ninguna evaluación en cuanto a la seguridad de la información y MAGERIT facilita dar el primer paso para identificar los impactos y riesgos a los que se encuentran expuestos los activos de la información, con un enfoque cualitativo y cuantitativo como consta en la Tabla 2; gracias a los métodos y formatos que constan en los tres libros de la metodología.

Magerit al permitir determinar los riesgos efectivo y residual, como se muestra en la Tabla 3 ayuda a tener un panorama bastante claro sobre la situación actual y determinar las salvaguardas que se podríam implementar en el FONAG. El nivel de detalle que describe la metodología Magerit (Tabla 4) para cada elemento de análisis, es el adecuado si se considera el tiempo y el alcance del proyecto

Finalmente, en la

Tabla **5** se evidencia que MAGERIT garantiza la autenticidad, confidencialidad y disponibilidad; y como consta en la Tabla 6 se muestra que el objetivo es gestionar la seguridad de la información. Estas dos acciones están alineadas con el interés institucional de proteger la infraestructura tecnológica del FONAG.

CAPÍTULO 3. SITUACIÓN ACTUAL FONAG

3.1 Aspectos Generales

3.1.1 Historia

En el año 1997, la Fundación Antisana, The Nature Conservancy (TNC) y La Agencia de los Estados Unidos para el Desarrollo Internacional (USAID), proponen a la Empresa Pública Metropolitana de Agua Potable y Saneamiento de Quito (EPMAPS) la creación de un fondo conjunto que contemple la participación voluntaria de usuarios del agua, con el objetivo de financiar proyectos de conservación y gestión de las cuencas hidrográficas. En el año 1998, se lanzó formalmente la propuesta gracias al apoyo político del alcalde de la ciudad, junto con el liderazgo técnico de las organizaciones mencionadas. Sin embargo, la inestabilidad política que vivía el Ecuador en esa época, así como otros factores, retrasaron su conformación oficial hasta el 2000.

FONAG nace el 25 de enero del año 2000, bajo la figura de fideicomiso mercantil de administración privada. Denominado legalmente "Fideicomiso Fondo Ambiental para la Protección de las Cuencas y Agua FONAG" cuenta con un patrimonio independiente de sus constituyentes originarios y adherentes. Los constituyentes originarios son la Empresa Pública Metropolitana de Agua Potable y Saneamiento y The Nature Conservancy, quienes realizaron un primer aporte de USD 20.000 y USD 1.000 respectivamente. Mediante contratos de adhesión, la Empresa Eléctrica Quito (EEQ) (2001), la Cervecería Nacional (CN) S.A (2003), la Agencia Suiza para el Desarrollo y Cooperación (COSUDE) (2005), y The Tesalia Springs Company S.A. (2007) se incorporaron como constituyentes adherentes.

En sus inicios FONAG se constituyó como un fondo patrimonial—el 100% de sus ingresos se destinaban a la capitalización y únicamente los réditos financieros eran invertidos en los programas. Esto significó que los primeros años, el Fondo no dispuso de recursos para implementar acciones, sino hasta contar con rendimientos suficientes como para financiarlas. A partir del 2011, una segunda reforma a la escritura del Fideicomiso señala que además de los rendimientos se podrá gastar hasta el 30% de lo efectivamente aportado anualmente por la EPMAPS - Agua de Quito, TNC y EEQ, montos que serán incluidos en el presupuesto anual.

En el 2012, la institución empieza su incursión en el desarrollo de aplicativos propios que le permitan gestionar y administrar la información hidroclimática generada con el objetivo de conocer el comportamiento de las cuencas hidrográficas. La primera versión de este programa denominada Sistema de Estandarización de Datos (SEDC), fue de

escritorio y permitía estandarizar y validar todos los datos tomados in situ de las estaciones hidrológicas, climáticas y meteorológicas.

Cuatro años después (2016), debido al crecimiento vertiginoso de la información y la evolución de la tecnología, se lanza una versión web que permite compartir los datos con todos los actores estratégicos y los usuarios interesados, de manera simple y efectiva. En la actualidad, el sistema con varias funciones adicionales y alberga otro tipo de información con el objetivo de ayudar a los tomadores de decisiones.

A la par de la evolución del primer sistema, en el 2018 se evidenció la necesidad de compartir la información cartográfica que generaba el FONAG, junto con los estudios que llevaba a cabo de manera particular o en conjunto con otros actores. Es así que en el 2019 se implementó un repositorio geográfico y documental, junto con un visor geográfico que permitía visualizar toda esta información de manera interactiva y amigable con el usuario.

Para el 2019, se hace evidente el desarrollo de un aplicativo propio que permita administrar, controlar y reportar los gastos que realiza la institución en la adquisición de bienes y servicios en pro de cumplir su principal objetivo. Dos años después se lanzó la primera versión del programa, facilitando algunas actividades al personal técnico y administrativo del FONAG. Cada una de las implementaciones de software llevadas a cabo en el FONAG han respondido a la necesidad de facilitar la gestión de la información y compartir los datos con todos los usuarios del agua.

La misión del FONAG es facilitar, en alianza con instituciones y actores locales, la protección de las cuencas hídricas que abastecen de agua al Distrito Metropolitano de Quito, a través de un mecanismo financiero que ejecuta programas y proyectos de conservación, restauración ecológica y educación ambiental, para una nueva cultura del agua y gestión integrada de los recursos hídricos.

3.2 Estructura Orgánica

3.2.1 Diagrama Organizacional

El FONAG tiene como su instancia máxima de toma de decisión a la Junta del Fideicomiso, la misma que está conformada por los constituyentes originarios y adherentes. Entre sus funciones está definir las políticas y principios que deberá seguir la Secretaría Técnica. De igual forma, esta instancia debe conocer los informes anuales de evaluación, ejecución y presupuesto presentados por el nivel ejecutor - Secretaría Técnica. La Junta se reúne de manera ordinaria cada tres meses y de manera extraordinaria cuando se requiera [20].

Para la administración del Fideicomiso se firmó un contrato con una fiducia privada, que se encarga de la recaudación, manejo de los recursos financieros y además funge de representante legal. El nivel operativo es ejercido por una Secretaría Técnica que es la encargada de ejecutar estrategias y programas, poner en marcha las decisiones de la Junta, y consolidar la institucionalidad del Fondo. En la Figura 8 se muestra de manera gráfica el funcionamiento del FONAG y como se interrelacionan los niveles: directivo, ejecutor y administrativo.

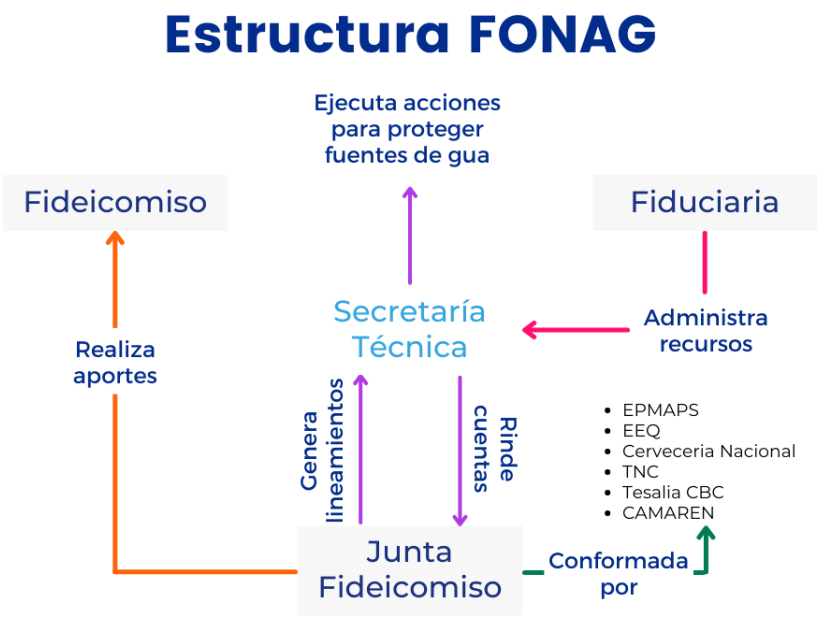

Figura 8 - Estructura FONAG. [20]

En la práctica la Secretaría Técnica es una entidad autónoma e independiente, conformada por 61 personas entre guardapáramos, técnicos ambientales, hidrólogos, educadores, administrativos, investigadores-- con capacidad de desarrollar planes operativos, ejecutar las acciones, monitorear avances, y rendir cuentas a la Junta sobre el cumplimiento de sus actividades. Plan Estratégico 2021-2025

El Plan Estratégico 2021-2025 (Figura 9) cuenta con dos objetivos, el primero relacionado directamente con el mandato de FONAG y el segundo, de soporte, que permite el correcto desempeño y funcionamiento institucional. Por cada objetivo existen estrategias soportadas por líneas de acción que tienen metas claras para un periodo de 5 años. Además, el Plan incluye una serie de actividades macro que están dentro de cada línea de acción, éstas son las guías para la estructura de los Planes Operativos Anuales para los próximos 5 años [21].

Figura 9. Estructura plan estratégico FONAG 2021-2025. [20]

3.3 Análisis de Situación Actual

Con base a las acciones macro y las líneas de acción, cada año se estructura el plan operativo anual donde se asigna un tiempo y presupuesto para la ejecución de diversas actividades y tareas que permitan cumplir con los objetivos del plan estratégico. Entre las principales líneas de acción que se llevan a cabo en la organización se tienen los siguientes:

- Generación de Información hidroclimática y calidad de agua
- Creación de acuerdos de conservación
- Restauración activa en zonas degradadas en áreas de importancia hídrica (Predios EPMAPS, zonas comunitarias y privadas)
- Educación ambiental no formal dirigida a la comunidad educativa

Las cuatro acciones mencionadas, se ejecutan con la ayuda de aplicaciones web para facilitar la administración de los datos, procesamiento de la información y respaldar la toma de decisiones de los altos mandos.

3.3.1 Acciones Principales

Generación de información hidroclimática y calidad de agua

El FONAG cuenta con una red de estaciones hidroclimáticas conformada por 119 estaciones que generan datos con una frecuencia promedio de cinco minutos, para diversas variables (precipitación, temperatura del aire, humedad del aire, entre otras). Por otro lado, el monitoreo de la calidad del agua considera registros frecuentes, no continuos, de variables físico - químicas de calidad de agua que constatan el estado sanitario de las fuentes de agua y tienen potencial para investigación de la calidad natural de los ecosistemas fuentes de agua. Como parte del monitoreo hidrológico y de calidad de agua se incluye el seguimiento al impacto que genera la restauración de humedales, en los cuales se mide de forma general, nivel freático y carbono orgánico disuelto [21]. Todo este monitoreo genera gran cantidad de datos, para lo cual se desarrolló una plataforma web para el manejo y administración de datos hidroclimáticos, calidad de agua y monitoreo de impacto en humedales.

Creación de acuerdos de conservación

Los acuerdos parten del principio de corresponsabilidad urbano-rural para la protección del agua, su sentido es generar puntos en común con respecto a visiones, alternativas y acciones que permitan reducir presiones que afectan la disponibilidad y gobernanza del agua. Los acuerdos actúan sobre los conflictos generados por procesos históricos de exclusión campo-ciudad, y surgen de la comprensión de relaciones y procesos a través de los cuales las ciudades aseguran su acceso al agua y las comunidades mejoran sus condiciones de vida.

El acuerdo es un documento vinculante, que narra el proceso, expone el sustento legal y detalla los compromisos y responsabilidades de las partes. El documento define el área que será destinada a conservación denominado “compromiso de sostenibilidad” y

señala los proyectos y acciones que se realizarán en el marco de este compromiso. Todas las acciones que realizará FONAG son valoradas, así como la contraparte que brindará la comunidad [21]. Para lograr la firma de un acuerdo, se levanta gran cantidad de información que respalda los compromisos y responsabilidades asumidos por ambas partes, esto implica que todos estos documentos deben guardarse de manera segura y confiable.

Restauración activa en zonas degradadas en áreas de importancia hídrica (Predios EPMAPS, zonas comunitarias y privadas)

La restauración activa consiste en la implementación de diversas estrategias que dependen del estado de degradación de los ecosistemas fuentes de agua. Esto implica la siembra de plantas en lugares desprovistos de vegetación, el enriquecimiento en zonas que necesitan incorporar un mayor número de especies según el ecosistema de referencia, o la restauración biofísica en lugares donde el estado de degradación es más severo [21]. Todas las restauraciones se registran en una base de datos cartográfica que luego se publica en un repositorio digital. Con esto se puede visualizar de manera visual las intervenciones del FONAG en territorio dentro de los ecosistemas degradados y realizar análisis en un futuro.

Educación ambiental no formal dirigida a la comunidad educativa

El programa de educación ejecuta diferentes intervenciones en la comunidad con el objetivo de concientizar a la población sobre la importación del cuidado de las fuentes de agua. Todas las acciones se evalúan con mecanismos pedagógicos específicos para conseguir un resultado lo más real posible acerca de los conocimientos y percepciones de la comunidad. Para el 2021, se inició la implementación de un sistema de evaluación que permita almacenar, procesar y analizar toda la información generada por los educadores, con la finalidad de facilitar el trabajo y evaluar los cambios en el tiempo.

3.3.2 Procesos administrativos

Para la consecución del plan operativo anual, el personal del FONAG requiere adquirir una gran cantidad de bienes y servicios bajo ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP), lo cual demanda una gran cantidad de esfuerzo y recursos en el cumplimiento de la normativa. Por ello desde el 2020, se implementó un sistema de control presupuestario (SCPF) para apoyar en el manejo presupuestario con

base a un proceso macro, establecido dentro del FONAG para la adquisición de bienes y servicios.

Todo las actividades y tareas que involucra gasto del presupuesto deben ser revisadas y reguladas por el área administrativa financiera, para que pueda garantizar el cumplimiento de la LOSNCP. Por esta razón, se seleccionó el proceso de adquisición de bienes y servicios, para realizar el análisis de riesgos propuesto en los objetivos específicos.

CAPÍTULO 4. ANÁLISIS DE RIESGOS

Para lograr mejorar y fortalecer la seguridad de la información de la infraestructura tecnológica del FONAG, se seguirán las actividades planteadas en la metodología MAGERIT (proceso de adquisición de bienes y servicios). Las actividades son las siguientes:

1. Identificar y valorar los activos de información del FONAG
2. Identificar y valorar las amenazas a las que están expuestos estos activos de información
3. Identificar las salvaguardas actuales con las que cuenta el FONAG
4. Evaluar el impacto posible sobre los procesos de la Institución si es que alguna amenaza se materializa.
5. Informar a los directivos y proponer un plan de mejora para una buena gestión de riesgos.

Es importante recalcar que la metodología MAGERIT se aplicará al proceso "Adquisición de bienes y servicios" que es uno de los procesos más críticos e importantes para la institución debido al tipo de información que manejan y la cantidad de personal que interviene.

4.1 Identificación de los activos

Como primer paso se identificaron los activos (Tabla 7) más importantes que intervienen el proceso de adquisición de bienes y servicios. Según [7] Un activo es cualquier componente o funcionalidad del sistema de información que puede ser atacado de manera deliberada o accidental con consecuencias para la organización.

Tabla 7. Lista de activos por categoría. [Elaboración propia]

Categoría	Código	Descripción
[ARCH] Arquitectura del sistema	SAP_POOL_SERVIDORES_AWS	Pool de servidores en la nube contratados con Amazon Web Services(AWS)
[D] Datos / Información	BACKUP_SERVIDORES_AWS	Respaldos periódicos (diario, semanal) de los servidores virtuales alojados en la nube de AWS
	FILES_USUARIO	Información generada por cada integrante del FONAG
	LOG_SCPF	Log transacciones SCPF
	PASSWORD_SERVICIOS	Archivo con usuarios y contraseñas de acceso a las diferentes consolas y servidores de la institución
	VR_REPOSITORIO_PROCESOS	Repositorio documental de procesos de adquisición alojado en ONEDRIVE
[S] Servicios	EMAIL_GOOGLE	Servicio de correo institucional en la nube de GOOGLE
	AV_KARPERSKY	Antivirus Karsperky

Categoría	Código	Descripción
[SW] Aplicaciones (Software)	OFFICE_MICROSOFT	Ofimática Office
	OS_WINDOWS_UBUNTU	Windows, Microsoft y Linux
	SUB_SCPF	Sistema de control presupuestario desarrollado a medida para el control de procesos de adquisición de bienes y servicios
	SUB_SCPF_PRUEBAS	Sistema de control presupuestario para desarrollo y capacitación
[HW] Equipos	FIREWALL_FORTINET	Equipo de protección para la navegación web
	HOST_SCPF	Servidor de aplicación y base de datos para el SCPF
	HOST_SCPF_PRUEBAS	Servidor réplica del SCPF para pruebas y capacitación
	PC_TRABAJO	Equipos de trabajo del personal de oficina
	ROUTER_HP	Equipo capa 2 para la conexión de la red LAN
[COM] Redes de Comunicaciones	INTERNET_TELCONET	Red internet para uso corporativo
	LAN_CAT5	Red LAN para uso corporativo
	WIFI_UBIQUITI	Red WIFI para uso corporativo
[AUX] Equipamiento auxiliar	CABLING_FONAG	Cableado LAN categoría 6
	UPS_PC_PERSONAL	Equipo de almacenamiento y protección de energía eléctrica
[L] Instalaciones	BUILDING_FONAG	Oficinas principales ubicadas en la Mariana de Jesús y Martín de Utreras
[P] Personal	UI_ABG_FONAG	Abogada
	UI_ACP_FONAG	Analista Contratación Pública
	UI_ASADF_FONAG	Asistente Administrativo Financiero
	UI_CADF_FONAG	Coordinadora Administrativo Financiero
	UI_COORD_FONAG	Coordinadoras FONAG
	UI_RES_TI	Responsable TI
	UI_RMS_FONAG	Responsable de Monitoreo y Seguimiento
	UI_SOPORTE_TI	Técnico soporte técnico
	UI_ST_FONAG	Secretario técnico
	UI_TEC_FONAG	Personal técnico del FONAG

4.2 Valoración de los activos

Para la valoración de activos se utilizó la escala numérica del 0 al 10, siendo 0 el valor más bajo y 10 el más alto que se muestra en Tabla 8.

Tabla 8. Criterios de valoración activos. [22]

Valor		Criterio
10	extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

En el punto 3 de MAGERIT – Libro I – Método, se detalla las siguientes dimensiones que se pueden valorar:

- Disponibilidad [D]: Nivel de perjuicio que causaría no tenerlo o no poder utilizarlo
- Integridad [I]: Nivel de perjuicio que causaría que estuviera dañado o corrupto
- Confidencialidad [C]: Nivel de daño que causaría que fuera divulgado a quien no se debe información específica
- Autenticidad [A]: Nivel de perjuicio que causaría no saber quién hace o ha hecho cada cosa.
- Trazabilidad [T]: Nivel de daño que causaría no saber quién hace qué y cuándo.

Tomando en cuenta los criterios de valoración y las dimensiones descritas se valoró cada activo del punto 4.1 de este documento, arrojando la información que se muestra en la Tabla 9.

Tabla 9. Valoración de activos esenciales. [Elaboración propia]

Código Activo	[D]	[I]	[C]	[A]	[T]
SAP_POOL_SERVIDORES_AWS	10			10	7
BACKUP_SERVIDORES_AWS	10	9	3	10	8
FILES_USUARIO	8	6	3	9	7
LOG_SCPF	5	10	10	10	8
PASSWORD_SERVICIOS		10	10	10	9
VR_REPOSITORIO_PROCESOS	10	9	2	10	8
EMAIL_GOOGLE	9			10	9
AV_KARPERSKY	7			9	7
OFFICE_MICROSOFT	8			9	7
OS_WINDOWS_UBUNTU	7			9	7
SUB_SCPF	10	9	3	10	9
SUB_SCPF_PRUEBAS	5			5	3
FIREWALL_FORTINET	8			9	7
HOST_SCPF	10			10	7
HOST_SCPF_PRUEBAS	3				
PC_TRABAJO	8			9	9
ROUTER_HP	8				
INTERNET_TELCONET	8				
LAN_CAT5	8				7
WIFI_UBIQUITI	5				7
CABLING_FONAG	7				
UPS_PC_PERSONAL	7				
BUILDING_FONAG			5		

Código Activo	[D]	[I]	[C]	[A]	[T]
UI_ABG_FONAG			3		
UI_ACP_FONAG			3		
UI_ASADF_FONAG			3		
UI_CADF_FONAG			3		
UI_COORD_FONAG			3		
UI_RES_TI			3		
UI_RMS_FONAG			3		
UI_SOPORTE_TI			5		
UI_ST_FONAG			3		
UI_TEC_FONAG			3		

4.3 Identificación de las amenazas

El tercer paso consiste en establecer las amenazas que pueden afectar a cada uno de los activos, considerando que una amenaza es un incidente latente que puede causar daño a un sistema de información a una organización [7]. El capítulo 5 de MAGERIT - Libro II – Catalogo de elementos, muestra como los activos se relacionan con las amenazas y que dimensiones se pueden ver afectadas [22]. Con esta información y la lista de activos se levantó la información que se muestra en la Tabla 10:

[D] Datos / Información

Tabla 10. Principales amenazas para los activos de la categoría: [D] Datos / Información. [Elaboración propia]

Código Activo	Amenaza
BACKUP_SERVIDORES_AWS	[E.2 Errores del administrador]
BACKUP_SERVIDORES_AWS	[A.5 Suplantación de la identidad del usuario]
BACKUP_SERVIDORES_AWS	[A.11 Acceso no autorizado]
BACKUP_SERVIDORES_AWS	[A.15 Modificación deliberada de la información]
BACKUP_SERVIDORES_AWS	[A.18 Destrucción de información]
BACKUP_SERVIDORES_AWS	[A.19 Divulgación de información]
FILES_USUARIO	[E.1 Errores de los usuarios]
FILES_USUARIO	[E.2 Errores del administrador]
FILES_USUARIO	[E.15 Alteración accidental de la información]
FILES_USUARIO	[A.5 Suplantación de la identidad del usuario]
FILES_USUARIO	[A.11 Acceso no autorizado]
FILES_USUARIO	[A.15 Modificación deliberada de la información]
FILES_USUARIO	[A.18 Destrucción de información]
FILES_USUARIO	[A.19 Divulgación de información]
LOG_SCPF	[A.11 Acceso no autorizado]
LOG_SCPF	[A.18 Destrucción de información]

Código Activo	Amenaza
LOG_SCPF	[A.19 Divulgación de información]
PASSWORD_SERVICIOS	[E.2 Errores del administrador]
PASSWORD_SERVICIOS	[A.5 Suplantación de la identidad del usuario]
PASSWORD_SERVICIOS	[A.11 Acceso no autorizado]
PASSWORD_SERVICIOS	[A.15 Modificación deliberada de la información]
PASSWORD_SERVICIOS	[A.18 Destrucción de información]
PASSWORD_SERVICIOS	[A.19 Divulgación de información]
VR_REPOSITORIO_PROCESOS	[E.1 Errores de los usuarios]
VR_REPOSITORIO_PROCESOS	[E.15 Alteración accidental de la información]
VR_REPOSITORIO_PROCESOS	[A.11 Acceso no autorizado]
VR_REPOSITORIO_PROCESOS	[A.15 Modificación deliberada de la información]
VR_REPOSITORIO_PROCESOS	[A.18 Destrucción de información]
VR_REPOSITORIO_PROCESOS	[A.19 Divulgación de información]

Debido a la cantidad de amenazas relacionadas para activo, solo se muestra una lista reducida, el detalle completo de las amenazas se puede visualizar en el ANEXO I de este documento.

4.4 Valoración de las amenazas

Cada amenaza afecta de manera diferente a un activo, por tanto, según [7] se debe valorar la influencia con base en dos aspectos:

- Frecuencia: cuán probable es que ocurra la amenaza. Tabla 11
- Degradación: cuán perjudicado resultaría el valor del activo en cada dimensión.

- **Tabla 12**

Tabla 11. Probabilidad de Ocurrencia. [7]

Código	**Escala**	**Criterio**	**Valoración**
MA	Casi Seguro	a diario	10
A	Muy alto	mensualmente	8
M	Posible	una vez al año	6
B	Poco probable	cada varios años	4
MB	Muy raro	siglos	2
NA	No aplica	No aplica	0

Tabla 12. Degradación de Valor. [7]

Código	Escala	Criterio	Valoración
MA	Muy alta	fácil	10
A	Alta	medio	8
M	Media	difícil	6
B	Baja	muy díficil	4
MB	Muy baja	extremandamente difícil	2
NA	No aplica	No aplica	0

En la Tabla 13 de detalla la frecuencia con que pueden ocurrir las amenazas que se levantaron el punto 4.3 junto con la afectación a cada una de las dimensiones de seguridad: disponibilidad [D], integridad [I], confidencialidad [C], autenticidad[A] y trazabilidad [T].

Tabla 13. Valoración amenazas. Activo: BACKUP_SERVIDORES_AWS. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	A	A		
[A.5 Suplantación de la identidad del usuario]	M		A	M	A	
[A.11 Acceso no autorizado]	M		A	A		
[A.15 Modificación deliberada de la información]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			A		

El detalle de la valoración de cada amenaza por activo se puede revisar en el Anexo II de este documento.

4.5 Identificación de las salvaguardas

Como quinto paso se identificaron las salvaguardas para tener una protección efectiva contra las amenazas del punto 4.4 de este documento. A continuación, se detallan las protecciones establecidas por el equipo del FONAG:

- [HW.A] Instalación de sistema contra incendios
- [HW.A] Instalación de alarmas contra incendio
- [HW.A] Uso y mantenimiento de extintores
- [HW.A] Desarrollo de plan de emergencia ante desastres
- [HW.A] Instalación de sistema contra inundaciones
- [HW.A] Protección de las instalaciones frente a descargas eléctricas
- [HW.op] Mantenimiento preventivo de limpieza, y reposición de componentes electromecánicos

- [HW.A] Disponer de sistemas de funcionamiento redundante
- [HW.A] Sistemas de alimentación ininterrumpida
- [HW.A] Sistemas de aire acondicionado, y alarma por exceso de temperatura y humedad
- [COM.A] Disponer rutas de comunicación redundantes
- [H.A] Disponer de reservas de recursos
- [D.C] Uso de técnicas de encriptación
- [D.A] Copias de seguridad, incluidos registros de transacciones para deshacer operaciones
- [SW.SC] Disociación de responsabilidades, para reducir daño de los errores
- [SW.SC] Políticas de seguridad con establecimiento de responsables
- [H.tools] Software de eliminación de virus, y de eliminación de software malicioso
- [H.AU] Procedimientos de reinstalación y configuración del sistema
- [D.A] Copias de seguridad.
- [D.A] Sistemas de revisión y validación de transacciones (mediante totales, revisión por otra persona u otras vías).
- [SW.CM] Entornos de prueba y sistemas de revisión
- [SW.CM] Plan de mantenimiento preventivo, para revisar fecha de actualización aplicada a las aplicaciones
- [HW.CM] Plan de mantenimiento preventivo para revisar componentes electrónicos
- [HW.op] Aplicaciones de monitorización de recursos disponibles con alarmas
- [SW.SC] Política de seguridad con establecimiento de responsables, y designación de suplentes de responsables
- [D.A] Copias impresas de procedimientos de reinstalación, y configuración del sistema
- [H.IA] Sistemas de autenticación fuertes, que incluyan medidas biométricas
- [S.SC] Impedir ejecución de procesos no autorizados
- [COM.C] Aleatorización de las rutas de comunicaciones, y encapsulamiento de protocolos
- [D.DS] Empleo de firmas digitales
- [D.C] Empleo de técnicas de criptografía
- [D.A] Copias de seguridad
- [S.www] Penalización a solicitudes recurrentes.
- [HW.op] Monitorización de recursos disponibles y alarma

- [HW.R] Alarmas antirrobo, sistemas de anclaje de equipos, técnicas de criptografía
- [D.A] Copias de seguridad fuera de las instalaciones, acuerdos de alquiler de equipos para casos de emergencia, copias impresas de procedimientos de reinstalación y configuración del sistema
- [PS.AT] Formación, empleo de mecanismos de autenticación fuertes con métodos biométricos

4.6 Valoración de las salvaguardas

Para la valoración de las salvaguardas (Tabla 14) se tomó en cuenta la información proporcionada en el punto 3 de [7].

Tabla 14. Eficacia y Madurez de las salvaguardas. [7]

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicial/ad hoc	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	Proceso Definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continúa

En la Tabla 15 se describe algunas de las relaciones entre las amenazas existentes y las salvaguardas que se levantaron para proteger los activos del FONAG, el resto de información se puede revisar en el ANEXO III**.** Análisis de salvaguardas por cada amenaza. Este proceso fue validado con los altos mandos de la institución.

Tabla 15. Valoración de las salvaguardas con las métricas: actual y objetivo. [Elaboración propia]

Amenaza	Salvaguarda	Actual	Objetivo
[N.1 Fuego]	[HW.A] Instalación de sistema contra incendios	L1	L2
[N.2 Daños por agua]	[HW.A] Instalación de sistema contra inundaciones	L0	L0
[N.* Otros]	[HW.A] Protección de las instalaciones frente a descargas eléctricas	L2	L4
[I.3 Contaminación mecánica]	[HW.op] Mantenimiento preventivo de limpieza, y reposición de componentes electromecánicos	L3	L4
[I.5 Averia de origen físico o lógico]	[HW.A] Disponer de sistemas de funcionamiento redundante	L0	L2
[I.6 Corte del suministro eléctrico]	[HW.A] Sistemas de alimentación ininterrumpida	L1	L1
[I.7 Condiciones inadecuadas de temperatura o humedad]	[HW.A] Sistemas de aire acondicionado, y alarma por exceso de temperatura y humedad	L0	L0
[I.8 Fallo de servicios de comunicaciones]	[COM.A] Disponer rutas de comunicación redundantes	L0	L0

Amenaza	Salvaguarda	Actual	Objetivo
[I.9 Interrupción de otros servicios y suministros esenciales]	[H.A] Disponer de reservas de recursos	L1	L2
[I.11 Emanaciones electromagnéticas]	[D.C] Uso de técnicas de encriptación	L0	L1
[E.21 Errores de mantenimiento / actualización de programas (software)]	[SW.CM] Plan de mantenimiento preventivo, para revisar fecha de actualización aplicada a las aplicaciones	L1	L3
[E.23 Errores de mantenimiento / actualización de equipos (hardware)]	[HW.CM] Plan de mantenimiento preventivo para revisar componenenes electrónicos	L3	L4
[A.29 Extorsión]	[D.A] Copias de seguridad	L1	L2
[A.29 Extorsión]	[D.C] Uso de técnicas de encriptación	L0	L1
[A.30 Ingeniería social (picaresca)]	[PS.AT] Formación, empleo de mecanismos de autenticación fuertes con métodos biométricos	L0	L1

4.7 Estimación del impacto

Para el cálculo del impacto se tomó como referencia el punto 1 de MAGERIT 3.0 – Libro III – Guía de Técnicas [23], pero utilizando una escala cuantitativa, tomando en cuenta el valor del activo y la degradación que puede provocar una amenaza, como se muestra en la Tabla 16 y Tabla 17.

Tabla 16. Cálculo del impacto en escala cuantitativa. [23]

Impacto		Degradación amenaza					
		10	**8**	**6**	**4**	**2**	**0**
Valor activo	**10**	100	80	60	40	20	0
	8	80	64	48	32	16	0
	6	60	48	36	24	12	0
	4	40	32	24	16	8	0
	2	20	16	12	8	4	0
	0	0	0	0	0	0	0

Tabla 17. Valoración del impacto en escala numérica. [23]

Valoración	Escala
100	Muy alta
80	Alta
60	Media
40	Baja
20	Muy baja
0	No aplica

El **impacto potencial** es el daño al que está expuesto el sistema de información, teniendo en cuenta el valor de los activos y la degradación de las amenazas, sin tener en cuenta las salvaguardas actuales. Con las valoraciones y el método de cálculo se obtuvo el impacto potencial para cada uno de los activos identificados en el punto 4.1 y que se muestra en la Tabla 18.

Tabla 18. Impacto Potencial. [Elaboración propia]

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[D] Datos / Información	BACKUP_SERVIDORES_AWS	80	69	22	80	
	FILES_USUARIO	56	45	17	72	
	LOG_SCPF	36	74	69	80	48
	PASSWORD_SERVICIOS		77	73	80	
	VR_REPOSITORIO_PROCESOS	70	67	11	80	
[S] Servicios	EMAIL_GOOGLE	72			80	54
[SW] Software - Aplicaciones Informáticas	AV_KARPERSKY	48			36	
	OFFICE_MICROSOFT	52			36	
	OS_WINDOWS_UBUNTU	52			36	
	SUB_SCPF	76	64	19	80	
	SUB_SCPF_PRUEBAS	19			20	
[HW] Equipamiento informático	FIREWALL_FORTINET	64				
	HOST_SCPF	80				
	HOST_SCPF_PRUEBAS	20				
	PC_TRABAJO	64				
	ROUTER_HP	61				
[COM] Redes de comunicaciones	INTERNET_TELCONET	59				
	LAN_CAT5	59				
	WIFI_UBIQUITI	37				
[AUX] Equipamiento auxiliar	CABLING_FONAG	55				
	UPS_PC_PERSONAL	56				
[L] Instalaciones	BUILDING_FONAG			30		
[P] Personal	UI_ABG_FONAG			14		
	UI_ACP_FONAG			14		
	UI_ASADF_FONAG			14		
	UI_CADF_FONAG			14		
	UI_COORD_FONAG			14		
	UI_RES_TI			14		
	UI_RMS_FONAG			14		
	UI_SOPORTE_TI			23		
	UI_ST_FONAG			14		
	UI_TEC_FONAG			14		

El **impacto Residual (Actual)** es el daño al que está expuesto el sistema de información, teniendo en cuenta el valor de los activos, la valoración de las amenazas y las salvaguardas existentes como se aprecia en la Tabla 19.

Tabla 19. Impacto Residual. [Elaboración propia]

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[D] Datos / Información	BACKUP_SERVIDORES_AWS	77	68	21	80	
	FILES_USUARIO	53	44	17	72	
	LOG_SCPF	35	71	67	76	43
	PASSWORD_SERVICIOS		76	72	80	
	VR_REPOSITORIO_PROCESOS	67	65	11	80	
[S] Servicios	EMAIL_GOOGLE	70			80	49
[SW] Software - Aplicaciones Informáticas	AV_KARPERSKY	44			36	
	OFFICE_MICROSOFT	47			36	
	OS_WINDOWS_UBUNTU	48			36	
	SUB_SCPF	70	60	18	80	
	SUB_SCPF_PRUEBAS	18			20	
[HW] Equipamiento informático	FIREWALL_FORTINET	52				
	HOST_SCPF	79				
	HOST_SCPF_PRUEBAS	20				
	PC_TRABAJO	52				
	ROUTER_HP	49				
[COM] Redes de comunicaciones	INTERNET_TELCONET	59				
	LAN_CAT5	59				
	WIFI_UBIQUITI	37				
[AUX] Equipamiento auxiliar	CABLING_FONAG	44				
	UPS_PC_PERSONAL	44				
[L] Instalaciones	BUILDING_FONAG			30		
[P] Personal	UI_ABG_FONAG			14		
	UI_ACP_FONAG			14		
	UI_ASADF_FONAG			14		
	UI_CADF_FONAG			14		
	UI_COORD_FONAG			14		
	UI_RES_TI			14		
	UI_RMS_FONAG			14		
	UI_SOPORTE_TI			23		
	UI_ST_FONAG			14		
	UI_TEC_FONAG			14		

En términos generales, se puede apreciar que no hay ningún activo que se encuentre en la escala de valoración “Muy alta” (Tabla 17). Estas valoraciones son producto del uso de servicios en la nube y la existencia de respaldos periódicos, es decir que ante un ataque no se vería comprometida la información. Por otra parte, la filosofía del FONAG es generar información de carácter público, para que sea utilizada por otras instituciones, lo que implica que la confidencialidad no sería afectada de manera grave ante una amenaza materializada.

En cuanto a la integridad y autenticidad si se requieren mejorar los mecanismos implementados para evitar que la información y los respaldos no se vean comprometidos ante un ingreso no autorizado o un acceso no permitido.

El reto para el personal de TICS es reducir el impacto de los activos que se encuentran en la escala “Alta” y “Media”, conforme a los recursos disponibles y las directrices de los altos mandos del FONAG.

4.8 Estimación del Riesgo

El **riesgo potencial**, es el daño probable sobre el sistema de información, conociendo el impacto de las amenazas sobre los activos, sin tomar en cuenta las salvaguardas, que se evidencia en la Tabla 20.

Tabla 20. Riesgo potencial. [Elaboración propia]

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[D] Datos / Información	BACKUP_SERVIDORES_AWS	38	33	12	48	
	FILES_USUARIO	29	25	9	43	
	LOG_SCPF	15	23	28	16	19
	PASSWORD_SERVICIOS		37	39	48	
	VR_REPOSITORIO_PROCESOS	35	37	6	32	
[S] Servicios	EMAIL_GOOGLE	29			48	22
[SW] Software - Aplicaciones Informáticas	AV_KARPERSKY	22			14	
	OFFICE_MICROSOFT	26			14	
	OS_WINDOWS_UBUNTU	27			14	
	SUB_SCPF	42	32	11	32	
	SUB_SCPF_PRUEBAS	10			8	
[HW] Equipamiento informático	FIREWALL_FORTINET	26				
	HOST_SCPF	27				
	HOST_SCPF_PRUEBAS	6				
	PC_TRABAJO	29				
	ROUTER_HP	25				

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[COM] Redes de comunicaciones	INTERNET_TELCONET	30				
	LAN_CAT5	29				
	WIFI_UBIQUITI	17				
[AUX] Equipamiento auxiliar	CABLING_FONAG	24				
	UPS_PC_PERSONAL	24				
[L] Instalaciones	BUILDING_FONAG			14		
[P] Personal	UI_ABG_FONAG			4		
	UI_ACP_FONAG			4		
	UI_ASADF_FONAG			4		
	UI_CADF_FONAG			4		
	UI_COORD_FONAG			4		
	UI_RES_TI			4		
	UI_RMS_FONAG			4		
	UI_SOPORTE_TI			7		
	UI_ST_FONAG			4		
	UI_TEC_FONAG			4		

El **riesgo residual (Actual),** dado un conjunto de salvaguardas desplegadas y una medida de madurez del proceso de gestión de seguridad, se obtiene un riesgo modificado, denominado valor residual que se puede revisar en la Tabla 21.

Tabla 21. Riesgo residual. [Elaboración propia]

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[D] Datos / Información	BACKUP_SERVIDORES_AWS	37	33	11	48	
	FILES_USUARIO	27	24	9	43	
	LOG_SCPF	14	22	27	15	17
	PASSWORD_SERVICIOS		36	38	48	
	VR_REPOSITORIO_PROCESOS	33	35	6	32	
[S] Servicios	EMAIL_GOOGLE	28			48	19
[SW] Software - Aplicaciones Informáticas	AV_KARPERSKY	20			14	
	OFFICE_MICROSOFT	24			14	
	OS_WINDOWS_UBUNTU	25			14	
	SUB_SCPF	38	30	10	32	
	SUB_SCPF_PRUEBAS	10			8	
[HW] Equipamiento informático	FIREWALL_FORTINET	21				
	HOST_SCPF	26				
	HOST_SCPF_PRUEBAS	6				

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
	PC_TRABAJO	23				
	ROUTER_HP	21				
[COM] Redes de comunicaciones	INTERNET_TELCONET	30				
	LAN_CAT5	29				
	WIFI_UBIQUITI	17				
[AUX] Equipamiento auxiliar	CABLING_FONAG	19				
	UPS_PC_PERSONAL	19				
[L] Instalaciones	BUILDING_FONAG			14		
[P] Personal	UI_ABG_FONAG			4		
	UI_ACP_FONAG			4		
	UI_ASADF_FONAG			4		
	UI_CADF_FONAG			4		
	UI_COORD_FONAG			4		
	UI_RES_TI			4		
	UI_RMS_FONAG			4		
	UI_SOPORTE_TI			7		
	UI_ST_FONAG			4		
	UI_TEC_FONAG			4		

El nivel de riesgo residual que tiene la infraestructura tecnológica esta entre “Media” y “Muy baja”, según la escala de valoración de la Tabla 17. Este nivel de riesgo es consecuencia de las políticas de seguridad implementadas desde hacer varios años y que ha permitido tener cierto nivel de protección en los activos de la institución.

4.9 Interpretación de resultados

Como último paso se obtuvo una comparación entre la situación potencial, actual y objetivo con resultados obtenidos de las actividades anteriores. En la Figura 10 se muestra que la diferencia entre el impacto potencial y actual no varía tanto, por las salvaguardas ya existentes. En cuanto al impacto objetivo se quiere alcanzar un nivel “Bajo”, para garantizar la integridad de la información y la disponibilidad de los recursos.

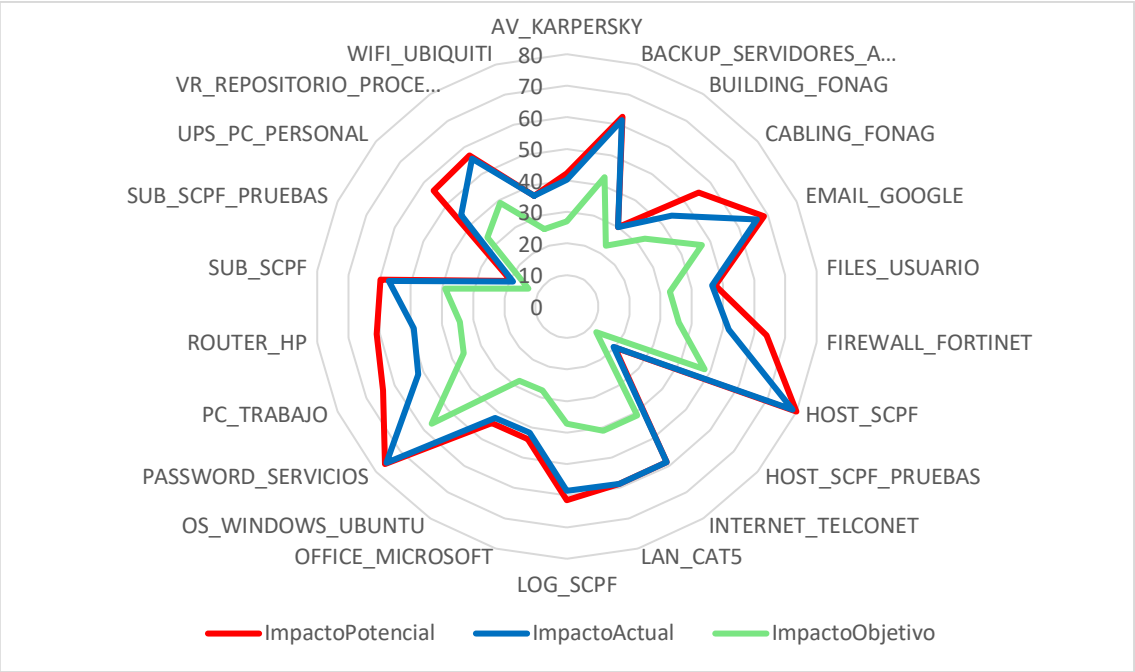

Figura 10. Resultado impacto activos FONAG. [Elaboración propia]

En la Figura 11, se aprecia en términos generales que el nivel de riesgo no supera los 50 puntos (sobre 100), lo que implica que no son necesarias acciones inmediatas para mitigar los riesgos, sin embargo, es importante mantener y mejorar las salvaguardas existentes para que no suba este puntaje.

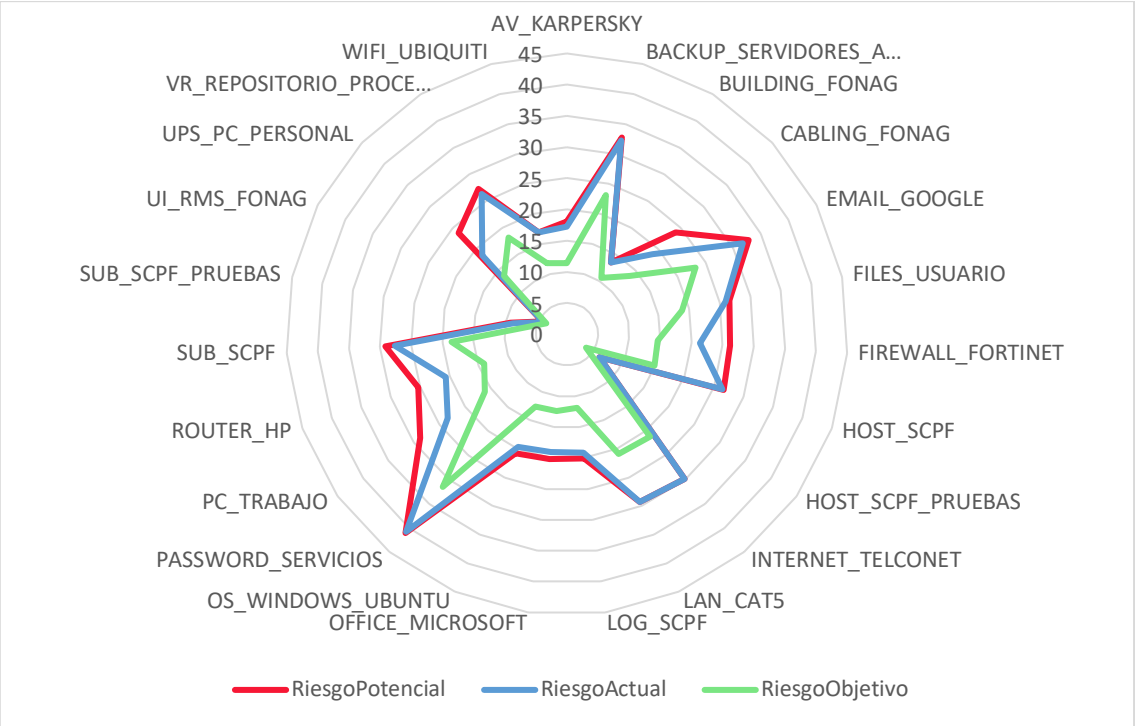

Figura 11. Resultado riesgo activos FONAG. [Elaboración propia]

Para el proceso analizado en este trabajo de titulación, se concluye que los activos de información que intervienen en el proceso de adquisición de bienes y servicios, tienen un nivel bajo de riesgo, pero se debe mejorar ciertas actividades para cerrar brechas de seguridad evidentes como se detalla en punto 5.3 de este documento. De igual manera se recomienda hacer un análisis de los otros procesos críticos de la institución para encontrar los riesgos existentes dentro de la infraestructura tecnológica.

CAPÍTULO 5. GESTIÓN DE RIESGOS

5.1 Identificación de riesgos críticos

Con base a la información levantada en el capítulo 4, se priorizaron algunos activos para reducir el nivel de amenaza existente. En la Tabla 22 de listan los activos con un riesgo residual (Tabla 21) mayor a 30 puntos sobre 100 en cualquiera de las dimensiones de seguridad.

Tabla 22. Lista de activos críticos. [Elaboración propia]

Categoría	Código Activo	[D]	[I]	[C]	[A]	[T]
[D] Datos / Información	BACKUP_SERVIDORES_AWS	37	33	11	48	
	FILES_USUARIO	27	24	9	43	
	PASSWORD_SERVICIOS		36	38	48	
	VR_REPOSITORIO_PROCESOS	33	35	6	32	
[S] Servicios	EMAIL_GOOGLE	28			48	19
	SUB_SCPF	38	30	10	32	

El activo más crítico en cuanto a la seguridad de la información es el BACKUP_SERVIDORES_AWS, por los puntajes obtenidos en las dimensiones de disponibilidad, integridad, confidencialidad y autenticidad. Este resultado refleja la importancia para la institución de contar con los respaldos del sistema de control presupuestario y la afectación que tendría en caso de ser vulnerado.

5.2 Calificación del riesgo

En la Tabla 23 se listan las amenazas con una puntuación mayor a 30 en cualquiera de las dimensiones de seguridad para los activos críticos

Tabla 23. Lista de amenazas para los activos críticos. [Elaboración propia]

Código	Amenaza	[D]	[I]	[C]	[A]	[T]
BACKUP_SERVIDORES_AWS	[A.11 Acceso no autorizado]		43	14		
	[A.18 Destrucción de información]	43				
	[A.5 Suplantación de la identidad del usuario]		43	11	48	
	[A.6 Abuso de privilegios de acceso]	32	29	10		
	[A.7 Uso no previsto]	32	29	10		
	[E.2 Errores del administrador]	48	43	14		
FILES_USUARIO	[A.18 Destrucción de información]	35				
	[A.5 Suplantación de la identidad del usuario]		29	11	43	
	[E.2 Errores del administrador]	38	29	11		

Código	Amenaza	[D]	[I]	[C]	[A]	[T]
PASSWORD_SERVICIOS	[A.11 Acceso no autorizado]		48	48		
	[A.15 Modificación deliberada de la información]			43		
	[A.19 Divulgación de información]			48		
	[A.5 Suplantación de la identidad del usuario]		48	36	48	
	[A.6 Abuso de privilegios de acceso]		32	32		
	[A.7 Uso no previsto]		32	32		
	[E.2 Errores del administrador]		48	48		
VR_REPOSITORIO_PROCESOS	[A.11 Acceso no autorizado]		43	7		
	[A.18 Destrucción de información]	43				
	[A.5 Suplantación de la identidad del usuario]		29	5	32	
	[A.7 Uso no previsto]	32	29	6		
	[E.1 Errores de los usuarios]	36	49	7		
	[E.15 Alteración accidental de la información]		39			
	[E.2 Errores del administrador]	32	29	3		
EMAIL_GOOGLE	[A.18 Destrucción de información]	39				
	[A.5 Suplantación de la identidad del usuario]				48	
	[E.2 Errores del administrador]	43				
SUB_SCPF	[A.10 Alteración de secuencia]		43			
	[A.11 Acceso no autorizado]		43	11		
	[A.18 Destrucción de información]	43				
	[A.5 Suplantación de la identidad del usuario]		29	7	32	
	[A.6 Abuso de privilegios de acceso]	32	29	10		
	[A.7 Uso no previsto]	32	29	10		
	[A.8 Difusión de software dañino]	38	35	12		
	[E.2 Errores del administrador]	48	43	14		
	[E.20 Vulnerabilidades de los programas (software)]	58	52	13		
	[I.5 Avería de origen físico o lógico]	48				

Las medidas que se deben implementar (en cada activo) para reducir el riesgo actual se describen a continuación:

BACKUP_SERVIDORES_AWS

- Implementar el doble factor de autenticación para los ingresos a la plataforma de Amazon Web Services.
- Implementar notificaciones de acceso a la plataforma de Amazon Web Services.
- Capacitar al administrador de los servidores en la nube para reducir el riesgo de alteraciones de la información, por acciones involuntarias

FILES_USUARIO y EMAIL_GOOGLE

- Capacitar al personal técnico para un manejo adecuado de la información y el uso correcto de los accesos a las cuentas de correo empresariales
- Implementar mecanismos de respaldo de la información adicionales para evitar pérdidas de información por manipulaciones indebidas o errores involuntarios.

PASSWORD_SERVICIOS

- Implementar gestor de contraseñas para el manejo de todas las sesiones de acceso a portales de configuración e información sensible
- Establecer un procedimiento de manejo de contraseñas para evitar divulgación o modificación de estas.

VR_REPOSITORIO_PROCESOS

- Migrar el repositorio de procesos desde una carpeta compartida hacía un sitio de sharepoint para controlar perfiles de seguridad y las acciones de cada usuario.
- Implementar copias de seguridad del repositorio de proceso en caso de que haya una alteración o perdida masiva

SUB_SCPF

- Implementar un mecanismo de doble autentificación para evitar suplantación de identidad
- Cambiar la configuración de producción del sistema presupuestario para mitigar los ataques, que comprendería tener instancias duplicadas y balanceadores de carga.

5.3 Plan mitigación de riesgos

En esta fase del proyecto se describirá como se recomienda implementar las medidas sugeridas en el punto 5.2 para el tratamiento de los riesgos. Las actividades principales son las siguientes:

1. Identificación de proyectos de seguridad
2. Plan de ejecución
3. Ejecución

5.3.1 Identificación de proyectos de Seguridad

Dentro de esta actividad se realizarán las 2 tareas: i) Normativa de seguridad y ii) Eliminar fallos de seguridad evidentes

Normativa de seguridad

Para los activos críticos se recomienda implementar las siguientes normativas como parte del manejo de los activos.

Documentación: BACKUP_SERVIDORES_AWS

- Cada servidor alojado en la nube debe tener una periodicidad de respaldo y el tiempo de permanencia de este, establecida por el responsable de TI y el coordinador administrativo financiero.
- El uso de Amazon Web Services debe ser exclusivo para aplicativos del FIDEICOMISO FONAG y se considerará una falta grave utilizar los recursos para usos particulares.

Documentación: FILES_USUARIO y EMAIL_GOOGLE

- El personal técnico del FONAG debe utilizar el correo y almacenamiento en la nube para actividades relacionadas con las necesidades del puesto y función que desempeña
- El uso de correo electrónico debe ser personal e intransferible, es decir no debe ser compartido con ninguna persona.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico

Documentación: PASSWORD_SERVICIOS

- Debe existir una cláusula de confidencialidad para el personal TI para evitar la divulgación de información sensible

Documentación: VR_REPOSITORIO_PROCESOS

- El uso del repositorio de procesos es exclusivo para almacenar información relacionada con los procesos de adquisición de bienes/servicios del FONAG y se prohíbe almacenar cualquier información de otro tipo.

Documentación: SUB_SCPF

- Las credenciales de acceso al sistema de control presupuestario no deben compartidas en ninguna circunstancia.
- Los usuarios deben cambiar periódicamente las credenciales de acceso para evitar suplantaciones o accesos no permitidos

Eliminar fallos de seguridad evidentes

- Las credenciales de acceso a los servidores no se cambian periódicamente y no está implementado un doble factor de autenticación, lo que implica un nivel de seguridad bastante bajo.
- El uso del correo y almacenamiento de la nube no está controlado para que no se carguen o compartan archivos maliciosos, lo que representa una amenaza de rasonware para la empresa
- El archivo de contraseñas está en texto legible lo que implica que alguien puede aplicar la ingeniería social y afectar las consolas de administración de los sistemas.
- El repositorio de procesos es una carpeta compartida sin los permisos adecuados para evitar la manipulación inadecuada de la información. Tampoco se controla el tipo de archivos que se cargan, lo cual implica una amenaza de rasonware.
- El acceso al sistema presupuestario no tiene implementado un doble factor de autentificación y algunos usuarios tienen claves muy débiles.

Clasificación de inventario

El FONAG, tiene clasificados todos los bienes físicos de la institución con base a un sistema de inventario, que controla los ingresos y salidas de los bienes adquiridos. Sin embargo, los activos de información no están guardados dentro de dicho registro. Con este análisis de riegos, se deja un registro de los elementos mencionados anteriormente y que puede ser alimentado con nuevos datos conforme el crecimiento de la institución.

5.3.2 Plan de ejecución

Para mitigar los riesgos identificados en este análisis se deben cumplir dos actividades principales: i) implementación de nuevas normativas y ii) depuración de fallos evidentes. Para ejecución del plan de mitigación de riesgos se propone el cronograma de la Figura 12.

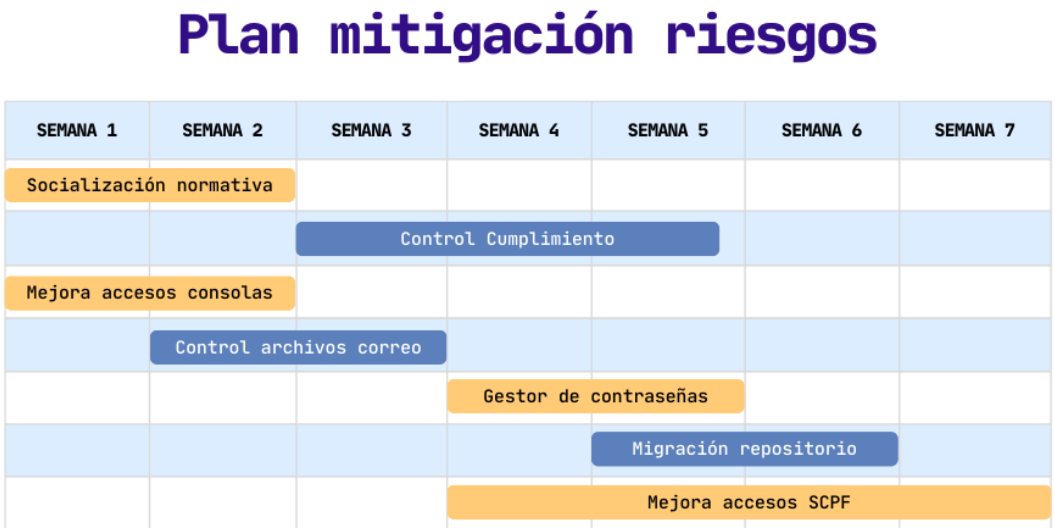

Figura 12. Cronograma ejecución mitigación de riesgos. [Elaboración propia]

Socialización normativa: Informar al personal por los medios de comunicación interna de la institución de las nuevas normativas que entran en vigor para precautelar la seguridad de la información.

Control cumplimiento: Hacer un adecuado seguimiento al cumplimiento de las nuevas normativas por parte del personal. En caso de incumplimiento se propone una entrevista particular para determinar los motivos y brindar las soluciones adecuadas. A pesar de que el cronograma marca tres semanas, esta tarea se deberá ejecutar de manera permanente.

Mejora acceso consolas: Implementar una normativa para cambio periódico (90 días) de contraseñas de acceso a las consolas de Amazon web Services, Karpersky y Microsoft.

Control archivos correo: Ejecutar los controles y mejoras de seguridad sugeridas por parte del proveedor de correo como: limitar el tamaño de archivos compartidos, excluir ciertos tipos de archivo y motivar el uso de repositorios compartidos. Además, se brindará una charla sobre la importancia de revisar y verificar los remitentes antes de abrir un archivo malicioso.

Gestor contraseñas: Instalar un gestor de contraseñas para el personal técnico de informática, con la finalidad de evitar accesos no autorizados. Adicionalmente se complementará los accesos con un factor de doble autenticación.

Migración de repositorio: El repositorio de procesos debe ser migrado a un sitio de SharePoint para poder controlar de manera efectiva los permisos de acceso y hacer un seguimiento de los cambios que realiza el personal. Además, se debe solicitar un servicio de respaldo para evitar pérdidas de la información.

Mejora accesos SCPF: En primera instancia se recomienda implementar un control de caducidad de contraseñas cada 180 días para evitar accesos no autorizados. Luego se debe actualizar el sistema para que tenga un doble factor de autenticación de los usuarios con privilegios de administrador.

5.3.3 Ejecución

La ejecución del plan debe ser coordinada con los directivos del FONAG y con su respectiva aprobación.

CAPÍTULO 6. PLAN GESTIÓN INCIDENCIAS

Debido a que es casi imposible eliminar todas las vulnerabilidades existentes dentro de un sistema de información, en este capítulo se describen los lineamientos para implementar un sistema de gestión de incidencias, que permita detectar, responder, reportar y aprender de las incidencias futuras [24].

6.1 Objetivo

Objetivo general: Establecer lineamientos que permitan gestionar de forma efectiva los incidentes de seguridad que afecten los activos de información.

Objetivos específicos

- Definir roles y responsabilidades del equipo de respuesta a incidentes para evaluar los riesgos; y mantener la operatividad, continuidad y disponibilidad de los servicios.
- Definir los procedimientos para reportar y escalar los incidentes de seguridad.

6.2 Servicios informáticos

A continuación, se detalla de manera general los servicios informáticos implementados en la institución.

Equipos de cómputo

Gestión de los computadores de oficina para que los funcionarios puedan ejecutar sus actividades cotidianas. Este proceso abarca: componentes, sistema operativo, aplicaciones, acceso a la red.

- Soporte técnico de hardware y software
- Acceso a internet
- Acceso a repositorio de procesos
- Acceso a la red inalámbrica
- Soporte de ofimática
- Aplicación de garantías técnicas
- Asignación de equipos
- Instalación de software
- Gestión de accesos a plataformas de información
- Revisión alertas consola antivirus
- Retiro de equipos
- Respaldo de información

- Mantenimiento preventivo

Servicio de productividad empresarial (Office 365)

Gestión de herramientas, aplicaciones y servicios orientados a la comunicación y trabajo colaborativo entre el personal de la institución

- Gestión de usuarios
- Asignación de licencias
- Gestión de repositorios de información
- Respaldo de información
- Gestión de recursos del calendario

Servicio de impresión y digitalización

El servicio funciona bajo demanda, donde mensualmente se paga por el número de impresiones realizadas.

- Configuración en equipos de cómputo
- Cambio de suministros
- Contacto con el proveedor del servicio

Servicio de servidores en la nube

Gestión de los recursos, actualizaciones y pagos que se coordinan constantemente con el proveedor del servicio.

- Monitoreo de recursos
- Configuración respaldos periódicos
- Gestión de recursos virtuales para cada plataforma
- Gestión de accesos y perfiles de usuario
- Instalación y renovación de certificados de seguridad

Sistemas de información web

Dentro de este componente, se manejan dos modalidades: puertas adentro y con contrataciones externas. El objetivo principal es mantener la operatividad de todas las plataformas de información al 95%.

- Actualización de paquetes, librerías y sistemas operativos
- Gestión de soporte técnico con el proveedor responsable de cada sistema web
- Implementación de nuevos requerimientos
- Migración de código e información
- Actualización de documentación

6.3 Roles y responsabilidades

En [25] se detalla los servicios que puede cubrir un equipo de respuesta a incidencias de seguridad informática (CSIRT), con base al tamaño de la organización se recomienda a considerar los siguientes:

- Alertas y advertencias
- Tratamiento de incidentes
- Análisis de incidentes
- Apoyo a la respuesta a incidentes
- Comunicados

En cuanto a las responsabilidades que debe asumir el CSIRT se establecen las siguientes:

1) controlar y minimizar los daños a la información
2) recolectar evidencias sobre los eventos ocurridos
3) coordinar una recuperación rápida y con el menor impacto de los sistemas de información
4) cerrar brechas de seguridad para evitar eventos similares en el futuro.

En cuanto a los roles que deben existir dentro del FONAG se deben considerar los siguientes:

Usuario sensibilizado: Personal del FONAG y usuarios externos con acceso a la infraestructura de la organización, que deben estar informados y sensibilizados acerca de las políticas y procedimientos relacionados a la seguridad de la información. Además, es importante que conozcan el proceso para reportar los problemas relacionados a la seguridad de la información para que los notifiquen en el momento indicado y a la persona correcta.

Responsable de atención al cliente: Persona responsable de recibir las notificaciones de los usuarios, registrar la información en la base de conocimiento y escalarlo al responsable correspondiente.

Gestor de incidentes: Persona encargada de diseñar, delegar, coordinar y dirigir las actividades durante el incidente de seguridad. Debe revisar y evaluar a gestión de los incidentes reportados. Es el contacto directo con los directivos de la organización.

Administrador del sistema: es el responsable de garantizar el funcionamiento de la infraestructura tecnológica y mantener la operatividad de los activos informáticos. Debe

ser capaz de analizar, identificar, contener y erradicar un incidente de seguridad de ser el caso.

Administrador sistemas de seguridad: es el responsable de gestionar la seguridad de los sistemas de información y las telecomunicaciones de la organización. Debe ser capaz de analizar, identificar, contener y erradicar un incidente de seguridad de ser el caso.

Analista del incidente: es el responsable de realizar una investigación de cada incidente suscitado e informar a las autoridades respectivas. El informe debe responder las siguientes interrogantes: qué, dónde, cuándo y cómo ocurrió el evento y determinar los responsables.

Gestor de comunicaciones: Su responsabilidad es comunicar a nivel interno y externo sobre el incidente ocurrido.

El CSIRT se puede conformar de manera mixta, juntando al personal interno y contratando un servicio de análisis de incidentes. FONAG debería cubrir los siguientes roles: responsable de atención al cliente, administrador del sistema y administrador de sistemas de seguridad con contrataciones a tiempo completo.

Los demás roles pueden ser cubiertos con la contratación de un servicio externo que analice y reporte las acciones necesarias para manejar de la manera óptima los incidentes que se puedan presentar en el futuro. En cuanto a los usuarios sensibilizados, la organización debe capacitar periódicamente al personal para que conozcan sobre los peligros de navegar en el internet y compartir la información personal.

6.4 Proceso resolución incidentes

En la Figura 13 se muestra el proceso que se debería seguir en caso de que se presente un incidente de seguridad de la información.

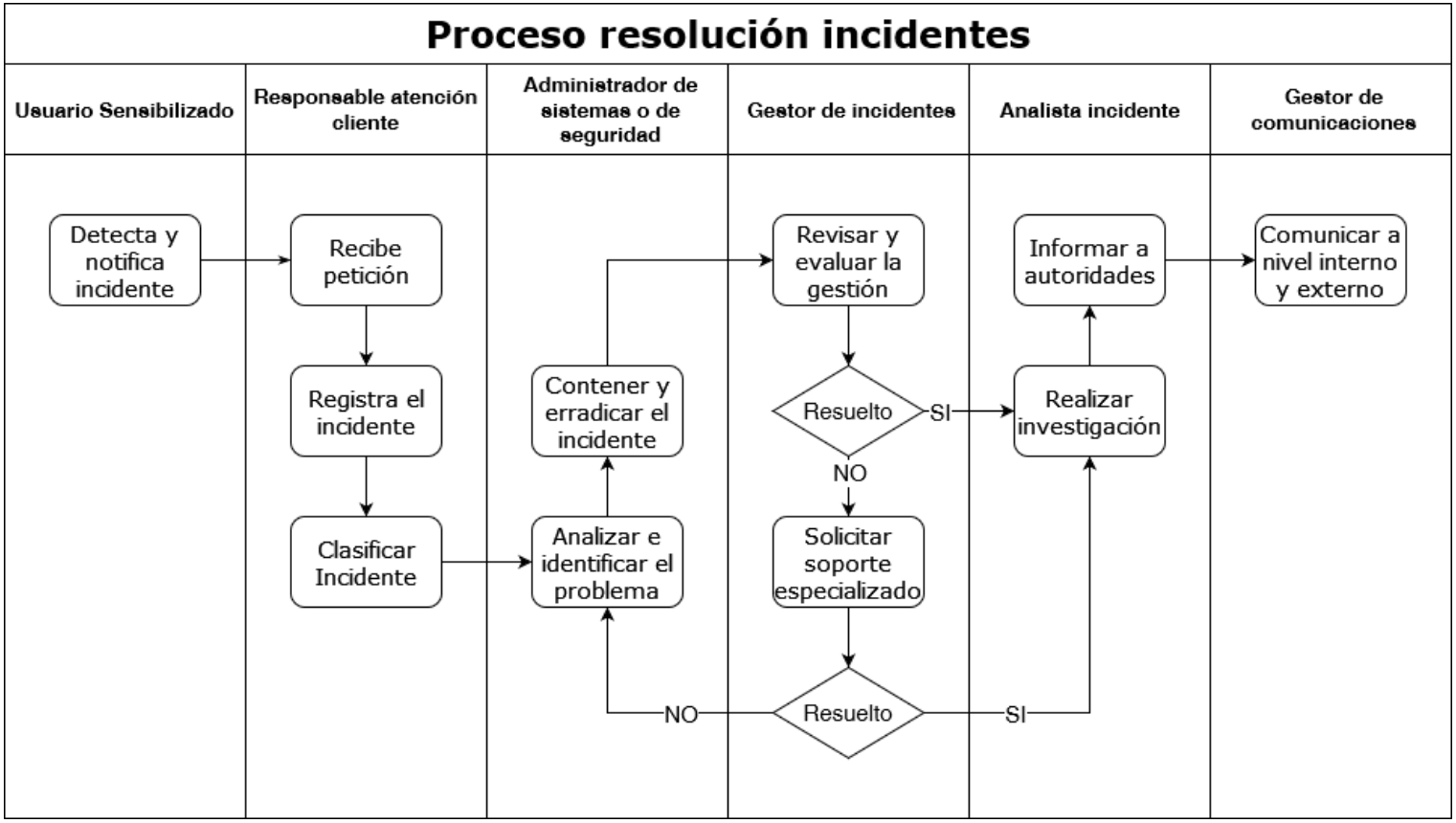

Figura 13. Gestión de Incidentes. [Elaboración propia]

6.5 Incidentes y acciones de mitigación

Para que el usuario sensibilizado pueda detectar y notificar un incidente, en la Tabla 24 se describen los principales incidentes de seguridad de la información y las acciones recomendadas para mitigarlos.

Tabla 24. Incidentes y acciones de mitigación FONAG. [Elaboración propia]

Prioridad	**Incidente Informático**	**Acciones Mitigación**
Crítica	Cualquier ataque malintencionado que tenga como objetivo dañar o destruir la información (malware)	Instalar programas de protección antivirus para evitar la instalación de software malicioso Capacitación al personal para que puedan identificar sitios maliciosos o de dudosa procedencia.
Alta	Intentos de acceso no autorizados a cualquiera de los sistemas web de la institución o servicios en la nube	Implementación de autentificación de doble factor para los servicios en la nube y sistemas web. Encriptación de información confidencial
Alta	Intentos de escalada de privilegios por parte de usuarios no autorizados.	Realizar una prueba de penetración en la arquitectura informática periódicamente para identificar y remediar las vulnerabilidades existentes. Limitar los permisos de acceso de usuario al mínimo posible para que puedan realizar su trabajo.
Crítica	Ataque malicioso o accidental por parte del personal interno, antiguos colaboradores o terceros.	Implementar programas de escaneo para software espía, antivirus, firewall. Contar con copias de seguridad periódicas.
Media	Ataques de denegación de servicio que afecten a los sistemas o equipos de la institución	Bloquear el tráfico falso en el firewall de la institución Mantener firewall actualizado con los últimos parches.
Media	Suplantación de identidad con el objetivo de obtener credenciales de acceso o distribuir programas maliciosos.	Capacitar al personal para que puedan identificar correos con suplantación de identidad. Implementar un filtro de correo electrónico para filtrar correos de phishing masivos.

Prioridad	Incidente Informático	Acciones Mitigación
Media	Intercepción o alteración de información mediante un ataque de hombre en el medio (MiTM)	Capacitar al personal sobre los riesgos de utilizar redes inalámbricas públicas. Implementar una red privada virtual (VPN) para garantizar conexiones seguras
Alta	Robo de contraseñas por parte de los atacantes.	Implementación de autentificación de doble factor para los servicios en la nube y sistemas web. Capacitar al personal sobre el manejo de gestores de contraseña.
Alta	Explotación de las vulnerabilidades del código de las aplicaciones web o de los mecanismos de autenticación	Mantener actualizado todos los paquetes, librerías y aplicativos necesarios para la ejecución del sistema web. Monitorear el tráfico de red hacia los servidores de aplicación para evitar posibles ataques.

6.6 Etapas de la gestión de incidencias

6.6.1 Preparación

Como parte de la gestión de incidentes, FONAG debe poner a disposición del especialista informático ciertos recursos para poder actuar ante cualquier ataque a la seguridad de la información. En la Tabla 25 se muestran algunas acciones preventivas que deben ejecutarse para mitigar ataques a la infraestructura informática.

Tabla 25. Acciones preventivas. [Elaboración propia]

Acciones preventivas	Responsable
Aplicar parches de seguridad y mantener actualizado el firewall	Proveedor Servicio Internet
Gestión de accesos y permisos	Especialista TICS
Revisar las reglas de seguridad del firewall de manera periódica	Especialista TICS
Instalación de software antivirus y monitoreo de la consola de administración	Técnico soporte informático
Capacitación al personal del FONAG sobre ciberseguridad	Proveedor externo

Entre los recursos hardware y software necesarios, se debe contar con las siguientes herramientas:

- Equipo forense: software libre que permita realizar un análisis post incidente de la evidencia sin contaminar la misma.
- Analizador de protocolo: software libre para resolver problemas de red, desarrollo de protocolos de comunicación y monitorear el tráfico de red.
- Gestión de activos: software que permita observar la lista de activos informáticos, asignación, ubicación física y estado.

El especialista de TICS debe asegurarse de tener la siguiente información para poder realizar un análisis forense:

- Listado de puertos activos y el sistema que los utiliza
- Diagrama de red de los recursos existentes
- Diagrama de arquitectura de los servidores físicos y en la nube
- Análisis de comportamiento de la red.

Por último, para la mitigación y remediación ante un ataque informático deben existir un respaldo de la información de cada usuario y de los servidores de aplicación.

6.6.2 Detección y análisis

En cuanto a la detección de un incidente, la principal fuente de información proviene del personal y el monitoreo de la infraestructura, por esta razón es muy importante capacitar al personal sobre los incidentes que pueden presentarse y la forma en que pueden notificar al personal correspondiente. Los reportes pueden ser mediante: whatsapp, vía telefónica y/o correo electrónico, dirigidos al responsable de atención al cliente. Para facilitar las tareas de mitigación y control se sugiere que el usuario presente el formulario del ANEXO IV.

El monitoreo de la infraestructura debe ser periódico y el responsable es especialista de TICS. Se debe revisar el funcionamiento adecuado de los activos de información y para ello debe contar con la siguiente información:

- Alertas ante caída de sistemas web
- Reportes de incidentes de seguridad
- Alertas de la consola de antivirus
- Alertas de tráfico inusual
- Espacio en disco y consumo de CPU de los equipos de computo
- Creación de cuentas de usuario
- Acceso o intento de acceso en cuentas de administrador
- Alertas de correos sospechosos o correos inusuales
- Logs de los servidores
- Logs de aplicaciones

Según [24], se deben clasificar los incidentes de seguridad con base a ciertos criterios, para este plan se tomará en cuenta la recomendación del nivel de impacto versus urgencia de resolverlo. En la Tabla 17, se definió como medir el impacto para cada uno de los activos de la institución y en la Tabla 26 se hace una correlación con el nivel de urgencia con el que se debe atender cada incidencia que se pueda presentar.

Tabla 26. Clasificación incidentes seguridad. [Elaboración propia]

		Nivel de Urgencia		
		Alta (10)	Media (6)	Baja (2)
Nivel de impacto	Muy alta (100)	100	60	20
	Alta (80)	80	48	16
	Media (60)	60	36	12
	Baja (40)	40	24	8
	Muy baja (20)	20	12	4

La prioridad se calcularía de la siguiente manera: (Nivel de impacto * Nivel de urgencia) /10. La clasificación quedaría de la siguiente manera:

- Crítico: 61 a 100
- Grave: 21 a 60
- Leve: 0-20

6.6.3 Contención, erradicación y recuperación

La contención tiene como objetivo detener el evento de seguridad, con la intención que no se propague y se pueda prevenir daños a los activos de información o fallos en la infraestructura tecnológica. En la Tabla 27, se muestran algunos ejemplos de incidentes y sus estrategias de contención.

Tabla 27. Ejemplos incidentes y contención. [Elaboración propia]

Incidente	Estrategia de contención
Cualquier ataque malintencionado que tenga como objetivo dañar o destruir la información (malware)	Aislar el equipo infectado y analizar el comportamiento del código malicioso.
Intentos de acceso no autorizados a cualquiera de los sistemas web de la institución o servicios en la nube	Bloquear del usuario y revisar los logs del sistema atacado
Intentos de escalada de privilegios por parte de usuarios no autorizados.	Bloquear del usuario, revisar los logs del sistema atacado.
Ataque malicioso o accidental por parte del personal interno, antiguos colaboradores o terceros.	Bloquear el usuario, restringir accesos compartidos y aislar aplicativos de manera temporal
Ataques de denegación de servicio que afecten a los sistemas o equipos de la institución	Bloquear el origen del ataque en el firewall y restringir el acceso al servicio caído.
Suplantación de identidad con el objetivo de obtener credenciales de acceso o distribuir programas maliciosos.	Bloquear el usuario y reiniciar la contraseña. En ciertos casos, suspender el acceso al servicio de manera temporal hasta identificar el usuario afectado
Intercepción o alteración de información mediante un ataque de hombre en el medio (MiTM)	En este tipo de incidentes, se debe enfocar en capacitar al usuario sobre los peligros de acceder a redes públicas.
Robo de contraseñas por parte de los atacantes.	Bloquear el usuario y reiniciar la contraseña. En ciertos casos, suspender el acceso al servicio de manera temporal hasta identificar el usuario afectado
Explotación de las vulnerabilidades del código de las aplicaciones web o de los mecanismos de autenticación	Levantar el aplicativo utilizando la copia de respaldo.

Una vez contenido el incidente, se procede la eliminación de cualquier rastro del evento y posteriormente se procede a la recuperación y restauración de los servicios afectados, con base las estrategias que se muestran en Tabla 28. El especialista TICS debe restablecer la funcionalidad de los sistemas afectados y aplicar salvaguardas que permitan prevenir nuevos incidentes similares en el futuro.

Tabla 28. Ejemplos de estrategias de recuperación. [Elaboración propia]

Incidente	Estrategia de recuperación
Cualquier ataque malintencionado que tenga como objetivo dañar o destruir la información (malware)	Reinstalación del sistema operativo y aplicativos. Restauración de copias de seguridad.
Intentos de acceso no autorizados a cualquiera de los sistemas web de la institución o servicios en la nube	Reinstalación del aplicativo y recuperación de datos.
Intentos de escalada de privilegios por parte de usuarios no autorizados.	Reinstalación del aplicativo y recuperación de datos
Ataque malicioso o accidental por parte del personal interno, antiguos colaboradores o terceros.	Reinstalación del sistema operativo y aplicativos. Restauración de copias de seguridad
Ataques de denegación de servicio que afecten a los sistemas o equipos de la institución	Restitución del servicio caído.
Suplantación de identidad con el objetivo de obtener credenciales de acceso o distribuir programas maliciosos.	Reseteo de contraseñas Reinstalación del sistema operativo y aplicativos. Restauración de copias de seguridad.
Intercepción o alteración de información mediante un ataque de hombre en el medio (MiTM)	Reseteo de contraseñas
Robo de contraseñas por parte de los atacantes.	Reseteo de contraseñas Reinstalación del aplicativo y recuperación de datos
Explotación de las vulnerabilidades del código de las aplicaciones web o de los mecanismos de autenticación	Reparar el aplicativo web, actualizar librerías y paquetes, restaurar el servicio

6.6.4 Actividades posts-incidentes

Luego de erradicar los rastros dejados por incidente y restaurar los servicios afectados es imprescindible registrar todas las actividades realizadas por el equipo CIRST, con la finalidad de evaluar la gestión del equipo y mejorar los controles de seguridad. En el ANEXO V se muestran las tablas de información que se deben llenar por cada incidente suscitado dentro de la organización.

Por cada evento de seguridad suscitado se debe realizar un informe que resumas todas las acciones realizadas, junto con las medidas que se tomaran para evitarlas en el futuro. Este documento debe ser enviado a la máxima autoridad para que tenga conocimiento y disponga de los recursos necesarios para mitigar las amenazas latentes.

CAPÍTULO 7. CONCLUSIONES

- Se realizó un análisis y comparación de las diferentes metodologías de evaluación de riesgos de seguridad de la información, investigando sus principales características, fases, tipo de enfoque, tipos de riesgos que abordan, elementos de análisis y objetivos; con esto se determinó que Magerit era la metodología que más se acopla a las necesidades del FONAG y el objeto de estudio de esta tesis.
- Se revisó la situación actual del FONAG en cuanto a procesos críticos, aplicaciones utilizadas y la información que manejan y se seleccionó el proceso “Adquisición de bienes y servicios”, donde se estudiaron las amenazas, activos de la información, vulnerabilidad y riesgos.
- Se implementó, todas las fases de la metodología de análisis de riesgos Magerit, y se determinó el nivel de impacto actual y residual para cada uno de los activos de la información que intervienen en el proceso de “adquisición de bienes y servicios”.
- Se desarrolló un plan de gestión de incidencias considerando los recursos disponibles del FONAG, para los servicios de TI existentes que permita gestionar los eventos de seguridad que se presenten en el futuro.

CAPÍTULO 8. RECOMENDACIONES

- Realizar un análisis de riesgo de manera periódica para los procesos críticos de la institución y determinar el nivel de impacto al que están expuestos, con la finalidad de mejorar las existentes o implementar nuevas salvaguardas.

- Considerar incluir el área de tics dentro de la estructura organizacional de la institución y el plan estratégico del 2025-2030, para que se pueda evaluar la gestión de la infraestructura tecnológica y la seguridad de la información de manera más efectiva.

REFERENCIAS BIBLIOGRÁFICAS

[1] Banco Interamericano de Desarrollo; Organización de los Estados Americanos, «CIBERSEGURIDAD», 2020. doi: http://dx.doi.org/10.18235/0002513.

[2] R. Katz, J. Juan, y F. Callorda, «El estado de la digitalización de América Latina frente a la pandemia del COVID-19», *Banco de Desarrollo de América Latina - Corporación Andina de Fomento (CAF)*, pp. 1-40, 2020.

[3] S. Morrow, «ThreatMetrix Cybercrime Report: An interview», 2019. https://bit.ly/2Zu0ELr (accedido 17 de febrero de 2021).

[4] MARSH, «El riesgo cibernético ya es prioridad empresarial en Latinoamérica, pero hay que mejorar», 2021. https://bit.ly/37rrg4a (accedido 17 de diciembre de 2021).

[5] R. Chávez, «Estado Actual de la Ciberseguridad 2020 Ecuador», *ITahora*, pp. 1-18, 2026.

[6] M. Ocampo, «Artículo de revisión de Metodologías de Análisis de Riesgos de la Información, enfocado a Pymes.», pp. 1-22, 2019.

[7] M. A. Amutio, J. Candau, y J. A. Mañas, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, Tercera. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. doi: 630-12-171-8.

[8] A. Abril, J. Pulido, y J. A. Bohada, «Análisis de riesgos en seguridad de la información», *Polo del Conocimiento*, vol. 3, n.º 4, p. 230, 2013, doi: 10.23857/pc.v3i4.809.

[9] C. Alberts, A. Dorofee, J. Stevens, y C. Woody, «Introduction to the OCTAVE Approach», 2003. doi: 10.1016/b978-0-7020-3055-0.00004-2.

[10] National Institute Standards and Technology, «NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments», *NIST Special Publication*, n.º September, p. 95, 2012.

[11] CEDIA-ISO, «Gestión del riesgo de las TI NTC 27005», 2008.

[12] M. Zevallos, «Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte», *Revista Peruana de Computación y Sistemas*, vol. 2, n.º 1, pp. 43-60, 2019.

[13] V. Jiménez Chaves, «El estudio de caso y su implementación en la investigación», *Revista Internacional de Investigación en Ciencias Sociales*, vol. 8, n.º 1, pp. 141-150, 2012.

[14] P. C. Martínez Carazo, «El método de estudio de caso Estrategia metodológica de la investigación científica», *pensamiento y gestión*, vol. N20, p. 29, 2006.

[15] E. Yacuzzi, «El estudio de caso como metodología de investigación: Teoría, mecanismos causales, validación», *econstor*, 2005.

[16] W. Stallings, *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE*, Septima. Harlow: PearsonEducation Limited, 2017.

[17] F. J. Valencia-Duque y 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 Iberica de Sistemas e Tecnologias de Informacao*, n.º 22, pp. 73-88, 2017, doi: 10.17013/risti.22.73-88.

[18] J. P. Kindinger y J. L. Darby, «Risk factor analysis—a new qualitative risk management tool», *Project Management Institute Annual Seminars & Symposium*, 2000.

[19] B. B. Roberts, «The Benefits of Integrated, Quantitative Risk Management», *INCOSE International Symposium*, vol. 11, n.º 1, pp. 120-125, 2001, doi: 10.1002/j.2334-5837.2001.tb02282.x.

[20] FONAG, «FONAG», *FONAG*, 2019. https://www.fonag.org.ec/web/ (accedido 1 de agosto de 2023).

[21] Fondo para la protección del Agua, «Plan Estratégico FONAG 2021-2025».

[22] M. A. Amutio, J. Candau, y J. A. Mañas, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*. 2012. [En línea]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

[23] M. A. Amutio, J. Candau, y J. A. Mañas, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*. 2012. [En línea]. Disponible en: http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Areadescargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

[24] «Código de prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)», may 2017. [En línea]. Disponible en: www.aenor.com

[25] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, y M. Zajicek, «Handbook for Computer Security Incident Response Teams (CSIRTs)», 20003.

ANEXOS

ANEXO I. Detalle de amenazas por activos

Categoría: [D] Datos / Información

Tabla 29. Registro de amenazas para los activos de la categoría Datos/Información. [Elaboración propia]

Código Activo	Amenaza
BACKUP_SERVIDORES_AWS	[E.2 Errores del administrador]
BACKUP_SERVIDORES_AWS	[E.15 Alteración accidental de la información]
BACKUP_SERVIDORES_AWS	[E.18 Destrucción de información]
BACKUP_SERVIDORES_AWS	[E.19 Fugas de información]
BACKUP_SERVIDORES_AWS	[A.5 Suplantación de la identidad del usuario]
BACKUP_SERVIDORES_AWS	[A.6 Abuso de privilegios de acceso]
BACKUP_SERVIDORES_AWS	[A.7 Uso no previsto]
BACKUP_SERVIDORES_AWS	[A.11 Acceso no autorizado]
BACKUP_SERVIDORES_AWS	[A.15 Modificación deliberada de la información]
BACKUP_SERVIDORES_AWS	[A.18 Destrucción de información]
BACKUP_SERVIDORES_AWS	[A.19 Divulgación de información]
FILES_USUARIO	[E.1 Errores de los usuarios]
FILES_USUARIO	[E.2 Errores del administrador]
FILES_USUARIO	[E.15 Alteración accidental de la información]
FILES_USUARIO	[E.18 Destrucción de información]
FILES_USUARIO	[E.19 Fugas de información]
FILES_USUARIO	[A.5 Suplantación de la identidad del usuario]
FILES_USUARIO	[A.6 Abuso de privilegios de acceso]
FILES_USUARIO	[A.7 Uso no previsto]
FILES_USUARIO	[A.11 Acceso no autorizado]
FILES_USUARIO	[A.15 Modificación deliberada de la información]
FILES_USUARIO	[A.18 Destrucción de información]
FILES_USUARIO	[A.19 Divulgación de información]
LOG_SCPF	[E.2 Errores del administrador]
LOG_SCPF	[E.18 Destrucción de información]
LOG_SCPF	[E.19 Fugas de información]
LOG_SCPF	[A.3 Manipulación de los registros de actividad (log]
LOG_SCPF	[A.4 Manipulación de la configuración]
LOG_SCPF	[A.5 Suplantación de la identidad del usuario]
LOG_SCPF	[A.6 Abuso de privilegios de acceso]
LOG_SCPF	[A.7 Uso no previsto]
LOG_SCPF	[A.11 Acceso no autorizado]
LOG_SCPF	[A.13 Repudio]
LOG_SCPF	[A.15 Modificación deliberada de la información]
LOG_SCPF	[A.18 Destrucción de información]
LOG_SCPF	[A.19 Divulgación de información]
PASSWORD_SERVICIOS	[E.2 Errores del administrador]
PASSWORD_SERVICIOS	[E.15 Alteración accidental de la información]

Código Activo	Amenaza
PASSWORD_SERVICIOS	[E.18 Destrucción de información]
PASSWORD_SERVICIOS	[E.19 Fugas de información]
PASSWORD_SERVICIOS	[A.5 Suplantación de la identidad del usuario]
PASSWORD_SERVICIOS	[A.6 Abuso de privilegios de acceso]
PASSWORD_SERVICIOS	[A.7 Uso no previsto]
PASSWORD_SERVICIOS	[A.11 Acceso no autorizado]
PASSWORD_SERVICIOS	[A.15 Modificación deliberada de la información]
PASSWORD_SERVICIOS	[A.18 Destrucción de información]
PASSWORD_SERVICIOS	[A.19 Divulgación de información]
VR_REPOSITORIO_PROCESOS	[E.1 Errores de los usuarios]
VR_REPOSITORIO_PROCESOS	[E.2 Errores del administrador]
VR_REPOSITORIO_PROCESOS	[E.15 Alteración accidental de la información]
VR_REPOSITORIO_PROCESOS	[E.18 Destrucción de información]
VR_REPOSITORIO_PROCESOS	[E.19 Fugas de información]
VR_REPOSITORIO_PROCESOS	[A.5 Suplantación de la identidad del usuario]
VR_REPOSITORIO_PROCESOS	[A.6 Abuso de privilegios de acceso]
VR_REPOSITORIO_PROCESOS	[A.7 Uso no previsto]
VR_REPOSITORIO_PROCESOS	[A.11 Acceso no autorizado]
VR_REPOSITORIO_PROCESOS	[A.15 Modificación deliberada de la información]
VR_REPOSITORIO_PROCESOS	[A.18 Destrucción de información]
VR_REPOSITORIO_PROCESOS	[A.19 Divulgación de información]

Categoría: [S] Servicios

Tabla 30. Registro de amenazas para los activos de la categoría Servicios. [Elaboración propia]

Código Activo	Amenaza
EMAIL_GOOGLE	[E.2 Errores del administrador]
EMAIL_GOOGLE	[E.9 Errores de [re-]encaminamiento]
EMAIL_GOOGLE	[E.10 Errores de secuencia]
EMAIL_GOOGLE	[E.15 Alteración accidental de la información]
EMAIL_GOOGLE	[E.18 Destrucción de información]
EMAIL_GOOGLE	[E.19 Fugas de información]
EMAIL_GOOGLE	[E.24 Caída del sistema por agotamiento de recursos]
EMAIL_GOOGLE	[A.5 Suplantación de la identidad del usuario]
EMAIL_GOOGLE	[A.6 Abuso de privilegios de acceso]
EMAIL_GOOGLE	[A.7 Uso no previsto]
EMAIL_GOOGLE	[A.9 [Re-]encaminamiento de mensajes]
EMAIL_GOOGLE	[A.10 Alteración de secuencia]
EMAIL_GOOGLE	[A.11 Acceso no autorizado]
EMAIL_GOOGLE	[A.13 Repudio]
EMAIL_GOOGLE	[A.15 Modificación deliberada de la información]
EMAIL_GOOGLE	[A.18 Destrucción de información]

Código Activo	Amenaza
EMAIL_GOOGLE	[A.19 Divulgación de información]
EMAIL_GOOGLE	[A.24 Denegación de servicio]

Categoría: [SW] Aplicaciones (Software)

Tabla 31. Registro de amenazas para los activos de la categoría Aplicaciones (Software). [Elaboración propia]

Código Activo	Amenaza
AV_KARPERSKY	[I.5 Avería de origen físico o lógico]
AV_KARPERSKY	[E.2 Errores del administrador]
AV_KARPERSKY	[E.8 Difusión de software dañino]
AV_KARPERSKY	[E.19 Fugas de información]
AV_KARPERSKY	[E.20 Vulnerabilidades de los programas (software)]
AV_KARPERSKY	[E.21 Errores de mantenimiento / actualización de programas (software)]
AV_KARPERSKY	[A.5 Suplantación de la identidad del usuario]
AV_KARPERSKY	[A.6 Abuso de privilegios de acceso]
AV_KARPERSKY	[A.7 Uso no previsto]
AV_KARPERSKY	[A.8 Difusión de software dañino]
AV_KARPERSKY	[A.9 [Re-]encaminamiento de mensajes]
AV_KARPERSKY	[A.10 Alteración de secuencia]
AV_KARPERSKY	[A.11 Acceso no autorizado]
AV_KARPERSKY	[A.15 Modificación deliberada de la información]
AV_KARPERSKY	[A.18 Destrucción de información]
AV_KARPERSKY	[A.19 Divulgación de información]
AV_KARPERSKY	[A.22 Manipulación de programas]
OFFICE_MICROSOFT	[I.5 Avería de origen físico o lógico]
OFFICE_MICROSOFT	[E.2 Errores del administrador]
OFFICE_MICROSOFT	[E.8 Difusión de software dañino]
OFFICE_MICROSOFT	[E.9 Errores de [re-]encaminamiento]
OFFICE_MICROSOFT	[E.19 Fugas de información]
OFFICE_MICROSOFT	[E.20 Vulnerabilidades de los programas (software)]
OFFICE_MICROSOFT	[E.21 Errores de mantenimiento / actualización de programas (software)]
OFFICE_MICROSOFT	[A.5 Suplantación de la identidad del usuario]
OFFICE_MICROSOFT	[A.6 Abuso de privilegios de acceso]
OFFICE_MICROSOFT	[A.7 Uso no previsto]
OFFICE_MICROSOFT	[A.8 Difusión de software dañino]
OFFICE_MICROSOFT	[A.9 [Re-]encaminamiento de mensajes]
OFFICE_MICROSOFT	[A.10 Alteración de secuencia]
OFFICE_MICROSOFT	[A.11 Acceso no autorizado]
OFFICE_MICROSOFT	[A.15 Modificación deliberada de la información]
OFFICE_MICROSOFT	[A.18 Destrucción de información]
OFFICE_MICROSOFT	[A.19 Divulgación de información]
OFFICE_MICROSOFT	[A.22 Manipulación de programas]

Código Activo	Amenaza
OS_WINDOWS_UBUNTU	[I.5 Avería de origen físico o lógico]
OS_WINDOWS_UBUNTU	[E.1 Errores de los usuarios]
OS_WINDOWS_UBUNTU	[E.2 Errores del administrador]
OS_WINDOWS_UBUNTU	[E.8 Difusión de software dañino]
OS_WINDOWS_UBUNTU	[E.19 Fugas de información]
OS_WINDOWS_UBUNTU	[E.20 Vulnerabilidades de los programas (software)]
OS_WINDOWS_UBUNTU	[E.21 Errores de mantenimiento / actualización de programas (software)]
OS_WINDOWS_UBUNTU	[A.5 Suplantación de la identidad del usuario]
OS_WINDOWS_UBUNTU	[A.6 Abuso de privilegios de acceso]
OS_WINDOWS_UBUNTU	[A.7 Uso no previsto]
OS_WINDOWS_UBUNTU	[A.8 Difusión de software dañino]
OS_WINDOWS_UBUNTU	[A.9 [Re-]encaminamiento de mensajes]
OS_WINDOWS_UBUNTU	[A.10 Alteración de secuencia]
OS_WINDOWS_UBUNTU	[A.11 Acceso no autorizado]
OS_WINDOWS_UBUNTU	[A.15 Modificación deliberada de la información]
OS_WINDOWS_UBUNTU	[A.18 Destrucción de información]
OS_WINDOWS_UBUNTU	[A.19 Divulgación de información]
OS_WINDOWS_UBUNTU	[A.22 Manipulación de programas]
SUB_SCPF	[I.5 Avería de origen físico o lógico]
SUB_SCPF	[E.1 Errores de los usuarios]
SUB_SCPF	[E.2 Errores del administrador]
SUB_SCPF	[E.8 Difusión de software dañino]
SUB_SCPF	[E.10 Errores de secuencia]
SUB_SCPF	[E.15 Alteración accidental de la información]
SUB_SCPF	[E.19 Fugas de información]
SUB_SCPF	[E.20 Vulnerabilidades de los programas (software)]
SUB_SCPF	[E.21 Errores de mantenimiento / actualización de programas (software)]
SUB_SCPF	[A.5 Suplantación de la identidad del usuario]
SUB_SCPF	[A.6 Abuso de privilegios de acceso]
SUB_SCPF	[A.7 Uso no previsto]
SUB_SCPF	[A.8 Difusión de software dañino]
SUB_SCPF	[A.9 [Re-]encaminamiento de mensajes]
SUB_SCPF	[A.10 Alteración de secuencia]
SUB_SCPF	[A.11 Acceso no autorizado]
SUB_SCPF	[A.15 Modificación deliberada de la información]
SUB_SCPF	[A.18 Destrucción de información]
SUB_SCPF	[A.19 Divulgación de información]
SUB_SCPF	[A.22 Manipulación de programas]
SUB_SCPF_PRUEBAS	[I.5 Avería de origen físico o lógico]
SUB_SCPF_PRUEBAS	[E.1 Errores de los usuarios]
SUB_SCPF_PRUEBAS	[E.2 Errores del administrador]
SUB_SCPF_PRUEBAS	[E.8 Difusión de software dañino]
SUB_SCPF_PRUEBAS	[E.19 Fugas de información]
SUB_SCPF_PRUEBAS	[E.20 Vulnerabilidades de los programas (software)]

Código Activo	Amenaza
SUB_SCPF_PRUEBAS	[E.21 Errores de mantenimiento / actualización de programas (software)]
SUB_SCPF_PRUEBAS	[A.5 Suplantación de la identidad del usuario]
SUB_SCPF_PRUEBAS	[A.6 Abuso de privilegios de acceso]
SUB_SCPF_PRUEBAS	[A.7 Uso no previsto]
SUB_SCPF_PRUEBAS	[A.8 Difusión de software dañino]
SUB_SCPF_PRUEBAS	[A.9 [Re-]encaminamiento de mensajes]
SUB_SCPF_PRUEBAS	[A.10 Alteración de secuencia]
SUB_SCPF_PRUEBAS	[A.11 Acceso no autorizado]
SUB_SCPF_PRUEBAS	[A.15 Modificación deliberada de la información]
SUB_SCPF_PRUEBAS	[A.18 Destrucción de información]
SUB_SCPF_PRUEBAS	[A.19 Divulgación de información]
SUB_SCPF_PRUEBAS	[A.22 Manipulación de programas]

Categoría: [HW] Equipos

Tabla 32. Registro de amenazas para los activos de la categoría Equipos. [Elaboración propia]

Código Activo	Amenaza
FIREWALL_FORTINET	[N.1 Fuego]
FIREWALL_FORTINET	[N.2 Daños por agua]
FIREWALL_FORTINET	[N.* Otros]
FIREWALL_FORTINET	[I.1 Fuego]
FIREWALL_FORTINET	[I.2 Daños por agua]
FIREWALL_FORTINET	[I.* Otros]
FIREWALL_FORTINET	[I.3 Contaminación mecánica]
FIREWALL_FORTINET	[I.5 Avería de origen físico o lógico]
FIREWALL_FORTINET	[I.6 Corte del suministro eléctrico]
FIREWALL_FORTINET	[I.7 Condiciones inadecuadas de temperatura o humedad]
FIREWALL_FORTINET	[I.11 Emanaciones electromagnéticas]
FIREWALL_FORTINET	[E.2 Errores del administrador]
FIREWALL_FORTINET	[E.23 Errores de mantenimiento / actualización de equipos (hardware)]
FIREWALL_FORTINET	[E.24 Caída del sistema por agotamiento de recursos]
FIREWALL_FORTINET	[E.25 Pérdida de equipos]
FIREWALL_FORTINET	[A.6 Abuso de privilegios de acceso]
FIREWALL_FORTINET	[A.7 Uso no previsto]
FIREWALL_FORTINET	[A.11 Acceso no autorizado]
FIREWALL_FORTINET	[A.23 Manipulación de los equipos]
FIREWALL_FORTINET	[A.24 Denegación de servicio]
FIREWALL_FORTINET	[A.25 Robo]
FIREWALL_FORTINET	[A.26 Ataque destructivo]
HOST_SCPF	[E.2 Errores del administrador]
HOST_SCPF	[E.24 Caída del sistema por agotamiento de recursos]
HOST_SCPF	[A.6 Abuso de privilegios de acceso]

Código Activo	Amenaza
HOST_SCPF	[A.7 Uso no previsto]
HOST_SCPF	[A.11 Acceso no autorizado]
HOST_SCPF	[A.24 Denegación de servicio]
HOST_SCPF	[A.26 Ataque destructivo]
HOST_SCPF_PRUEBAS	[E.2 Errores del administrador]
HOST_SCPF_PRUEBAS	[E.24 Caída del sistema por agotamiento de recursos]
HOST_SCPF_PRUEBAS	[A.6 Abuso de privilegios de acceso]
HOST_SCPF_PRUEBAS	[A.7 Uso no previsto]
HOST_SCPF_PRUEBAS	[A.11 Acceso no autorizado]
HOST_SCPF_PRUEBAS	[A.24 Denegación de servicio]
HOST_SCPF_PRUEBAS	[A.26 Ataque destructivo]
PC_TRABAJO	[N.1 Fuego]
PC_TRABAJO	[N.2 Daños por agua]
PC_TRABAJO	[N.* Otros]
PC_TRABAJO	[I.1 Fuego]
PC_TRABAJO	[I.2 Daños por agua]
PC_TRABAJO	[I.* Otros]
PC_TRABAJO	[I.3 Contaminación mecánica]
PC_TRABAJO	[I.5 Avería de origen físico o lógico]
PC_TRABAJO	[I.6 Corte del suministro eléctrico]
PC_TRABAJO	[I.7 Condiciones inadecuadas de temperatura o humedad]
PC_TRABAJO	[I.11 Emanaciones electromagnéticas]
PC_TRABAJO	[E.2 Errores del administrador]
PC_TRABAJO	[E.23 Errores de mantenimiento / actualización de equipos (hardware)]
PC_TRABAJO	[E.24 Caída del sistema por agotamiento de recursos]
PC_TRABAJO	[E.25 Pérdida de equipos]
PC_TRABAJO	[A.6 Abuso de privilegios de acceso]
PC_TRABAJO	[A.7 Uso no previsto]
PC_TRABAJO	[A.11 Acceso no autorizado]
PC_TRABAJO	[A.23 Manipulación de los equipos]
PC_TRABAJO	[A.24 Denegación de servicio]
PC_TRABAJO	[A.25 Robo]
PC_TRABAJO	[A.26 Ataque destructivo]
ROUTER_HP	[N.1 Fuego]
ROUTER_HP	[N.2 Daños por agua]
ROUTER_HP	[N.* Otros]
ROUTER_HP	[I.1 Fuego]
ROUTER_HP	[I.2 Daños por agua]
ROUTER_HP	[I.* Otros]
ROUTER_HP	[I.3 Contaminación mecánica]
ROUTER_HP	[I.5 Avería de origen físico o lógico]
ROUTER_HP	[I.6 Corte del suministro eléctrico]
ROUTER_HP	[I.7 Condiciones inadecuadas de temperatura o humedad]
ROUTER_HP	[I.9 Interrupción de otros servicios y suministros esenciales]

Código Activo	Amenaza
ROUTER_HP	[I.11 Emanaciones electromagnéticas]
ROUTER_HP	[E.2 Errores del administrador]
ROUTER_HP	[E.23 Errores de mantenimiento / actualización de equipos (hardware)]
ROUTER_HP	[E.24 Caída del sistema por agotamiento de recursos]
ROUTER_HP	[E.25 Pérdida de equipos]
ROUTER_HP	[A.6 Abuso de privilegios de acceso]
ROUTER_HP	[A.7 Uso no previsto]
ROUTER_HP	[A.23 Manipulación de los equipos]
ROUTER_HP	[A.24 Denegación de servicio]
ROUTER_HP	[A.25 Robo]
ROUTER_HP	[A.26 Ataque destructivo]

Categoría: [COM] Redes de Comunicaciones

Tabla 33. Registro de amenazas para los activos de la categoría Redes de Comunicaciones. [Elaboración propia]

Código Activo	Amenaza
INTERNET_TELCONET	[I.8 Fallo de servicios de comunicaciones]
INTERNET_TELCONET	[E.2 Errores del administrador]
INTERNET_TELCONET	[E.9 Errores de [re-]encaminamiento]
INTERNET_TELCONET	[E.10 Errores de secuencia]
INTERNET_TELCONET	[E.19 Fugas de información]
INTERNET_TELCONET	[E.24 Caída del sistema por agotamiento de recursos]
INTERNET_TELCONET	[A.5 Suplantación de la identidad del usuario]
INTERNET_TELCONET	[A.6 Abuso de privilegios de acceso]
INTERNET_TELCONET	[A.7 Uso no previsto]
INTERNET_TELCONET	[A.9 [Re-]encaminamiento de mensajes]
INTERNET_TELCONET	[A.10 Alteración de secuencia]
INTERNET_TELCONET	[A.12 Análisis de tráfico]
INTERNET_TELCONET	[A.14 Interceptación de información (escucha)]
INTERNET_TELCONET	[A.15 Modificación deliberada de la información]
INTERNET_TELCONET	[A.19 Divulgación de información]
INTERNET_TELCONET	[A.24 Denegación de servicio]
LAN_CAT5	[I.8 Fallo de servicios de comunicaciones]
LAN_CAT5	[E.2 Errores del administrador]
LAN_CAT5	[E.9 Errores de [re-]encaminamiento]
LAN_CAT5	[E.10 Errores de secuencia]
LAN_CAT5	[E.19 Fugas de información]
LAN_CAT5	[E.24 Caída del sistema por agotamiento de recursos]
LAN_CAT5	[A.5 Suplantación de la identidad del usuario]
LAN_CAT5	[A.6 Abuso de privilegios de acceso]
LAN_CAT5	[A.7 Uso no previsto]
LAN_CAT5	[A.9 [Re-]encaminamiento de mensajes]

Código Activo	Amenaza
LAN_CAT5	[A.10 Alteración de secuencia]
LAN_CAT5	[A.11 Acceso no autorizado]
LAN_CAT5	[A.12 Análisis de tráfico]
LAN_CAT5	[A.14 Interceptación de información (escucha)]
LAN_CAT5	[A.19 Divulgación de información]
LAN_CAT5	[A.24 Denegación de servicio]
WIFI_UBIQUITI	[I.8 Fallo de servicios de comunicaciones]
WIFI_UBIQUITI	[E.2 Errores del administrador]
WIFI_UBIQUITI	[E.9 Errores de [re-]encaminamiento]
WIFI_UBIQUITI	[E.10 Errores de secuencia]
WIFI_UBIQUITI	[E.19 Fugas de información]
WIFI_UBIQUITI	[E.24 Caída del sistema por agotamiento de recursos]
WIFI_UBIQUITI	[A.5 Suplantación de la identidad del usuario]
WIFI_UBIQUITI	[A.6 Abuso de privilegios de acceso]
WIFI_UBIQUITI	[A.7 Uso no previsto]
WIFI_UBIQUITI	[A.9 [Re-]encaminamiento de mensajes]
WIFI_UBIQUITI	[A.10 Alteración de secuencia]
WIFI_UBIQUITI	[A.11 Acceso no autorizado]
WIFI_UBIQUITI	[A.12 Análisis de tráfico]
WIFI_UBIQUITI	[A.14 Interceptación de información (escucha)]
WIFI_UBIQUITI	[A.15 Modificación deliberada de la información]
WIFI_UBIQUITI	[A.19 Divulgación de información]
WIFI_UBIQUITI	[A.24 Denegación de servicio]

Categoría: [AUX] Equipamiento auxiliar

Tabla 34. Registro de amenazas para los activos de la categoría Equipamiento Auxiliar. [Elaboración propia]

Código Activo	Amenaza
CABLING_FONAG	[N.1 Fuego]
CABLING_FONAG	[N.2 Daños por agua]
CABLING_FONAG	[N.* Otros]
CABLING_FONAG	[I.1 Fuego]
CABLING_FONAG	[I.2 Daños por agua]
CABLING_FONAG	[I.* Otros]
CABLING_FONAG	[I.3 Contaminación mecánica]
CABLING_FONAG	[I.5 Avería de origen físico o lógico]
CABLING_FONAG	[I.6 Corte del suministro eléctrico]
CABLING_FONAG	[I.7 Condiciones inadecuadas de temperatura o humedad]
CABLING_FONAG	[I.9 Interrupción de otros servicios y suministros esenciales]
CABLING_FONAG	[I.11 Emanaciones electromagnéticas]
CABLING_FONAG	[E.23 Errores de mantenimiento / actualización de equipos (hardware)]
CABLING_FONAG	[E.25 Pérdida de equipos]

Código Activo	Amenaza
CABLING_FONAG	[A.7 Uso no previsto]
CABLING_FONAG	[A.23 Manipulación de los equipos]
CABLING_FONAG	[A.25 Robo]
CABLING_FONAG	[A.26 Ataque destructivo]
UPS_PC_PERSONAL	[N.1 Fuego]
UPS_PC_PERSONAL	[N.2 Daños por agua]
UPS_PC_PERSONAL	[N.* Otros]
UPS_PC_PERSONAL	[I.1 Fuego]
UPS_PC_PERSONAL	[I.2 Daños por agua]
UPS_PC_PERSONAL	[I.* Otros]
UPS_PC_PERSONAL	[I.3 Contaminación mecánica]
UPS_PC_PERSONAL	[I.5 Avería de origen físico o lógico]
UPS_PC_PERSONAL	[I.6 Corte del suministro eléctrico]
UPS_PC_PERSONAL	[I.7 Condiciones inadecuadas de temperatura o humedad]
UPS_PC_PERSONAL	[I.11 Emanaciones electromagnéticas]
UPS_PC_PERSONAL	[E.23 Errores de mantenimiento / actualización de equipos (hardware)]
UPS_PC_PERSONAL	[E.25 Pérdida de equipos]
UPS_PC_PERSONAL	[A.7 Uso no previsto]
UPS_PC_PERSONAL	[A.23 Manipulación de los equipos]
UPS_PC_PERSONAL	[A.25 Robo]
UPS_PC_PERSONAL	[A.26 Ataque destructivo]

Categoría: [L] Instalaciones

Tabla 35. Registro de amenazas para los activos de la categoría Instalaciones. [Elaboración propia]

Código Activo	Amenaza
BUILDING_FONAG	[N.1 Fuego]
BUILDING_FONAG	[N.2 Daños por agua]
BUILDING_FONAG	[N.* Otros]
BUILDING_FONAG	[I.1 Fuego]
BUILDING_FONAG	[I.2 Daños por agua]
BUILDING_FONAG	[I.* Otros]
BUILDING_FONAG	[I.11 Emanaciones electromagnéticas]
BUILDING_FONAG	[E.19 Fugas de información]
BUILDING_FONAG	[A.7 Uso no previsto]
BUILDING_FONAG	[A.11 Acceso no autorizado]
BUILDING_FONAG	[A.26 Ataque destructivo]
BUILDING_FONAG	[A.27 Ocupación enemiga]

Categoría: [P] Personal

Tabla 36. Registro de amenazas para los activos de la categoría Personal. [Elaboración propia]

Código Activo	Amenaza
UI_ABG_FONAG	[E.7 Deficiencias en la organización]
UI_ABG_FONAG	[E.19 Fugas de información]
UI_ABG_FONAG	[E.28 Indisponibilidad del personal]
UI_ABG_FONAG	[A.28 Indisponibilidad del personal]
UI_ABG_FONAG	[A.29 Extorsión]
UI_ABG_FONAG	[A.30 Ingeniería social (picaresca)]
UI_ACP_FONAG	[E.7 Deficiencias en la organización]
UI_ACP_FONAG	[E.19 Fugas de información]
UI_ACP_FONAG	[E.28 Indisponibilidad del personal]
UI_ACP_FONAG	[A.28 Indisponibilidad del personal]
UI_ACP_FONAG	[A.29 Extorsión]
UI_ACP_FONAG	[A.30 Ingeniería social (picaresca)]
UI_ASADF_FONAG	[E.7 Deficiencias en la organización]
UI_ASADF_FONAG	[E.19 Fugas de información]
UI_ASADF_FONAG	[E.28 Indisponibilidad del personal]
UI_ASADF_FONAG	[A.28 Indisponibilidad del personal]
UI_ASADF_FONAG	[A.29 Extorsión]
UI_ASADF_FONAG	[A.30 Ingeniería social (picaresca)]
UI_CADF_FONAG	[E.7 Deficiencias en la organización]
UI_CADF_FONAG	[E.19 Fugas de información]
UI_CADF_FONAG	[E.28 Indisponibilidad del personal]
UI_CADF_FONAG	[A.28 Indisponibilidad del personal]
UI_CADF_FONAG	[A.29 Extorsión]
UI_CADF_FONAG	[A.30 Ingeniería social (picaresca)]
UI_COORD_FONAG	[E.7 Deficiencias en la organización]
UI_COORD_FONAG	[E.19 Fugas de información]
UI_COORD_FONAG	[E.28 Indisponibilidad del personal]
UI_COORD_FONAG	[A.28 Indisponibilidad del personal]
UI_COORD_FONAG	[A.29 Extorsión]
UI_COORD_FONAG	[A.30 Ingeniería social (picaresca)]
UI_RES_TI	[E.7 Deficiencias en la organización]
UI_RES_TI	[E.19 Fugas de información]
UI_RES_TI	[E.28 Indisponibilidad del personal]
UI_RES_TI	[A.28 Indisponibilidad del personal]
UI_RES_TI	[A.29 Extorsión]
UI_RES_TI	[A.30 Ingeniería social (picaresca)]
UI_RMS_FONAG	[E.7 Deficiencias en la organización]
UI_RMS_FONAG	[E.19 Fugas de información]
UI_RMS_FONAG	[E.28 Indisponibilidad del personal]
UI_RMS_FONAG	[A.28 Indisponibilidad del personal]
UI_RMS_FONAG	[A.29 Extorsión]
UI_RMS_FONAG	[A.30 Ingeniería social (picaresca)]

Código Activo	Amenaza
UI_SOPORTE_TI	[E.7 Deficiencias en la organización]
UI_SOPORTE_TI	[E.19 Fugas de información]
UI_SOPORTE_TI	[E.28 Indisponibilidad del personal]
UI_SOPORTE_TI	[A.28 Indisponibilidad del personal]
UI_SOPORTE_TI	[A.29 Extorsión]
UI_SOPORTE_TI	[A.30 Ingeniería social (picaresca)]
UI_ST_FONAG	[E.7 Deficiencias en la organización]
UI_ST_FONAG	[E.19 Fugas de información]
UI_ST_FONAG	[E.28 Indisponibilidad del personal]
UI_ST_FONAG	[A.28 Indisponibilidad del personal]
UI_ST_FONAG	[A.29 Extorsión]
UI_ST_FONAG	[A.30 Ingeniería social (picaresca)]
UI_TEC_FONAG	[E.7 Deficiencias en la organización]
UI_TEC_FONAG	[E.19 Fugas de información]
UI_TEC_FONAG	[E.28 Indisponibilidad del personal]
UI_TEC_FONAG	[A.28 Indisponibilidad del personal]
UI_TEC_FONAG	[A.29 Extorsión]
UI_TEC_FONAG	[A.30 Ingeniería social (picaresca)]

ANEXO II. Detalle valoración de amenazas

Categoría: [D] Datos / Información

Tabla 37. Valoración amenazas. Activo: FILES_USUARIO. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.1 Errores de los usuarios]	A	B	M	B		
[E.2 Errores del administrador]	M	A	A	M		
[E.15 Alteración accidental de la información]	M		M			
[A.5 Suplantación de la identidad del usuario]	M		A	M	A	
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			M		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		

Tabla 38. Valoración amenazas. Activo: LOG_SCPF. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[A.11 Acceso no autorizado]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		

Tabla 39. Valoración amenazas. Activo: PASSWORD_SERVICIOS. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	A	A		
[A.5 Suplantación de la identidad del usuario]	M		A	M	A	
[A.11 Acceso no autorizado]	M		A	A		
[A.15 Modificación deliberada de la información]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			A		

Tabla 40. Valoración amenazas. Activo: VR_REPOSITORIO_PROCESOS. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.1 Errores de los usuarios]	MA	B	M	B		
[E.15 Alteración accidental de la información]	A		M			
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			M		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		

Categoría: [S] Servicios

Tabla 41. Valoración amenazas. Activo: EMAIL_GOOGLE. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	A	A		
[A.5 Suplantación de la identidad del usuario]	M		A	M	A	
[A.9 [Re-]encaminamiento de mensajes]	M			A		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		

Categoría: [SW] Aplicaciones (Software)

Tabla 42. Valoración amenazas. Activo: AV_KARPERSKY. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	A	A		
[A.8 Difusión de software dañino]	M	A	A	A		
[A.9 [Re-]encaminamiento de mensajes]	M			B		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			A		

Tabla 43. Valoración amenazas. Activo: OFFICE_MICROSOFT. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	B	B		
[E.20 Vulnerabilidades de los programas (software)]	M	M	A	M		
[A.8 Difusión de software dañino]	M	A	A	A		
[A.9 [Re-]encaminamiento de mensajes]	M			B		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	B		
[A.15 Modificación deliberada de la información]	M			M		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		

Tabla 44. Valoración amenazas. Activo: OS_WINDOWS_UBUNTU. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.1 Errores de los usuarios]	M	M	M	B		
[E.2 Errores del administrador]	M	A	B	B		

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.20 Vulnerabilidades de los programas (software)]	M	A	A	M		
[E.21 Errores de mantenimiento / actualización de programas (software)]	M	A	M			
[A.8 Difusión de software dañino]	M	A	A	A		
[A.9 [Re-]encaminamiento de mensajes]	M			A		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			A		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		
[A.22 Manipulación de programas]	M			M		

Tabla 45. Valoración amenazas. Activo: SUB_SCPF. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.5 Avería de origen físico o lógico]	M	A				
[E.1 Errores de los usuarios]	A	B	B	B		
[E.2 Errores del administrador]	M	A	A	A		
[E.20 Vulnerabilidades de los programas (software)]	A	A	A	M		
[A.8 Difusión de software dañino]	M	A	A	A		
[A.9 [Re-]encaminamiento de mensajes]	M			A		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.15 Modificación deliberada de la información]	M			M		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		
[A.22 Manipulación de programas]	M			M		

Tabla 46. Valoración amenazas. Activo: SUB_SCPF_PRUEBAS. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.5 Avería de origen físico o lógico]	M	A				
[E.1 Errores de los usuarios]	M	MB	MB	MB		
[E.2 Errores del administrador]	M	MB	MB	MB		
[E.20 Vulnerabilidades de los programas (software)]	A	MB	MB	MB		
[A.8 Difusión de software dañino]	M	B	B	B		
[A.9 [Re-]encaminamiento de mensajes]	M			B		
[A.10 Alteración de secuencia]	M		B			
[A.11 Acceso no autorizado]	M		B	B		
[A.15 Modificación deliberada de la información]	M			B		
[A.18 Destrucción de información]	M	A				
[A.19 Divulgación de información]	M			M		
[A.22 Manipulación de programas]	M			M		

Categoría: [HW] Equipos

Tabla 47. Valoración amenazas. Activo: FIREWALL_FORTINET. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.6 Corte del suministro eléctrico]	M	A				
[E.2 Errores del administrador]	M	A	A	A		
[A.11 Acceso no autorizado]	M		A	A		
[A.23 Manipulación de los equipos]	M	A	A	A		
[A.24 Denegación de servicio]	M	A				

Tabla 48. Valoración amenazas. Activo: HOST_SCPF. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	A	M		
[A.11 Acceso no autorizado]	M		A	M		

Tabla 49. Valoración amenazas. Activo: HOST_SCPF_PRUEBAS. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.2 Errores del administrador]	M	A	B	B		
[A.11 Acceso no autorizado]	M		B	MB		

Tabla 50. Valoración amenazas. Activo: PC_TRABAJO. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.3 Contaminación mecánica]	M	A				
[I.6 Corte del suministro eléctrico]	M	A				
[E.2 Errores del administrador]	M	A	A	A		
[E.24 Caída del sistema por agotamiento de recursos]	M	A				
[A.7 Uso no previsto]	M	A	A	A		
[A.11 Acceso no autorizado]	M		A	M		
[A.23 Manipulación de los equipos]	M	A	A	M		
[A.24 Denegación de servicio]	M	A				
[I.3 Contaminación mecánica]	M	A				

Tabla 51. Valoración amenazas. Activo: ROUTER_HP. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.5 Avería de origen físico o lógico]	M	A				
[I.6 Corte del suministro eléctrico]	M	A				
[E.2 Errores del administrador]	M	B	B	B		
[A.23 Manipulación de los equipos]	M	A	NA	NA		
[A.24 Denegación de servicio]	M	A				

Categoría: [COM] Redes de Comunicaciones

Tabla 52. Valoración amenazas. Activo: INTERNET_TELCONET. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.8 Fallo de servicios de comunicaciones]	M	A				
[E.2 Errores del administrador]	M	A	B	B		
[A.12 Análisis de tráfico]	M			M		
[A.14 Interceptación de información (escucha)]	M			M		
[A.15 Modificación deliberada de la información]	M			A		
[A.19 Divulgación de información]	M			M		
[A.24 Denegación de servicio]	M	A				

Tabla 53. Valoración amenazas. Activo: LAN_CAT5. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.8 Fallo de servicios de comunicaciones]	M	A				
[E.2 Errores del administrador]	M	M	M	M		
[A.9 [Re-]encaminamiento de mensajes]	M			A		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.12 Análisis de tráfico]	M			M		
[A.14 Interceptación de información (escucha)]	M			M		
[A.19 Divulgación de información]	M			M		
[A.24 Denegación de servicio]	M	A				

Tabla 54. Valoración amenazas. Activo: WIFI_UBIQUITI. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.8 Fallo de servicios de comunicaciones]	M	A				
[E.2 Errores del administrador]	M	M	M	M		
[A.9 [Re-]encaminamiento de mensajes]	M			A		
[A.10 Alteración de secuencia]	M		A			
[A.11 Acceso no autorizado]	M		A	M		
[A.12 Análisis de tráfico]	M			M		
[A.14 Interceptación de información (escucha)]	M			M		
[A.15 Modificación deliberada de la información]	M			M		
[A.19 Divulgación de información]	M			M		

Categoría: [AUX] Equipamiento auxiliar

Tabla 55. Valoración amenazas. Activo: CABLING_FONAG. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.3 Contaminación mecánica]	M	A				
[I.5 Avería de origen físico o lógico]	M	A				
[I.6 Corte del suministro eléctrico]	M	A				

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.9 Interrupción de otros servicios y suministros esenciales]	M	M				
[A.23 Manipulación de los equipos]	M	A	NA	NA		

Tabla 56. Valoración amenazas. Activo: UPS_PC_PERSONAL. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[I.3 Contaminación mecánica]	M	A				
[I.5 Avería de origen físico o lógico]	M	A				
[I.6 Corte del suministro eléctrico]	M	A				
[A.23 Manipulación de los equipos]	M	A	NA	NA		

[L] Instalaciones

Tabla 57. Valoración amenazas. Activo: BUILDING_FONAG. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[A.11 Acceso no autorizado]	M		A	M		

[P] Personal

Tabla 58. Valoración amenazas. Activo: UI_COORD_FONAG. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.7 Deficiencias en la organización]	M	B				

Tabla 59. Valoración amenazas. Activo: UI_TEC_FONAG. [Elaboración propia]

Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]
[E.7 Deficiencias en la organización]	M	B				

ANEXO III. Análisis de salvaguardas por cada amenaza

Tabla 60. Análisis de salvaguardas actual y objetivo. [Elaboración propia]

Amenaza	Salvaguarda	Actual	Objetivo
[N.1 Fuego]	[HW.A] Instalación de sistema contra incendios	L1	L2
[N.1 Fuego]	[HW.A] Instalación de alarmas contra incendio	L1	L2
[N.1 Fuego]	[HW.A] Uso y mantenimiento de extintores	L3	L4
[N.1 Fuego]	[HW.A] Desarrollo de plan de emergencia ante desastres	L2	L3
[N.2 Daños por agua]	[HW.A] Instalación de sistema contra inundaciones	L0	L0
[N.* Otros]	[HW.A] Protección de las instalaciones frente a descargas eléctricas	L2	L4
[N.* Otros]	[HW.A] Desarrollo de plan de emergencia ante desastres	L2	L3
[I.1 Fuego]	[HW.A] Instalación de sistema contra incendios	L1	L2
[I.1 Fuego]	[HW.A] Instalación de alarmas contra incendio	L1	L2
[I.1 Fuego]	[HW.A] Uso y mantenimiento de extintores	L3	L4
[I.1 Fuego]	[HW.A] Desarrollo de plan de emergencia ante desastres	L2	L3
[I.2 Daños por agua]	[HW.A] Instalación de sistema contra inundaciones	L0	L0
[I.* Otros]	[HW.A] Protección de las instalaciones frente a descargas eléctricas	L2	L4
[I.* Otros]	[HW.A] Desarrollo de plan de emergencia ante desastres	L2	L3
[I.3 Contaminación mecánica]	[HW.op] Mantenimiento preventivo de limpieza, y reposición de componentes electromecánicos	L3	L4
[I.5 Averia de origen físico o lógico]	[HW.A] Disponer de sistemas de funcionamiento redundante	L0	L2
[I.6 Corte del suministro eléctrico]	[HW.A] Sistemas de alimentación ininterrumpida	L1	L1
[I.7 Condiciones inadecuadas de temperatura o humedad]	[HW.A] Sistemas de aire acondicionado, y alarma por exceso de temperatura y humedad	L0	L0
[I.8 Fallo de servicios de comunicaciones]	[COM.A] Disponer rutas de comunicación redundantes	L0	L0
[I.9 Interrupción de otros servicios y suministros esenciales]	[H.A] Disponer de reservas de recursos	L1	L2
[I.11 Emanaciones electromagnéticas]	[D.C] Uso de técnicas de encriptación	L0	L1
[E.1 Errores de los usuarios]	[D.A] Copias de seguridad, incluidos registros de transacciones para deshacer operaciones	L1	L2
[E.2 Errores del administrador]	[SW.SC] Disociación de responsabilidades, para reducir daño de los errores	L0	L2
[E.7 Deficiencias en la organización]	[SW.SC] Políticas de seguridad con establecimiento de responsables	L0	L2
[E.8 Difusión de software dañino]	[H.tools] Software de eliminación de virus, y de eliminación de software malicioso	L2	L3
[E.8 Difusión de software dañino]	[H.AU] Procedimientos de reinstalación y configuración del sistema	L0	L1
[E.8 Difusión de software dañino]	[D.A] Copias de seguridad.	L1	L2
[E.9 Errores de [re-]encaminamiento]	[D.C] Uso de técnicas de encriptación	L0	L1
[E.10 Errores de secuencia]	[D.A] Copias de seguridad, incluidos registros de transacciones para deshacer operaciones	L1	L2

Amenaza	Salvaguarda	Actual	Objetivo
[E.15 Alteración accidental de la información]	[D.A] Sistemas de revisión y validación de transacciones (mediante totales, revisión por otra persona u otras vías).	L1	L2
[E.18 Destrucción de información]	[D.A] Copias de seguridad, incluidos registros de transacciones para deshacer operaciones	L1	L2
[E.19 Fugas de información]	[D.C] Uso de técnicas de encriptación	L0	L1
[E.20 Vulnerabilidades de los programas (software)]	[SW.CM] Entornos de prueba y sistemas de revisión	L1	L2
[E.21 Errores de mantenimiento / actualización de programas (software)]	[SW.CM] Plan de mantenimiento preventivo, para revisar fecha de actualización aplicada a las aplicaciones	L1	L3
[E.23 Errores de mantenimiento / actualización de equipos (hardware)]	[HW.CM] Plan de mantenimiento preventivo para revisar componenenes electrónicos	L3	L4
[E.24 Caída del sistema por agotamiento de recursos]	[HW.op] Aplicaciones de monitorización de recursos disponibles con alarmas	L0	L1
[E.25 Pérdida de equipos]	[D.C] Uso de técnicas de encriptación	L0	L1
[E.28 Indisponibilidad del personal]	[SW.SC] Política de seguridad con establecimiento de responsables, y designación de suplentes de responsables	L0	L2
[A.3 Manipulación de los registros de actividad (log]	[D.A] Copias de seguridad, incluidos registros de transacciones para deshacer operaciones	L1	L2
[A.4 Manipulación de la configuración]	[D.A] Copias impresas de procedimientos de reinstalación, y configuración del sistema	L1	L2
[A.5 Suplantación de la identidad del usuario]	[H.IA] Sistemas de autenticación fuertes, que incluyan medidas biométricas	L0	L0
[A.6 Abuso de privilegios de acceso]	[SW.SC] Políticas de seguridad con establecimiento de responsables	L0	L2
[A.7 Uso no previsto]	[S.SC] Impedir ejecución de procesos no autorizados	L0	L2
[A.8 Difusión de software dañino]	[H.tools] Software de eliminación de virus, y de eliminación de software malicioso	L2	L3
[A.8 Difusión de software dañino]	[H.AU] Procedimientos de reinstalación y configuración del sistema	L0	L1
[A.8 Difusión de software dañino]	[D.A] Copias de seguridad.	L1	L2
[A.9 [Re-]encaminamiento de mensajes]	[D.C] Uso de técnicas de encriptación	L0	L1
[A.10 Alteración de secuencia]	[D.C] Uso de técnicas de encriptación	L0	L1
[A.11 Acceso no autorizado]	[H.IA] Sistemas de autenticación fuertes, que incluyan medidas biométricas	L0	L0
[A.12 Análisis de tráfico]	[COM.C] Aleatorización de las rutas de comunicaciones, y encapsulamiento de protocolos	L0	L0
[A.13 Repudio]	[D.DS] Empleo de firmas digitales	L1	L2
[A.14 Interceptación de información (escucha)]	[D.C] Empleo de técnicas de criptografía	L0	L1
[A.15 Modificación deliberada de la información]	[D.A] Copias de seguridad	L1	L2
[A.18 Destrucción de información]	[D.A] Copias de seguridad	L1	L2
[A.19 Divulgación de información]	[D.C] Empleo de técnicas de criptografía	L0	L1
[A.22 Manipulación de programas]	[SW.SC] Políticas de seguridad con establecimiento de responsables	L0	L2

Amenaza	Salvaguarda	Actual	Objetivo
[A.23 Manipulación de los equipos]	[SW.SC] Políticas de seguridad con establecimiento de responsables	L0	L2
[A.24 Denegación de servicio]	[S.www] Penalización a solicitudes recurrentes.	L0	L2
[A.24 Denegación de servicio]	[HW.op] Monitorización de recursos disponibles y alarma	L0	L1
[A.25 Robo]	[HW.R] Alarmas antirrobo, sistemas de anclaje de equipos, técnicas de criptografía	L0	L0
[A.26 Ataque destructivo]	[D.A] Copias de seguridad fuera de las instalaciones, acuerdos de alquiler de equipos para casos de emergencia, copias impresas de procedimientos de reinstalación y configuración del sistema	L1	L2
[A.27 Ocupación enemiga]	[D.A] Copias de seguridad	L1	L2
[A.28 Indisponibilidad del personal]	[SW.SC] Política de seguridad con establecimiento de responsables, y designación de suplentes de responsables	L0	L2
[A.29 Extorsión]	[D.A] Copias de seguridad	L1	L2
[A.29 Extorsión]	[D.C] Uso de técnicas de encriptación	L0	L1
[A.30 Ingeniería social (picaresca)]	[PS.AT] Formación, empleo de mecanismos de autenticación fuertes con métodos biométricos	L0	L1

ANEXO IV. Formulario notificación incidentes

FONDO PARA LA PROTECCIÓN DEL AGUA

Cód.: FOR-SEG-001
Versión: 1.0
Fecha de vigencia (formato): agosto 2023

INFORMACIÓN GENERAL			
Fecha:	dd/mm/aaaa	**Tipo de Usuario:**	[ ] Usuario Interno [ ] Usuario Externo
Persona que reporta/informa:	Nombres y apellidos completos	**Programa/área:**	
Número de Cédula		**Número Celular:**	
Correo electrónico:			

INFORMACIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN
Fecha y hora que detectó el incidente: dd/mm/aaaa
Lugar donde tuvo lugar el Incidente:
El incidente aún está en ejecución: Si [ ] No [ ]
Describa el incidente: (considere responder las siguientes preguntas; ¿qué pasó?, ¿dónde pasó?, ¿cuándo pasó?, ¿cómo pasó?, ¿qué servicios y cómo se afectaron?)
Describa brevemente cómo detectó el incidente:

EVIDENCIA
Detallar y de ser el caso, adjuntar la evidencia del incidente (fotos, capturas de pantalla, etc.)
FIRMA:

ANEXO V. Formatos gestión de incidentes

Código	Fecha-hora	Persona que reporta	Detalle del incidente	Servicios Afectados	Evidencia

Figura 14. Registro de incidentes reportados. [Elaboración propia]

Fecha-hora	Código Incidente	Tiempo de respuesta	Estrategia de contención	Responsable	Observaciones

Figura 15. Registro de actividades de contención. [Elaboración propia]

Fecha-hora	Código Incidente	Tiempo de trabajo	Estrategia de recuperación	Responsable	Observaciones

Figura 16. Registro de actividades de recuperación. [Elaboración propia]