TEC | Tecnológico de Costa Rica

Escuela de Administración de Tecnologías de Información

Propuesta de Manual de Auditoría en ciberseguridad basado en el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica de Ciberseguridad del BCCR

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Modalidad Proyecto de Graduación

Elaborado por: Jennifer Paola Lobo Quirós

Prof. Tutor: Máster. Agustín Francesa Alfaro

Cartago, Costa Rica

II Semestre

Noviembre, 2024

Hoja de Aprobación

INSTITUTO TECNOLÓGICO DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

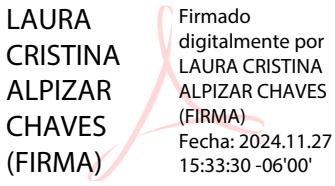
Los miembros del Tribunal Examinador de la Escuela de Administración de Tecnologías de Información, recomendamos que el siguiente informe del Trabajo Final de Graduación del estudiante Jennifer Paola Lobo Quirós sea aceptado como requisito parcial para obtener el grado académico de Licenciatura de Tecnología de Información.

Agustín Francesa Alfaro

Profesor Tutor

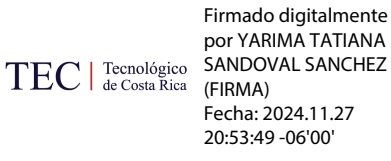
Christian Chaves Mora

Lector externo



Laura Alpízar Chaves

Lectora académica



Yarima Sandoval Sánchez

Coordinadora de Trabajo Final de Graduación

Dedicatoria

Dedico este trabajo principalmente a mis padres, Marlen y Henry, por años de sacrificio, por apoyarme en mis estudios, por el profundo amor con el que guiaron mis pasos y por creer en mí, incluso más que yo misma.

A mi hija, que en sus pocos años de vida ha sido mi motor principal para esforzarme y avanzar. ¡Qué este esfuerzo sea un paso más en el camino que compartimos, lleno de amor, aprendizajes y sueños por cumplir!

A mi tutor y profesores del TEC por haber sido mis guías con su conocimiento y por su anuencia a siempre colaborar.

A mis amigos y compañeros de carrera, por ser incondicionales y haberme apoyado todos estos años de carrera.

Resumen

Lobo, J. (2024). Propuesta de Manual de Auditoría en ciberseguridad basado en el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE emitida por el Banco Central de Costa Rica. (Trabajo Final de Graduación). Escuela de Administración de Tecnologías de Información. Tecnológico de Costa Rica.

El presente Trabajo Final de Graduación tiene como objetivo principal desarrollar un Manual de Auditoría en ciberseguridad para el área de auditoría de TI, utilizando como referencia el marco de trabajo NIST - Cybersecurity Framework y la Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE. La propuesta surge de la necesidad de tener un abordaje correcto para las auditorías de ciberseguridad porque las evaluaciones actuales carecen de un enfoque sistemático y de herramientas adecuadas, lo que dificulta la consistencia y claridad en la aplicación de controles.

La investigación se basa en un enfoque cualitativo y emplea una metodología de investigación-acción, estructurada en varias fases. La primera fase consiste en un análisis de la situación actual del departamento de auditoría de TI, seguido de la identificación de los componentes relevantes del marco NIST - Cybersecurity Framework y la Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE. Posteriormente, se elabora un Manual de Auditoría que establece directrices claras y procedimientos estandarizados para la ejecución de auditorías en ciberseguridad, facilita así la evaluación de riesgos y el cumplimiento normativo.

El marco de trabajo NIST - Cybersecurity Framework proporciona un enfoque integral para la gestión de riesgos cibernéticos, mientras que la Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE asegura el alineamiento con las regulaciones costarricenses. Estos marcos permiten establecer un conjunto de prácticas y criterios que los auditores deben seguir, lo que contribuye a la mejora continua del proceso de auditoría.

Los resultados del estudio destacan la importancia de la capacitación del personal en el uso del manual y la herramienta de auditoría desarrollada. Además, se propone la creación de un repositorio centralizado de recursos de auditoría para mejorar el acceso a la información y la consulta de procedimientos, garantizando así un enfoque más eficiente en la evaluación de controles de ciberseguridad.

Palabras clave: auditoría de TI, ciberseguridad, NIST - Cybersecurity Framework, Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE, estandarización.

Abstract

Lobo, J. (2024). *Proposal for a cybersecurity audit manual based on the NIST Cybersecurity Framework and the Technical Standard - Cybersecurity Requirements for Participation in SINPE issued by the Central Bank of Costa Rica.* (Final Graduation Project). School of Information Technology Management. Technological Institute of Costa Rica.

This Graduation Project's main objective is to develop a cybersecurity audit manual for the IT audit area, using the NIST Cybersecurity Framework and the Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE as references. The proposal arises from the need for an appropriate approach to cybersecurity audits, as current evaluations lack a systematic approach and adequate tools, which complicates consistency and clarity in applying controls.

The research is based on a qualitative approach and uses action-research methodology, structured in several phases. The first phase consists of an analysis of the current situation in the IT audit department, followed by the identification of relevant components from the NIST Cybersecurity Framework and the Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE. Subsequently, an audit manual is developed, establishing clear guidelines and standardized procedures for conducting cybersecurity audits, thus facilitating risk assessment and regulatory compliance.

The NIST Cybersecurity Framework provides a comprehensive approach to cyber risk management, while the Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE ensures alignment with Costa Rican regulations. These frameworks help establish a set of practices and criteria that auditors must follow, contributing to the continuous improvement of the audit process.

The study results highlight the importance of training staff in the use of the developed manual and audit tool. Additionally, the creation of a centralized audit resource repository is proposed to improve access to information and consultation of procedures, thus ensuring a more efficient approach to cybersecurity control evaluation.

Keywords: IT audit, cybersecurity, NIST Cybersecurity Framework, Norma Técnica - Requisitos de Ciberseguridad para Participar en el SINPE, standardization.

Tabla de Contenidos

Índice de Tablas

Índice de Figuras

1. Introducción

Este trabajo desarrolla un Manual de auditoría en ciberseguridad basado en el marco NIST - Cybersecurity Framework y adaptado a los requisitos de la reciente Norma Técnica del Banco Central de Costa Rica (BCCR), con el objetivo de estandarizar y mejorar el proceso de auditoría en el Despacho. Al implementar este manual, se espera aumentar la consistencia y eficiencia de las auditorías, reducir la dependencia del conocimiento individual y garantizar el cumplimiento normativo, fortalece así la posición competitiva del Despacho en un entorno regulado.

1.1. Descripción General

El proyecto se refiere a un manual de auditoría en ciberseguridad basado en el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica de Ciberseguridad del Banco Central de Costa Rica (BCCR), con el objetivo de estandarizar y mejorar la valoración de las implicaciones de los riesgos en las empresas auditadas, propiamente en el tema de ciberseguridad.

Para este documento, se detallan aspectos tales como:

- Contexto sobre el desarrollo del Trabajo Final de Graduación: incluye aspectos como misión, visión, propuesta de valor equipo de trabajo, gobierno corporativo y proyectos similares, los cuales se detallan posteriormente.
- Planteamiento del problema: contempla puntos como la situación problemática y los beneficios esperados del proyecto, los cuales se desarrollan seguidamente.
- Objetivos: corresponde con los ejes medulares para la realización del proyecto, incluye objetivo general y objetivos específicos.
- Justificación: describe la solución y especifica la importancia de este proyecto para la carrera de Administración de Tecnología de Información.
- Alcance: abarca puntos referentes a entregables, exclusiones, supuestos y limitaciones del proyecto, que corresponden con entregables del proyecto.
- Metodología: abarca temas como el tipo, enfoque y diseño, sujetos y variables de investigación, fuentes de información y procedimiento metodológico.
- Análisis de resultados: presenta los hallazgos obtenidos tras aplicar las técnicas e instrumentos definidos en la metodología.
- Propuesta de solución: detalla las recomendaciones y entregables diseñados para abordar la problemática identificada.

1.2. Antecedentes

Seguidamente, se brinda un contexto de la institución para la cual se desarrolla el presente proyecto, incluye aspectos como: antecedentes históricos, misión, visión, valores y equipo de trabajo, junto con proyectos similares, tanto internos como externos.

1.2.1. Descripción de la organización

El Despacho es una firma de auditoría y consultoría del área financiera y de tecnologías de información, que inició actividades a partir de enero de 1975. El Despacho, a través de los años, se ha consolidado como una de las principales Firmas de auditoría y consultoría del país, que atendiera a todos los sectores económicos (Despacho, 2024).

1.2.2. Misión

"Somos una firma con presencia local e internacional, dedicada a la prestación de servicios de auditoría y consultoría, orientados a brindar soluciones integrales mediante nuestro capital humano, a clientes del sector privado y público" (Despacho, 2024).

1.2.3. Visión

"Ser una firma reconocida en servicios de auditoría y consultoría, con estándares de control de calidad, actualización profesional y herramientas tecnológicas flexibles a los cambios dinámicos del entorno económico, que nos distingan y proporcionen valor agregado a nuestros clientes" (Despacho, 2024).

1.2.4. Propuesta de valor

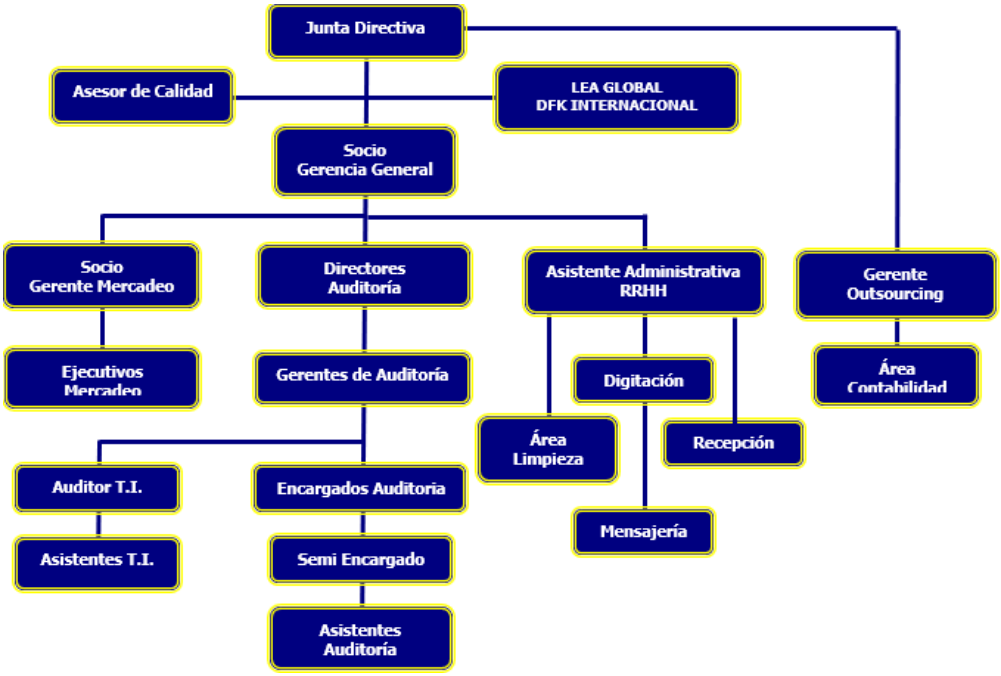
Entre los valores del Despacho destacan: (Despacho, 2024)

- Compromiso.
- Calidad.
- Servicio al cliente.
- Ética.
- Integridad.
- Respeto

1.2.5. Equipo de trabajo

Como se muestra en la Figura 1, la organización, cuenta con una Junta Directiva, que tiene a su cargo al Asesor de Calidad, al Socio de Gerencia General, a Lea Global DFK Internacional y al Gerente de outsourcing. En el caso del Socio de Gerencia General, tiene a su cargo los gerentes de auditoría y estos a los encargados de auditoría y en el rol de asistentes de auditoría se encuentra en este caso, la estudiante que realiza el Trabajo Final de Graduación.

Figura 1: Organigrama del Despacho.



1.3. Trabajos similares realizados dentro y fuera de la organización

Como lo menciona (Robles, 2021), en su trabajo para optar por el grado de Licenciatura de la carrera de Administración de Tecnología de Información, la Seguridad de la Información, según ISO27001, está relacionada con la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, también abarca los procedimientos que deben seguir los empleados y la dirección de una compañía para garantizar la protección de los datos confidenciales y de los sistemas de información frente a las amenazas actuales Por otro lado, se indica que, existe una amenaza invisible que aumenta en el espacio digital: el riesgo de ataques cibernéticos que se aprovechan de dependencia de las herramientas digitales y la incertidumbre de la crisis, incluyendo razones como:

- Una mayor dependencia de la infraestructura digital aumenta el costo de las fallas.
- El ciberdelito explota el miedo y la incertidumbre.
- Más tiempo en línea podría conducir a comportamientos más riesgosos.

Álvarez (2017), por otro lado, en su trabajo para optar por el grado de Licenciatura de la carrera de Administración de Tecnología de Información, indica que, llevar controles de auditoría que carezcan de una alineación con marcos de referencia reconocidos a nivel mundial, permite a los auditores estar en sintonía con los encargados de TI con las empresas auditadas, permitiendo a las empresas adaptarse a una metodología estándar aprobada por la industria a nivel mundial (ITIL V2011, COBIT 5 o ISO 20000), además, las empresas auditadas conocerán bajo qué marco de trabajo serán evaluadas, de forma que se genere una credibilidad sobre tal trabajo.

Menciona, a su vez que, la evidencia de auditoría es la información obtenida por el Auditor durante el periodo de evaluación y que respalda las opiniones, resultados y oportunidades de mejora sobre los controles auditados, incluye técnicas como: investigación y confirmación, observación, inspección, procedimiento analítico, recálculo, análisis de rendimiento, entre otras técnicas.

Azofeifa (2019), del mismo modo en su trabajo para optar por el grado de Licenciatura de la carrera de Administración de Tecnología de Información, plantea una propuesta metodológica relacionada con la determinación del nivel de madurez de la atención de riesgos de ciberseguridad, tomando en cuenta aspectos afines a: matrices de evaluación, modelo de madurez, gestión de riesgos, guía de ayuda, presentación de resultados, entre otros aspectos relevantes.

Cerdas (2018), aunado a esto, en su trabajo para optar por el grado de Licenciatura de la carrera de Administración de Tecnología de Información menciona que la ISO 19001:2001 define los criterios de auditoría como el grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoría. En el caso del Despacho, las fuentes más comunes para establecer los criterios de auditoría son COBIT 5 y las Normas Técnicas de la CGR. Además, se definen las principales fuentes de información que son tomadas como las mejores prácticas a la hora de realizar una auditoría de TI, destaca:

- **Normas:** especificación técnica de aplicación repetitiva o continuada, cuya observancia no es obligatoria, establecida con la participación de todas las partes interesadas, que aprueba un organismo reconocido a nivel nacional o internacional.
- **Reglamentos:** pueden exigir el cumplimiento de los requisitos definidos en una o varias normas. Es en este caso cuando la norma pasa a ser de obligado cumplimiento para las organizaciones afectadas.

- **Buenas prácticas:** se entiende un conjunto coherente de acciones que han rendido buen o incluso excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados.

Cerdas (2018), por otra parte, menciona que la ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, que no es certificable y que contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

1.4. Planteamiento del problema

En este apartado se explican aspectos relacionados con la situación problemática que se busca resolver por medio de la realización del Trabajo Final de Graduación, para ello se utiliza el árbol del problema para evidenciar de una manera más precisa la situación problemática analizada. Por otro lado, se indican los beneficios esperados a raíz de la realización del proyecto y que el Despacho verá evidenciados en un corto o mediano plazo.

1.4.1. *Situación problemática*

La empresa se dedica a brindar servicios de auditoría y asesoría a clientes que buscan identificar y mitigar los riesgos inherentes a sus actividades, especialmente ante los cambios en el entorno empresarial, sin embargo, enfrenta un problema significativo relacionado con el inadecuado abordaje de las auditorías de ciberseguridad por parte del equipo de TI, derivado de la reciente publicación de las normas del Banco Central de Costa Rica (BCCR).

Al ingresar al Despacho, cada auditor recibe el material necesario para las auditorías, principalmente basado en el marco de referencia COBIT 19. Adicionalmente, se proporciona un Manual de Auditoría desarrollado en un Trabajo Final de Graduación para la obtención del grado de licenciatura en Administración de Tecnología de Información. Este manual detalla cómo auditar con COBIT 19, los criterios por evaluar y las herramientas necesarias para aplicar pruebas en cada control. Este material es parte de un proceso de capacitación que dura tres días, seguido por un periodo de prueba de tres meses.

No se cuenta, sin embargo, con recursos predefinidos para las auditorías de ciberseguridad, y en la actualidad solamente se utiliza la Norma Técnica del BCCR (Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE), publicada en 2023. Esto ha generado una falta de precedentes en un proceso estandarizado para auditar ciberseguridad, lo que se evidencia en la ausencia de plantillas de pruebas y de criterios claros para evaluar los controles. Como resultado, los auditores carecen del conocimiento necesario para identificar los requerimientos adecuados.

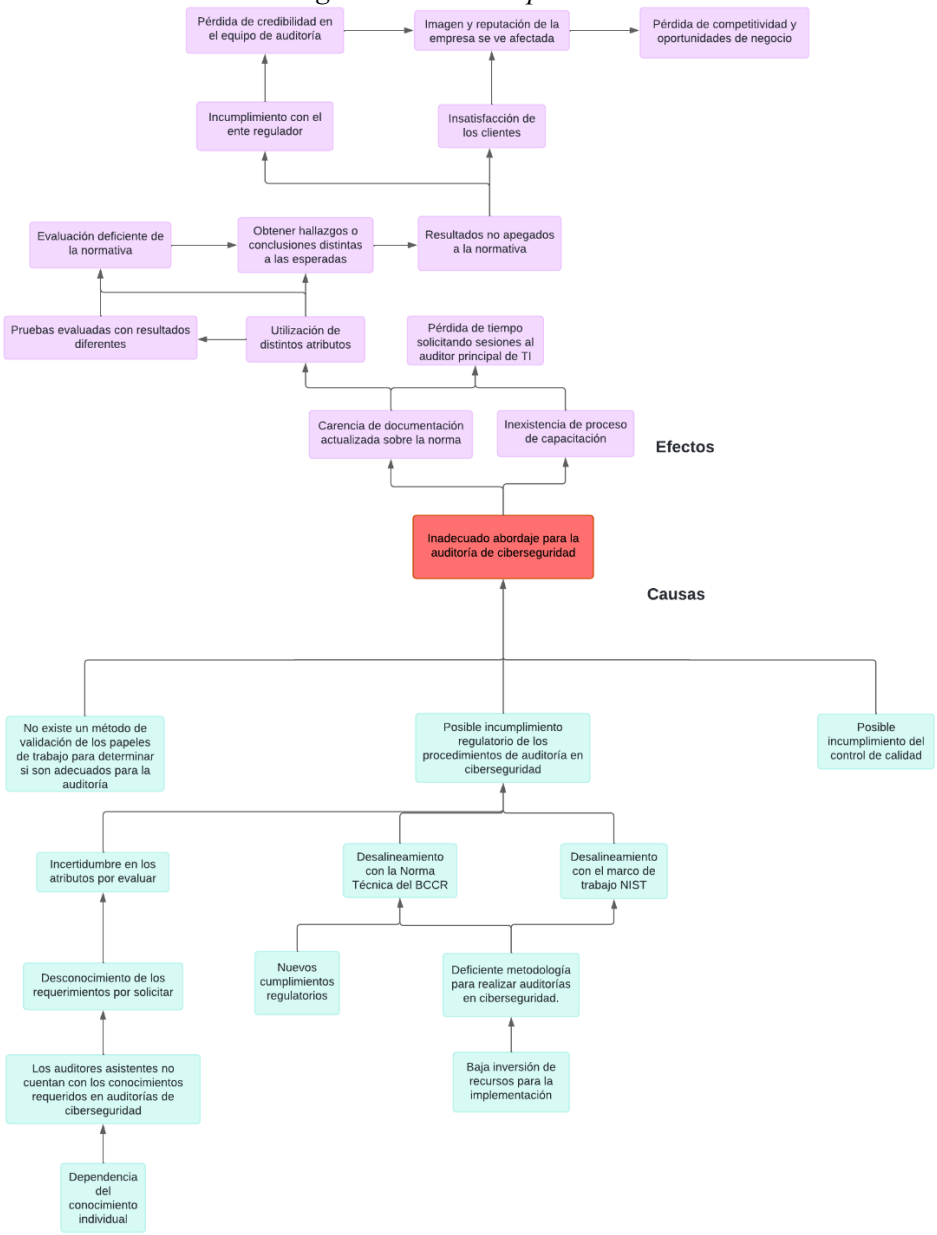
La plataforma tecnológica del Sistema Nacional de Pagos Electrónicos (SINPE), por otro lado, cuenta con una certificación internacional en seguridad de la información desde hace más de 15 años, la cual exige el cumplimiento de requisitos y controles tecnológicos para proteger la confidencialidad, integridad y disponibilidad de la información. Esto es crucial para mantener la confianza en el sistema por parte de entidades financieras, instituciones públicas, usuarios y el público en general (Banco Central de Costa Rica, 2023).

A pesar de la importancia de estas regulaciones, el Despacho no ha adaptado sus procedimientos de auditoría para cumplir con el nuevo marco normativo, lo que ha resultado en un abordaje deficiente de las auditorías de ciberseguridad. Esta situación ha revelado una brecha

significativa en la capacidad de las auditorías para ser reconocidas como válidas y conformes con las regulaciones del país. Las consecuencias de esto incluyen la pérdida de oportunidades de negocio y la confianza de los clientes.

La falta de conocimientos en ciberseguridad por parte de los auditores, además sumada a la dependencia del conocimiento individual, agrava el problema. Aunque el socio encargado de TI posee el conocimiento necesario para realizar auditorías de ciberseguridad y asegurar el cumplimiento normativo, esta información no está documentada ni estandarizada, lo que impide que los auditores asistentes accedan a ella de manera eficiente. Esto resalta la necesidad urgente de establecer un enfoque estandarizado y alineado con la Norma Técnica del BCCR para las auditorías de ciberseguridad. La Figura 2 muestra el árbol del problema.

Figura 2: Árbol del problema.



1.5. Justificación del proyecto

Para el Despacho, que brinda servicios de auditoría incluidas las de ciberseguridad, el fracaso en identificar vulnerabilidades críticas o en cumplir con las normativas vigentes no solamente pondría en riesgo los activos de sus clientes, sino que también es posible que comprometa el mantener u obtener la certificación de estos clientes como afiliados al SINPE. La reciente publicación de la Norma Técnica - Requisitos de Ciberseguridad para participar en SINPE emitida ha elevado las exigencias y no adaptarse a estas nuevas regulaciones podría resultar en la pérdida masiva de clientes y oportunidades, lo que afectaría de manera irreparable la sostenibilidad del Despacho en el mercado.

El desarrollo de un manual de auditoría en ciberseguridad basado en el marco de trabajo NIST – Cybersecurity Framework y alineado con la Norma Técnica del BCCR es fundamental para que el Despacho pueda mantener su competitividad y seguir ofreciendo servicios de alta calidad a sus clientes. Sin este manual, existe el riesgo de que las auditorías realizadas no cumplan con los estándares actuales, lo que podría debilitar la confianza de los clientes en el Despacho y llevar a la pérdida de oportunidades de negocio.

Este proyecto permite, además, que el Despacho elimine la dependencia del conocimiento individual de sus auditores y establezca un proceso uniforme y documentado que garantice la consistencia y calidad en las auditorías de ciberseguridad. Al tener un enfoque claro y estandarizado, el Despacho podrá enfrentarse de manera más eficaz a los retos actuales en el ámbito de la ciberseguridad, demostrando su capacidad para adaptarse a las nuevas regulaciones y mantener su posición como proveedor confiable de servicios de auditoría.

Este proyecto también es una oportunidad para integrar y aplicar las áreas de conocimiento adquiridas en la carrera de Administración de Tecnología de Información, incluyendo la seguridad en sistemas de información, auditoría de TI, administración de proyectos e ingeniería de requerimientos. El desarrollo de este manual requiere de habilidades tanto técnicas como blandas, reflejando la formación integral recibida y demostrando la capacidad para generar soluciones prácticas a problemas complejos.

En conclusión, este proyecto es crucial para fortalecer el servicio que ofrece el Despacho y garantizar que las auditorías de ciberseguridad, específicamente las realizadas a los afiliados al Sistema Nacional de Pagos Electrónicos (SINPE) para obtener o mantener su certificación de participación en SINPE, se realicen de manera estandarizada y conforme con las normativas más recientes, beneficiando tanto al Despacho como a sus clientes.

1.6. Beneficios esperados del proyecto

Entre los beneficios esperados al desarrollar el proyecto, se encuentran los siguientes segmentados entre beneficios directos e indirectos:

1.6.1. Beneficios directos

- Estandarización de conocimientos, tanto en el área técnica, como en entender el ciclo de auditoría del Despacho para el área de ciberseguridad.

- Controles de evaluación basados en las mejores prácticas como NIST - Cybersecurity Framework, la ISO 27001, la NIST SP 800-53 rev 5.1.1 reconocidas globalmente, además de la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE.
- Mayor entendimiento en los controles evaluados de la empresa auditada, al estar alineado a un marco de trabajo reconocido por las organizaciones.
- Mejora en las evaluaciones, al contar con procedimientos de auditoría más detallados basándose en las mejores prácticas internacionales.
- Mayor confiabilidad para el equipo en las herramientas que ayudan a realizar el proceso de la auditoría en ciberseguridad.

1.6.2. Beneficios indirectos

- Mayor atracción de clientes en el territorio nacional, al brindar auditorías más completas que aumentan la satisfacción de estos.
- Aumento en el valor agregado brindado a la empresa cliente, a partir de resultados más adecuados y precisos sobre la evaluación realizada.

1.7. Objetivos

Una vez indicada la situación problemática junto con los beneficios que traerá el proyecto para el Despacho, se presentan los objetivos del Manual de Auditoría basado en el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE emitida por el BCCR, incluyendo tanto objetivos generales como específicos.

1.7.1. Objetivo general

Proponer un Manual de Auditoría en ciberseguridad, basado en el NIST - Cybersecurity Framework y la Norma Técnica del BCCR, para estandarizar las auditorías de TI en un Despacho de auditoría, alineado con las normativas vigentes, durante el segundo semestre de 2024.

1.7.2. Objetivos específicos

1) Determinar los componentes del marco de trabajo NIST - Cybersecurity Framework para el diseño de herramientas requeridas para el área de auditoría de TI.
2) Analizar la situación actual del departamento de auditoría de TI del Despacho, mediante un análisis de brecha para la recomendación de mejoras a la evaluación de controles de ciberseguridad presentes en la Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE.
3) Elaborar un Manual de Auditoría tomando como referencia el marco de trabajo NIST Cybersecurity Framework y la Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE para la aplicación de una auditoría basada en ciberseguridad favoreciendo el cumplimiento con los entes regulatorios costarricenses.

1.8. Alcance

Este proyecto abarca la creación de un manual de auditoría en ciberseguridad específicamente para los afiliados al SINPE o que desean obtener la certificación para participar

en SINPE, de manera que se asegure un abordaje adecuado al mejorar y estandarizar las auditorías de ciberseguridad en el Despacho.

A continuación, se detallan las actividades a realizar para cumplir con el alcance del presente proyecto:

- **Análisis de la Situación Actual**:
    - Se realizará un análisis exhaustivo de los procesos actuales de auditoría en ciberseguridad en el Despacho. Este análisis se documentará según las fases del ciclo de auditoría del Despacho.
    - Como parte del análisis, se llevará a cabo un análisis de brechas, identificando la situación actual, la situación deseada y el plan de acción correspondiente.
- **Identificación de Componentes del marco NIST - Cybersecurity Framework**:
    - Se procederá a la identificación de los componentes del marco NIST - Cybersecurity Framework.
    - Paralelamente, se compararán estos componentes con los procesos evaluados en la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, seleccionando aquellos que estén alineados y ajustados a las normativas regulatorias.
- **Elaboración del Manual de Auditoría en Ciberseguridad**:

  Se diseñará un Manual de Auditoría en ciberseguridad, que incluirá:
    - **Contexto de la organización:** El manual comenzará con un contexto sobre la organización y los servicios que se ofrecen.
    - **Introducción a las auditorías de ciberseguridad**: Incluirá una introducción que describa el enfoque y procedimiento de las auditorías de ciberseguridad realizadas por el Despacho.
    - **Explicación de los tipos de controles y sus categorías**: Se proporcionará una explicación de los tipos de controles de ciberseguridad que se evaluarán durante las auditorías. Además, se explicará la categorización de los afiliados de acuerdo con la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE.
    - **Lista de requerimientos por solicitar a los clientes**: Se incluirá un apartado que especifique los requerimientos que deben solicitarse a los clientes como parte del inicio de la auditoría. Esta lista servirá como guía para que los auditores recopilen la información necesaria para evaluar de manera adecuada la ciberseguridad de las organizaciones auditadas, en conformidad con los controles exigidos a los afiliados del SINPE.
    - **Lista de atributos para evaluar los controles**: El manual también contendrá una lista detallada de los atributos que se utilizarán para evaluar cada control de ciberseguridad. Estos atributos se alinearán con la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, mientras que la explicación sobre cómo

evaluar cada control se basa en diversas buenas prácticas en materia de ciberseguridad, garantizando que las evaluaciones sean consistentes y cumplan con las regulaciones vigentes.

- **Sección de herramienta para ejecutar el manual**: En esta sección se explicará la herramienta para ejecutar el manual, lo que debe llenarse en cada columna y se indicarán los criterios que se utilizarán para las auditorías de ciberseguridad según la comparación obtenida entre la NIST - Cybersecurity Framework y la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE.

Su estructura, además, se definirá basado en la ISO 10013.

- **Elaboración de la Herramienta de Auditoría**:
  - Se desarrollará una herramienta, basada en los apartados para el informe de auditoría que solicita la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, que permitirá a los auditores aplicar de manera práctica el manual. Esta herramienta facilitará la documentación y análisis de los hallazgos durante las auditorías, asegurando consistencia en las evaluaciones y cumplimiento con las normativas vigentes.

Este proyecto se desarrollará durante el segundo semestre de 2024, con el propósito de optimizar las auditorías de ciberseguridad realizadas por el Despacho, asegurando que sean efectivas, estandarizadas y conformes a las normativas regulatorias vigentes.

1.8.1. Supuestos del proyecto

En este inciso, se indican los aspectos que se toman como supuestos para la realización del proyecto y que se asumen como punto de partida para su realización.

1) La información por parte de la organización es brindada a la estudiante en el momento oportuno.
2) Los involucrados en el proyecto tienen interés en el desarrollo del proyecto.
3) Los involucrados en el proceso destinarán el tiempo necesario para evaluar y dar el visto bueno sobre los entregables para asegurar la calidad de estos.
4) Debido a que la mayor parte de los clientes del Despacho son del sector público, se espera que las normativas a las que están sujetas estas organizaciones no cambien de forma drástica en el corto tiempo.
5) Se consideran las buenas prácticas mencionadas en la introducción como las más aptas para la gestión de las tecnologías de información y de los procesos de auditoría.
6) Los colaboradores cuentan con la experiencia y conocimiento necesario sobre la situación actual y los procesos de negocio en los cuales participan.
7) Se considera que la herramienta de auditoría puede ser cualquier aplicación ofimática que se adecúe a las necesidades del Despacho.

1.8.2. Entregables del proyecto

A continuación, se plantean los productos entregables que se brindan al concluir el desarrollo del proyecto:

1.8.2.1. Documento académico

Este documento incluye los aspectos relacionados con la introducción, Marco Conceptual, Marco Metodológico, análisis de resultados, propuesta de solución, además de conclusiones y recomendaciones derivadas de la realización del proyecto.

Al concluir el trabajo será entregado a la organización y a la Escuela de Administración de Tecnología de Información para optar por el grado de licenciatura en la carrera de Administración de Tecnología de Información.

1.8.2.2. Herramienta del procedimiento de ciberseguridad

Una vez identificados los componentes de la NIST – Cybersecurity Framework se procede a elaborar la herramienta del procedimiento de auditoría con los componentes de la NIST – Cybersecurity Framework identificados, todos los controles de la Norma Técnica del BCCR y los atributos por evaluar para cada control.

1.8.2.3. Manual de auditoría en ciberseguridad

Este entregable está relacionado con todos los aspectos que incluye el Manual de Auditoría en ciberseguridad, incluye aspectos como las fases de: planificación, ejecución, cierre y evaluación del proceso de auditoría en ciberseguridad.

1.8.3. Limitaciones del proyecto

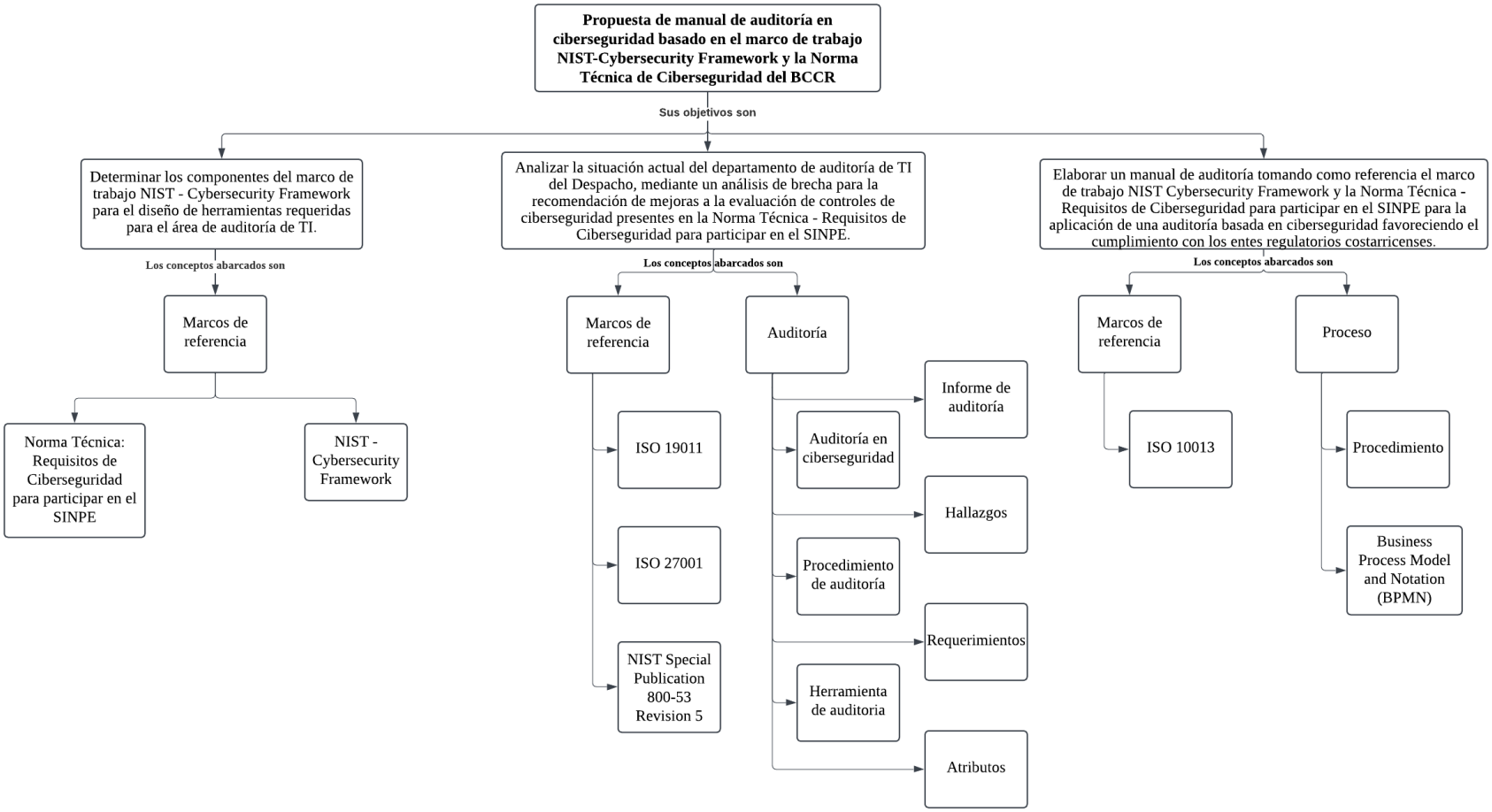
En este apartado, se incluyen los aspectos que se toman como limitaciones para la realización del proyecto y que podrían de una u otra forma causar ciertas dificultades durante su realización:

1. Disponibilidad del personal involucrado para atender consultas sobre el proyecto.
2. Uso de material confidencial de la organización.
3. Algunos aspectos relacionados con la operación del negocio y ajenos a dicho departamento no se encuentran documentados, lo cual hace que la información deba obtenerse a través de entrevistas, cuestionarios u otros artefactos de recopilación de información.
4. Los procedimientos actuales en aspectos de ciberseguridad se basan en el conocimiento tácito, es decir, no existe una documentación actual, si no que forma parte del modelo mental, producto de la experiencia que han adquirido en su labor diaria.

2. Marco conceptual

El Marco Conceptual proporciona la base teórica necesaria para comprender las secciones de esta investigación y desarrollar el manual de auditoría en ciberseguridad. En este capítulo se presentan los conceptos y mejores prácticas que respaldan el enfoque propuesto para evaluar y gestionar controles en ciberseguridad. En la Figura 3 se encuentra un marco conceptual que engloba la relación de todos los conceptos por objetivos, a un alto nivel, para una mejor comprensión visual del lector.

Figura 3: Marco conceptual



2.1. Auditoría

La auditoría según la Asociación de Auditoría y Control de Sistemas de Información (ISACA, 2015) es la "Inspección y verificación formal para comprobar si se está siguiendo un estándar o un conjunto de pautas, comprobar que los registros son precisos, o que se estén cumpliendo los objetivos de eficiencia y eficacia" (p. 6).

Julián Pérez Porto y Ana Gardey, segmentan y definen el término auditoría de la siguiente manera:

> "Auditoría es un término que puede hacer referencia a tres cosas diferentes pero conectadas entre sí: puede referirse al trabajo que realiza un auditor, a la tarea de estudiar la economía de una empresa, o a la oficina donde se realizan estas tareas (donde trabaja el auditor)". (Pérez Porto & Gardey, 2021)

Otra definición la provee la norma ISO 19011, que define la auditoría como un proceso organizado, imparcial y documentado que permite obtener y evaluar evidencias objetivas de manera neutral, con el propósito de determinar el nivel de cumplimiento respecto a los criterios de auditoría establecidos (ISO, 2018).

A raíz de esta definición se identifica que las auditorías deben estar basadas en estándares o marcos de referencia e incluir un método de evaluación para asegurar que estos criterios se cumplan efectivamente.

2.1.1. Auditoría en ciberseguridad

Es un tipo específico de auditoría de TI centrado en evaluar las prácticas de ciberseguridad de una organización. Su objetivo es revisar y evaluar la implementación y efectividad de controles de seguridad específicos para mitigar riesgos cibernéticos y proteger la infraestructura digital de las instituciones auditadas (Center for Internet Security, 2024).

Según lo anterior, la auditoría en ciberseguridad es una herramienta fundamental que permite a la organización evaluar su nivel de protección frente a riesgos digitales. Su objetivo es identificar áreas de mejora y asegurar que los sistemas de seguridad estén alineados con los estándares y marcos de referencia establecidos, garantizando la protección de los datos y la integridad de las operaciones tecnológicas.

2.1.2. Procedimiento de auditoría

El procedimiento de auditoría incluye todas las pruebas y evaluaciones realizadas para verificar el cumplimiento de los controles establecidos, según ISO (2018) implican el uso de *técnicas y herramientas* para evaluar la conformidad con los criterios de auditoría.

La NIA 500 indica los procedimientos para la recopilación de evidencia de auditoría suficiente y adecuada al contexto, estos son:

- Inspección: implica examinar documentos que pueden ser físicos o electrónicos (IAASB, 2021).
- Observación: consiste en presenciar la ejecución de un proceso o procedimiento mientras es aplicado por otra persona (IAASB, 2021).

- Confirmación externa: consiste en evidencia obtenida mediante la respuesta directa escrita por un canal físico o electrónico y que está dirigida al auditor (IAASB, 2021).
- Indagación: cosiste en realizar la búsqueda de información a través de personas expertas. (IAASB, 2021). Es importante resaltar que, de acuerdo con la NIA 330, en el apartado A26 se indica que la indagación, por si sola, no es suficientemente segura para permitir probar la eficacia operativa de un control. Por lo tanto, se deberán aplicar otros procedimientos en conjunto a la indagación para sustentar la conclusión (IAASB, 2021).

De este modo, al aplicar estos procedimientos de auditoría de manera integral, se garantiza una evaluación más precisa y confiable de los controles. Las distintas técnicas mencionadas proporcionan una base sólida de evidencia que permite a los auditores formar conclusiones bien fundamentadas sobre el cumplimiento de los criterios establecidos, asegurando la efectividad de la auditoría

2.1.3. Herramienta de auditoria

Una herramienta es un "instrumento que sirve para hacer algo o conseguir un fin" (Real Academia Española, s.f.).

En la práctica, una herramienta de auditoría facilita la recopilación de evidencia, el análisis de datos y la formulación de hallazgos y recomendaciones para mejorar los procesos auditados (Gantz, 2014).

En síntesis, las herramientas de auditoría varían en complejidad, abarcando desde cuestionarios básicos hasta avanzados guiones capaces de interactuar con los sistemas para extraer información específica (ISACA, 2016).

2.1.4. Atributos

Los atributos en la auditoría se refieren a las características esenciales de los controles o procesos evaluados, tales como precisión, confiabilidad, disponibilidad e integridad. Estos atributos son críticos para determinar la efectividad de los controles y para identificar áreas que requieren mejoras (ISO, 2018).

De acuerdo con lo indicado por IAASB (2021), el diseño de pruebas de controles incluye la identificación de condiciones que representan características o atributos relacionados con la ejecución adecuada del control, así como aquellas que evidencian desviaciones. Esto permite al auditor evaluar la presencia o ausencia de dichas condiciones para obtener evidencia de auditoría relevante.

Por lo anterior, como parte de la herramienta de auditoría se deben definir los atributos que cubran el estudio del control con el fin de permitir al auditor evaluar su cumplimiento.

2.1.5. Requerimientos

Los requerimientos en una auditoría se dividen en iniciales y adicionales. Los iniciales se establecen al inicio del proceso de auditoría, mientras que los adicionales se identifican a lo largo del proceso para abordar nuevas necesidades o ajustes. Estos requerimientos son esenciales para asegurar que todos los aspectos de la auditoría sean cubiertos adecuadamente (ISO, 19011).

2.1.6. Informe de auditoría

El informe de auditoría documenta los hallazgos, recomendaciones y conclusiones del proceso de auditoría. Un informe efectivo debe proporcionar una visión clara y detallada de los resultados y debe estar dirigido a los interesados relevantes (ISO, 19011).

Un informe de auditoría según la Organización Internacional de Normalización y Foro Internacional de Acreditación (2016b), puede ser un documento independiente o complementarse con otros documentos. Indica, además, que la estructura de estos informes puede variar según el tipo de auditoría, pero generalmente incluye los siguientes elementos clave:

1. Introducción: hace referencia a las normativas y directrices relevantes.

2. Resumen ejecutivo: presenta un resumen de la eficacia del sistema de gestión, destacando fortalezas, debilidades y áreas de mejora, junto con hallazgos clave y recomendaciones.

3. Compromiso y liderazgo de la dirección: evalúa el liderazgo y la efectividad de los procesos para establecer y comunicar políticas y objetivos, además del seguimiento de los resultados.

4. Acciones sobre auditorías anteriores: comenta sobre las acciones correctivas tomadas y su efectividad en la resolución de problemas previos.

5. Auditoría interna y mejora continua: analiza la efectividad de los procesos de auditoría interna, revisión por la dirección y las iniciativas de mejora continua.

6. Impacto de cambios significativos: informa sobre cualquier cambio relevante en la organización que pueda haber afectado el sistema de gestión.

7. Requisitos del sistema e interrelaciones: detalla cómo los diferentes procesos y áreas del sistema de gestión se interrelacionan y afectan la conformidad con los requisitos.

8. Inspección del sitio: comenta sobre las condiciones observadas durante la auditoría en el sitio, incluyendo cualquier hallazgo inusual.

9. Cumplimiento de requisitos legales y comunicaciones: revisa cómo la organización cumple con los requisitos legales y cómo comunica cualquier cambio relevante.

10. Eficacia continuada del sistema de gestión: evalúa si el sistema sigue siendo efectivo y relevante, considerando cambios internos y externos.

11. Cuestiones que requieren atención: enumera cualquier problema pendiente, como no conformidades no resueltas o áreas de preocupación.

12. Exención de responsabilidad: incluye una declaración sobre la naturaleza de la auditoría, destacando que está basada en una muestra de la información disponible y que puede haber incertidumbres en los resultados.

Este esquema garantiza que todos los aspectos relevantes sean cubiertos de manera clara y estructurada, facilitando la toma de decisiones y la mejora continua dentro de la organización (Organización Internacional de Normalización y Foro Internacional de Acreditación, 2016).

2.1.7. Hallazgos

Según la definición en la norma ISO 9000, un hallazgo es el "incumplimiento de un requisito" (ISO, 2015).

Hay tres partes en un hallazgo (también llamado “no conformidad”) bien documentado, de acuerdo con Organización Internacional de Normalización y Foro Internacional de Acreditación (2016b) estas son:

- La evidencia recopilada que sustenta los hallazgos del auditor.
- Un registro del estándar o requisito con el que se identificó la no conformidad.
- La formulación clara de la declaración de no conformidad.

Los hallazgos en una auditoría representan las observaciones y conclusiones obtenidas a partir de la evaluación de los controles y procesos. Estos hallazgos son fundamentales para entender el estado actual del sistema y para proponer mejoras (ISO, 19011).

2.2. Proceso

Un proceso según AXELOS (2019) es “un conjunto de actividades interrelacionadas o que interactúan entre sí y que transforman entradas en salidas” (p.50).

Desde el contexto de auditoría, el proceso corresponde a un conjunto de etapas estructuradas (con entradas y salidas) que guían la realización de una auditoría desde su planificación hasta el seguimiento de las acciones correctivas. La ISO (2018) define el proceso de auditoría como “un conjunto de actividades influenciadas por las políticas y procedimientos de la empresa que toma entradas de varias fuentes (incluidos otros procesos), manipula las entradas y produce salidas”.

En el contexto empresarial, los procesos se componen de actividades interrelacionadas que buscan generar valor para los clientes dentro de la operación diaria de la empresa (SYDLE, 2024). Analizar, gestionar y optimizar estos procesos es clave para mejorar la eficiencia operativa, asegurar la calidad de los productos o servicios y potenciar la capacidad de la organización para afrontar desafíos y cambios en su entorno.

2.2.1. Procedimiento

Los procesos se detallan en procedimientos, los cuales especifican las instrucciones de trabajo para llevarlos a cabo, es decir, explica cómo se realiza un proceso (AXELOS, 2019).

A partir del concepto anterior, los procedimientos desglosan los procesos en pasos específicos que facilitan su ejecución. Al explicar de manera detallada cómo se debe realizar un proceso, convierte a los procedimientos en una herramienta clave para traducir los procesos en acciones concretas y comprensibles para quienes los ejecutan.

2.2.2. Business Process Model and Notation (BPMN)

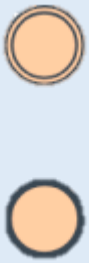
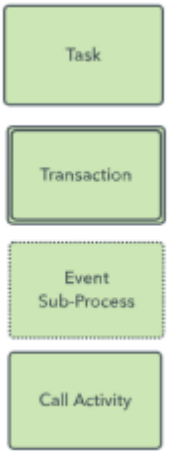
Según Lucidchart (s.f.), la Business Process Modeling Notation (BPMN) es un método de diagramación que permite modelar los pasos de un proceso empresarial desde el inicio hasta el final. Un aspecto esencial en la gestión de procesos de negocio (BPM) es que BPMN proporciona una representación visual detallada de la secuencia de flujos de información y de las actividades empresariales necesarias para completar un proceso.

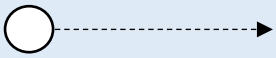
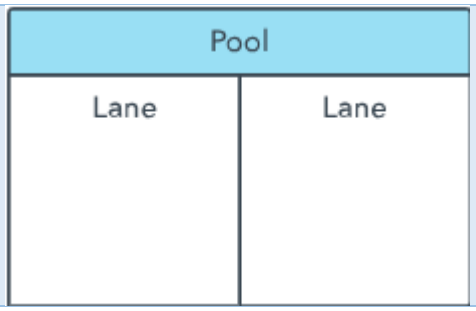
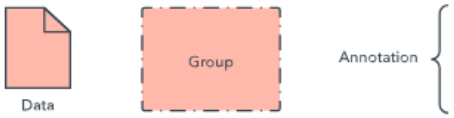
La versión 2.0 de BPMN, actualmente, según Lucidchart (s.f.), se compone de los siguientes cuatro elementos principales:

- Objetos de flujo: eventos, actividades y portales.
- Objetos de conexión: flujo de secuencia, flujo de mensaje y asociación.
- Carriles: piscina o carril.
- Artefactos: objeto de datos, grupo y anotación.

Cada uno de estos elementos se detalla en la Tabla 1.

Tabla 1: Elementos de la notación BPMN 2.0

Elemento	Descripción	Representación
Evento	Según Lucidchart (s.f), se representan con un círculo e indica que algo sucede en el proceso. Un borde de doble línea indica un evento intermedio, y un borde grueso señala el final de un evento.	
Actividad	Según Lucidchart (s.f), es una acción o tarea ejecutada dentro de un proceso de negocio, representada como un rectángulo de esquinas redondeadas en el diagrama. Las actividades pueden incluir tareas específicas y subprocesos que contribuyen a completar el flujo de trabajo.	

Elemento	Descripción	Representación
Compuerta lógica	Según Lucidchart (s.f), es un elemento representado por un rombo que se utiliza para dividir el flujo de un proceso en varias rutas, permite que una actividad conduzca a diferentes flujos de negocio.	
Flujo de secuencia	Según Lucidchart (s.f), es una línea sólida con una flecha que indica el orden en el que se realizan las actividades en un proceso.	
Flujo de mensajes	Según Lucidchart (s.f), representa los mensajes que un participante del proceso envía a otro.	
Asociación	Según Lucidchart (s.f), "muestra relaciones entre los artefactos y los objetos de flujo"	
Carril y piscina	Según Lucidchart (s.f), los carriles sirven para organizar visualmente los elementos de un proceso en un diagrama BPMN. Permiten agrupar los objetos en carriles individuales y asignar cada aspecto del proceso a uno diferente, los cuales pueden disponerse en orientación horizontal o vertical.	
Artefacto	Según Lucidchart (s.f), los artefactos representan información importante para el modelo en su conjunto, pero no se centran en elementos específicos dentro del proceso. Los tres tipos de artefactos son: las anotaciones, los grupos y los objetos de datos.	

Nota. Tomado de Lucidchart (s.f).

En este sentido, el Business Process Modeling Notation (BPMN) 2.0 proporciona una forma eficaz de representar visualmente los procesos empresariales, destacando la secuencia de actividades y flujos de información esenciales para completar cada tarea. Su aplicación en este proyecto consiste en estructurar y analizar los procesos de auditoría, al mismo tiempo que facilita la documentación de los procesos actuales, en línea con las normativas y mejores prácticas que recomiendan que los procesos empresariales estén debidamente documentados.

2.3. Marcos de referencia

A nivel mundial, existen diversos marcos de referencia y mejores prácticas que orientan las acciones de las empresas en el ámbito de la tecnología de la información (TI). Según Osores (2014), una mejor práctica se define como "una forma de hacer las cosas o una serie de principios generalmente aceptados en un ámbito profesional, que aportan valor al negocio; en el caso de las TI, a través del manejo de la información".

En este apartado, se presentan algunas de estas mejores prácticas y marcos de referencia que son relevantes para el presente trabajo final de graduación.

2.3.1. NIST - Cybersecurity Framework

El NIST Cybersecurity Framework (Marco de Ciberseguridad del NIST) proporciona un enfoque estructurado para gestionar y reducir el riesgo de ciberseguridad en organizaciones. Publicado por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), este marco está diseñado para ser adaptable a las necesidades y capacidades de diferentes tipos de organizaciones y sectores (National Institute of Standards and Technology, 2018).

El marco propone un enfoque metodológico para salvaguardar la privacidad y proteger tanto a los componentes esenciales de la infraestructura crítica y los procesos organizacionales. Este marco se fundamenta en una amplia gama de normas, lineamientos y prácticas que han evolucionado con el tiempo, adaptándose a los avances tecnológicos. Basado en estándares y guías reconocidos a nivel global, desarrollados y actualizados por la industria, el marco proporciona herramientas y métodos que permiten alcanzar los objetivos esperados en alineación con las prioridades del negocio. Estas soluciones reflejan la dimensión global de los riesgos de seguridad cibernética e información, adaptándose continuamente a las necesidades empresariales (NIST, 2018).

El marco de ciberseguridad se compone de tres elementos fundamentales: el núcleo, los niveles de implementación y los perfiles, los cuales se explicarán en detalle más adelante.

2.3.1.1. Núcleo del Marco

De acuerdo con el NIST (2018), el núcleo del marco establece un conjunto de actividades y resultados esperados en materia de ciberseguridad, presentados mediante un lenguaje accesible y comprensible. Este componente orienta a las organizaciones en la identificación, gestión y mitigación de riesgos cibernéticos, sirviendo como un complemento a sus procesos existentes de seguridad y gestión de riesgos.

El núcleo ofrece un enfoque estructurado para alcanzar objetivos específicos en seguridad cibernética, incluyendo ejemplos prácticos de cómo lograrlos. No se trata de una lista de verificación, sino de una representación de los resultados clave que las partes interesadas consideran esenciales para gestionar los riesgos en ciberseguridad (NIST, 2018).

Este núcleo está compuesto por cuatro elementos principales: funciones, categorías, subcategorías y referencias informativas, los cuales se ilustran en la Figura 4.

Figura 4: Núcleo del marco: Funciones, Categorías, Subcategorías y Referencias

Nota: Recuperado de (NIST, 2018, p. 6)

La Tabla 2 muestra cómo interactúan y se integran los diferentes elementos que conforman el núcleo del Marco.

Tabla 2: Elementos del núcleo del marco NIST

Elementos	Descripción
Funciones	Definen las actividades fundamentales de ciberseguridad en su nivel más alto. Las Funciones están alineadas con metodologías reconocidas para la gestión de incidentes y permiten evidenciar el impacto de las inversiones en seguridad cibernética.
Categorías	Representan divisiones dentro de una función, agrupando resultados de ciberseguridad relacionados con necesidades específicas del programa y actividades particulares. Algunos ejemplos de categorías son "Administración de activos", "Control de acceso" y "Tecnología de protección".
Subcategorías	Desglosan las categorías en resultados concretos asociados a actividades técnicas o de gestión. Estas subcategorías ofrecen un conjunto de resultados orientativos que, aunque no abarcan todas las posibilidades, contribuyen al cumplimiento de los objetivos establecidos en cada categoría.
Referencias Informativas	Consisten en apartados específicos de normas, directrices y prácticas compartidas entre diversos sectores de infraestructura crítica, que describen métodos para alcanzar los resultados definidos en cada Subcategoría. Las referencias informativas incluidas en el Núcleo del Marco son ejemplos representativos y no abarcan todas las opciones posibles.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 6-7), por National Institute of Standards and Technology. (2018)

Según el NIST (2018), las funciones constituyen el nivel más alto de organización dentro del marco, estructurando las actividades esenciales de ciberseguridad en categorías y subcategorías. Estas funciones se agrupan en cinco pilares fundamentales: Identificar, Proteger, Detectar, Responder y Recuperar.

Estas cinco funciones fueron seleccionadas porque representan los pilares esenciales para implementar un programa de ciberseguridad integral y efectivo. Además, permiten a las organizaciones comunicar de manera clara su enfoque de gestión de riesgos cibernéticos a un nivel estratégico y respaldan la toma de decisiones en la gestión de riesgos (NIST, 2018).

Para facilitar su aplicación, cada componente del Núcleo del Marco cuenta con un identificador único. Las funciones y categorías se distinguen mediante identificadores alfabéticos, mientras que las subcategorías dentro de cada categoría se numeran. En la descripción de cada función se incluyen las categorías y subcategorías correspondientes.

A continuación, se describen las funciones que conforman el núcleo del marco, junto con las categorías y subcategorías asociadas:

- **Identificar**: consiste en desarrollar una comprensión organizacional para gestionar el riesgo de ciberseguridad. Incluye la identificación de los activos, el perfil de riesgo y la evaluación de riesgos (NIST, 2018). En la Tabla 3 se muestran las categorías y subcategorías para la función "Identificar" del marco NIST.

Tabla 3: Elementos del núcleo del marco NIST -Función Identificar

Categoría	Subcategoría
Administración de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.
	ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.
	ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.
	ID.AM-4: Los sistemas de información externos están catalogados.
	ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.
	ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.
Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.

Categoría	Subcategoría
interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-2:** Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.
	ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.
	ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.
	ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.
	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.
	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
	ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.
Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-1:** Se identifican y se documentan las vulnerabilidades de los activos.
	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.
	ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.
	ID.RA-4: Se identifican los impactos y las probabilidades del negocio.
	ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.
	ID.RA-6: Se identifican y priorizan las respuestas al riesgo.
Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.
	ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.

Categoría	Subcategoría
organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-3:** La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.
Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
	ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.
	ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.
	ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
	ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 24-29), por National Institute of Standards and Technology. (2018)

- **Proteger**: incluye las medidas de seguridad y controles diseñados para proteger los activos y las operaciones frente a amenazas (NIST, 2018). En la Tabla 4 se muestran las categorías y subcategorías para esta función.

Tabla 4: Elementos del núcleo del marco NIST – Función Proteger

Categoría	Subcategoría
Control de acceso (PR.AC): El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
	PR.AC-3: Se gestiona el acceso remoto.

Categoría	Subcategoría
coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-4:** Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).
Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.
	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.
	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
	PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.
	PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos.
	PR.DS-2: Los datos en tránsito están protegidos.
	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.
	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.
Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
	PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.

Categoría	Subcategoría
procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-4:** Se encuentran establecidos procesos de control de cambio de la configuración.
	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.
	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
	PR.IP-7: Se mejoran los procesos de protección.
	PR.IP-8: Se comparte la efectividad de las tecnologías de protección.
	PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
	PR.IP-10: Se prueban los planes de respuesta y recuperación.
	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, des aprovisionamiento, selección del personal).
	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.
	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.
Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
	PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.
	PR.PT-4: Las redes de comunicaciones y control están protegidas.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 29-37), por National Institute of Standards and Technology. (2018)

- **Detectar**: se enfoca en las actividades para identificar la ocurrencia de un evento de ciberseguridad en el momento en que sucede (NIST, 2018). En la Tabla 5 se muestran las categorías y subcategorías para esta función.

Tabla 5: Elementos del núcleo del marco NIST – Función Detectar

Categoría	Subcategoría
Anomalías y Eventos (DE.AE): Se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
	DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.
	DE.AE-4: Se determina el impacto de los eventos.
	DE.AE-5: Se establecen umbrales de alerta de incidentes.
Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.
	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.
	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
	DE.CM-4: Se detecta el código malicioso.
	DE.CM-5: Se detecta el código móvil no autorizado.
	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.
	DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
	DE.CM-8: Se realizan escaneos de vulnerabilidades.
Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.
	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.
	DE.DP-3: Se prueban los procesos de detección.
	DE.DP-4: Se comunica la información de la detección de eventos.
	DE.DP-5: Los procesos de detección se mejoran continuamente.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 37-40), por National Institute of Standards and Technology. (2018)

- **Responder**: enfocado en las actividades para responder de manera efectiva a un incidente de ciberseguridad, incluyendo la comunicación y las medidas para mitigar el impacto (NIST, 2018). En la Tabla 6 se muestran las categorías y subcategorías para esta función.

Tabla 6: Elementos del núcleo del marco NIST – Función Responder

Categoría	Subcategoría
Planificación de la Respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.
Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley.	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
	RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.
	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.
	RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.
	RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.
Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1:** Se investigan las notificaciones de los sistemas de detección.
	RS.AN-2: Se comprende el impacto del incidente.
	RS.AN-3: Se realizan análisis forenses.
	RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.
Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** Los incidentes son contenidos.
	RS.MI-2: Los incidentes son mitigados.
	RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.
Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.
	RS.IM-2: Se actualizan las estrategias de respuesta.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 41-43), por National Institute of Standards and Technology. (2018)

- **Recuperar**: incluye las actividades necesarias para restaurar las capacidades o servicios que se vieron afectados por un incidente de ciberseguridad (NIST, 2018). En la Tabla 7 se muestran las categorías y subcategorías para esta función.

Tabla 7: Elementos del núcleo del marco NIST – Función Recuperar

Categoría	Subcategoría
Planificación de la recuperación (RC.RP): Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.
	RC.IM-2: Se actualizan las estrategias de recuperación.
Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-1:** Se gestionan las relaciones públicas.
	RC.CO-2: La reputación se repara después de un incidente.
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.

Nota: Adaptado de Framework for Improving Critical Infrastructure Cybersecurity. (pág. 41-43), por National Institute of Standards and Technology. (2018)

2.3.1.2. Perfiles del marco

Según NIST (2018), los perfiles del marco representan la forma en que una organización alinea sus objetivos, requisitos, tolerancia al riesgo y recursos con los resultados que se desean alcanzar según el núcleo del marco. Los perfiles tienen como propósito principal identificar y priorizar oportunidades para mejorar la ciberseguridad dentro de una organización. Estos perfiles incluyen tanto el estado actual como una proyección hacia el estado deseado, lo que se logra mediante la identificación de las actividades de ciberseguridad gestionadas por la organización. Para este componente del marco, se analizan planes de acción basados en el perfil actual y en la definición de un posible estado futuro deseado.

2.3.1.3. Niveles de implementación del marco

Según NIST (2018), los niveles de implementación del marco proporcionan a las organizaciones un contexto sobre cómo gestionan los riesgos de ciberseguridad. Estos niveles orientan a las organizaciones a determinar el nivel adecuado de rigor para su programa de ciberseguridad y, a menudo, sirven como una herramienta de comunicación para discutir temas como el apetito por el riesgo, la prioridad de la misión y el presupuesto.

El marco se divide en cuatro niveles de implementación, cada uno con componentes de diseño específicos y diferentes grados de cumplimiento, estos niveles son:

- Nivel 1: Parcial.
- Nivel 2: Riesgo informado.
- Nivel 3: Repetible.
- Nivel 4: Adaptable.

Dado lo anterior, los niveles de implementación del marco NIST son fundamentales para guiar a las organizaciones en la gestión estratégica de riesgos de ciberseguridad. Al ofrecer un enfoque escalonado, estos niveles permiten a las organizaciones evaluar su madurez en ciberseguridad, establecer objetivos claros de mejora y priorizar recursos de acuerdo con su apetito por el riesgo y sus necesidades operativas.

2.3.2. Norma Técnica: Requisitos de Ciberseguridad para participar en el SINPE

Esta norma establece que “las entidades afiliadas al Sinpe deberán cumplir una serie de regulaciones dirigidas a adoptar marcos de ciberseguridad adecuados para la protección del sistema, considerando los servicios particulares que cada afiliado tiene autorizados, de manera que el nivel de rigurosidad de los controles esté determinado por el nivel de exposición que tiene los servicios por medios digitales” (Banco Central de Costa Rica, 2023).

Las características sobre los controles, el cumplimiento, la periodicidad, así como requerimientos de la Norma Técnica sobre el informe que debe ser enviado al Banco Central de Costa Rica se explican en la Tabla 8.

Tabla 8: Características de la Norma Técnica del BCCR

Característica	Descripción
Alcance de la Norma Técnica	La norma regula aspectos relacionados con: • Infraestructura requerida para operar el SINPE. • Equipos de conexión al SINPE. • Usuarios del SINPE. • Capa de intercambio de datos. • Servidores interconectados al SINPE.
Tipos de controles	• Controles obligatorios: requieren cumplimiento total por parte de los afiliados. • Controles opcionales: mejoran la ciberseguridad y podrían volverse obligatorios en el futuro.
Tipos de conexión	Los tipos de conexión se refieren a las diferentes formas en que los afiliados interactúan con los servicios del SINPE, dependiendo de su infraestructura tecnológica y los canales que utilizan para realizar transacciones. • Categoría 1: Afiliados con servicios expuestos a *web services*, que requieren mayores niveles de cumplimiento para proteger el sistema debido a su interacción externa. • Categoría 2: Afiliados que solo utilizan servicios directos del SINPE en terminales conectadas al SINPE.
Cumplimiento	Tanto los afiliados actuales como los interesados en unirse al SINPE deben presentar un informe de cumplimiento emitido por un auditor, con no más de un mes de antigüedad, que confirme que la entidad cumple plenamente con los controles establecidos, de acuerdo con el nivel de riesgo correspondiente. La entidad que presenta la certificación debe garantizar ante el BCCR que el auditor seleccionado cumple con los requisitos de la norma, y reflejar esta validación en el oficio enviado. Si el auditor no cumple con dichos requisitos, el BCCR invalidará la certificación.
Incumplimiento	• Entidades en proceso de afiliación: no se autoriza la afiliación hasta cumplir todos los requisitos. • Entidades afiliadas: el incumplimiento se reporta a sus autoridades y al BCCR, con posibles procedimientos administrativos.
Pruebas de auditoría	El informe de auditoría debe incluir: Resumen ejecutivo, introducción, marco organizacional, equipo de auditores, alcance, metodología, hallazgos, conclusión, plan de mitigación y anexos.
Periodicidad	• La certificación tendrá una vigencia comprendida entre el 1 de julio del año en curso y el 30 de junio del año siguiente, con la posibilidad de presentarse durante el semestre previo. Es decir, debe enviarse anualmente el informe de auditoría para mantener la certificación. • El responsable de la entidad debe enviar la certificación al BCCR mediante el canal seguro habilitado en la extranet, utilizando los accesos proporcionados para subir el documento al sitio correspondiente. El envío debe realizarse con una nota formal firmada digitalmente por el Gerente General o el Representante Legal.

Nota: Adaptado de Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE, por Banco Central de Costa Rica. (2018)

Adicionalmente, los controles de ciberseguridad requeridos según el BCCR (2023) corresponden a los siguientes:

- **6.1. Inventario y control de los activos de hardware:** este control tiene como objetivo "identificar la totalidad de los activos que necesitan ser monitoreados y protegidos, así como apoyar en la identificación de activos no autorizados y no administrados" (BCCR, 2023, p.7).
- **6.2. Inventario y control de los activos de software:** este control tiene como objetivo "mantener una gestión activa y un adecuado control de los activos de software para prevenir ataques" (BCCR, 2023, p.8).
- **6.3**. **Protección de los datos:** este control tiene como objetivo "mantener una adecuada privacidad de los datos sensibles durante todo su ciclo de vida, sin importar el medio en que se encuentren" (BCCR, 2023, p.9).
- **6.4. Configuración segura:** este control tiene como objetivo "establecer la línea base de configuración requerida para mantener la seguridad de la infraestructura" (BCCR, 2023, p.10).
- **6.5. Administración de cuentas y control de accesos:** este control tiene como objetivo "establecer los mecanismos mínimos necesarios para prevenir accesos no autorizados a los activos" (BCCR, 2023, p.11).
- **6.6. Gestión de vulnerabilidades:** este control tiene como objetivo "establecer un proceso adecuado para gestionar las vulnerabilidades de la infraestructura, para minimizar el riesgo de sufrir un incidente de ciberseguridad asociado a la explotación exitosa de la debilidad de un activo" (BCCR, 2023, p.13).
- **6.7. Gestión de bitácoras de auditoría:** este control tiene como objetivo "establecer una gestión adecuada de las bitácoras de auditoría, mantener un monitoreo de la infraestructura que permita detectar situaciones anómalas y realizar análisis forense cuando sea requerido" (BCCR, 2023, p.14).
- **6.8. Protección del correo electrónico y la navegación por Internet:** este control tiene como objetivo "definir mecanismos de protección para el usuario final ante posibles eventos de riesgo asociados a los principales vectores de ataque, en este caso el correo electrónico y la navegación en Internet" (BCCR, 2023, p.15).
- **6.9. Defensa contra código malicioso:** este control tiene como objetivo "implementar controles para la protección contra código malicioso en la infraestructura de la organización, como una medida para prevenir infecciones que pudieran generar fugas de información, denegación de servicios o daños a los activos" (BCCR, 2023, p.16).
- **6.10. Recuperación de datos:** este control tiene como objetivo "establecer mecanismos para la recuperación de la información ante incidentes que pudieran afectar su disponibilidad" (BCCR, 2023, p.17).
- **6.11. Gestión de la infraestructura de red:** este control tiene como objetivo "definir los controles básicos que permitan establecer un nivel de seguridad aceptable de las comunicaciones, frente a eventuales ataques contra la red" (BCCR, 2023, p.17).

- **6.12. Monitoreo y defensa de la red:** este control tiene como objetivo "definir mecanismos para monitoreo y respuesta efectivos, que permitan responder de forma rápida ante posibles amenazas" (BCCR, 2023, p.18).
- **6.13. Concientización en Ciberseguridad y formación de habilidades:** este control tiene como objetivo "definir un programa de concientización en ciberseguridad que permita complementar los controles definidos, para abordar el riesgo asociado a los ataques dirigidos a las personas que interactúan con los servicios de Sinpe" (BCCR, 2023, p.19).
- **6.14. Gestión de proveedores de servicios:** este control tiene como objetivo "establecer mecanismos que permitan asegurar de forma básica las relaciones con terceros, y definir las responsabilidades en cuanto a la protección de la información y los activos" (BCCR, 2023, p.20).
- **6.15. Seguridad en las aplicaciones:** este control tiene como objetivo "establecer controles básicos de seguridad en el desarrollo de las aplicaciones, para prevenir vulnerabilidades en el código que pudieran ser explotadas por los atacantes establecer controles básicos de seguridad en el desarrollo de las aplicaciones, para prevenir vulnerabilidades en el código que pudieran ser explotadas por los atacantes" (BCCR, 2023, p.20).
- **6.16. Gestión de respuesta ante incidentes:** este control tiene como objetivo "definir procedimientos adecuados de respuesta ante incidentes de ciberseguridad, para responder de la forma más eficiente a los ataques, así como definir las estrategias de comunicación a otros interesados ante un evento de este tipo" (BCCR, 2023, p.22).

Estos controles son fundamentales para la participación en el SINPE porque permiten "fortalecer la red de seguridad del sistema y prevenir riesgos de ciberataques" (BCCR, 2023).

Por lo anterior, es posible indicar que este marco normativo define los controles y las condiciones necesarias para garantizar la seguridad en las transacciones electrónicas, lo que permite estructurar y evaluar auditorías de ciberseguridad efectivas, alineadas con las exigencias del Banco Central de Costa Rica. La aplicación de estos requisitos es clave para asegurar el cumplimiento normativo en las organizaciones y para diseñar un manual de auditoría que optimice la gestión de riesgos en el ámbito financiero.

2.3.3. ISO 27001

De acuerdo con la International Organization for Standardization (2013) esta norma ha sido diseñada para ofrecer los criterios necesarios para la creación, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.

La norma ISO/IEC 27001 establece controles destinados a la gestión de un sistema de seguridad de la información. Cubre aspectos como las tecnologías de la información, técnicas de seguridad y sistemas de gestión relacionados con la seguridad de la información, entre otros elementos. Su propósito es proporcionar un conjunto de requisitos para la creación, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información (ISO, 2013).

De acuerdo con ISO (2013), la elección de implementar un sistema de gestión de seguridad debe responder a una necesidad estratégica dentro de la organización. Para ello, es crucial

considerar el alineamiento estratégico, las necesidades y los objetivos de la entidad, ya que estos factores influyen directamente en la implementación efectiva de dicho sistema. Tras evaluar este alineamiento, es fundamental comprender los requisitos de seguridad, los procesos organizacionales existentes o en desarrollo, así como el tamaño y la estructura de la organización.

En el Anexo A de la ISO (2013), se presentan 114 controles agrupados en 14 dominios que ayudan a las organizaciones a gestionar y proteger su información de manera efectiva, estos dominios son:

- Política de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y ambiental
- Seguridad en las operaciones
- Seguridad en las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relaciones con proveedores
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

En función de lo anterior, los controles de la ISO 27001 sirven como pilares fundamentales para establecer un sistema integral de seguridad de la información. Su correcta aplicación permite abordar de manera proactiva los riesgos asociados a la gestión de la información y garantizar un enfoque consistente hacia la mejora continua y el cumplimiento regulatorio.

2.3.4. ISO 19011

Esta normativa proporciona directrices para la auditoría de sistemas de gestión. La International Organization for Standardization (2018) establece que esta norma es aplicable a todas las organizaciones que deseen llevar a cabo auditorías de sus sistemas de gestión, independientemente de su tipo y tamaño, incluye principios de auditoría, gestión de un programa de auditoría, y la realización de auditorías de sistemas de gestión.

La norma ISO 19011 proporciona directrices fundamentales para la auditoría de sistemas de gestión, y es una de las herramientas clave en la gestión de la calidad de procesos organizacionales. De acuerdo con la International Organization for Standardization (ISO, 2018), esta norma establece un marco claro y estructurado para llevar a cabo auditorías internas o externas a sistemas de gestión, independientemente del tamaño, sector o naturaleza de la organización. Abarca desde los principios básicos de auditoría hasta la implementación de un programa de auditoría completo, abordando tanto la gestión como la ejecución de las auditorías.

Uno de los aspectos más relevantes de la ISO 19011 es su enfoque en los principios de auditoría, los cuales garantizan la objetividad, independencia, competencia y confidencialidad durante todo el proceso de auditoría. Esto es esencial para obtener resultados verídicos y fiables,

que puedan contribuir a la mejora continua de los sistemas de gestión auditados. Además, la norma se enfoca en la gestión del programa de auditoría, estableciendo pautas para planificar, ejecutar, monitorear y revisar el programa de auditoría de manera efectiva (ISO, 2018).

El ciclo de auditoría, descrito en la norma a través de las cuatro fases: planificar, hacer, verificar y actuar, proporciona una metodología sistemática que facilita la implementación de auditorías eficaces. Estas fases permiten a los auditores realizar una evaluación exhaustiva y detallada de los procesos, identificar áreas de mejora y asegurar que los controles y procedimientos están alineados con los objetivos organizacionales y las normativas pertinentes.

Por lo descrito anteriormente, este es el marco de referencia utilizado para realizar la comparación con el ciclo de auditoría actual del Despacho, ya que, a través de este enfoque se podrá determinar si el ciclo de auditoría actual cumple con los principios y fases sugeridas por la norma, y se podrán identificar oportunidades para optimizar los procesos de auditoría en función de los estándares internacionales. La integración de las directrices de la ISO 19011 contribuirá a un sistema de auditoría más robusto, alineado con las mejores prácticas y capaz de abordar de manera más efectiva los desafíos presentes en el proceso de auditoría de ciberseguridad del Despacho.

2.3.5. ISO 10013

Para la elaboración del manual propuesto, se utiliza como marco de referencia esta norma, porque ofrece un marco para el desarrollo y la implementación de manuales que describen el sistema de gestión de calidad de una organización y su aplicación en la práctica (Organization for Standardization, 2021).

Esto justifica su uso como marco de referencia para crear el manual, porque establece un marco claro para la documentación y asegura que los manuales sean coherentes y comprensibles, lo que facilita la aplicación práctica de los principios de gestión de calidad en diferentes contextos organizacionales. A través de su enfoque estructurado, ISO 10013 ayuda a garantizar que los manuales no solo describan los procesos, sino que también sirvan como una herramienta eficaz para la mejora continua y el cumplimiento normativo (ISO, 2021).

A continuación, se presentan las principales directrices que establece la ISO 10013, las cuales permiten comprender los requisitos clave que la norma estipula para el desarrollo y la implementación de manuales de calidad, destacando la importancia de seguir estas directrices para asegurar una correcta documentación de los procesos de auditoría en ciberseguridad del Despacho, estas directrices según ISO (2021) son:

- **Estructura clara y comprensible**: la ISO 10013 sugiere que el manual debe tener una estructura clara, que permita a todas las partes interesadas comprender fácilmente los procesos y los procedimientos establecidos. Debe ser un documento accesible tanto para el personal interno como para los auditores.
- **Documentación adecuada**: el manual debe describir no solo los procedimientos, sino también cómo se gestionan los recursos, cómo se gestionan los riesgos y cómo se monitorean las actividades.
- **Enfoque en la mejora continua**: el manual debe ser un documento vivo que se actualice regularmente en respuesta a los resultados de auditorías, revisiones de gestión y cualquier cambio en los procesos o en las necesidades de la organización.

- **Participación de la alta dirección**: un aspecto que la norma sugiere es que el desarrollo del manual debe involucrar a la alta dirección, ya que este debe reflejar las políticas y estrategias de la organización. Esto asegura que el manual esté alineado con los objetivos estratégicos y con el compromiso de la dirección hacia la mejora de la calidad en los procesos actuales.
- **Contexto organizacional**: la ISO 10013 también sugiere que el manual debe abordar el contexto específico de la organización, es decir, debe considerar factores como el tamaño de la empresa, el tipo de productos o servicios que ofrece y los riesgos específicos a los que se enfrenta.
- **Enfoque en la satisfacción del cliente**: el manual debe tener en cuenta cómo las acciones documentadas contribuyen a cumplir con los requisitos del cliente y mejorar su experiencia.
- **Accesibilidad y facilidad de actualización**: además, la norma destaca que el manual de calidad debe ser fácilmente accesible y actualizable. Esto significa que debe haber mecanismos claros para asegurar que cualquier cambio en los procesos o políticas de la organización se refleje rápidamente en la documentación.

De acuerdo con las directrices anteriores, es posible determinar la importancia de estas para el desarrollo de manuales de calidad, ya que establecen criterios claros para asegurar una correcta documentación de los procesos. Estas directrices promueven una estructura comprensible, una actualización continua en respuesta a cambios organizacionales, y una accesibilidad eficiente. En el contexto de este proyecto, son utilizadas para garantizar que el manual de auditoría en ciberseguridad esté alineado con las mejores prácticas, facilite la gestión de procesos y cumpla con los requisitos específicos del Despacho.

2.3.6. NIST Special Publication 800-53 Revisión 5

Los atributos por proponer para evaluar, como parte de la elaboración del manual y de la herramienta de auditoría son basados en el marco NIST – Cybersecurity Framework y la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, sin embargo, también se propone qué debería evaluarse por cada control según los atributos definidos, para ampliar esta explicación se consultaron diversos marcos de referencia, entre estos la NIST SP 800-53 revisión 5, debido a que este marco proporciona un catálogo de controles de seguridad y privacidad para sistemas de información cuyo objetivo es mejorar la seguridad de la información mediante la implementación de controles adecuados para mitigar riesgos según (National Institute of Standards and Technology, 2020).

En este marco, los controles están agrupados en 20 familias. Cada familia agrupa controles que están relacionados con un tema específico. Cada familia de controles se identifica de manera única mediante un identificador de dos caracteres. Los controles de seguridad y privacidad abarcan aspectos como políticas, supervisión, procesos manuales y mecanismos automatizados, los cuales se implementan a través de sistemas o mediante acciones de personas (NIST, 2020). En la Figura 5 se presentan las familias de controles de seguridad y privacidad junto con sus respectivos identificadores.

Figura 5: Familias del marco NIST SP 800-53

IDENTIFICADOR	FAMILIA	IDENTIFICADOR	FAMILIA
AC	Control de Acceso	PE	Protección física y ambiental
AT	Concienciación y Capacitación	PL	Planificación
AU	Auditoría y Responsabilidad	PM	Gestión de programas
CA	Evaluación, autorización y monitoreo	PS	Seguridad del personal
CM	Gestión de configuración	PT	Procesamiento y transparencia de datos
CP	Planificación de continuidad	RA	Evaluación de riesgos
IA	Identificación y autenticación	SA	Adquisición de sistemas y servicios
IR	Respuesta a incidentes	SC	Protección de sistemas y comunicaciones
MA	Mantenimiento	SI	Integridad de sistemas e información
MP	Protección de medios	SR	Gestión de riesgos en la cadena de suministro

Nota: Adaptado de Security and Privacy Controls for Information Systems and Organizations. (pág. 8), por National Institute of Standards and Technology. (2020)

Por lo anterior, el marco se utiliza como referencia para enriquecer el proceso de revisión de los controles establecidos en la Norma Técnica del BCCR. Este marco proporciona una estructura detallada, que permite una evaluación más exhaustiva de los aspectos de seguridad y privacidad. De esta manera, se amplía y profundiza el análisis de los controles, asegurando una comprensión más completa de su implementación y eficacia dentro del contexto de auditoría en ciberseguridad.

3. Marco Metodológico

Como parte de la metodología para el desarrollo del proyecto, se contemplan aspectos tales como: tipo de investigación, enfoque y diseño de la investigación, fuentes de investigación, sujetos de información, entre otros aspectos que se detallan seguidamente:

3.1. Tipo de investigación

Es importante mencionar que, una investigación, se caracteriza por tener diferentes alcances, por ello, es importante definir cada uno de los tipos de alcance posibles y a partir de estos, seleccionar aquel que mejor se adapta al proyecto.

Según Hernández-Sampieri, R., & Mendoza, C. (2018), el alcance del estudio depende de la estrategia de investigación que se tome y es el resultado de la revisión literaria que permite indicar el resultado que será obtenido luego de realizar el estudio, estableciendo los siguientes alcances:

3.1.1. Correlacional

Asocia variables mediante un patrón predecible para un grupo o población, usualmente a través de métodos estadísticos, ya sea cuantitativos o cualitativos. Según (Galarza, 2020), surge la necesidad de plantear una hipótesis en donde se proponga una relación entre dos o más variables. En el nivel cuantitativo surge la aplicación de procesos estadísticos que buscan extrapolar los resultados de la investigación para beneficiar a toda la población, mientras que en el cualitativo se proponen estudios con análisis del contenido lingüístico.

3.1.2. Descriptivo

Como menciona (Galarza, 2020), en una investigación descriptiva, se conocen de antemano las características de un fenómeno y busca exponer su presencia en un grupo determinado. Cuando se analizan aspectos cuantitativos, se aplican medidas de tendencia central y de dispersión.

3.1.3. Exploratorio

Tal y como lo menciona (Galarza, 2020), es posible utilizar tanto el método cualitativo, en el cual la investigación es aplicada en fenómenos que no se han investigado previamente y se tiene el interés de examinar sus características, mientras que, en el método cuantitativo, se aplican procesos de análisis de datos básicos en donde se puede identificar la frecuencia en la cual se presenta el fenómeno de interés y sus características generales.

3.1.4. Explicativo

En este caso, (Galarza, 2020) indica que, se busca una explicación y determinación de los fenómenos. En el contexto cuantitativo se pueden aplicar estudios de tipo predictivo en donde se pueda establecer una relación causal entre diversas variables, por otro lado, en los estudios experimentales, en los cuales se pueda generar una manipulación intencionada de la variable independiente, pueden permitir la comprobación de hipótesis que expliquen el comportamiento de un determinado fenómeno.

Producto del análisis anterior sobre los tipos de investigación, se determina que el alcance de la investigación de este proyecto es de tipo descriptivo, puesto que este tipo de alcance muestra

información detallada respecto a un fenómeno o problema en particular, esto para describir con precisión sus variables o dimensiones.

Se descarta el enfoque correlacional porque no se pretende estimar el comportamiento futuro de dos variables, tampoco es exploratorio porque esta problemática es ampliamente conocida y existen varios marcos de referencia para solucionarla y no es explicativo porque el problema se busca solucionar, no determinar a fondo sus causas.

3.2. Enfoque de la investigación

Para este punto, se describe el enfoque y diseño de la investigación que se utilizará para el desarrollo del proyecto, lo cual se describe a continuación:

Según Hernández-Sampieri, R., & Mendoza, C. (2018), ha surgido una gran cantidad de corrientes de pensamiento basadas en la búsqueda del conocimiento, tales como: el empirismo (se asume que la ciencia se genera directamente de la experiencia), el materialismo dialéctico (explica la realidad para posteriormente comprenderla), la fenomenología (comprende las experiencias vividas por el ser humano) y el estructuralismo (analiza un objeto como un todo).

El enfoque cuantitativo, según Hernández-Sampieri, R., & Mendoza, C. (2018), parte de una idea general, que, por medio de múltiples iteraciones, se logra acotar y delimitar. Posteriormente, se plantean los objetivos y preguntas de la investigación, que son complementadas con revisiones literarias y una perspectiva teórica. Entre sus características destacan:

- Necesidad de medir el fenómeno o problema de estudio.
- Las hipótesis se generan al recolectar y analizar datos.
- La recolección de datos se basa en la medición.
- Los datos se representan numéricamente y se analizan de forma estadística.
- Busca identificar leyes universales y causales.

El enfoque mixto, según Hernández-Sampieri, R., & Mendoza, C. (2018) utiliza las fortalezas de los datos cuantitativos y cualitativos en una misma investigación, tratando de minimizar sus debilidades potenciales al mismo tiempo que responde al planteamiento del problema.

El enfoque cualitativo no presenta claridad sobre las preguntas de investigación, es decir, las hipótesis se desarrollan antes, durante y después de la recolección y análisis de datos, no se presenta un comportamiento de manera secuencial, sino que las actividades pueden ejecutarse en cualquier dirección a través del esquema investigativo, siendo este comportamiento precisamente lo que permite el descubrimiento de las preguntas de investigación y su respectivo perfeccionamiento (Hernández-Sampieri, R., & Mendoza, C., 2018).

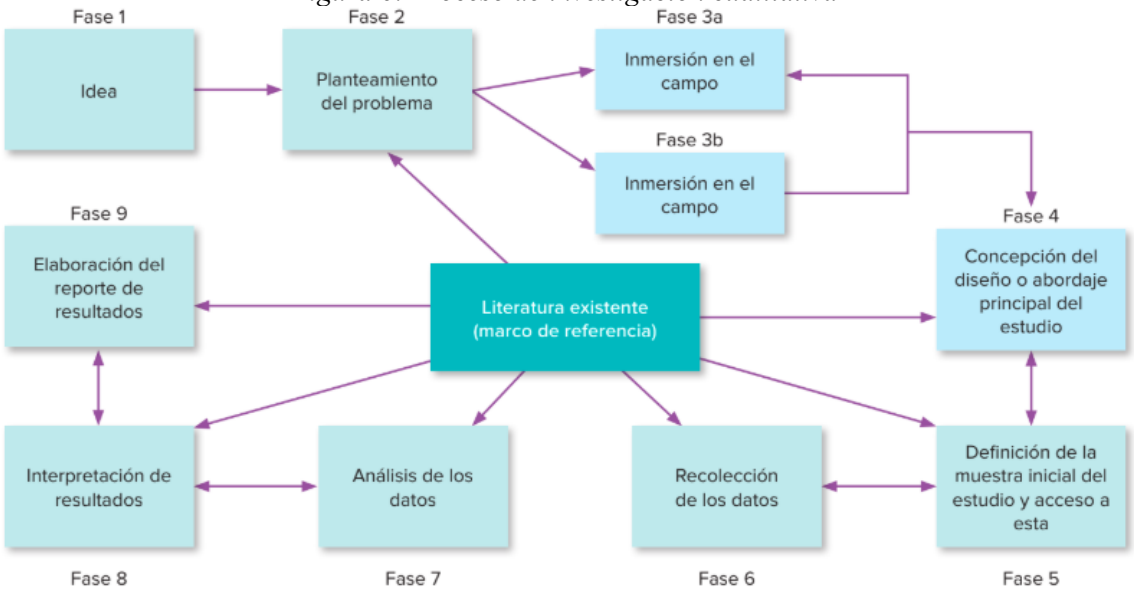
Hernández-Sampieri, R., & Mendoza, C. (2018) señala una serie de características asociadas al enfoque cualitativo, entre las cuales destacan:

- Se plantea un problema, pero no sigue un proceso definido.
- Se fundamenta en la lógica y en el proceso inductivo.
- No prueban hipótesis, se generan a través del proceso investigativo.
- Cuenta con datos no estandarizados.

- Emplea técnicas de recolección de datos como entrevistas, observación, revisión documental y discusión de experiencias.
- No se evalúa de forma probabilística.

Con base en lo anterior, se concluye que el enfoque cualitativo resulta efectivo para estudiar fenómenos organizacionales, ya que inicia sin teorías preconcebidas, lo que permite a los investigadores observar los datos reales y ajustar sus teorías en función de estos. La Figura 6 ilustra el proceso característico de una investigación cualitativa.

Figura 6: Proceso de investigación cualitativa



Nota: Recuperado de Hernández-Sampieri, R., & Mendoza, C. (2018)

Ahora bien, tomando en cuenta las características y tratamiento de datos, según los enfoques de investigación mencionados, para el desarrollo de esta investigación, se ha seleccionado el enfoque cualitativo, debido a las siguientes razones:

- El proyecto busca comprender la forma en la cual, se desarrollan las auditorías de TI en términos de ciberseguridad, es decir, no se trata de evaluar o medir su desempeño.
- La información o documentación histórica es poca, por esto, es imposible plantear una hipótesis a partir de los datos teóricos, pues estos no reflejan la realidad.
- Los resultados del proyecto son planteados en términos de un producto terminado y con un conjunto de características deseables, no en función de un resultado o una expresión medible a través de algún instrumento estadístico o probabilístico.
- La finalidad de este proyecto es comprender y crear conocimiento a partir de los datos, es decir, busca realizar una generalización a partir de una muestra de datos.

3.3. Diseño de la investigación

Según señala Hernández-Sampieri, R., & Mendoza, C. (2018), existen al menos cinco diseños genéricos de investigación cualitativa, entre los cuales destacan: diseños de teoría fundamentada, diseños etnográficos, diseños fenomenológicos, diseños narrativos y diseños de

investigación-acción. Por ende, en la Tabla 9, se definieron los tipos de investigación cualitativa existentes.

Tabla 9: Diseños de investigación cualitativa

Pregunta de investigación	Diseño	Información proporcionada
Preguntas sobre procesos y relaciones entre conceptos que conforman un fenómeno.	**Teoría fundamentada**	Categorías del proceso o fenómeno y sus vínculos. Teoría que explica el proceso o fenómeno (problema de investigación).
Preguntas sobre las características, estructura y funcionamiento de un sistema social (grupo, organización, comunidad, subcultura, cultura), desde una familia, hermandad o hinchada hasta una megaciudad.	**Etnográfico**	Descripción y explicación de los elementos y categorías que integran al sistema social: historia y evolución, estructura (social, política, económica, etc.), interacciones, lenguaje, reglas y normas, patrones de conducta, mitos y ritos.
Preguntas orientadas a comprender una sucesión de eventos, a través de las historias o narrativas de quienes la vivieron (experiencias de vida bajo una secuencia cronológica). Eventos como una catástrofe, una elección, la biografía de un individuo, entre otros.	**Narrativo**	Historias sobre procesos, hechos, eventos y experiencias, siguiendo una línea de tiempo, ensambladas en una narrativa general. Categorías relacionadas con tales historias y narrativa.
Preguntas sobre la esencia de las experiencias: lo que varias personas experimentan en común respecto a un fenómeno o proceso.	**Fenomenológico**	Experiencias comunes y distintas. Categorías que se presentan frecuentemente en las experiencias.
Preguntas sobre problemáticas o situaciones de un grupo o comunidad (incluyendo cambios).	**Investigación/acción**	Diagnóstico de problemáticas sociales, políticas, laborales, económicas, entre otros., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones.

Nota: Adaptado de Preguntas de investigación cualitativas, diseños cualitativos e información que se obtiene al implementarlos. (pág. 525), por Hernández-Sampieri, R., & Mendoza, C. (2020)

Para el problema de estudio que se presenta en esta investigación en particular, se utilizará el diseño de investigación-acción, el cual se caracteriza por su enfoque en el diagnóstico de problemáticas específicas, en este caso relacionadas con los procesos de auditoría en ciberseguridad. Como se observa en la Tabla 9 este diseño permite analizar las causas y consecuencias de dichas problemáticas y proponer soluciones prácticas y aplicables.

3.4. Fuentes de datos e información

Las fuentes de información se pueden considerar como uno de los principales insumos para obtener conocimiento sobre el estado del arte del estudio, las cuales suelen ser utilizadas como un mecanismo consultivo, sin embargo, no son necesariamente vinculantes con el desarrollo de los temas contenidos en el proceso investigativo en cuestión. Adicionalmente, en el estudio del conocimiento, existe un consenso que segmenta las fuentes de información en dos tipos esenciales, los cuales se describen en seguida:

3.4.1. Fuentes primarias

Según (Martínez, 2012), las fuentes primarias o información de primera mano, incluyen toda la información que ha sido obtenida, organizada y formulada por un investigador. En términos generales, este tipo de información no ha sido tratada de ninguna manera, es decir, que carece de interpretaciones y tampoco ha sido sometida a procedimientos de filtrado. En la Tabla 10, se presentan las fuentes primarias que han sido utilizadas en la presente investigación:

Tabla 10:Fuentes primarias.

Fuente	Importancia
Entrevista al socio encargado de auditoría TI.	Brinda la experiencia en el campo requerido y conoce del quehacer del Despacho a cabalidad.
Juicio de experto de auditores de TI.	Tienen la experiencia y conocimiento directo en la ejecución de auditorías de ciberseguridad dentro del Despacho. Su participación proporciona información valiosa sobre los procesos actuales, desafíos y deficiencias en la práctica de auditoría.
Marco de trabajo NIST - Cybersecurity Framework.	Este marco ayuda a los negocios a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Por otro lado, le brinda al negocio una reseña de las mejores prácticas para decidir dónde se tiene que concentrar el tiempo y el dinero en aspectos afines a la protección de ciberseguridad.
Norma Técnica de Ciberseguridad del BCCR.	Esta norma establece los requisitos y disposiciones de carácter complementario al Reglamento del Sistema de Pagos y el marco normativo emitido por el Banco Central de Costa Rica (BCCR) para regular los aspectos relacionados con los controles de ciberseguridad que deben cumplir los afiliados al Sistema Nacional de Pagos Electrónicos (SINPE).
ISO 19011	La ISO 19011 proporciona un marco metodológico para evaluar la conformidad y eficacia de los procesos de auditoría, en este contexto, la norma se utiliza como base para realizar el análisis de brechas, comparando las prácticas actuales con los estándares establecidos.
ISO 10013	La ISO 10013 ofrece directrices específicas para la elaboración de documentación de sistemas de gestión, incluyendo manuales, procedimientos y registros. En este proyecto, la norma es clave para estructurar el manual de auditoría en ciberseguridad, asegurando que su diseño, contenido y organización cumplan con estándares de calidad que faciliten su comprensión, implementación y adaptación a las necesidades del Despacho.

3.4.2. Fuentes secundarias

Las fuentes de información secundaria llamadas información de segunda mano, se obtienen de fuentes documentales que provienen de otras investigaciones (Martínez, 2012). Este tipo de fuentes por lo general contienen información sintetizada y reorganizada, la cual en muchas ocasiones se representa a través de colecciones de datos o enciclopedias. En la Tabla 11, se presentan las fuentes secundarias que han sido utilizadas en la presente investigación:

Tabla 11: Fuentes secundarias

Documento	Importancia
Repositorio de proyectos finales de graduación de maestría del Instituto Tecnológico de Costa Rica.	Sirven como un insumo para tener una base sobre la cual trabajar el proyecto en cuestión, además, brinda información que en ocasiones no es tomada en cuenta al iniciar el desarrollo del estudio.
Trabajos finales de graduación de la Escuela de Administración de Tecnologías de Información del Instituto Tecnológico de Costa Rica.	Sirven como un insumo para tener una base sobre la cual trabajar el proyecto en cuestión, además, brinda información que en ocasiones no es tomada en cuenta al iniciar el desarrollo del estudio.
Fuentes de sitios web relacionados con ciberseguridad y auditoría.	Brindan una posibilidad adicional de acceder a información actualizada y de diferentes localidades a nivel global.
Marcos de referencia en Ciberseguridad	Proporcionan un enfoque estructurado y coherente para la gestión de la ciberseguridad, facilitando la identificación, evaluación y mitigación de riesgos, como apoyo a la normativa que aplica en Costa Rica que corresponde a la Norma Técnica del BCCR.

3.5. Sujetos de investigación

En la Tabla 12, se muestran los roles de las personas que contribuirán de manera directa en la elaboración del proyecto, para los cuales se indica el rol, años de experiencia, caracterización y justificación de la importancia de este sujeto.

Tabla 12: Cuadro de sujetos de investigación.

Rol del sujeto	Años de experiencia	Caracterización del sujeto	Justificación de la importancia de este sujeto
Asistente de auditoría de TI	1 año	Personal que tiene como función principal realizar pruebas de auditoría, licenciado de informática o tecnologías de información.	Es la fuente de información para conocer la situación actual de las pruebas, cuáles son los atributos que actualmente se revisan por cada prueba, el procedimiento a seguir, las fuentes que consultan en caso de necesitar apoyo externo.

Rol del sujeto	Años de experiencia	Caracterización del sujeto	Justificación de la importancia de este sujeto
Encargado de auditoría de TI – Auditor asistente	3 años	Realiza la planificación de los procesos de auditoría correspondientes al Despacho.	Son fuentes de información para conocer el ciclo actual de auditoría, cómo se gestiona cada fase y cuáles son las actividades que se realizan.
Socio auditor de TI	15 años	Dentro del departamento supervisa las actividades realizadas por los equipos de auditoría.	Brinda orientación de cómo abarcar el trabajo final de graduación, además se encarga de aprobar las mejoras propuestas, incluyendo la explicación y el procedimiento de cada tema planteado.

3.6. Variables o categorías de la investigación

El cuadro de variables de una investigación brinda la definición conceptual de las variables basadas en los objetivos específicos del proyecto, donde al final se busca especificar en indicadores. Según la definición propuesta por Hernández-Sampieri, R., & Mendoza, C. (2018) "Las variables de la investigación son las propiedades medidas y que forman parte de las hipótesis o simplemente que se pretenden explorar o describir" (p. 319). Las variables de la investigación para el trabajo son identificadas y descritas en la Tabla 13.

Tabla 13: Cuadro de categorías de investigación

Categoría	Importancia	Indicador
Análisis de brechas del procedimiento de auditoría en ciberseguridad	Permite identificar las diferencias entre los procedimientos actuales y los estándares, lo que es clave para estandarizar los procesos de auditoría y mejorar su efectividad.	Listado de brechas identificadas.
Componentes del NIST - Cybersecurity Framework	Permite una lineación de estos componentes con la Norma Técnica del BCCR, brindando así una guía y mayor apoyo a los auditores en sus evaluaciones.	Lista de componentes alineados con la Norma Técnica.
Componentes de la Norma Técnica del BCCR	Es necesario identificar, comprender y aplicar los componentes de esta normativa para garantizar el cumplimiento con las regulaciones locales.	Lista de atributos alineados con los controles de la Norma Técnica.
Manual de auditoría en ciberseguridad alineado con la normativa	Facilita la estandarización de las auditorías de ciberseguridad, asegurando que los procedimientos cumplan con los requerimientos legales y regulatorios.	Manual desarrollado y alineado con la normativa vigente
Herramienta de auditoría	Clave para la implementación práctica del manual, permitiendo realizar auditorías de manera eficiente y sistemática, lo cual es esencial para mantener la consistencia y calidad en los procesos de auditoría.	Herramienta diseñada para la ejecución práctica del manual.

3.7. Técnicas e instrumentos de recolección de datos

La recolección de datos es un proceso clave que permite obtener información valiosa para el análisis y la comprensión de los fenómenos estudiados. Este paso garantiza que las decisiones y conclusiones derivadas del estudio estén basadas en información concreta y pertinente.

Para llevar a cabo este proceso de manera efectiva, se emplean diferentes técnicas e instrumentos que permiten captar datos desde varias perspectivas. En este trabajo, se seleccionaron aquellos métodos que se consideran más adecuados para explorar y analizar las características del contexto investigado. A continuación, se presentan las técnicas e instrumentos de recolección de datos empleados.

3.7.1. Entrevista

La entrevista es una técnica cualitativa clave para recolectar información directa y en profundidad de los involucrados en un proceso o fenómeno de estudio. Según Hernández-Sampieri, R., & Mendoza, C. (2018), permite obtener datos relevantes a través de la interacción directa con los sujetos, facilitando la exploración de sus experiencias, conocimientos y percepciones sobre el tema en investigación.

En este proyecto, la entrevista será utilizada para profundizar en el procedimiento de auditoría en ciberseguridad alineado con la normativa y en el análisis de brechas del procedimiento de auditoría en ciberseguridad. El instrumento de esta técnica es una guía de entrevista dirigida a auditores y responsables del área de TI del Despacho, puede consultar el instrumento en el Apéndice D.

3.7.2. Documentos, registros, materiales y artefactos

La revisión documental, tal como lo señala Hernández-Sampieri, R., & Mendoza, C. (2018), implica un análisis exhaustivo de documentos existentes que aportan información valiosa sobre el tema de estudio.

En este proyecto, se llevó a cabo una revisión de diversas fuentes documentales. Para el análisis de brechas del procedimiento de auditoría en ciberseguridad, se revisó la documentación actual del Despacho para realizar auditorías en ciberseguridad y la normativa que utilizan para realizarlas.

Se analizaron los componentes del NIST - Cybersecurity Framework y la Norma Técnica del BCCR a partir de los documentos oficiales. Finalmente, se revisaron tanto los marcos abordados en este proyecto como el resultado del proceso de comparación de controles entre la Norma Técnica del BCCR y la NIST - Cybersecurity Framework para la elaboración de la herramienta de auditoría, para conocer el formato del instrumento consulte el Apéndice I.

3.7.3. Grupos de Enfoque

Los grupos de enfoque permiten recopilar datos a través de discusiones en grupo donde los participantes intercambian opiniones y experiencias sobre un tema específico (Hernández-Sampieri, R., & Mendoza, C., 2018).

En este proyecto, se organizaron grupos de enfoque con los auditores de TI para explorar a profundidad la situación actual del proceso de las auditorías en ciberseguridad, puede consultar el instrumento en el Apéndice A.

3.7.4. Análisis de Brecha

Según Awadh (2022), el análisis de brecha es fundamental para la planificación estratégica y la toma de decisiones, ya que proporciona una visión clara de las deficiencias y oportunidades de mejora.

En el contexto de este proyecto, se realizó un análisis de brecha en el proceso de auditorías de ciberseguridad, comparando las prácticas actuales con los estándares establecidos por la ISO 19011, dado que este análisis permite identificar las deficiencias y áreas de mejora en los procedimientos actuales del Despacho, permitiendo evaluar la alineación con las buenas prácticas internacionales para proponer un plan de acción que promueva el cierre de las brechas identificadas. Consulte el instrumento en el Apéndice H.

3.8. Procedimiento metodológico de la Investigación

Seguidamente, se procede a definir la metodología de trabajo empleada durante el proceso investigativo, considerando aspectos como la relación de las fases metodológicas con los diferentes objetivos específicos de la investigación.

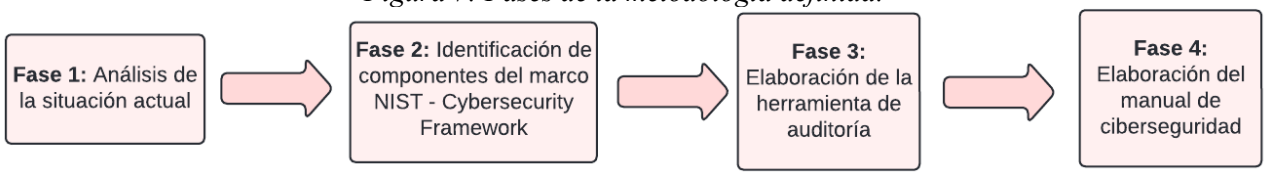
Este procedimiento metodológico está diseñado para desarrollar como entregable final, un manual de auditoría en ciberseguridad, siguiendo un enfoque sistemático que abarca desde el análisis de la situación actual hasta la elaboración de herramientas de auditoría. Por esto, la metodología propuesta del proyecto se sustenta en la norma ISO 19011:2018, la cual proporciona un marco estructurado para la planificación, realización y seguimiento de auditorías.

La metodología incluye la definición de entradas, actividades y salidas para cada fase, y se apoya en buenas prácticas para garantizar la coherencia y la calidad de los resultados. La elección de las fases metodológicas se fundamenta en su capacidad para abordar de manera integral los objetivos del proyecto y garantizar una integración lógica entre ellas considerando, además, el alcance del proyecto.

3.8.1. Diagrama propuesto para las fases del procedimiento metodológico

En la Figura 7, se presentan las cuatro fases de la metodología de la investigación definida.

Figura 7: Fases de la metodología definida.



A continuación, se explica cada una de las fases con sus respectivas entradas, actividades y salidas.

3.8.1.1. Fase I: Análisis de la situación actual

Para esta fase, se realizará un análisis de los procedimientos y la documentación con la cual cuenta el área de auditoría del Despacho, que se encuentre relacionada con el proceso de auditoría en ciberseguridad con la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE. Esta fase permite identificar los elementos clave involucrados en las distintas etapas del ciclo de auditoría, documentar cómo se están llevando a cabo las auditorías en la actualidad, y analizar las deficiencias o áreas de mejora que puedan existir. El objetivo principal es obtener una visión real y detallada del proceso actual que sirva de referencia para las fases posteriores.

En la fase de análisis de la situación actual, se documentará el ciclo de auditoría que se lleva a cabo en el Despacho que se obtendrá por medio de la aplicación de dos instrumentos, una entrevista al socio auditor de TI y un grupo focal con el equipo de auditores. Esta información permitirá contrastar el proceso vigente con el ciclo de auditoría definido por la norma ISO 19011:2018, que establece la necesidad de documentar y estructurar las actividades en las fases de planificar, hacer, verificar y actuar (ISO, 2018).

El propósito de este contraste es identificar oportunidades de mejora en los procesos y procedimientos actuales del ciclo de auditoría, proporcionando una base sólida que justifique la necesidad de la propuesta de solución planteada para abordar la problemática de esta investigación. A partir de esta identificación de situación actual de las auditorías, se identificarán las debilidades u oportunidades de mejora de este ciclo, lo que servirá como insumo para realizar un análisis de brechas.

Dicho análisis se enfocará en las deficiencias detectadas, tomando como referencia de "situación deseada" las directrices establecidas en la ISO 19011. El propósito es determinar la brecha existente y, a partir de ello, definir un plan de acción que garantice que el proceso de ejecución de auditorías sea estandarizado, consistente y que la evaluación realizada se apegue a las normativas vigentes.

En la Tabla 14, se detallan, tanto las entradas, como actividades realizadas y las salidas obtenidas a raíz de lo realizado en esta fase.

Tabla 14: Resumen de la fase I.

Entradas	Actividades	Salidas
• Documentación de la organización, se utiliza la plantilla establecida en el Apéndice M. • Una entrevista al socio auditor de TI, ver en el Apéndice E. • Marco de trabajo NIST-Cybersecurity Framework. • Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE. • Un grupo focal al equipo de auditores, ver en Apéndice B. • ISO 19011:2018	• Aplicación de entrevista y del grupo focal. • Documentar la situación actual utilizando los resultados del instrumento entrevista y grupo focal. • Identificar las debilidades identificadas en la situación actual del Despacho. • Revisar la ISO 19011 para usar como referencia de la situación deseada a elegir con respecto a las debilidades identificadas.	• Análisis de la situación actual, descrito por fases del ciclo de auditoría del Despacho, posteriormente, se describen las debilidades actuales de la realización de auditorías en ciberseguridad para la evaluación de controles que deben cumplir los afiliados al SINPE. • Análisis de brecha, es una tabla que lleva como columnas la situación actual, la situación deseada y el plan de acción.

3.8.1.2. Fase II: Identificación de componentes del marco NIST – Cybersecurity Framework

En esta sección se identificarán los controles del marco NIST que están relacionados con la Norma Técnica de Ciberseguridad del BCCR para el área de auditoría de TI.

Según la ISO (2018) en su capítulo cinco, los criterios de auditoría son esenciales para determinar la conformidad o no conformidad durante una evaluación. Estos criterios pueden abarcar políticas, procesos o procedimientos aplicables, y es posible utilizar más de un criterio a la vez. Esto justifica la aplicación de ambas normativas en el presente proyecto: la Norma NIST – Cybersecurity Framework y la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE.

Además, debido al alcance del proyecto, se seleccionarán los componentes del marco NIST – Cybersecurity Framework que tengan relación con los controles de la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE para brindarle al auditor una guía sobre qué revisar según cada actividad de la Norma NIST – Cybersecurity Framework como complemento a lo establecido en los controles de la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE. En esta fase se llevarán a cabo las siguientes actividades:

1. Identificación de Componentes del marco NIST – Cybersecurity Framework Se procederá con la identificación de los controles del NIST que son aplicables a las auditorías de ciberseguridad realizadas por el Despacho. Esta identificación se llevará a cabo mediante la aplicación del instrumento revisión documental.
2. Comparación con la Norma Técnica: Paralelamente a la actividad anterior, se realizará una comparación con la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE para garantizar que los componentes seleccionados estén alineados y ajustados a las normativas regulatorias.

El resultado de esta comparación será el insumo para desarrollar la herramienta de auditoría que se utilizará en la ejecución del manual de auditoría propuesto. Para esta etapa, se emplearán la revisión documental y una reunión con el socio auditor de TI. En la Tabla 15, se detallan, tanto las entradas, como actividades realizadas y las salidas obtenidas a raíz de lo realizado en esta fase.

Tabla 15: Resumen de la fase II.

Entradas	Actividades	Salidas
• Marco de trabajo NIST-Cybersecurity Framework. • Norma Técnica del BCCR. • Una reunión con el socio auditor de TI.	• Documentar los componentes de la Norma NIST requeridos en temas de ciberseguridad. • Comparar los componentes de la Norma NIST con los controles de la Norma Técnica del BCCR. • Realizar reunión para verificar la elección de los componentes requeridos que se utilizarán para el manual y la herramienta de auditoría.	• Componentes de la Norma NIST requeridos para el manual de auditoría. Es una tabla que incluye: o Función de la NIST o Categoría de la NIST o Subcategoría (Control NIST) o Control de la Norma Técnica del BCCR. o Por cada control de la Norma Técnica, se identifican los controles de la NIST que se relacionan.

3.8.1.3. Fase III: Elaboración de la herramienta de auditoría

En esta etapa, se procederá con el desarrollo de una herramienta que corresponde a un conjunto de procedimientos de auditoría elaborados en formato Word. Esta herramienta estará basada en el marco de trabajo establecido por la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, pero será adaptada específicamente para incluir los componentes identificados durante la fase previa denominada "Identificación de componentes del marco NIST – Cybersecurity Framework". Además, integrará todos los controles estipulados por la Norma Técnica emitida por el Banco Central de Costa Rica (BCCR).

Es importante destacar que los controles definidos en la Norma Técnica serán implementados en su totalidad, ya que esta norma es de cumplimiento obligatorio para todas las organizaciones afiliadas al sistema SINPE dentro del territorio costarricense. De esta manera, se garantiza que las organizaciones cumplan con los requisitos de ciberseguridad necesarios para operar en dicho sistema.

Para la ejecución de esta fase, se tomarán como insumos fundamentales los resultados obtenidos en las etapas previas del proyecto. Estos resultados servirán de base para estructurar la herramienta, asegurando que se alinee con los estándares internacionales del marco NIST y con los requisitos específicos establecidos por el BCCR. En la Tabla 16, se detallan las entradas, las actividades realizadas y las salidas obtenidas como resultado de las acciones llevadas a cabo en esta fase.

Tabla 16: Resumen de la fase III.

Entradas	Actividades	Salidas
• Componentes identificados en la fase "Identificación de componentes de la Norma NIST – Cybersecurity Framework" de la norma NIST-Cybersecurity Framework. • Manual de auditoría en ciberseguridad • Marco de trabajo NIST-Cybersecurity Framework.	• Identificar basado en la plantilla de la norma NIST-Cybersecurity Framework, la estructura de la herramienta de auditoría a elaborar. • Agregar a la herramienta, los atributos para evaluar controles identificados en la fase de "Elaboración del manual de Ciberseguridad". • Agregar a la plantilla los componentes identificados en la fase "Identificación de componentes de la Norma NIST – Cybersecurity Framework".	Herramienta de auditoría para ejecutar el manual de auditoría y estandarizar la realización de los procedimientos de auditoría, es una plantilla realizada en Word que debe incluir: • Información de la empresa auditada. • Información de los responsables de realizar el procedimiento de auditoría. • Criterio de la Norma Técnica del BCCR y componentes de la Norma NIST – Cybersecurity Framework, específicamente las subcategorías. • Métodos de indagación. • Resultados y conclusiones (atributos evaluados, resultado y papeles de trabajo). • Sección de cumplimiento (Cumple, No cumple, Cumple parcialmente) • Sección para documentar hallazgos (hallazgo y estado del hallazgo).

3.8.1.4. Fase IV: Elaboración del Manual de Ciberseguridad

En esta fase, se desarrollará un manual de auditoría en ciberseguridad fundamentado en el marco de trabajo NIST – Cybersecurity Framework y la Norma Técnica de Ciberseguridad del BCCR, con el propósito de estandarizar el proceso de auditoría y garantizar que se cumpla la normativa aplicable a este tipo de auditoría.

El diseño de la propuesta para el manual de auditoría se basa en la ISO 10013. Las actividades de esta fase son:

1. Elegir los capítulos por documentar en el manual y sus respectivos apartados basado en la ISO 10013, como instrumento se utilizará la revisión documental.
2. Elegir los atributos a utilizar para evaluar los controles de la Norma Técnica – Requisitos de Ciberseguridad para participar en el SINPE, para esta actividad se realizará una revisión documental para proponer los atributos a evaluar y una reunión con el socio auditor de TI con el propósito de obtener la aprobación de los atributos propuestos.
3. Completar los apartados definidos en la actividad uno de esta fase, para esta actividad se realizará una reunión que será con el socio auditor de TI, con el propósito de obtener su aprobación.

Esto no sólo busca cumplir con los estándares y normativas establecidos, sino que también pretende servir como una guía práctica y funcional para los auditores de TI. Su enfoque es proporcionar claridad en los procedimientos y asegurar que los controles se implementen de manera efectiva, contribuyendo así a fortalecer la postura de ciberseguridad de las organizaciones afiliadas al sistema SINPE.

En la Tabla 17, se detallan las entradas, las actividades realizadas y las salidas obtenidas como resultado de las acciones llevadas a cabo en esta fase.

Tabla 17: Resumen de la fase IV.

Entradas	Actividades	Salidas
• Componentes identificados en la fase "Identificación de componentes de la Norma NIST – Cybersecurity Framework" de la norma NIST-Cybersecurity Framework. • Controles de la Norma Técnica del BCCR. • ISO 19011. • ISO 10013. • Reunión con el socio auditor de TI, ver formato de minuta en Apéndice G.	• Establecer los atributos por evaluar para cada control. • Elaborar estructura del manual basado en la ISO 19011 y la ISO 10013. • Reunirse con el socio auditor de TI para presentar propuesta de estructura del manual y obtener su aprobación. • Completar los apartados que se definieron en la estructura del manual.	Manual de auditoría en ciberseguridad basado en la ISO 10013, este marco propone que el manual debe incluir: • Un alcance • Un propósito • Contexto de la empresa. • Explicación de los procesos actuales. • Diagramas de los procesos actuales. • Normativa aplicable. • Un control de documentos. • Anexos. Al final la aplicación de esta fase se obtendría el manual de auditoría con las secciones que propone la ISO 10013 adaptadas a lo que aplique para el proceso de auditorías específicamente.

3.9. Operacionalización de las variables o categorías.

De acuerdo con los objetivos específicos planteados en este trabajo, que se detallan a continuación:

- **OE 1:** Analizar la situación actual del departamento de auditoría de TI del Despacho, mediante un análisis de brecha para la recomendación de mejoras a la evaluación de controles de ciberseguridad presentes en la Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE emitida por el Banco Central de Costa Rica.
- **OE 2:** Determinar los componentes del marco de trabajo NIST - Cybersecurity Framework para el diseño de herramientas requeridas para el área de auditoría de TI.
- **OE 3:** Elaborar un manual de auditoría tomando como referencia el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica del BCCR para la aplicación de una auditoría basada en ciberseguridad favoreciendo el cumplimiento con los entes regulatorios costarricenses.

Y las fases para la elaboración del proyecto definidas anteriormente:

- **Fase I:** Análisis de la situación actual
- **Fase II:** Identificación de componentes del marco NIST - Cybersecurity Framework
- **Fase III:** Elaboración de la herramienta de auditoría
- **Fase IV:** Elaboración del manual de ciberseguridad

La operacionalización de las variables identificadas para este proyecto se expresa en la Tabla 18.

Tabla 18: Operacionalización de variables.

Fase	Objetivo específico	Instrumentos	Variables	Sujetos
Fase I	OE 1	• Guía de entrevista. • Revisión documental. • Grupo focal.	Análisis de brechas del procedimiento de auditoría en ciberseguridad	• Asistente de auditoría de TI • Encargado de auditoría de TI • Gerente de auditoría de TI
Fase II	OE 2	• Revisión documental.	Componentes del NIST - Cybersecurity Framework	No aplica.
Fase III	OE 3	• Revisión documental.	Herramienta de auditoría	No aplica.
Fase IV	OE 3	• Revisión documental.	• Componentes de la Norma Técnica del BCCR • Manual de auditoría en ciberseguridad alineado con la normativa	No aplica.

3.10. Tabla resumen del procedimiento metodológico de la Investigación

A continuación, la Tabla 19 refleja el resumen del procedimiento metodológico de la investigación por medio de la matriz de trazabilidad de los objetivos.

Tabla 19: Matriz de Trazabilidad.

Objetivo	Metodología	Análisis de resultados	Propuesta de solución	Conclusiones	Recomendaciones
OE 1	3.8 3.8.1 3.8.1.1	4.1.1 4.1.2 4.1.3 4.1.4 4.1.5 4.2	No aplica	6 (consultar Objetivo específico dos)	7
OE 2	3.8 3.8.1 3.8.1.2 3.8.1.3	4.1 4.4 4.1.1	5.1	6 (consultar Objetivo específico uno)	7
OE 3	3.8 3.8.1 3.8.1.4	4 4.5	5 5.2 5.2.1 5.2.2 5.2.3 5.3	6 (consultar Objetivo específico tres)	7

4. Análisis de resultados

En este capítulo se presentan los resultados del estudio, organizados de manera que faciliten su comprensión. Se analiza la información recopilada según los objetivos planteados, proporcionando una visión clara y estructurada de los aspectos evaluados.

Específicamente, en el capítulo se presenta el análisis de la situación actual, base para la generación del análisis de brechas. Además, se detalla la identificación de los componentes del NIST - Cybersecurity Framework alineados con la Norma Técnica del Banco Central de Costa Rica (BCCR) y la definición de atributos necesarios para evaluar, de manera completa y estandarizada, los controles de dicha norma. También se incluye un estudio de los requisitos de la Norma Técnica, orientado a definir la estructura de la herramienta de auditoría, y un análisis de las directrices de la ISO 10013, que sirve para establecer las secciones necesarias para desarrollar el manual de auditoría en el capítulo de propuesta de solución.

4.1. Análisis de situación actual

Como resultado de la entrevista realizada al socio auditor de TI, es posible explicar previamente a las fases del ciclo actual de auditoría, la razón de realizar auditorías en ciberseguridad para la participación en el SINPE.

4.1.1. Contexto sobre las auditorías de requisitos auditorías en ciberseguridad para la participación en el SINPE.

Existen dos motivos para solicitar estas auditorías, para obtener la certificación o bien para mantener la certificación para participación en el SINPE.

La necesidad por parte de las entidades de obtener esta certificación abre paso a requerir una auditoría según lo estipula la Norma Técnica – Requisitos de ciberseguridad para participar en el SINPE emitida por el BCCR que da inicio de la siguiente manera:

1. Según sus necesidades, la entidad crea un cartel que llega a distintos oferentes.
2. Cuando llega al Despacho, este se analiza y se procede a realizar una oferta que será enviada al cliente por medio del área de mercadeo.
3. Una vez revisada la oferta por el cliente, si está de acuerdo, se inicia la contratación lo que da inicio formalmente a la realización de la auditoría.

Posterior a la firma del contrato, se establecen las fechas de visita con el cliente, las entregas de los informes de auditoría se deben realizar para todas las entidades como máximo el 31 de julio. Esto implica que el Despacho pueda tener múltiples auditorías de este tipo con la misma o similar fecha de entrega del informe al cliente. Para estos casos se requiere avanzar en paralelo o ir adelantando para que el cliente no incumpla con el requisito de enviar el informe antes de la fecha máxima de entrega al BCCR.

4.1.2. Ciclo de auditoría actual

De acuerdo con las respuestas obtenidas en la entrevista que puede consultar en el Apéndice F, el ciclo de auditoría actual comprende las siguientes fases:

Planeación

Esta primera fase del ciclo de auditoría actual en el Despacho incluye la realización de las actividades desglosadas en la Tabla 20.

Tabla 20: Ciclo de auditoría actual: fase de planeación.

Fase del ciclo de auditoría	Actividades
Planeación	1. El socio auditor de TI realiza sesiones correspondientes al inicio de la auditoría con el cliente.
	2. El socio auditor de TI elabora el plan de auditoría el cuál define los siguientes aspectos: a. Objetivo de la auditoría. b. Alcance de la auditoría. c. Actividades que se realizarán para cumplir el proceso de auditoría con sus respectivas fechas.
	3. El socio auditor de TI realiza la solicitud de requerimientos iniciales en función de la categoría del cliente, es decir, estos requerimientos se alinearán con los clientes categoría 1 o con los clientes categoría 2. La información solicitada se basa en lo requerido por la Norma Técnica del BCCR. Estos requerimientos iniciales son el insumo para iniciar la segunda fase del ciclo de auditoría.
	4. El auditor encargado elabora el plan de trabajo, este define los siguientes aspectos: a. Controles por evaluar. b. Fechas de entrega de informes preliminares según se haya acordado con el cliente inicialmente como parte de la planificación de la auditoría. Estos informes preliminares corresponden a la evaluación de los controles organizados en grupos, de manera que semanalmente sea posible entregarle un avance al cliente de los controles que se han evaluado, y así, tenga conocimiento del nivel de cumplimiento o de los hallazgos identificados, de esta manera puedan aportar información adicional (si cuentan con esta y si se requiere) que evidencie el cumplimiento de los controles evaluados. c. Responsables de evaluar cada control.

Ejecución:

Esta segunda fase del ciclo de auditoría actual en el Despacho incluye la realización de las actividades desglosadas en la Tabla 21.

Tabla 21: Ciclo de auditoría actual: fase de ejecución.

Fase del ciclo de auditoría	Actividades
Ejecución	1. Solicitud de requerimientos adicionales (si se requieren), esta actividad es responsabilidad del equipo de auditores asignados en el plan de trabajo de cada auditoría.
	2. Realización los procedimientos de auditoría, estos comprenden pruebas sustantivas y de cumplimiento, esta actividad es responsabilidad del equipo de auditores asignados en el plan de trabajo de cada auditoría.
	3. Elaboración de informes preliminares, generalmente son informes semanales e incluyen los controles que se hayan evaluado hasta el momento.
	4. Reuniones de seguimiento para presentar el avance de la auditoría y para que el equipo de auditores realice consultas que tengan sobre la información suministrada o realicen solitudes de información adicional. Esta actividad es realizada por el equipo de auditores asignados en el plan de trabajo de cada auditoría y generalmente, participa también el socio auditor de TI.
	5. Elaboración del informe final, este informe debe cumplir con el formato definido en la Norma Técnica del BCCR.

Cierre:

Esta tercera fase del ciclo de auditoría actual en el Despacho incluye la realización de las actividades desglosadas en la Tabla 22.

Tabla 22: Ciclo de auditoría actual: fase de cierre.

Fase del ciclo de auditoría	Actividades
Cierre	1. Mercadeo trabaja en dar el formato respectivo al informe de auditoría.
	2. El socio auditor de TI envía al cliente el informe final.
	3. Se realiza una sesión para presentar los resultados, si existen observaciones, el grupo de auditores trabajan en las correcciones y se procede al envío de la versión final del informe por medio del socio auditor de TI.
	4. Una vez enviado el informe al BCCR por parte del cliente, si no cumplió con el 100% de los controles obligatorios, el cliente debe enviar al Despacho el plan de acción para realizar nuevamente la revisión de los controles que no cumplieron. El informe debe enviarse a más tardar el 31 de octubre de cada año (el primer año para obtener la certificación y los años posteriores para mantener la certificación, plazo establecido en la normativa del BCCR) , como se indicó, esto para los clientes que incumplen los controles obligatorios.

Evaluación:

Esta cuarta fase del ciclo de auditoría actual en el Despacho incluye la realización de las actividades desglosadas en la Tabla 23.

Tabla 23: Ciclo de auditoría actual: fase de evaluación.

Fase del ciclo de auditoría	Actividades
Evaluación	1. El socio auditor de TI realiza la evaluación de cada auditor con respecto a su desempeño en la auditoría finalizada.
	2. El socio auditor de TI envía los resultados a los auditores evaluados.
	3. Los auditores se reúnen individualmente con el socio auditor de TI para conversar sobre los resultados, el socio auditor les da a conocer fortalezas y oportunidades de mejora a cada auditor.

4.1.3. Hallazgos Revisión documental: herramienta actual para procedimientos de auditoría en ciberseguridad.

Producto de la revisión documental se determinó que la herramienta de auditoría actual de los procedimientos de auditoría es una plantilla en Word de uso general en los distintos tipos de auditoría, es decir, se utiliza la misma para todas las auditorías de TI que realiza el Despacho independientemente de la normativa que se utilice. En el Apéndice M se indican las secciones de esta herramienta.

4.1.4. Hallazgos de la entrevista al socio auditor: situación actual.

Las respuestas a la entrevista al socio auditor en el Apéndice F no solo permitió identificar el ciclo de auditoría actual, sino también, deficiencias en la realización de las auditorías de ciberseguridad para la certificación para la participación en el SINPE, las cuales se describen en la Tabla 24.

Tabla 24: Hallazgos de la entrevista.

Hallazgos
1. Desde la perspectiva del socio auditor de TI a pesar del cumplimiento puntual con los plazos de entrega de los informes de auditoría, internamente si ocurren problemas que vuelven ineficiente la ejecución de las auditorías.
2. Se menciona que no se realizan reuniones entre el socio auditor y el equipo de auditores de manera regular, por tanto, se dificulta la comunicación y si existe alguna discrepancia con un cliente o alguna duda sobre la evaluación de algún control para cuando el socio auditor consulta si se está presentando alguna de estas situaciones, ya ha pasado mucho tiempo.
3. Las dudas de los auditores respecto a los controles a evaluar generan un aumento en el tiempo necesario para analizar los requerimientos iniciales.
4. Producto del retraso en tiempo para el análisis de la información suministrada como parte de los requerimientos iniciales, se retrasa el envío de solicitudes de requerimientos adicionales,

Hallazgos
lo que ocasiona demoras en la recepción de la información solicitada por parte del cliente, impidiendo que el equipo avance en la evaluación de los controles.
5. Según el socio auditor de TI las actividades que consumen mayor tiempo o recursos, por causa de los problemas mencionados en los puntos anteriores, son: a) La realización de pruebas sustantivas y de cumplimiento. b) La realización de entrevistas para revisar la plataforma porque la normativa incluye sistemas, plataforma, red, y activos. c) La revisión de requerimientos iniciales para la solicitud de requerimientos adicionales**.**

4.1.5. Hallazgos del grupo focal al grupo de auditores: situación actual.

Se llevó a cabo un grupo focal con los cuatro auditores de TI actuales del Despacho, ver en Apéndice C, quienes son los responsables de desarrollar los procedimientos de auditoría. Durante esta sesión, identificaron varios problemas en el procedimiento actual para realizar auditorías de ciberseguridad para participar en SINPE, estas deficiencias se describen en la Tabla 25.

Cabe recalcar que el 100% de los auditores coincidió en las respuestas brindadas para cada uno de los hallazgos identificados.

Tabla 25: Hallazgos del grupo focal.

Hallazgos
1. Se concluye que, en la realización de auditorías de ciberseguridad, en comparación con aquellas basadas en COBIT o las Normas del MICIT, que solían ser las más comunes para los auditores de TI antes de la publicación de la Norma Técnica del BCCR, el conocimiento específico de cada auditor en ciberseguridad tiene un impacto significativo en el proceso.
2. No saben cuáles son los requerimientos iniciales por solicitar, han visto que varían según la empresa y eso genera confusión porque esperan que al ser una norma aplique lo mismo para todos.
3. Actualmente no existen definidos atributos estandarizados.
4. Existen algunos controles para los cuales no comprenden en su totalidad qué deben revisar específicamente o cuál evidencia permite verificar que están en cumplimiento con la Norma Técnica del BCCR.
5. El desconocimiento de los atributos por evaluar o la falta de entendimiento de algunos controles de la Norma Técnica, así como la inexistencia de una plantilla con lo requerido para hacer los procedimientos de auditoría en este tipo específico de auditorías les representa un retraso en los tiempos de ejecución de la auditoría, principalmente en la revisión de requerimientos adicionales para determinar si se requiere solicitar requerimientos adicionales y en la elaboración de los procedimientos de auditoría.
6. Con respecto a los procedimientos de auditoría actuales indican que otro problema que enfrentan es no conocer con qué profundidad se debe evaluar un control sin salirse o sin incumplir el alcance que la norma espera del mismo, esto se relaciona a la inexistencia de atributos que les permita identificar cómo evaluar cada control.

Hallazgos
7. En sesiones con el cliente o en solicitud de requerimientos adicionales ha sucedido que el cliente no entiende qué información requieren entregar y los auditores al no comprender a plenitud la norma, no logran comunicarle al cliente u orientarlo con respecto a la información que debería tener o presentar para cumplir con lo estipulado en la normativa.
8. Ante la incertidumbre de qué evaluar o qué significa lo solicitado por algún control de la Norma Técnica emitida por el BCCR, todos los participantes coincidieron en que, primeramente, consultan en internet por medio de Google, posteriormente, si las dudas persisten solicitan apoyo a los compañeros auditores y finalmente, si por medio de ambos recursos anteriores no se evacuó la duda, se consulta con el socio auditor de TI.
9. Por lo reciente de la normativa y las pocas auditorías de este tipo que se han realizado, consideran que se requiere documentación que permita abordar las auditorías de ciberseguridad básicamente desde la primera actividad de la fase de ejecución que sería el análisis de los requerimientos iniciales.
10. Todos los auditores plantean que, para realizar las auditorías en ciberseguridad, principalmente para nuevos colaboradores se requiere que como parte de su capacitación se les explique cada uno de los controles, qué se debe revisar y qué evidencias se deben solicitar al cliente.

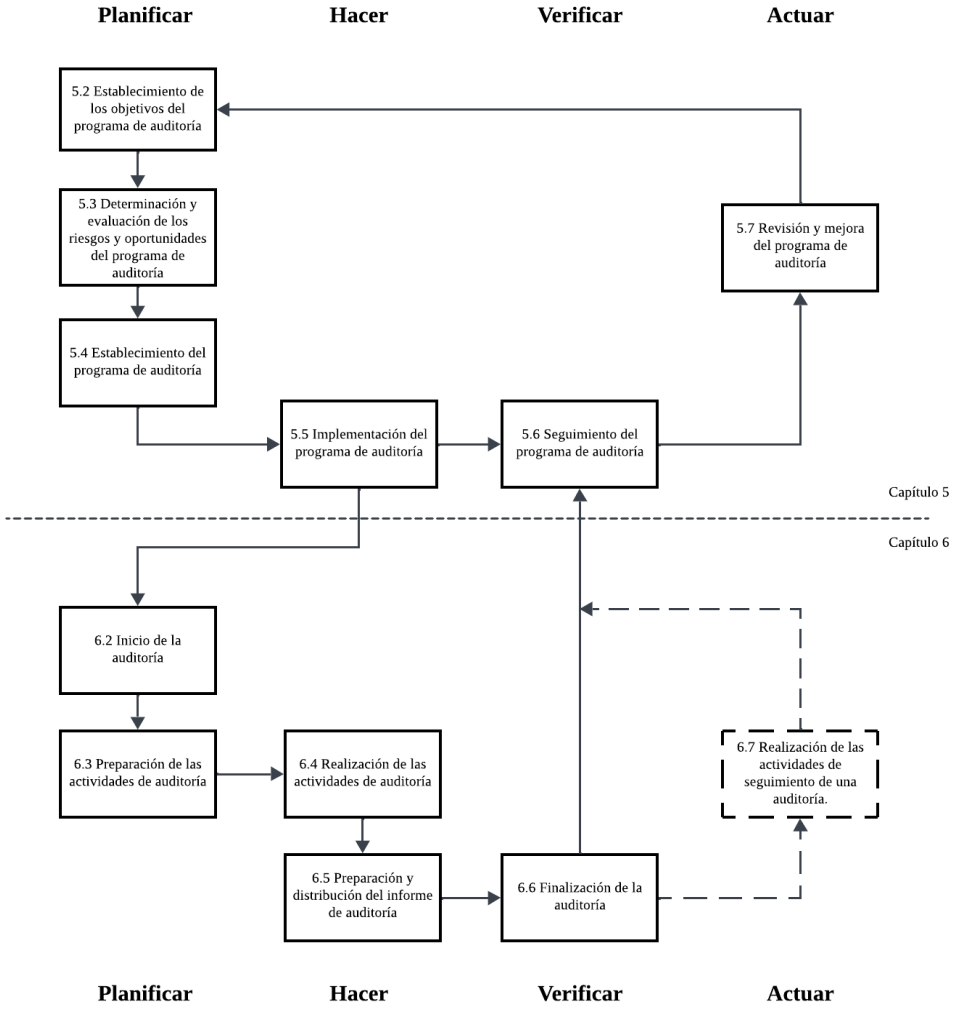
Producto del análisis efectuado a las respuestas obtenidas por el grupo de auditores y a la entrevista realizada al socio auditor de TI, es posible determinar que las deficiencias se ubican en la fase de ejecución, además, por alcance del proyecto será esta fase la que se trabaje como mejora. La fase de planeación, cierre y evaluación son actividades formalmente establecidas en el Despacho, por tanto, se mantendrán sin cambios.

Con respecto a la fase de ejecución, pese a que el Despacho cumple con los tiempos establecidos en el plan de auditoría, internamente si presenta cuellos de botella y múltiples oportunidades de mejora con respecto al procedimiento para realizar las evaluaciones de los controles según lo indica el socio auditor de TI en respuesta a la entrevista en el Apéndice F.

Por este motivo, cabe resaltar que en este proyecto no se realizará una mejora al ciclo actual de auditoría porque este proceso, con respecto a sus fases y actividades macro, aún con la implementación de la propuesta es el mismo, sino que se trabaja en una mejora al procedimiento específico del proceso de “Ejecución” del ciclo de auditoría.

En la Figura 8 se muestra el flujo del proceso para la gestión de un programa de auditoría propuesto en la ISO 19011.

Figura 8: Ciclo de auditoría según ISO 19011.



Nota: Recuperado de (ISO, 2018, p. 10)

De acuerdo con la figura anterior es posible concluir que, en general, el ciclo de auditoría del Despacho está alineado con el ciclo sugerido por la ISO 19011. Sin embargo, existen diferencias en algunas actividades de la fase de "Ejecutar" (equivalente a la fase de "Ejecución" en el Despacho), las cuales no se alinean en su totalidad con las buenas prácticas. Esta brecha se detalla en la sección 4.2 del documento.

4.2. Análisis de brecha

En esta sección se realiza un análisis de brecha comparando la situación actual del abordaje de las auditorías en ciberseguridad en el Despacho con los lineamientos establecidos por la norma ISO 19011 la cual ofrece una guía definida y estructurada para la gestión eficiente de auditorías, estos lineamientos de la ISO 19011 representan la situación deseada.

Este análisis presentado en la Tabla 26 permite identificar la situación actual del abordaje de auditorías de ciberseguridad en el Despacho, la situación deseada por medio de lo estipulado en la ISO 19011, la brecha existente y el plan de acción para cerrar cada una de las brechas identificadas.

Tabla 26: Análisis de brecha.

Situación actual (¿Dónde estoy/Qué tengo?)	Situación deseada (¿Dónde quiero llegar/ Qué quiero tener?)	Brechas	Plan de acción para cerrar las brechas (¿Cómo lo voy a lograr?)
Los auditores desconocen los requerimientos iniciales por solicitar.	Las personas responsables de la gestión del programa de auditoría deberían tener la competencia necesaria para gestionar el programa de auditoría incluyendo conocimientos sobre: • Los requisitos legales y reglamentarios aplicables y otros requisitos pertinentes a las actividades de negocio del auditado (ISO, 2018).	Desconocimiento de los auditores sobre los requerimientos iniciales por solicitar.	Elaborar un Manual de Auditoría que entre sus secciones incluya: • Una lista de requerimientos iniciales por solicitar a los clientes en auditorías de ciberseguridad.
El ciclo de auditorías en ciberseguridad para participación en SINPE no se encuentra documentado, los auditores no cuentan con una metodología o explicación del proceso que los guíe.	Las personas responsables de la gestión del programa de auditoría deberían: asegurarse de que se prepara y mantiene la información documentada apropiada, incluyendo los registros del programa de auditoría (ISO, 2018).	Falta de documentación del ciclo de auditorías en ciberseguridad para participación en SINPE.	Suministrar el manual a los auditores de TI del Despacho como material de capacitación. Agregar al manual de auditoría: • Que entre sus secciones incluya una destinada a la explicación de las fases del ciclo de auditoría y respectivas actividades de estas fases, para auditorías en ciberseguridad para participación en el SINPE.
No existe un procedimiento estandarizado para la ejecución de auditorías, cada auditor revisa según	Principios, procesos y métodos de auditoría: los conocimientos y habilidades en esta área permiten al auditor asegurarse de que las auditorías se realizan de manera	Ausencia de un procedimiento estandarizado para la ejecución de auditorías	• Agregar al manual de auditoría una sección que incluya la lista de atributos por revisar para cada control de la Norma Técnica del

Situación actual (¿Dónde estoy/Qué tengo?)	Situación deseada (¿Dónde quiero llegar/ Qué quiero tener?)	Brechas	Plan de acción para cerrar las brechas (¿Cómo lo voy a lograr?)
su criterio sin atributos definidos, lo que genera retrasos y que las conclusiones de los auditores sean inconsistentes.	coherente y sistemática (ISO, 2018).		BCCR, así como la explicación de cómo se debe evaluar el control. • Elaborar una herramienta de auditoría en Word que permita realizar los procedimientos de auditoría basada en la Norma NIST - Cybersecurity framework y la Norma Técnica del BCCR.
El equipo de auditores carece de claridad sobre los criterios de evaluación de los controles y de los requisitos de la información del cliente con respecto al cumplimiento normativo, debido a la reciente implementación de la Norma Técnica del BCCR.	Según ISO (2018) un auditor debería ser capaz de: • Verificar la pertinencia y exactitud de la información recopilada. • Confirmar que la evidencia de la auditoría es suficiente y apropiada para apoyar los hallazgos y conclusiones de la auditoría	Falta de claridad sobre los criterios de evaluación de los controles.	Agregar a la herramienta de auditoría los elementos del marco NIST identificados en la sección “ Fase II: Identificación de componentes del marco NIST – Cybersecurity Framework” de manera que tenga mayor referencia de los requisitos con los cuáles debería cumplir el auditado.
Los auditores, al no comprender plenamente la norma, no logran comunicar ni orientar al cliente sobre la información que debe presentar para cumplir con lo estipulado. Esto genera malentendidos y falta de claridad respecto a las no conformidades.	Los hallazgos de auditoría deberían revisarse con el auditado para reconocer que la evidencia de la auditoría es exacta y que las no conformidades se han comprendido. Se debería realizar todo el esfuerzo posible para resolver cualquier opinión divergente relativa a las evidencias o a los hallazgos de la auditoría (ISO, 2018).	Desconocimiento de los auditores sobre los requisitos específicos de la norma.	Agregar a la herramienta de auditoría las secciones de conclusiones y hallazgos, ayudando a estructurar de manera clara las evidencias y no conformidades a revisar con el cliente.

4.3. Identificación de los componentes de la Norma NIST - Cybersecurity Framework

En la fase dos de la metodología de investigación propuesta se llevó a cabo una revisión documental como instrumento principal para identificar los componentes de la NIST - Cybersecurity Framework.

Posteriormente, se realizó una comparación entre estos componentes y los controles de la Norma Técnica del BCCR, este análisis permitió identificar la relación entre algunos componentes de la NIST - Cybersecurity Framework y los controles establecidos en la Norma Técnica del BCCR.

Como se mencionó anteriormente, todos los controles de la Norma Técnica se aplicarán, ya que son los requeridos para que las entidades obtengan su certificación para participar en el SINPE. Por otro lado, los componentes del NIST – Cybersecurity Framework se incluirán como valor agregado en la evaluación de la auditoría, proporcionando una referencia adicional de buenas prácticas en ciberseguridad junto con la Norma Técnica del BCCR. Esta combinación no solo permitirá fortalecer los controles, sino también ofrecer una visión más integral y alineada con estándares internacionales, mejorando la calidad de la auditoría.

En la Tabla 27 se muestran los resultados de la identificación de los componentes del NIST alineados con la Norma Técnica. Primero, se indica el control de la Norma, seguido de las funciones y categorías del NIST, y finalmente las subcategorías identificadas. Estos componentes se integrarán en la herramienta de auditoría como criterios de referencia.

Tabla 27: Identificación de componentes de la norma NIST – Cybersecurity Framework.

Control de la Norma Técnica del BCCR	Función NIST	Categoría NIST	Controles NIST
6.1: Inventario y control de los activos de hardware	Identificar	Gestión de Activos (ID.AM)	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.
6.2: Inventario y control de los activos de software	Identificar	Gestión de Activos (ID.AM)	ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.
6.3: Protección de los datos	Proteger	Seguridad de los datos (PR.DS)	PR.DS-1: Los datos en reposo están protegidos. PR.DS-2: Los datos en tránsito están protegidos. PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
		Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
6.4: Configuración segura	Proteger	Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
		Tecnología de protección (PR.PT)	PR.PT-4: Las redes de comunicaciones y control están protegidas.
	Detectar	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética. DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
		Procesos de Detección (DE.DP)	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.

Control de la Norma Técnica del BCCR	Función NIST	Categoría NIST	Controles NIST
6.5: Administración de cuentas y control de accesos	Proteger	Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados. PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones. PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
		Tecnología de protección (PR.PT)	PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.
6.6: Gestión de vulnerabilidades	Identificar	Evaluación de riesgos (ID.RA)	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.
	Proteger	Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
	Detectar	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-8: Se realizan escaneos de vulnerabilidades.
		Procesos de Detección (DE.DP)	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad. DE.DP-5: los procesos de detección se mejoran continuamente.
6.7: Gestión de bitácoras de auditoría	Detectar	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética. DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
		Tecnología de protección (PR.PT)	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
6.8: Protección del correo electrónico y navegador web	Proteger	Seguridad de los datos (PR.DS)	PR.DS-2 Los datos en tránsito están protegidos. PR.DS-5 Se implementan protecciones contra las filtraciones de datos.
		Tecnología de protección (PR.PT)	PR.PT-4 Las redes de comunicaciones y control están protegidas.

Control de la Norma Técnica del BCCR	Función NIST	Categoría NIST	Controles NIST
6.9: Defensa contra código malicioso	Proteger	Seguridad de los datos (PR.DS)	PR.DS-6 Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
	Detectar	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4: Se detecta el código malicioso.
6.10: Recuperación de datos	Recuperar	Seguridad de los datos (PR.DS)	PR.DS-1 Los datos en reposo están protegidos.
		Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-4 Se realizan, se mantienen y se prueban copias de seguridad de la información.
6.11: Gestión de la infraestructura de red	Proteger	Tecnología de protección (PR.PT)	PR.PT-4 Las redes de comunicaciones y control están protegidas.
		Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-3 Se gestiona el acceso remoto. PR.AC-5 Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).
6.12: Monitoreo y defensa de la red	Proteger	Tecnología de protección (PR.PT)	PR.PT-4 Las redes de comunicaciones y control están protegidas.
	Detectar	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.
6.13: Concientización en ciberseguridad y formación de habilidades	Proteger	Concienciación y capacitación (PR.AT)	PR.AT-1: Todos los usuarios están informados y capacitados. PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades. PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades. PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
6.14: Gestión de proveedores de servicios	Proteger	Gestión de activos (ID.AM)	ID.AM-6 Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.

Control de la Norma Técnica del BCCR	Función NIST	Categoría NIST	Controles NIST
		Gestión del riesgo de la cadena de suministro (ID.SC)	ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético. ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético. ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
6.15: Seguridad en las aplicaciones	Proteger	Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas. PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
		Seguridad de los datos (PR.DS)	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.
6.16: Gestión de respuesta ante incidentes	Responder	Planificación de la Respuesta (RS.RP)	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.
		Comunicaciones (RS.CO)	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta. RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.
		Análisis (RS.AN)	RS.AN-2: Se comprende el impacto del incidente. RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.
		Mitigación (RS.MI)	RS.MI-2: Los incidentes son mitigados. RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.

Nota: Adaptado de NIST (2018)

4.4. Herramienta de auditoría

En la fase tres de la metodología de investigación, denominada "Elaboración de la herramienta de auditoría", se desarrolla una plantilla en Word con el objetivo de estandarizar los procedimientos de auditoría, un aspecto del que actualmente carece el Despacho. Sin embargo, en esta sección no se procederá con la creación de la herramienta, sino que se introducirá la importancia de su desarrollo y se identificará su estrcutura.

La herramienta de auditoría permitirá que los auditores comprendan claramente lo que deben solicitar y cómo guiar al cliente respecto a la información necesaria como evidencia. Al definir de manera precisa los atributos a evaluar, se garantiza que todos los auditores realicen las evaluaciones de manera consistente, lo que facilitará la obtención de conclusiones y hallazgos de forma objetiva y coherente, conforme a lo estipulado en la ISO 19011 (ISO, 2018).

Para la elaboración de la herramienta, el socio auditor de TI solicitó utilizar el formato de tablas en Word empleado en las demás herramientas de auditoría, como las basadas en COBIT o el MICITT, con el fin de mantener un estándar en las herramientas utilizadas en el Despacho. Sin embargo, la Norma Técnica del BCCR establece secciones específicas para la redacción del informe de auditoría. Por lo tanto, la herramienta se desarrolla en Word, incorporando estas secciones y, además, los atributos correspondientes para evaluar los controles de la Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE.

De este modo, por medio de la herramienta, se centraliza la información necesaria para facilitar la elaboración del informe, reduciendo los tiempos de redacción y revisión de conclusiones escritas en los procedimientos de auditoría. Así, en lugar de redactar el informe desde cero, los auditores solo deben transferir la información ingresada en la herramienta a la plantilla del informe que previamente realiza el socio auditor de TI para que la completen los auditores con los resultados de la evaluación.

A través de la revisión documental, se identifican las secciones del informe requeridas por la Norma Técnica del BCCR las cuales se pueden consultar en el Apéndice L, estas se añaden a la plantilla actual como secciones adicionales para la elaboración de la herramienta de auditoría en ciberseguridad. Estas secciones son:

- Sección para indicar si cumple o no cumple con el control.
- Sección para indicar si se identificaron hallazgos.
- Sección para redactar hallazgos, esta incluye una columna para agregar el subcontrol que presenta un hallazgo identificado y otra columna para redactar el hallazgo.

La sección de hallazgos propuesta además de agilizar que en la herramienta de auditoría se realice todo lo requerido para llenar la plantilla del informe, también permite dar un seguimiento cuando la entidad envíe su plan de mitigación en caso de no cumplir con el 100% de los controles obligatorios como lo establece la normativa. De manera que en la misma herramienta sea posible visualizar la conclusión para los controles incumplidos y sus respectivos hallazgos.

4.4.1. Selección de atributos a evaluar

Para la selección de atributos a evaluar se utiliza como referencia lo estipulado en la Norma Técnica del BCCR por ser la normativa aplicable para el proceso de certificación para la

participación en SINPE y se utiliza también la NIST Cybersecurity Framework como marco internacional que establece criterios para la ciberseguridad.

Cabe aclarar que la normativa solicita que se cumplan requerimientos variados como, por ejemplo: implementar mecanismos o herramientas, establecer políticas, realizar revisiones periódicas, mantener inventarios, entre otros. Esta variedad de requisitos provoca que no sea posible generar atributos estandarizados para todos los controles como por ejemplo definir solo si cumple con existencia, estructura y cumplimiento, que es lo evaluado en las demás auditorías de TI del Despacho. Esta variedad requiere hacer una identificación propia de cada control según lo solicitado en la normativa y según los componentes de la NIST - Cybersecurity Framework que se identificaron como relacionados con cada control de la Norma Técnica del BCCR en la Tabla 27.

Este análisis de los requerimientos específicos a revisar por atributo se realiza con base en diversas normativas, con el objetivo de adquirir un mayor conocimiento sobre los estándares de cumplimiento en ciberseguridad. Esto permite llevar a cabo un análisis de los controles que garantice su alineación con la normativa y facilite la redacción de las conclusiones del informe de auditoría, asegurando el nivel de detalle que el BCCR requiere para considerar los controles como cumplidos.

Las normativas utilizadas para establecer los requerimientos específicos por revisar para cada atributo son las siguientes:

- Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE
- NIST Cybersecurity Framework
- ISO 27001
- NIST Special Publication 800-53 revisión 5.1.1

4.4.1.1. 6.1 Inventario y control de los activos de hardware

Para el control 6.1, en la Tabla 28 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 28: Selección de atributos y evidencia requerida control 6.1

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un inventario de la infraestructura SINPE	La estructura del inventario del Ambiente de Interfaz con el SINPE debería incluir al menos: • Nombre del dispositivo • La dirección de red (si es estática) • La función o servicio.	Se debe revisar: • Que cuenten con del inventario del Ambiente de Interfaz con el SINPE. • Que La estructura del inventario del Ambiente de Interfaz con el SINPE incluya al menos: o Nombre del dispositivo. o La dirección de red (si es estática). o La función o servicio.
Evidencia de actualización del inventario de la infraestructura SINPE	Evidencia de revisión y actualización del inventario al menos una vez al año.	• Revisar si cuentan con evidencias de las revisiones y/o actualizaciones realizadas al inventario. • Verificar que se hayan realizado las revisiones y/o actualizaciones al menos anualmente.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un diagrama de red detallado	Diagrama de red detallado y actualizado del ambiente de interfaz con el SINPE. Incluir en el diagrama información detallada de la red, protocolos y puertos utilizados.	Verificar que el diagrama de red sea detallado, por ejemplo: • Servidores, routers, switches, firewalls, estaciones de trabajo, sistemas de almacenamiento, entre otros. • El nombre del dispositivo debe estar claramente indicado en el diagrama • Direcciones IP de cada dispositivo Revisar que obligatoriamente incluya: • Protocolos utilizados (ej. TCP/IP, HTTP, HTTPS, SSH, entre otros.). • Puertos utilizados.
Evidencia de actualización del diagrama de red	Evidencia de revisión y actualización del diagrama de red al menos una vez al año o cuando sufra modificaciones que requieran su actualización.	Revisar que mantengan evidencia de revisiones al diagrama de red, que sean realizadas al menos anualmente.

4.4.1.2. 6.2 Inventario y control de los activos de software

Para el control 6.2, en la Tabla 29 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 29: Selección de atributos y evidencia requerida control 6.2

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un inventario de software en la infraestructura SINPE	Inventario detallado de todo el software instalado en la infraestructura del ambiente de interfaz con el SINPE. Incluir nombre, fabricante, versión y propósito.	Revisar si existe un inventario de software en la infraestructura SINPE. Revisar sobre la estructura del inventario de software instalado en la infraestructura del Ambiente de Interfaz con el SINPE que incluya al menos:

Atributo	Evidencia requerida	¿Cómo revisar el control?
		• Nombre del software. • El fabricante del software. • La versión del software. • El propósito del software. Sobre los softwares en inventario se debe validar: • Que únicamente se mantengan las versiones de software que cuenten con el debido soporte.
Evidencia de actualización del inventario de software en la infraestructura SINPE	Evidencia de revisión y actualización del inventario al menos una vez al año.	Revisar que cuenten con evidencia de revisión y/o actualización del inventario, esta debe ser al menos una vez al año.
Existencia de una lista de software autorizado	• Lista de software autorizado para el ambiente de interfaz con el SINPE. • Controles implementados para eliminar software no autorizado o fuera de soporte de los equipos.	Revisar que cuenten con: • Una lista actualizada de software permitido para el Ambiente de Interfaz con el SINPE. • Implementación de controles para eliminar el software no autorizado o fuera de soporte de los equipos. Verificar que se encuentren documentados estos controles.
Evidencia de actualización de la lista de software autorizado	• Evidencia de revisión y actualización del inventario al menos cada 6 meses. • Excepciones detectadas con el debido plan remedial.	• Se debe revisar que cuenten con evidencia de revisión y/o actualización de la lista de software permitido, esta debe ser al menos cada seis meses. • Se debe revisar el inventario de software suministrado en el control 6.2.1 contra la lista de software permitido. ○ Para los softwares detectados que no son autorizados o están fuera de soporte, verificar que estén documentadas estas excepciones y que cuenten con su debido plan remedial.

4.4.1.3. 6.3. Protección de los datos

Para el control 6.3, en la Tabla 30 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 30: Selección de atributos y evidencia requerida control 6.3

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un procedimiento para la gestión de datos sensibles.	Procedimiento establecido para la identificación y gestión de datos confidenciales o sensibles (saldos de las cuentas de valores y efectivo, monto de las transacciones del SINPE en efectivo y valores, identificación y nombre del cliente origen y destino de las transacciones del SINPE) que dé cobertura a aquellos relacionados con el SINPE.	Revisar que cuenten con un procedimiento que identifique los datos sensibles o confidenciales relacionados con SINPE y que establezca el manejo adecuado que debe recibir. Los datos sensibles pueden ser: saldos de las cuentas de valores y efectivo, monto de las transacciones del SINPE en efectivo y valores, identificación y nombre del cliente origen y destino de las transacciones del SINPE. Validar que el procedimiento incluya en su estructura como mínimo los siguientes aspectos: • Identificar los datos sensibles o confidenciales relacionados con SINPE. • La confidencialidad de los datos (verificar que se realice una clasificación de la información). • Requerimientos legales. • El propietario de los datos sensibles identificados. • Descripción del manejo adecuado de los datos sensibles.
Implementación de mecanismos de cifrado de datos en tránsito	Procedimiento para cifrar los datos confidenciales en tránsito, transmitidos entre la plataforma tecnológica y el ambiente interfaz del SINPE.	Revisar que cuenten con evidencia de cifrado de los datos en tránsito, transmitidos entre la Plataforma Tecnológica del Afiliado y el Ambiente de Interfaz del SINPE. Se debe revisar que este cifrado se realice por medio de protocolos seguros como, por ejemplo: • TLS (Transport Layer Security). • IPSec (Internet Protocol Security). • SSH (Secure Shell). • HTTPS (HTTP Secure).

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de una política de disposición y/o destrucción de medios y hardware	Política para la disposición y/o destrucción en medios de almacenamiento (incluido el hardware) cuando se cumple su tiempo máximo de operación y se debe dar de baja o debe enviarse fuera de la organización.	Revisar que cuenten con una política para la gestión del ciclo de la información en medios de almacenamiento (incluido el hardware). La política debe establecer sobre la información, lo siguiente: • Cuando se cumple su tiempo máximo de operación. • Cuando se debe eliminar la información. • Cuando debe enviarse fuera de la organización por temas de soporte. Adicionalmente, revisar: • Que se defina el ciclo de la información en medios de almacenamiento. • Que se establezcan responsables de realizar la destrucción de medios y hardware.
Implementación de mecanismos de cifrado de datos en reposo	Procedimiento para cifrar los datos sensibles o confidenciales que se encuentren en reposo.	Revisar que cuenten con mecanismos de protección de datos en reposo utilizados. Por ejemplo, la implementación de uno o varios de los siguientes: • Mecanismos de cifrado. • Configuraciones o conjuntos de reglas para firewalls. • Sistemas de detección y prevención de intrusiones. • Enrutadores de filtrado. • Escaneo frecuente para identificar código malicioso en reposo.

4.4.1.4. 6.4. Configuración segura

Para el control 6.4, en la Tabla 31 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 31: Selección de atributos y evidencia requerida control 6.4

Atributo	Evidencia requerida	¿Cómo revisar el control?

Existencia de un proceso de configuración segura	Proceso establecido para la configuración (hardening) basado en un marco de ciberseguridad para la infraestructura del ambiente de interfaz con el SINPE. Adjuntar evidencia del cumplimiento del proceso de configuración establecido, así como de las excepciones identificadas.	Revisar que exista un proceso operativo sobre configuración segura.
		Por ejemplo, el marco CIS establece las siguientes mejores prácticas y mecanismos para asegurar la configuración de sistemas y aplicaciones:
		• CIS Benchmarks: Se recomienda realizar auditorías regulares contra estos benchmarks para asegurar que los sistemas cumplan con las configuraciones seguras.
		• Políticas de Contraseña.
		• Mantenimiento de Actualizaciones: asegurar que todos los sistemas operativos y aplicaciones se mantengan actualizados con los últimos parches de seguridad.
		• Control de Acceso: principio de mínimos privilegios.
		• Protección de Datos.
		• Configuración de Redes
		  ○ Seguridad de Perímetro: Se deben configurar firewalls y dispositivos de seguridad perimetral para restringir el acceso no autorizado a la red.
		  ○ Segmentación de red.
		  ○ Múltiples Capas de Seguridad: Aplicar múltiples capas de defensa, como el uso de antivirus, detección de intrusiones y políticas de seguridad física.

Existencia de mecanismos de revisión de configuración segura	• Evidencia de mecanismos de revisión anuales de cumplimiento de la configuración segura establecida. • Evidencia de la documentación de las excepciones.	Se debe revisar que cuenten con evidencia de revisiones anuales de cumplimiento de la configuración segura establecida. Debe verificarse que exista un cumplimiento de la configuración segura. Si alguna configuración no cumple, se debe validar que mantengan documentadas las excepciones.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de un firewall	Configuración de las reglas de firewall incluyendo todos los servicios, protocolos y puertos. Incluir justificación del negocio y la aprobación para cada regla. Adjuntar última revisión de las reglas.	Se debe verificar que cuenten con la implementación de un firewall, revisar que cumpla con los siguientes aspectos: • Controlar con mínimo privilegio todas las comunicaciones entre el Ambiente de Interfaz con el SINPE y cualquier otra red, incluida la salida a Internet. • Restringir conexiones innecesarias. • Debe permitir una adecuada segmentación de redes, estos son ejemplos de pruebas a realizar para evaluar este punto: o Verificar que los dispositivos en diferentes segmentos de la red no puedan comunicarse entre sí si no tienen permisos específicos (solicitar en reunión con cliente que se realice esta prueba). o Confirmar que los puertos específicos estén abiertos o cerrados según las reglas de firewall definidas (solicitar en reunión con cliente que se realice esta revisión). • La configuración de las reglas del firewall debe incluir: o Una lista documentada de todos los servicios, protocolos y puertos. o La justificación de negocio y la aprobación para cada una de dichas reglas. Se debe validar que realicen revisiones de las reglas de firewall al menos cada seis meses.

4.4.1.5. 6.5. Administración de cuentas y control de accesos

Para el control 6.5, en la Tabla 32 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 32: Selección de atributos y evidencia requerida control 6.5

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un inventario de software en la infraestructura SINPE	Inventario de todo el personal con acceso al ambiente de interfaz con el SINPE, incluir cuentas de usuario, de administración y servicio.	Revisar que cuenten con un inventario de las cuentas de todo el personal con acceso al Ambiente de Interfaz con el SINPE. Verificar que la estructura del inventario de cuentas incluya al menos: • Nombre de la persona responsable de la cuenta. • Detalle de la cuenta de usuario (FQDN). • Tipo de cuenta (usuario, servicio, administración) • Dominio. • Departamento. Validar si existe evidencia de revisiones a las cuentas, los roles y sus privilegios, al menos de forma semestral y evidencia de la aprobación por el superior jerárquico.
Inhabilitación de cuentas	Evidencia de la deshabilitación de cuentas inactivas.	La revisión sobre deshabilitación de cuentas inactivas se realiza de la siguiente manera: • Se debe solicitar un reporte a recursos Humanos sobre el listado de exfuncionarios para el periodo evaluado. • Se debe revisar el reporte de Recursos Humanos contra el inventario de cuentas suministrado, para verificar que se realice la inactivación de cuentas correspondiente.
Existencia de una política de contraseñas	Política para la administración de contraseñas en las cuentas.	Revisar que exista una política de contraseñas en las cuentas que se identificaron en el inventario del control 6.5.1. Debe verificar que la política de contraseñas debe contemple al menos las siguientes características: • Cada usuario debe tener una contraseña única. • Si utiliza Autenticación Multifactor (MFA), las contraseñas deben ser de al menos ocho caracteres. • Si no tiene implementado Autenticación Multifactor (MFA), las contraseñas deben tener al menos 14 caracteres. • Que implementen mecanismos para forzar su complejidad, de acuerdo con las mejores prácticas internacionales. Por ejemplo:

Atributo	Evidencia requerida	¿Cómo revisar el control?
		○ Uso de caracteres especiales. ○ Uso de mayúsculas. ○ Uso de minúsculas. ○ Uso de números. Se debe revisar evidencia de la configuración de las contraseñas para verificar que solicite un cambio al menos cada 90 días naturales, cuando no se utilice Autenticación Multifactor (MFA).
Implementación de restricciones en perfiles administrador	Inventario de cuentas de tipo administración y servicio.	Validar si cuentan con evidencia de la restricción de las actividades propias de usuario final, por ejemplo: navegación por Internet y acceso al correo electrónico. Un ejemplo de la evidencia por revisar: Evidencia de la implementación de firewalls para bloquear el acceso a sitios web no autorizados y usar filtros de contenido para restringir el acceso a categorías específicas de sitios.
Existencia de un proceso para conceder accesos	Procedimiento para otorgar, revocar o modificar los accesos a la infraestructura del ambiente de interfaz con el SINPE.	Existencia de un proceso para otorgar, revocar o modificar los accesos a la infraestructura del Ambiente de Interfaz con el SINPE basado en el principio de mínimo privilegio.
Implementación de la Autenticación Multifactor	Evidencia de la implementación de la Autenticación Multifactor (MFA) para todos los accesos administrativos a la infraestructura del Ambiente de Interfaz con el SINPE.	Se debe revisar que al intentar ingresar a la infraestructura del Ambiente de Interfaz con el SINPE, el sistema solicite una doble autenticación. Es decir, que no puedan ingresar solo con la contraseña del usuario.

4.4.1.6. 6.6. Gestión de vulnerabilidades

Para el control 6.6, en la Tabla 33 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 33: Selección de atributos y evidencia requerida control 6.6

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un procedimiento para gestión de vulnerabilidades	Existencia de un procedimiento para gestionar vulnerabilidades.	Se debe validar que exista un procedimiento para gestionar vulnerabilidades. Validar que como mínimo la estructura del documento incluya: • Análisis de vulnerabilidades (proceso para identificar y evaluar vulnerabilidades). • Remediación de vulnerabilidades.
Evidencia de actualización del procedimiento para gestión de vulnerabilidades	Indicar última fecha de revisión.	Se debe validar que exista evidencia de la revisión y actualización de la documentación sobre gestión de vulnerabilidades anualmente, o cuando ocurran cambios significativos que puedan afectar este control.
Existencia de análisis de vulnerabilidades internos y externos	Existencia de escaneos de vulnerabilidades internos y externos (red interna y fuera de la red de la institución).	Validar que se realicen escaneos de vulnerabilidades internos y externos (red interna y fuera de la red de la institución). Debe cumplir con al menos las siguientes características: • Se realiza al menos una vez por semestre para la infraestructura del Ambiente de Interfaz con el SINPE. • Se documentan los hallazgos detectados (vulnerabilidades identificadas). • Se corrigen las vulnerabilidades detectadas y documentadas según como lo establece la política o procedimiento para gestión de vulnerabilidades.
Existencia de un proceso de gestión de parches y actualizaciones	Proceso para implementar parchados o actualizaciones.	Se debe revisar que exista un procedimiento para gestionar el parchado y las actualizaciones. Además, verificar que cuenten con evidencia de la ejecución del procedimiento. Es decir, que se hayan realizado parchados o actualizaciones según se definió en el procedimiento.

4.4.1.7. 6.7. Gestión de bitácoras de auditoría

Para el control 6.7, en la Tabla 34 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 34: Selección de atributos y evidencia requerida control 6.7

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un procedimiento para gestionar las bitácoras de auditoría	Procedimiento para gestionar bitácoras de auditoría de toda la infraestructura del ambiente de interfaz con el SINPE.	Se debe verificar la existencia de un procedimiento para gestionar las bitácoras de auditoría. Validar que como mínimo aborde en su estructura: • Recopilación de registros. • Revisión de registros. • Retención de registros. Revisar que existan registros de auditoría de toda la infraestructura del Ambiente de Interfaz con el SINPE. Como mínimo, el registro debe incluir: • El origen del evento. • La fecha. • El nombre de usuario. • La marca de tiempo (hora del registro). • El dominio. • Las direcciones de origen. • Las direcciones de destino.
Existencia de un proceso de retención de registros	Procedimiento para gestionar bitácoras de auditoría de toda la infraestructura del ambiente de interfaz con el SINPE.	Revisar que cuenten con evidencia de retención de registros de auditoría según lo estipularon en el procedimiento de gestión de bitácoras de auditoría establecido. Validar que cuenten con evidencia la cual indique que la retención sea mínimamente de 90 días.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Estandarización de la hora los registros de auditoría	Procedimiento para estandarizar la hora dentro de la infraestructura.	Verificar que los registros de auditoría consuman la hora de al menos dos orígenes de hora sincronizados dentro de la infraestructura (esto significa que la hora de los dispositivos en la infraestructura debe estar sincronizada). Por ejemplo: Que consuma la hora de un protocolo Network Time Protocol (NTP) y del equipo físico.
Existencia de revisiones a las bitácoras de auditoría	Evidencia de las revisiones de los registros de auditoria para detectar posibles anomalías o eventos anormales que podrían representar una amenaza. Incluir procedimiento.	Verificar que exista evidencia de revisión a los registros de auditoría, además, validar que esta revisión se realice al menos semanalmente.

4.4.1.8. 6.8. Protección del correo electrónico y la navegación por Internet

Para el control 6.8, en la Tabla 35 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 35: Selección de atributos y evidencia requerida control 6.8

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de un filtrado de navegación	Procedimiento para aplicar y mantener actualizados los filtros de navegación para limitar la conexión de los activos a sitios web potencialmente maliciosos o no probados.	Por revisar sobre este control: • Filtros configurados para limitar la conexión a sitios potencialmente maliciosos o no aprobados. • Se debe revisar un intento de acceso a sitios configurados con limitaciones de conexión para verificar la efectividad del filtro.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de protección contra correo no deseado	Procedimiento para implementar y mantener una herramienta de filtrado de correo no deseado.	Validar que exista y se utilice una herramienta de filtrado de correo no deseado. Por revisar sobre este control: • Existencia de la herramienta. • Configuración en la herramienta para filtrar correo no deseado.
Implementación de protección antimalware en el correo	Protección antimalware implementado a nivel del servidor de correo electrónico. Adjuntar detalles.	Verificar que cuenten con evidencia de protecciones antimalware a nivel de servidor de correo electrónico, por ejemplo: • Análisis de datos adjuntos. • Espacio aislado (entorno seguro donde se pueden ejecutar y analizar archivos adjuntos de correos electrónicos de forma controlada) • Que dispongan de software con capacidad de configuración antimalware habilitada
Implementación de bloqueo de archivos innecesarios	Política de bloqueo en el correo electrónico de archivos adjuntos riesgosos o innecesarios. Adjuntar revisiones realizadas.	Revisar si exista una política de bloqueo de archivos adjuntos riesgosos o innecesarios. Validar que se realicen revisiones a la lista de bloqueo de archivos innecesarios configurada, al menos semestralmente.

4.4.1.9. 6.9. Defensa contra código malicioso

Para el control 6.9, en la Tabla 36 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 36: Selección de atributos y evidencia requerida control 6.9

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de software de protección contra código malicioso	Detalles del software de protección implementado contra código malicioso en todos los activos del ambiente de interfaz con el SINPE.	Verificar que tengan implementado un software de protección contra código malicioso en todos los activos del Ambiente de Interfaz con el SINPE.
Evidencia de actualización automática de firmas contra código malicioso	Configuración de las actualizaciones automáticas de las herramientas contra código malicioso.	Por revisar sobre este control: • La opción de actualización automática debe estar habilitada en las soluciones de seguridad (software de protección contra código malicioso seleccionado) implementadas en la infraestructura Revisar la configuración de los programas para confirmar que están configurados para buscar e instalar actualizaciones de firmas de manera regular.
Implementación de herramientas basadas en comportamiento	Detalles de la herramienta utilizada contra código malicioso basada en el comportamiento.	Verificar el uso de software contra código malicioso basado en el comportamiento.

4.4.1.10. 6.10. Recuperación de datos

Para el control 6.10, en la Tabla 37 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 37: Selección de atributos y evidencia requerida control 6.10

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un procedimiento de recuperación de datos	Procedimiento para la recuperación de datos del ambiente de interfaz con el SINPE. Adjuntar evidencia de su implementación.	Revisar que exista un procedimiento de recuperación de datos definida en la institución. Validar que la estructura del procedimiento incluya al menos los siguientes aspectos: • Alcance de las actividades de recuperación. • Priorización de la recuperación. • Definir pruebas de recuperación. • Seguridad de los datos de respaldo: debe contemplar el proceso de realización de respaldos de los datos. Además, validar si existe evidencia de la ejecución del procedimiento, es decir, si este se cumple.
Evidencia de revisiones al procedimiento de recuperación de datos	Adjuntar fecha de última revisión al procedimiento de recuperación de datos.	Revisar que la frecuencia de revisión y actualización del procedimiento de recuperación de datos sea la siguiente: • Anualmente. • O cuando ocurran cambios significativos que puedan afectar la política.

4.4.1.11. 6.11. Gestión de la infraestructura de red

Para el control 6.11, en la Tabla 38 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 38: Selección de atributos y evidencia requerida control 6.11

Atributo	Evidencia requerida	¿Cómo revisar el control?

Existencia de una arquitectura de red segura	Arquitectura de red donde se ubican los equipos del ambiente de interfaz con el SINPE.	Se debe revisar que cuenten con una arquitectura de la red (donde se ubican los equipos del Ambiente de Interfaz con el SINPE) segmentada.
		Por revisar sobre este control:
		• Verificar que los segmentos de red están identificados y separados física y lógicamente: por ejemplo, red institucional y red de ambiente de interfaz SINPE.
		• La segmentación se puede lograr por medio de alguno de los siguientes elementos, verificar por medio de cuál se realiza:
		  ○ Puertas de enlace (gateway)
		  ○ Routers.
		  ○ Firewalls.
		  ○ Ssitemas de virtualización
		  ○ Túneles cifrados

Implementación de protocolos seguros	Protocolos utilizados para la administración de red.	Verificar que cuenten con evidencia del uso de protocolos seguros de red, por ejemplo: • SSH (Secure Shell). • SNMP v3 (Simple Network Management Protocol version 3). • HTTPS (HTTP Secure).

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de mecanismos AAA.	Detallar mecanismos de identidad utilizados (Autenticación, Autorización y Auditoria) para el acceso administrativo a la infraestructura de red.	Revisar que para el acceso administrativo a la infraestructura de red se implementen los siguientes mecanismos: • Autenticación: pueden ser por medio de contraseñas, autenticadores físicos, biometría o la autenticación multifactor (este puede incluir una combinación de los métodos anteriores). • Autorización: verificar que cuenten con controles de accesos a la red definidos para usuarios del Ambiente de Interfaz SINPE (por ejemplo, tokens de acceso). • Auditoría: verificar que se mantengan registros de todas las actividades de los usuarios dentro del sistema, por ejemplo: validar que se registren los accesos al ambiente de interfaz con SINPE.
Implementación de control de acceso para activos remotos	Mecanismos utilizados para establecer conexiones remotas a la red empresarial, por ejemplo, VPN.	Verificar que cuenten con evidencia del uso de mecanismos seguros para establecer conexiones remotas, como, por ejemplo: • Uso de VPN.

4.4.1.12. 6.12. Gestión de riesgos

Para el control 6.12, en la Tabla 39 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 39: Selección de atributos y evidencia requerida control 6.12

Atributo	Evidencia requerida	¿Cómo revisar el control?
Implementación de una solución de prevención de intrusiones entre las redes	Detalle de la solución de prevención de intrusiones implementada entre las redes organizacionales y la red del ambiente de interfaz con el SINPE.	Revisar que se haya implementado una solución de prevención de intrusiones (IPS) en las redes (la empresarial y la del Ambiente de Interfaz con el SINPE). Ejemplos de tipos de soluciones a implementar: • Sistema de prevención de intrusiones en la red (NIPS). • Proveedor de servicios en la nube (CSP).

Implementación de un EDR	Detalle de la solución implementada para la detección y respuesta a nivel de host.	Revisar que cuenten con una herramienta de ciberseguridad diseñada para monitorizar, detectar y responder a amenazas a nivel de host.
Implementación de filtrado en la capa de aplicación	Evidencia del filtrado del tráfico externo, en donde se identifique las aplicaciones para bloquear o permitir, según corresponda.	Se debe revisar que realicen un filtrado de tráfico externo que bloquee o permita aplicaciones en el Ambiente de Interfaz con el SINPE mediante la configuración de políticas. Por revisar sobre este control: • El uso de herramientas que permita hacer filtrado web externo, por ejemplo, un firewall de próxima generación. • La lista de aplicaciones bloqueadas.

4.4.1.13. 6.13. Protección de datos personales

Para el control 6.13, en la Tabla 40 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 40: Selección de atributos y evidencia requerida control 6.13

Atributo	Evidencia requerida	¿Cómo revisar el control?

Existencia de un programa de concientización en ciberseguridad	Programa establecido de concientización sobre ciberseguridad. Detallar su ejecución.	Revisar que cuenten con un programa de capacitación, de concientización sobre ciberseguridad.
		
		Validar que el programa cumpla con las siguientes características:
		• Las capacitaciones deben educar al personal sobre cómo interactuar con los activos y datos de la empresa de manera segura.
		• Sobre la frecuencia de realización de capacitaciones:
		  ○ Al momento de contratar.
		  ○ Mínimo anualmente.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de capacitaciones sobre ciberseguridad	Capacitaciones efectuadas en habilidades y concientización sobre ciberseguridad para funciones específicas. Ejemplo curso de administración de sistemas seguros para profesionales de TI, capacitación en prevención y concientización de vulnerabilidades de OWASP, ingeniería social para roles de alto perfil, etc.	Validar que se realizaron capacitaciones en función de los roles y responsabilidades asignados a los colaboradores. Ejemplos de tipos de capacitaciones basadas en roles: • Administración de sistemas seguros: Dirigido a profesionales de TI para enseñarles las mejores prácticas en la configuración y mantenimiento de sistemas seguros. • Prevención de vulnerabilidades de OWASP® Top 10: Capacitación para desarrolladores de aplicaciones web sobre las vulnerabilidades más críticas y cómo prevenirlas. • Ingeniería social: Formación avanzada para roles de alto perfil sobre tácticas de ingeniería social y cómo reconocer y mitigar estos riesgos. Al revisar, la evidencia puede ser, por ejemplo: certificados de participación, correos de invitación a las capacitaciones, capturas de pantalla de la sesión (si es virtual), fotos de la capacitación (si es presencial). • Además, validar que se brinde detalle de la capacitación efectuada y para qué funciones específicas.

4.4.1.14. 6.14. Continuidad del negocio

Para el control 6.14, en la Tabla 41 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 41: Selección de atributos y evidencia requerida control 6.14

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de una política de gestión de proveedores de servicios	Política para la gestión de proveedores de servicios relacionados con la implementación de servicios de interacción directa con el SINPE. Adjuntar fecha de última actualización.	Verificar la existencia de una política de gestión de proveedores para contratos relacionados con la implementación de servicios de interacción directa con el SINPE. Revisar que la estructura de la política incluya como mínimo: • Inventario de todos los proveedores de servicio. • La clasificación de los proveedores: las clasificaciones pueden incluir una o más características, como la sensibilidad de los datos, el volumen de datos, los requisitos de disponibilidad, las regulaciones aplicables, el riesgo inherente y el riesgo mitigado. • Evaluación a los proveedores. • Seguimiento a los proveedores. • Requisitos de ciberseguridad para los proveedores. • Aspectos sobre cancelación de la relación con los proveedores de servicios.
Evidencia de revisión de la política de gestión de proveedores de servicios	Fecha de última revisión a la política de gestión de proveedores de servicios.	Revisar que exista evidencia de la revisión y actualización de la política de gestión de proveedores, además, verificar que esta revisión sea: • Anualmente. • O cuando ocurran cambios significativos.

4.4.1.15. 6.15. Seguridad en las aplicaciones

Para el control 6.15, en la Tabla 42 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 42: Selección de atributos y evidencia requerida control 6.15

Atributo	Evidencia requerida	¿Cómo revisar el control?
Evidencia de separación de los ambientes de prueba y producción	Evidencia de la existencia de entornos separados para sistemas de producción y no producción. Incluir política sobre utilización de datos sensibles en el ambiente de no producción.	Validar que tengan separados los ambientes de prueba y de producción. Además, se debe verificar que los datos sensibles de producción no sean utilizados en el ambiente de pruebas (revisar lo que indica sobre este aspecto el procedimiento de gestión de datos sensibles y validar su cumplimiento).
Existencia de un procedimiento sobre desarrollo de aplicaciones	Procedimiento para el desarrollo de aplicaciones seguras.	Revisar que cuenten con la existencia de un procedimiento sobre desarrollo de aplicaciones. Además, validar que en su estructura se contemplen al menos los siguientes aspectos: • Estándares de diseño de aplicaciones seguras. • Prácticas de codificación segura. • Capacitación de desarrolladores. • Gestión de vulnerabilidades. • Seguridad de código de terceros • Procedimientos de prueba de seguridad de aplicaciones.
Evidencia de revisión del procedimiento sobre desarrollo de aplicaciones	Detallar fecha última actualización del procedimiento sobre el desarrollo de aplicaciones.	Revisar que cuenten con evidencia de revisiones y actualizaciones del procedimiento sobre desarrollo de aplicaciones, validar que la frecuencia sea al menos: • Anualmente. • O cuando ocurran cambios significativos.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Existencia de un proceso para gestionar las vulnerabilidades de las aplicaciones	Procedimiento para la gestión de las vulnerabilidades de las aplicaciones.	Revisar que cuenten con un procedimiento para gestionar las vulnerabilidades de las aplicaciones, verificar que incluya: • Una política de manejo de vulnerabilidades. • Proceso de admisión, asignación, remediación y pruebas de remediación de las vulnerabilidades reportadas.
Evidencia de revisión del procedimiento para gestionar las vulnerabilidades de las aplicaciones	Detallar fecha última de actualización del procedimiento para la gestión de las vulnerabilidades de las aplicaciones.	Revisar que exista evidencia de revisiones y actualizaciones del procedimiento para gestionar las vulnerabilidades de las aplicaciones, validar que la frecuencia sea: • Anualmente. • O cuando ocurran cambios significativos.
Implementación de verificaciones de seguridad a nivel de código	Detalle de los mecanismos de análisis estático y dinámico implementados en el ciclo de desarrollo de aplicaciones para realizar comprobaciones de seguridad en el código.	Evidencia sobre el uso mecanismos de análisis estático y dinámico, para realizar comprobaciones de seguridad en el código.

4.4.1.16. 6.16. Gestión de respuesta ante incidentes

Para el control 6.16, en la Tabla 43 se presentan los atributos propuestos junto con los requerimientos específicos que deben revisarse para cada atributo identificado y la indicación de cómo debe revisarse el control.

Tabla 43: Selección de atributos y evidencia requerida control 6.16

Atributo	Evidencia requerida	¿Cómo revisar el control?
Evidencia de asignación de roles para manejo de incidentes	Detalle del personal encargado de administrar el manejo de incidentes. Incluir responsabilidades.	Revisar que exista evidencia de la definición de roles con sus respectivas responsabilidades sobre el manejo de incidentes. Por ejemplo: • Encargado de coordinar el manejo de incidentes. • Encargado de documentar la respuesta a incidentes y los esfuerzos de recuperación. Se debe validar que exista evidencia la cual demuestre por sus fechas, que estas responsabilidades y el personal asignado son revisados anualmente o cuando ocurran cambios significativos.
Existencia de un procedimiento de gestión incidentes de ciberseguridad	Procedimiento para la atención de incidentes de ciberseguridad.	Se debe revisar que exista un procedimiento de gestión de incidentes de ciberseguridad. Además, se debe revisar que su estructura contemple al menos los siguientes aspectos: • Declaración de incidentes. • Roles y responsabilidades. • Triage o determinación de severidad. • Procedimientos detallados de respuesta. • Plan de comunicación (escalamiento, información de contacto y plantillas para comunicación). • Instrucciones (playbooks) de respuesta.

Atributo	Evidencia requerida	¿Cómo revisar el control?
Evidencia de revisión del procedimiento de gestión incidentes de ciberseguridad	Detallar fecha última de actualización del procedimiento para la gestión de incidentes de ciberseguridad.	Frecuencia de revisión y actualización del procedimiento de gestión incidentes de ciberseguridad: • Anualmente. • O cuando ocurran cambios significativos. Se debe suministrar evidencia de estas revisiones y actualizaciones.
Evidencia de asignación de contactos	Procedimiento para establecer y mantener información de contacto de las partes que necesitan ser informadas de incidentes de ciberseguridad.	Se debe revisar que exista evidencia sobre información de contactos debidamente documentada de las partes que necesitan ser informadas de incidentes de ciberseguridad. Los contactos pueden incluir: • Personal interno, proveedores externos, proveedores de seguros, agencias gubernamentales u otras partes interesadas. • En el caso de un incidente relacionado con el Ambiente de Interfaz con el SINPE, deberá informarse de forma inmediata al Centro de Atención del Cliente del BCCR del incidente y documentarlo en el proceso de atención de incidentes e informarse a las partes identificadas en los incidentes de seguridad. Se debe verificar que exista evidencia sobre revisiones y/o actualizaciones a los contactos, que las fechas en la evidencia reflejen que esta revisión se realiza al menos anualmente.

4.4.2. Estructura de herramienta de auditoría

Esta herramienta tiene como objetivo validar el estado actual de las organizaciones mediante la evaluación de diversos controles, para así determinar si existen riesgos cibernéticos significativos que comprometan la seguridad de la interacción con la plataforma SINPE, exponiéndolas a posibles ataques cibernéticos.

Se realizó una revisión de la Norma Técnica de Ciberseguridad del BCCR que se puede consultar en el Apéndice L, en particular su anexo A, que especifica las secciones requeridas en el informe de auditoría necesario para la certificación para participar en SINPE. A partir de esta estructura, se define qué secciones debe incluir la herramienta para facilitar la realización de los procedimientos de auditoría. El objetivo es asegurar que toda la información relevante para la elaboración del informe esté correctamente reflejada en la herramienta.

La creación efectiva de la herramienta se abordará en el capítulo cinco, como parte de la propuesta de solución, ya que es un componente esencial para la ejecución del manual de auditoría. En esta sección, solo se establecerá la estructura que servirá de base para la posterior elaboración de la herramienta. Esta estructura no solo guiará el proceso de auditoría, sino que también garantizará la estandarización y claridad en las evaluaciones realizadas por los auditores.

La herramienta está realizada en un documento Word con tablas donde se deberá llenar la información solicitada, en la Tabla 44, se describen las secciones que se deben incluir en esta herramienta.

Tabla 44: Descripción de la herramienta.

Sección	Descripción
Información general de la auditoría	Esta sección se destina a identificar la institución auditada, se debe indicar: • El nombre de la organización evaluada. • El periodo que se está evaluando. • El área encargada, que son quienes implementan los requisitos necesarios para el cumplimiento de los controles y hacia quienes se dirigen las recomendaciones en los hallazgos de auditoría.

Sección	Descripción
Conclusión de la prueba	Se utiliza para dar estados generales de los procedimientos de auditoría en las reuniones de seguimiento, indica si el cumplimiento del control en general es satisfactorio, satisfactorio con excepciones o insatisfactorio. • Satisfactorio: todos los atributos de los subcontroles se cumplen. • Satisfactorio con excepciones: no todos los atributos de los subcontroles se cumplen. • Insatisfactorio: ningún atributo de los subcontroles se cumple.
Roles en la elaboración del procedimiento	Esta sección define quienes participaron en la elaboración del procedimiento de auditoría y que rol ejercen. Los roles son: • Elaborar • Revisar • Aprobar Se debe indicar el nombre del encargado de elaborar, revisar y aprobar el procedimiento de auditoría, así como la fecha en que se realizó.
Criterio	La sección de criterios primeramente es para indicar el control de la norma técnica del BCCR con sus respectivos subcontroles y después, las subcategorías de la NIST - Cybersecurity Framework como criterio de referencia adicional para el auditor, identificados en la sección 4.3 de este documento.
Lista de requerimientos evaluados	Apartado para documentar los requerimientos iniciales solicitados al cliente sobre los controles correspondientes al procedimiento de auditoría a realizar.
Métodos de indagación	Selección del método de indagación utilizado en el procedimiento de auditoría.
Procedimiento de la prueba	Resumen de la información solicitada al cliente y qué se espera determinar con esta.

Sección	Descripción
Resultados y conclusiones de la prueba	Apartado para documentar las observaciones del resultado de cada subcontrol. Esta sección incluye una columna para indicar: • Los atributos por evaluar. • Una columna para agregar un *check* si el atributo se cumple satisfactorio, una equis amarilla si cumple satisfactorio con excepciones o una equis roja si el cumplimiento del atributo es insatisfactorio. • También, tiene la columna para documentar los papeles de trabajo utilizados.
Resumen de cumplimiento	Resumen final de la evaluación de cada subcontrol, la norma establece que por subcontrol se debe indicar su cumplimiento: • Cumple: el control cumple su objetivo y no se determinan hallazgos u oportunidades de mejora significativa. • Cumple parcialmente: el objetivo del control si cumple, sin embargo, hay oportunidades de mejora que pueden significar algún riesgo para el ambiente de interfaz con SINPE. • No cumple: el objetivo de control no se cumple y hay hallazgos significativos que comprometen el ambiente de interfaz con SINPE. Además, por cada subcontrol, la normativa requiere que se especifique si se identificaron hallazgos.
Hallazgos identificados	Sección para redactar hallazgos por cada subcontrol que lo amerite.

4.5. Procedimiento para la elaboración del manual de auditoría

En esta sección, no se procederá con la elaboración del manual, sino que se presentarán los resultados de la revisión documental, con el fin de determinar, según los lineamientos de la ISO 10013, la estructura que deberá tener el manual de auditoría. La creación efectiva del manual se abordará en el capítulo cinco, como parte de la propuesta de solución, ya que será en ese capítulo donde se desarrollará el contenido completo y detallado del manual.

Para la elaboración del manual de auditoría se toma como referencia la ISO 10013, la cual establece que las organizaciones deben mantener la información de sus procesos o flujos de trabajo debidamente documentada, pero que a pesar de proveer la norma una estructura de documentación, esta puede variar según las necesidades de cada organización. La ISO 10013 sugiere que la información documentada contenga las siguientes secciones:

- Información sobre la organización.
- Términos y definiciones.
- Procesos de la organización (incluyendo el flujo o mapa de procesos).
- Procedimientos documentados o una referencia a ellos.

A continuación, se detalla el procedimiento para la elaboración del manual de auditorías en ciberseguridad para la certificación para participación en SINPE.

En primer lugar, en la Tabla 45 se define la estructura del manual, organizándolo en capítulos para obtener un contenido claro y una mayor comprensión por parte del lector:

Tabla 45: Elaboración del manual: estructura.

Capítulo	Descripción
Uno. Generalidades.	• Este capítulo introduce el manual proporcionando información clave sobre su alcance, propósito y el contexto de la entidad que lo desarrolla. • Se incluye una descripción del Despacho para que los lectores comprendan el contexto de la empresa auditora. • También se describen la misión y visión del Despacho, y se listan los servicios que ofrece, lo cual contextualiza el papel de la auditoría en el conjunto de actividades de la entidad. Esta sección es fundamental para establecer una base sólida antes de abordar aspectos más técnicos y específicos, permitiendo que cualquier lector, independientemente de su nivel de conocimiento, tenga una comprensión clara del contexto organizativo.

Capítulo	Descripción
Dos. Contexto auditorías de ciberseguridad en el Despacho.	Identificados los servicios brindados por el Despacho en el capítulo anterior, este capítulo profundiza en los detalles del Despacho en cuanto al servicio de las auditorías de TI, específicamente a las de ciberseguridad para la revisión de requisitos para participación en SINPE: • Auditorías en Ciberseguridad: ofrece una visión general del enfoque de auditoría de ciberseguridad en el Despacho. • Tipos de Controles: describe los controles que son objeto de revisión durante las auditorías, categorizados según lo expone la normativa aplicable. • Tipos de Conexión con el SINPE: explica las diferentes modalidades de conexión que las instituciones pueden tener con el Sistema Nacional de Pagos Electrónicos (SINPE). • Plazos de Entrega del Informe: establece las expectativas y cronogramas para la entrega de informes finales de auditoría, según lo establece la Norma Técnica del BCCR. • Estructura del Informe: presenta el formato estándar que deben seguir los informes, ayudando a los auditores a tener conocimiento sobre la redacción de este tipo de informes en específico. • Listado de Requerimientos Iniciales: incluye una serie de requerimientos iniciales específicos que deben solicitarse al inicio de cada auditoría, con el fin de garantizar que los clientes proporcionen toda la información relevante para verificar la conformidad con los controles establecidos por la normativa aplicable. • Redacción de Hallazgos y Conclusiones: proporciona los lineamientos para redactar hallazgos utilizando la Norma Técnica del BCCR como criterio, asegurando que los resultados sean comprensibles para el cliente. • Normativa Aplicable: detalla la normativa que debe cumplirse durante las auditorías, además de otras referencias, proporcionando un marco legal y normativo de referencia para los auditores.

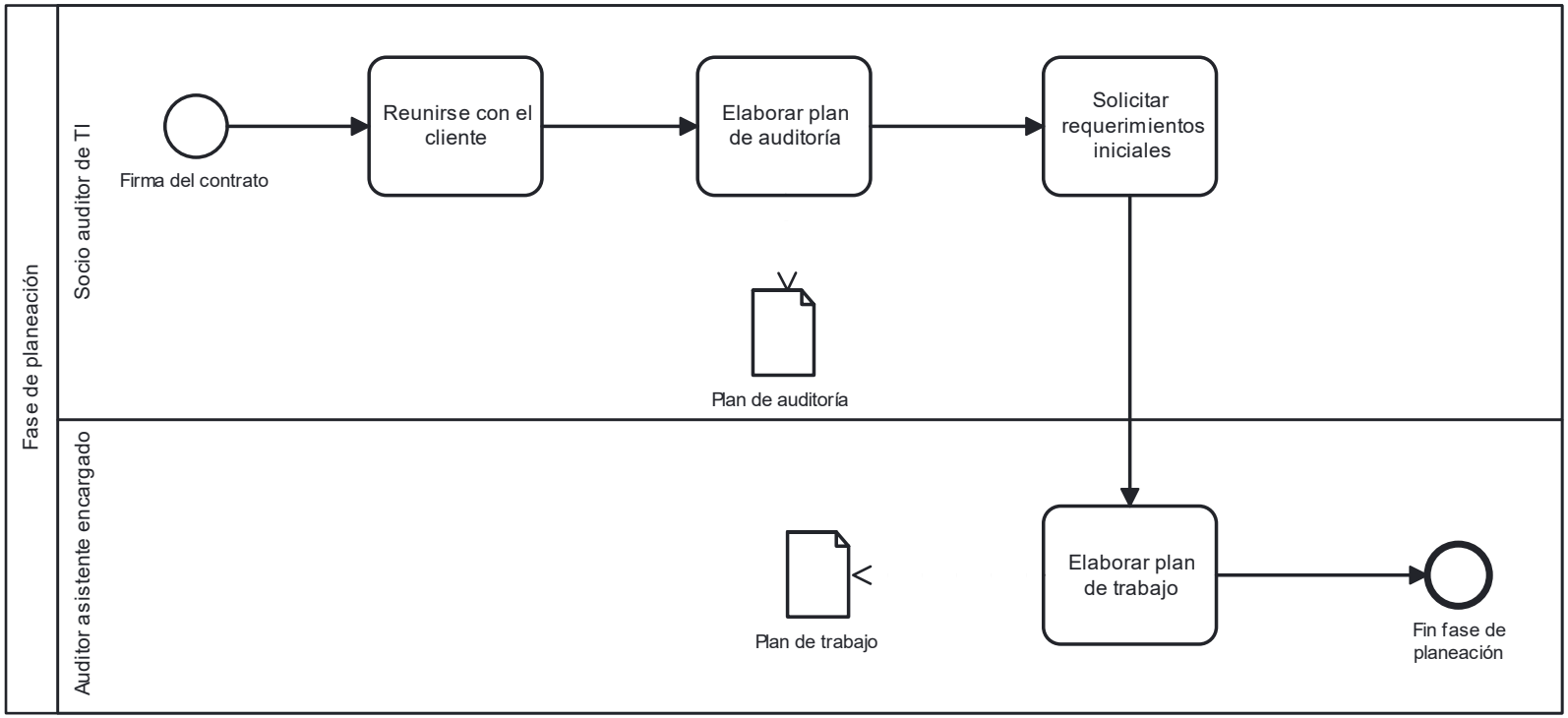
Capítulo	Descripción
Tres. Ciclo de auditoría de ciberseguridad en el Despacho.	Este capítulo cubre todo el ciclo de auditoría, desde la planificación hasta la evaluación final. • Por cada fase del ciclo de auditoría se detallan sus actividades, además, se adjunta el diagrama que permite entender el paso a paso para ejecutar cada fase. • En la fase de ejecución, se presentan los 16 controles establecidos por la Norma Técnica - Requisitos de Ciberseguridad para la participación en el SINPE. Cada control incluye: o El objetivo del control. o Definiciones de conceptos que facilitan la comprensión de lo requerido por la normativa. o Además, se incluye el procedimiento de auditoría, en este se indican los subcontroles a evaluar y se proporciona una tabla con los atributos propuestos en la fase previa del presente proyecto, así como los requerimientos específicos para cada atributo, los cuales servirán como evidencia para verificar el cumplimiento de los controles. Estos requerimientos orientan al auditor, proporcionando un mayor detalle sobre la información que debe revisar y una referencia para determinar si la evidencia presentada se ajusta a lo establecido en la normativa. Para explicar cada fase del ciclo de auditoría con sus respectivas actividades se utiliza como referencia el análisis realizado en el capítulo anterior, específicamente en la sección Análisis de situación actual.
Cuatro. Herramienta de auditoría para ejecutar el manual	Este capítulo describe la herramienta de auditoría que se utilizará para ejecutar las evaluaciones de los controles de ciberseguridad: • Propósito: define el propósito e importancia de utilizar la herramienta de auditoría propuesta. • Descripción de la Herramienta: explica las características de la herramienta, qué secciones incluye y cómo debe utilizarse. Finalmente, se incluye un enlace al repositorio que contiene la herramienta propuesta para cada control de la normativa. La decisión de proporcionar acceso a la herramienta a través de un enlace se fundamenta en que el manual se entregará a los auditores en formato digital. Esto no solo facilita el acceso inmediato a la herramienta, sino que también permite a los auditores utilizarla de manera interactiva durante el proceso de auditoría, mejorando así la eficiencia y efectividad de sus evaluaciones.

Sobre los flujos de proceso que solicita la ISO 10013, se crearon como parte de la mejora al ciclo de auditoría en el Despacho, pues este no se encuentra documentado, por este motivo se procedió a documentar por medio de diagramas dicho proceso. Los diagramas elaborados para documentar el ciclo actual de auditoría del Despacho se realizaron haciendo uso de BPMN, serán incorporados al manual de auditoría como se menciona en la Tabla 45 y pueden ser visualizados a continuación.

4.5.1. Planeación

El diagrama del proceso de planeación correspondiente al ciclo de auditoría del Despacho se visualiza en la Figura 9, sus actividades están explicadas en la Tabla 20.

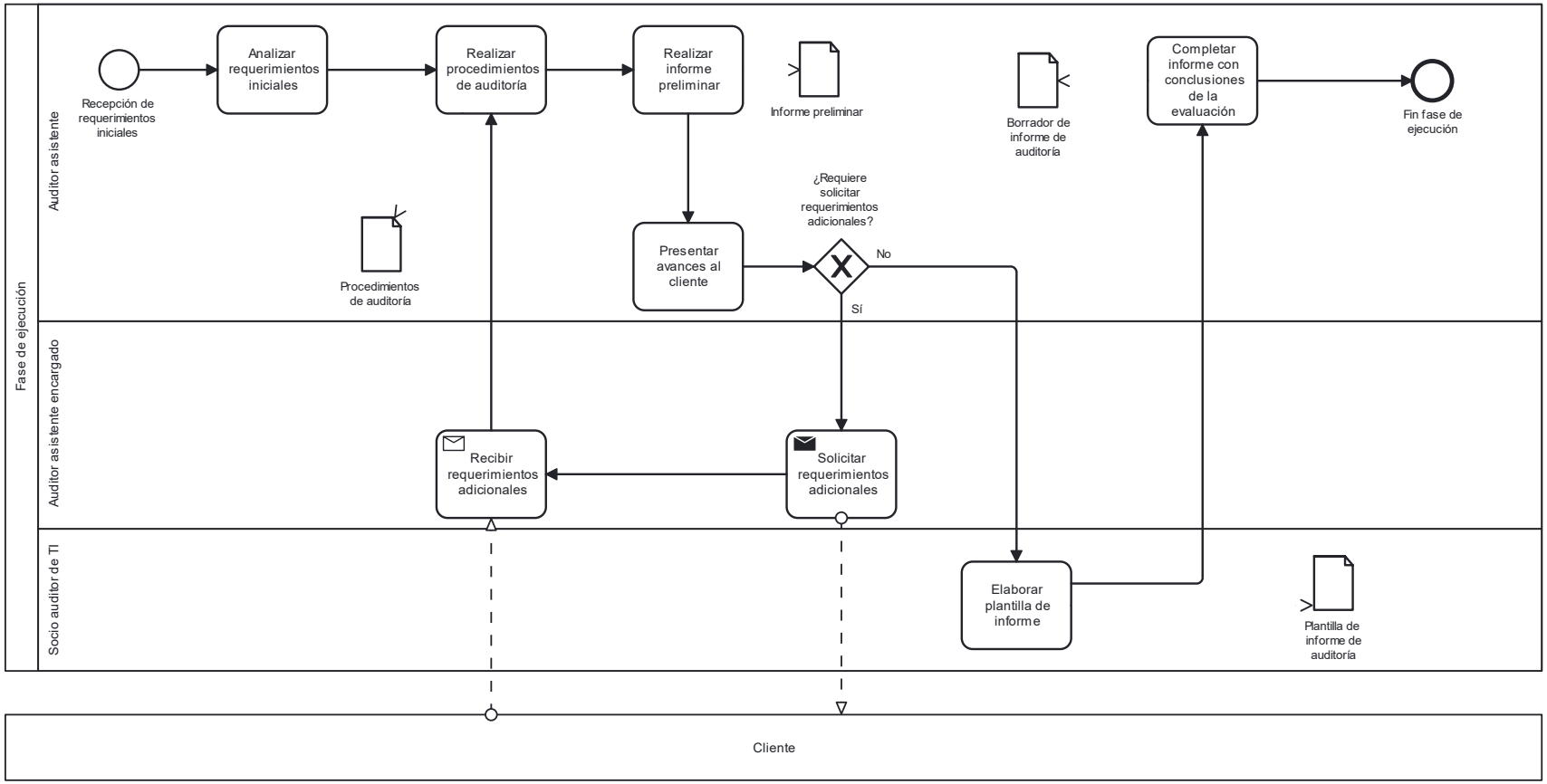
Figura 9: Proceso de la fase de Planeación



4.5.2. Ejecución

El diagrama del proceso de planeación correspondiente al ciclo de auditoría del Despacho se visualiza en la Figura 10 sus actividades están explicadas en la Tabla 21.

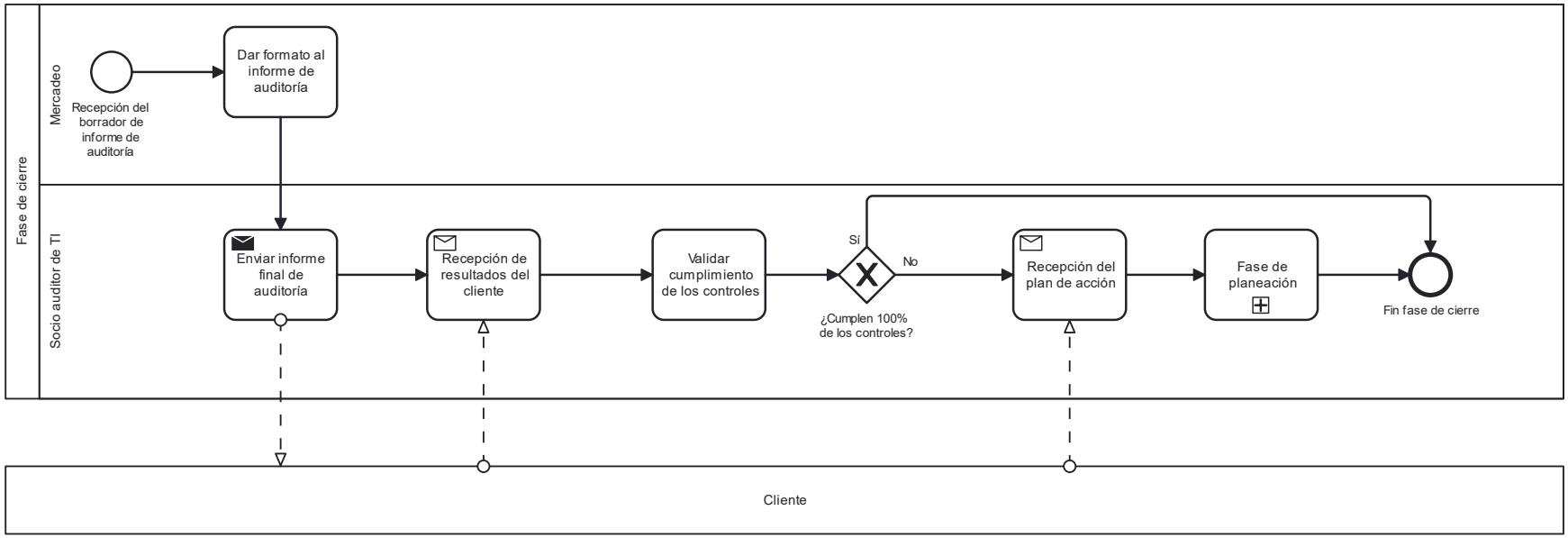
Figura 10: Proceso de la fase de ejecución



4.5.3. Cierre

El diagrama del proceso de planeación correspondiente al ciclo de auditoría del Despacho se visualiza en la Figura 11 sus actividades están explicadas en la Tabla 22.

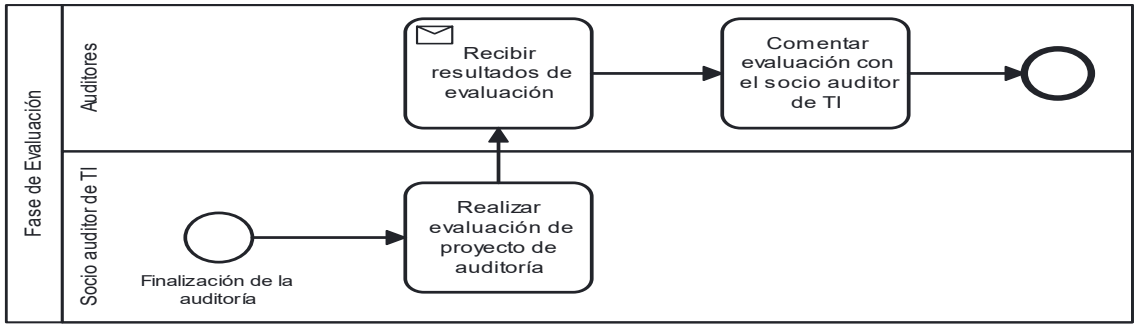
Figura 11: Proceso de la fase de cierre



4.5.4 Evaluación

El diagrama del proceso de planeación correspondiente al ciclo de auditoría del Despacho se visualiza en la Figura 12 y sus actividades están explicadas en la Tabla 23.

Figura 12: Proceso de la fase de evaluación



En relación con la estructura sugerida por la ISO 10013, se ha optado por implementarla en su totalidad, excepto la sección de términos y definiciones. Esta sección se ha adaptado para integrarse en la documentación de los procesos de la organización, específicamente en la fase de ejecución. Se ha determinado que incluir conceptos específicos de los subcontroles por evaluar aporta más valor en este contexto que solo una lista de definiciones generales del manual.

Esta modificación no solamente optimiza la utilidad del manual al contextualizar los términos en función de los procesos específicos que se evalúan, sino que también facilita la comprensión para los auditores, quienes necesitan referirse a los conceptos relevantes en el momento de aplicar los controles. De esta forma, se asegura que la información sea accesible y pertinente, mejorando así la efectividad del proceso de auditoría. Finalmente, la estructura del manual de auditoría fue aprobado para su elaboración por el socio auditor de TI según minuta en el Apéndice P.

5. Propuesta de solución

Este capítulo describe la propuesta de solución diseñada, está enfocada en mejorar el abordaje y la eficiencia del proceso de auditorías en ciberseguridad, evitar la posible invalidez legal de estas auditorías realizadas por el Despacho al asegurar que estén alineadas a la normativa aplicable y garantizar la coherencia en la evaluación de controles. Se detallarán los componentes clave de la propuesta y cómo estos resuelven las problemáticas identificadas en el análisis de la situación actual.

5.1. Herramienta de auditoría

Esta herramienta se creó para los 16 controles de la Norma Técnica: Requisitos de Ciberseguridad para participar en el SINPE, puede consultar un ejemplo específico de la herramienta en la Figura 13 y la Figura 14. Se adjunta dividida en dos figuras para mejorar la visualización del lector.

Figura 13: Ejemplo de herramienta de auditoría

	Documento de prueba
	RESULTADO DE LA PRUEBA

ORGANIZACIÓN:	
PERIODO AUDITADO:	
ÁREA:	
ESTADO DE LA PRUEBA	Elija un elemento.

FECHA	ROL	NOMBRE
	Elaborar	
	Revisar	
	Aprobar	

CRITERIO	
Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE	
Control	6.1. Inventario y control de los activos de hardware.
Subcontroles	6.1.1 Establecer y mantener un inventario de la infraestructura. 6.1.2 Establecer y mantener un diagrama de red detallado.
NIST Cibersecurity Framework	
Categoría	Gestión de activos (ID.AM).
Subcategorías	ID.AM-1 Los dispositivos y sistemas físicos dentro de la organización están inventariados.

Lista de Requerimientos evaluados	
ID	**Requerimiento**
6.1.1	Establecer y mantener un inventario de la infraestructura.
6.1.2	Establecer y mantener un diagrama de red detallado.

Métodos de indagación	
	Entrevista
	Observación
✓	Revisión documental
	Otro:

PROCEDIMIENTO DE LA PRUEBA
Se verificará que se cumpla con mantener un inventario actualizado y completo de todos los componentes de la infraestructura de TI. Además, se solicita el diagrama de red detallado con el fin de validar que el diagrama represente adecuadamente la configuración actual de la red y que cumpla con las directrices de ciberseguridad requeridas.

Figura 14: Ejemplo de herramienta de auditoría segunda parte

	Documento de prueba
	RESULTADO DE LA PRUEBA

RESULTADOS Y CONCLUSIONES DE LA PRUEBA

Atributo probado	✓ - ✗ - ✘	Resultado	Papeles de trabajo
Existencia de un inventario de la infraestructura SINPE.	✓		
Evidencia de actualización del inventario de la infraestructura SINPE.	✗		
Existencia de un diagrama de red detallado.	✘		
Conclusión de la prueba:			
Dado lo anterior, se concluye que la prueba es satisfactoria.			

RESUMEN DE CUMPLIMIENTO		
Subcontrol	**Resultado**	**¿Hallazgo?**
6.1.1 Establecer y mantener un inventario de la infraestructura.	Cumple	No
6.1.2 Establecer y mantener un diagrama de red detallado.	Cumple Parcialmente	Sí

HALLAZGOS IDENTIFICADOS	
SUBCONTROL	**HALLAZGO**

5.2. Implementación de la propuesta

Para implementar la propuesta, una vez elaborado el Manual de Auditoría con su respectiva herramienta de auditoría, se entregará de manera digital a los colaboradores del Despacho, esto para facilitar la distribución y el acceso a la información.

Adicionalmente, según la ISO 10013 en la cual se basó la elaboración del manual, cuando se genera información documentada también se debe capacitar a las personas que trabajan bajo el control de la organización en relación con la documentación, ya sea nueva o actualizada (ISO, 2021). Realizar esta capacitación no solamente asegura que el personal esté correctamente informado, sino que también permite aplicar correctamente los procesos documentados. Esto es necesario para que los auditores puedan abordar las auditorías en ciberseguridad de manera eficaz, enfrentando los desafíos y asegurando el cumplimiento de las normativas.

Aunque el manual por sí mismo proporciona las directrices necesarias para llevar a cabo las auditorías, la capacitación, según lo señalado en la norma, es una recomendación adicional que no estaba contemplada en el alcance original del proyecto, sin embargo, dado el tiempo disponible, se incluyó como un valor agregado que refuerza la implementación del manual y asegura la correcta aplicación de las auditorías en ciberseguridad.

Como se mencionó previamente, la capacitación debe involucrar a las personas responsables de manejar la información documentada. En este sentido, la propuesta del cronograma de capacitación comienza con la identificación de los roles clave relacionados con el manual, asegurando que los actores encargados de llevar a cabo las auditorías de ciberseguridad reconozcan a los responsables directos de implementar y seguir las directrices establecidas en el manual.

Se garantiza, de esta forma, que la capacitación sea relevante y adaptada a las necesidades específicas de cada función dentro del Despacho, permite que cada persona tenga la capacidad de abordar de manera eficaz las auditorías de ciberseguridad conforme a los procesos documentados.

5.2.1. Identificación de roles en relación con el manual

Antes de implementar el cronograma de capacitación, en la Tabla 46 se identifican los roles clave que interactuarán con el manual durante su aplicación. Cada uno de estos roles tiene una función específica en relación con el manual, lo que asegura que las auditorías sean abordadas de manera adecuada y conforme con los procesos documentados. A continuación, se presentan los roles y sus funciones específicas dentro del contexto del manual, lo que facilitará su comprensión y aplicación durante las auditorías.

Tabla 46: Roles involucrados con el manual propuesto

Rol	Función
Socio Auditor de TI	Es el responsable de garantizar la correcta implementación del Manual de Auditoría de ciberseguridad, asegurando que esté alineado con los requisitos normativos y las mejores prácticas. También supervisa que el manual sea actualizado y distribuido a los colaboradores del Despacho, asegurando que el equipo siga las directrices establecidas para las auditorías.
Auditor Encargado	Facilita la comprensión y aplicación del manual a los auditores asistentes y nuevos colaboradores. Además, ofrece soporte y resuelve dudas relacionadas con el contenido del manual durante el proceso de auditoría. A pesar de contar con experiencia previa en realización de auditorías de ciberseguridad, deben consultar el manual para reforzar su conocimiento y garantizar la correcta aplicación de los procedimientos.
Auditores Asistentes	Son responsables de comprender y aplicar el manual durante las auditorías. A pesar de contar con experiencia previa en la realización de auditorías en ciberseguridad, deben consultar el manual para reforzar su conocimiento y garantizar la correcta aplicación de los procedimientos.
Nuevo Colaborador	Como parte del proceso de integración, debe estudiar el manual en su totalidad siguiendo el cronograma de capacitación. Este rol se centra en familiarizarse con los procedimientos de auditoría, la documentación y la herramienta propuesta, ya que esta es su primera capacitación en auditorías de ciberseguridad realizadas por el Despacho. Debe cumplir con los plazos establecidos en el cronograma de capacitación para poder desempeñarse adecuadamente en el proceso.

Para asegurar la correcta implementación del Manual de Auditoría de Ciberseguridad, por ende, el cumplimiento con los controles establecidos en la Norma Técnica del BCCR, se propone un cronograma de capacitación dividido en dos fases, una para los auditores actuales y otra para los nuevos colaboradores. El objetivo es que cada grupo reciba una formación adecuada a su nivel de conocimiento y experiencia en auditorías de este tipo.

5.2.2. Cronograma de capacitación propuesto

Con respecto al cronograma de capacitación para auditores actuales en el Despacho, es decir, el auditor encargado, los auditores asistentes e incluso el Socio Auditor de TI, es posible observarlo en la Tabla 47.

Tabla 47: Cronograma propuesto para auditores actuales

Propuesta de cronograma	Detalles	
Roles	**Capacitador:**	Estudiante de TFG
	Participantes:	Auditor encargado. Auditores asistentes. Socio auditor de TI.
Duración por control	Una hora aproximadamente.	
Jornadas laborales	8 horas.	
Cantidad de controles a evaluar	16 controles.	
Estructura	Se realizarán cuatro días consecutivos de capacitación, con cuatro horas de formación cada día.	
Total de horas	16 horas de capacitación distribuidas en cuatro días.	
Actividades	**Primer día:** • Analizar lista de requerimientos adicionales que se deben solicitar a los clientes. • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.1. Inventario y control de los activos de hardware. o 6.2. Inventario y control de los activos de software. o 6.3. Protección de los datos. o 6.4. Configuración segura.	
	Segundo día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.5. Administración de cuentas y control de accesos. o 6.6. Gestión de vulnerabilidades. o 6.7. Gestión de bitácoras de auditoría. o 6.8. Protección del correo electrónico y la navegación por Internet.	

Propuesta de cronograma	Detalles
	Tercer día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.9. Defensa contra código malicioso. o 6.10. Recuperación de datos. o 6.11. Gestión de la infraestructura de red. o 6.12. Monitoreo y defensa de la red.
	Cuarto día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.13. Concientización en Ciberseguridad y formación de habilidades. o 6.14. Gestión de proveedores de servicios. o 6.15. Seguridad en las aplicaciones. o 6.16. Gestión de respuesta ante incidentes.

Este cronograma se justifica debido a la experiencia previa de los auditores actuales en auditorías de ciberseguridad dentro del Despacho, esto les ha permitido adquirir un mayor conocimiento tanto de la norma técnica como de la elaboración de procedimientos de auditoría. Necesitan, por lo tanto, menos horas con respecto a nuevos colaboradores para cubrir los aspectos clave.

Para el cronograma de capacitación de nuevos colaboradores en el Despacho, es decir, nuevos auditores de TI, se presenta la propuesta en la Tabla 48.

Tabla 48: Cronograma propuesto para nuevos colaboradores de TI.

Propuesta de cronograma	Detalles	
Roles	**Capacitador:**	Socio Auditor de TI. Auditor encargado.
	Participantes:	Nuevo colaborador.
Duración por control	Dos horas aproximadamente.	
Jornadas laborales	8 horas.	
Cantidad de controles a evaluar	16 controles.	

<table>
<tr><th>Propuesta de cronograma</th><th colspan="2">Detalles</th></tr>
<tr><td rowspan="3">Estructura</td><td>Cantidad de semanas de capacitación:</td><td>Dos semanas.</td></tr>
<tr><td>Días por semana:</td><td>Cuatro días.</td></tr>
<tr><td>Horas por día:</td><td>Cuatro horas.</td></tr>
<tr><td>Total de horas</td><td colspan="2">32 horas de capacitación distribuidas en ocho días.</td></tr>
<tr><td rowspan="3">Actividades</td><td colspan="2">Primer día:
Analizar la lista de requerimientos adicionales que se deben solicitar a los clientes.
Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR:
6.1. Inventario y control de los activos de hardware.
6.2. Inventario y control de los activos de software.
Analizar procedimientos de auditoría anteriores por cada control estudiado.
Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día uno.</td></tr>
<tr><td colspan="2">Segundo día:
Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR:
6.3. Protección de los datos.
6.4. Configuración segura.
Analizar procedimientos de auditoría anteriores por cada control estudiado.
Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día dos.</td></tr>
<tr><td colspan="2">Tercer día:
Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR:
6.5. Administración de cuentas y control de accesos.
6.6. Gestión de vulnerabilidades.
Analizar procedimientos de auditoría anteriores por cada control estudiado.
Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día tres.</td></tr>
</table>

Propuesta de cronograma	Detalles
	Cuarto día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.7. Gestión de bitácoras de auditoría. o 6.8. Protección del correo electrónico y la navegación por Internet. • Analizar procedimientos de auditoría anteriores por cada control estudiado. • Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día cuatro.
	Quinto día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.9. Defensa contra código malicioso. o 6.10. Recuperación de datos. • Analizar procedimientos de auditoría anteriores por cada control estudiado. • Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día cinco.
	Sexto día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.11. Gestión de la infraestructura de red. o 6.12. Monitoreo y defensa de la red. • Analizar procedimientos de auditoría anteriores por cada control estudiado. • Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día seis.
	Sétimo día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.13. Concientización en Ciberseguridad y formación de habilidades. o 6.14. Gestión de proveedores de servicios.

Propuesta de cronograma	Detalles
	Octavo día: • Identificar las actividades asociadas a cada subcontrol para asegurar la recopilación de evidencias necesarias que validen el cumplimiento de los controles. Lo anterior, para los siguientes controles de la Norma Técnica del BCCR: o 6.15. Seguridad en las aplicaciones. o 6.16. Gestión de respuesta ante incidentes. • Analizar procedimientos de auditoría anteriores por cada control estudiado. • Conocer la herramienta de auditoría propuesta, específicamente la correspondiente a los controles estudiados en el día ocho.

Al finalizar el último día de capacitación de nuevos colaboradores, se recomienda que, en el caso que el Despacho esté ejecutando auditorías de los requisitos de ciberseguridad para la participación en SINPE, el nuevo colaborador sea asignado como auditor asistente en una de estas auditorías para aplicar su conocimiento adquirido.

Posterior a las capacitaciones, además, se recomienda implementar indicadores de desempeño para medir la eficiencia y efectividad del manual y la herramienta de auditoría. Estos indicadores permitirán identificar mejoras en el proceso de auditorías en ciberseguridad para la evaluación de controles que deben cumplir los afiliados al SINPE y áreas que podrían optimizarse aún más.

5.2.3. Métricas de desempeño propuestas

Como valor agregado a la realización de este proyecto también se proponen dos métricas de desempeño, estas métricas permitirán evaluar cómo el manual impacta en la consistencia, precisión y eficiencia de las auditorías, garantizando que los procedimientos establecidos se estén aplicando correctamente.

Definir estas métricas es importante porque proporcionará una herramienta objetiva para identificar posibles mejoras, asegurando que el manual cumpla con su propósito de estandarizar y optimizar el proceso de auditoría, contribuyendo a la reducción de riesgos cibernéticos en las organizaciones.

5.2.3.1. Tiempo Promedio de Ejecución de Auditorías

El primer indicador de desempeño propuesto corresponde al tiempo promedio de ejecución de auditorías, este indicador medirá el tiempo promedio que se tarda en realizar las auditorías, desde la planificación hasta la entrega del informe final. Además, este indicador permitirá identificar posibles cuellos de botella o áreas en las que se puedan optimizar los recursos y las técnicas de auditoría. Los detalles y la fórmula para su cálculo se encuentran en la Tabla 49, lo que proporcionará una base cuantificable para medir el impacto de las mejoras implementadas en el manual de auditoría.

Tabla 49: Métrica de desempeño propuesta #1.

Descripción del indicador	Este indicador mide el tiempo promedio dedicado por los auditores para completar una auditoría. Con esta métrica, es posible identificar si la estandarización de procesos ha contribuido a reducir los tiempos de auditoría.
Fórmula	• Duración de cada auditoría **(DA)**: Mide el tiempo que tardó en completarse cada auditoría individual, es decir, desde su inicio hasta su finalización. • Cantidad de auditorías completadas **(TAC)**: Es el número total de auditorías que fueron terminadas durante el periodo evaluado. $$Tiempo\ promedio\ de\ ejecución = \frac{\sum DA}{TAC}$$
Explicación del indicador	Se realiza una suma del tiempo que tomó completar cada auditoría individual y se divide entre la cantidad total de auditorías que se han completado en el periodo evaluado. Esto da un promedio de tiempo de ejecución por auditoría.
Interpretación del indicador	Si el tiempo promedio calculado disminuye después de la implementación de las capacitaciones, el manual y la herramienta de auditoría son un indicador de que los cambios han mejorado la eficiencia.

5.2.3.2. Porcentaje de Auditorías Realizadas en Paralelo

El segundo indicador de desempeño propuesto corresponde al porcentaje de auditorías realizadas en paralelo, los detalles y la fórmula para su cálculo se encuentran en la Tabla 50.

Tabla 50:Métrica de desempeño propuesta #2.

Descripción del indicador	Este indicador mide la proporción de auditorías que el equipo logra realizar de manera simultánea, lo que refleja la capacidad de gestionar auditorías en paralelo, por tanto, una mayor eficiencia del equipo.
Fórmula	• Cantidad de auditorías realizadas en paralelo **(AP)**: Contabiliza el número de auditorías que se completaron en el periodo evaluado y que se realizaron simultáneamente, es decir, en paralelo. • Total de auditorías realizadas **(TAR)**: Es el total de auditorías completadas en el mismo periodo de tiempo (por ejemplo, todas las auditorías realizadas en el mes). • Multiplicación por 100: Multiplicar por 100 convierte el resultado en un porcentaje. $$Porcentaje\ de\ Auditorías\ Paralelas = \left(\frac{AP}{TAR}\right) \cdot 100$$

Explicación del indicador	Se divide la cantidad de auditorías realizadas en paralelo entre el total de auditorías completadas para obtener la proporción de auditorías que fueron ejecutadas simultáneamente en relación con todas las auditorías realizadas. Se multiplica por 100 para expresar el resultado en porcentaje. Esto da un porcentaje de auditoría que se ejecutan paralelamente.
Interpretación del indicador	Un valor alto indica que el equipo de auditoría puede gestionar auditorías simultáneamente de manera efectiva, esto indicaría que, con el apoyo del manual y la herramienta de auditoría, el equipo está logrando gestionar auditorías simultáneas, lo cual optimiza el uso de recursos y permite atender a más clientes o proyectos en el mismo tiempo.

5.3. Análisis de Viabilidad de la Propuesta

Realizar un análisis de viabilidad es esencial para asegurar que la implementación de la propuesta en la organización sea tanto factible como beneficiosa. Este análisis busca evaluar diferentes aspectos que permitan determinar si la propuesta aporta un valor adecuado y si los recursos disponibles son suficientes para garantizar su éxito a largo plazo.

En este caso, se empleará el análisis costo-beneficio, enfocado en dos actividades clave: el cálculo de costos y la evaluación de los beneficios no financieros. De este modo, se examinarán diversos factores cruciales para justificar la adopción de la solución propuesta.

5.3.1. Cálculo del costo

A continuación, se presenta el cálculo de los costos totales para el análisis costo-beneficio del proyecto, estos corresponden al costo de implementación. Los costos han sido estimados en función de los siguientes supuestos:

- Se utiliza el salario mínimo correspondiente al título de licenciado de la lista de salarios mínimos para el 2024 del Ministerio de Trabajo equivalente a ₡765 986 mensuales y ₡4 787,41 por hora (Ministerio de Trabajo y Seguridad Social de Costa Rica, 2024), esto para los salarios de los auditores y del socio auditor de TI.
- El salario del estudiante lo determinó la empresa, corresponde a ₡3 750 la hora.
- La distribución de tiempos para la capacitación se basa en el cronograma de capacitación planteado para los auditores actuales, los cuales son cuatro, considerando que no existen nuevos colaboradores en este momento en el Despacho, requiere un total de 16 horas. Los asistentes requeridos e indispensables es el estudiante como capacitador y los auditores.
- El socio de TI dedica una hora a la semana para revisión y apoyo al estudiante.

Una vez establecidos los supuestos, se detallan los cálculos correspondientes a cada uno de los rubros de costos que se deben considerar.

- El salario del socio auditor de TI: se estima un total de 16 horas distribuidas en 16 semanas de participación, lo cual tiene un costo de ₡76 598,56.

- El costo de la capacitación: la capacitación tiene una duración de 16 horas, por tanto, el costo por auditor es de ₡76 598,56, esto genera un total de ₡306 394,24.
- Costo del desarrollo del Trabajo Final de Graduación (TFG)**:** la empresa cubrirá 20 horas a la semana del estudiante durante un total de 16 semanas. El costo se calcula incluyendo las garantías sociales: 26.67% de aporte patronal y aguinaldo, resultando en un total de ₡405 010.

A continuación, la Tabla 51 desglosa los costos de desarrollo de la propuesta.

Tabla 51: Costos de elaboración e implementación de la propuesta.

Rubro		Costo
Desarrollo del TFG	Salario del estudiante total	₡300 000
	Aguinaldo	₡25 000
	Aporte patronal total	₡80 010
Salario del Socio Auditor de TI		₡76 598,56
Capacitación		₡306 394,24
Total		**₡788 002,8**

De acuerdo con la información de la Tabla 51, el costo total de implementación asciende a ₡788 002,8.

5.3.2. Beneficios no financieros

Los beneficios no financieros asociados a la implementación de la propuesta son fundamentales para demostrar el impacto positivo que puede generar más allá de los resultados económicos. Aunque no se reflejan directamente en términos monetarios, estos beneficios ofrecen mejoras significativas en la operación, seguridad y reputación de la organización.

En esta sección, se detallan los beneficios no financieros clave, abordando cómo contribuyen al fortalecimiento de los procesos de auditoría, la reducción de riesgos y la optimización del conocimiento organizacional, asegurando la viabilidad y sostenibilidad a largo plazo de la propuesta. Estos beneficios no financieros son los siguientes:

- **Mejora en la conformidad regulatoria:** Basado en la Norma Técnica del BCCR y el marco NIST Cybersecurity Framework para la definición y evaluación de controles, el manual permitirá a los auditores asegurar el cumplimiento adecuado de las normativas regulatorias del BCCR. Esto garantiza que las evaluaciones se realicen conforme con los requisitos establecidos.
- **Reducción de riesgos:** Al garantizar el cumplimiento regulatorio en las evaluaciones, se minimiza el riesgo de presentar informes que el BCCR pueda rechazar debido a una incorrecta evaluación de los controles. De este modo, el Despacho evita potenciales problemas legales o demandas ante las autoridades competentes.

- **Estandarización de procesos de auditoría:** El manual promoverá auditorías más consistentes y estructuradas, eliminando la variabilidad entre auditores y adoptando un enfoque sistemático.
  Esto no solamente reducirá los tiempos y costos operativos de las auditorías, sino que permitirá cumplir con los plazos de entrega del informe al cliente, mientras que internamente los auditores podrán finalizar sus evaluaciones en menor tiempo. Además, les permitirá asumir nuevos proyectos de manera paralela, lo que incrementará el número de clientes y, en consecuencia, los ingresos del Despacho.
- **Incremento en la confianza de las partes interesadas:** Al contar con una metodología de auditoría en ciberseguridad bien definida y con herramientas de apoyo, se incrementará la satisfacción de los clientes, quienes confiarán en la capacidad del Despacho para realizar las evaluaciones necesarias para su certificación en SINPE. Esto atraerá a más clientes que busquen servicios confiables y efectivos.
- **Facilita la capacitación del personal:** El manual servirá como una herramienta clave para la formación de nuevos auditores y personal de TI, mejorando sus competencias en ciberseguridad y auditoría sin la necesidad de recurrir a formaciones externas, lo que elimina la posibilidad de mayores costos para el Despacho a largo plazo.
- **Mejora en la gestión del conocimiento:** Al documentar el ciclo de auditoría en ciberseguridad para la certificación en SINPE y los procedimientos de auditoría correspondientes, el manual funcionará como un repositorio de conocimiento. Esto facilitará la transferencia de información dentro del equipo y garantizará la continuidad del trabajo, incluso en situaciones de rotación de personal.

El análisis de viabilidad, tanto en términos de costos como de beneficios no financieros, demuestra que la propuesta es económicamente factible y aporta un valor significativo a largo plazo. Los beneficios no financieros, como la mejora en la conformidad regulatoria, la reducción de riesgos y la estandarización de los procesos de auditoría, aseguran que el Despacho pueda seguir operando de manera eficiente y conforme a las normativas vigentes.

La implementación de la propuesta de solución, finalmente, ha logrado abordar de manera efectiva la problemática central planteada en este trabajo, que es el inadecuado abordaje de las auditorías de ciberseguridad por parte del equipo de TI, derivado de la reciente publicación de las normas del Banco Central de Costa Rica (BCCR). El manual de auditoría quedó elaborado con un total de 45 páginas, incluyó las secciones planteadas en la Tabla 45 y los diagramas de procesos elaborados, por la extensión del manual se adjunta una vista general de este en el Apéndice V, además, la versión final de este y de la herramienta de auditoría fueron aprobados por el socio auditor de TI del Despacho según minuta en el Apéndice S.

A través del desarrollo del Manual de Auditoría y su herramienta asociada, se ha alineado el proceso de auditoría con la Norma Técnica del BCCR y el NIST Cybersecurity Framework, proporcionando un enfoque estructurado y normativo para evaluar los controles de ciberseguridad, este alineamiento se verificó y se aprobó por el socio auditor de TI a través de reuniones. Esto asegura que el equipo cuente con los recursos necesarios para ejecutar las auditorías de ciberseguridad requeridas para la participación en el SINPE, garantizando el cumplimiento con las normativas regulatorias.

6. Conclusiones

En este capítulo se presenta un resumen de los descubrimientos relevantes a partir del desarrollo del proyecto, los cuales están agrupados por objetivos específicos.

6.1. Objetivo específico uno

Determinar los componentes del marco de trabajo NIST-Cybersecurity Framework para el diseño de herramientas requeridas para el área de auditoría de TI.

De acuerdo con los resultados obtenidos de la revisión documental del Marco de Referencia se concluye:

- Se identificaron 45 subcategorías del NIST-Cybersecurity Framework que son aplicables directamente a los controles de la Norma Técnica del BCCR tal y como se detalla en la sección 4.1. Esto permitió diseñar una herramienta de auditoría que cubra los requerimientos de ambos marcos de manera que las evaluaciones estén apegadas a la normativa vigente.
- Para los 16 controles que corresponden al 100 % de los controles de la Norma Técnica del BCCR, se identificaron componentes relacionados del NIST-Cybersecurity Framework, lo que valida la compatibilidad entre ambos marcos para su uso conjunto como criterios en la ejecución de las pruebas de auditoría, como se puede comprobar en la sección 4.1.

6.2. Objetivo específico dos

Analizar la situación actual del Departamento de Auditoría de TI del Despacho, mediante un análisis de brecha para la recomendación de mejoras a la evaluación de auditorías en ciberseguridad para la certificación de participación en SINPE.

Producto de la aplicación de los instrumentos definidos se concluye lo siguiente para el objetivo específico dos:

- El análisis de brecha realizado en la fase de evaluación reveló que el Despacho se encuentra desalineado en seis directrices con respecto a la ISO 19011 específicamente en las actividades correspondientes a la fase de ejecución como puede validarse en la sección 4.2. Esto evidencia una deficiencia que impacta la consistencia en la evaluación de los controles porque esta se realiza en la fase de ejecución.
- Los hallazgos de las entrevistas y el grupo focal con los auditores de TI confirmaron que los cuatro auditores de TI del Despacho, es decir, el 100 % de los auditores dependen de consultas a fuentes de información externas como Google ante falta de documentación que los guíe en la evaluación de los controles de la Norma Técnica del BCCR, lo que genera disparidades en la aplicación de los controles y afecta la calidad de las auditorías realizadas como se determinó en la sección 4.1.
- Los cuatro auditores de TI además del Socio Auditor de TI, consideran que el Despacho requiere un Manual de Auditorías en ciberseguridad para estandarizar los procedimientos de auditoría y evitar la pérdida de tiempo en consultar fuentes de información externas como se determinó en la sección 4.1.4 y 0.
- No existe una capacitación estructurada en ciberseguridad para los auditores según respuestas del grupo focal, especialmente para nuevos colaboradores que les guíe sobre los

aspectos a evaluar, los requerimientos por solicitar y las evidencias requeridas como se puede comprobar en la sección 0.

6.3. Objetivo específico tres

Elaborar un Manual de Auditoría tomando como referencia el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica del BCCR para la aplicación de una auditoría basada en ciberseguridad favoreciendo el cumplimiento con los entes regulatorios costarricenses.

- El manual desarrollado documenta las fases del ciclo completo de auditoría para ciberseguridad en el Despacho (planeación, ejecución, cierre y seguimiento), alineadas con la ISO 19011 y adaptadas a los requerimientos del BCCR como se detalla en la sección 0. Este enfoque estandariza el proceso de auditoría en ciberseguridad y asegura un cumplimiento más riguroso de las normativas.
- Según los resultados del análisis no financiero, la implementación del manual elimina la necesidad de que los auditores consulten fuentes externas para interpretar los controles. Esto implica una reducción en el tiempo de ejecución de las auditorías, particularmente en la fase de evaluación de los controles, permitiendo atender auditorías en paralelo aumentando así la cantidad de clientes como se puede comprobar en la sección 5.3.2.
- Se logró desarrollar una herramienta de auditoría en Word, alineada con los requisitos estipulados en el Anexo de la Norma Técnica del BCCR para la elaboración de informes de auditoría que se envían al BCCR como se demuestra en la sección 5.1. La herramienta permite a los auditores ingresar la información y completar a partir de esta el informe final, lo que estandariza las evaluaciones y simplifica la elaboración de conclusiones sobre el cumplimiento o no de los controles.
- Como valor agregado al proyecto, se desarrollaron dos propuestas de capacitación para los auditores de TI: una enfocada en el equipo actual y otra diseñada específicamente para los nuevos integrantes. Cada propuesta se fundamenta en la estandarización del proceso de auditoría en ciberseguridad, el uso del manual y de la herramienta de auditoría tal y como se detalla en la sección 5.2.2.
- Se logró incorporar indicadores de desempeño como un valor agregado al proyecto. Estos indicadores permiten monitorear la eficacia de los auditores en la realización de auditorías de ciberseguridad, en relación con el uso del manual de auditoría desarrollado en este proyecto auditoría tal y como se detalla en la sección 5.2.3.

7. Recomendaciones

1. Se recomienda que todos los auditores adopten la herramienta de auditoría desarrollada, basada en el NIST - Cybersecurity Framework y la Norma Técnica del BCCR, para garantizar que las evaluaciones se realicen conforme con los criterios de auditoría definidos, estandarizando los procedimientos y reduciendo la variabilidad en la aplicación de los controles.
2. Evaluar el impacto del programa de capacitación propuesto, en la reducción de la dependencia de fuentes externas por parte de los auditores para garantizar una aplicación más consistente de los controles en las auditorías.
3. Revisar y actualizar anualmente el Manual de Auditoría para incorporar nuevos ajustes que surjan a la Norma Técnica: Requisitos de Ciberseguridad para participar en el SINPE, garantizando así que se mantenga vigente y aplicable a las normativas del BCCR.
4. Implementar los dos indicadores de desempeño propuestos para monitorear la eficacia del uso del manual en auditorías de ciberseguridad. Además, se recomienda añadir otros indicadores, de ser necesario, que complementen el análisis de la eficiencia y la calidad en las auditorías, adaptándolos a las necesidades específicas del Despacho.
5. Promover que los auditores consulten el manual y la herramienta de auditoría desarrollada antes de recurrir a fuentes externas como Google, para evitar disparidades en la evaluación de los controles y asegurar una aplicación estandarizada de los mismos.
6. Se recomienda crear un repositorio centralizado de información donde se almacenen todos los recursos relevantes del Área de Auditoría de TI, incluye los 16 archivos de la herramienta de auditoría, el manual elaborado y cualquier otra documentación relacionada con las auditorías de TI del Despacho. Este repositorio debe ser accesible para todo el equipo de auditoría y actualizarse periódicamente para asegurar que la información esté siempre disponible.
7. Se recomienda que el Gerente de TI organice reuniones mensuales con el equipo de auditoría de TI para discutir las áreas de mejora y las dificultades encontradas durante la ejecución de las auditorías.
8. Se recomienda que, cuando las fuentes de la Norma Técnica del BCCR y el NIST-Cybersecurity Framework no resuelvan las dudas de los auditores, se consulte el apartado de referencias complementarias del manual, evitando el uso de buscadores o fuentes externas para prevenir información errónea y pérdida de tiempo en la ejecución de auditorías.

8. Referencias

Álvarez, A. J. (2017). *Propuesta de definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las organizaciones auditadas, Caso JM Auditores.*

Awadh, M. A. (2022). *Utilizing Multi-Criteria decision making to evaluate the quality ofhealthcare services*. Sustainability. https://doi.org/10.3390/su141912745

Axelos. (2019). *ITIL Foundation.* The Stationery Office.

Azofeifa, H. (2019). *Propuesta de Metodología para Determinar el Nivel de Madurez de la Atención de Riesgos de Ciberseguridad según el Marco de Trabajo NIST.*

Banco Central de Costa Rica. (2023). *Norma Técnica - Requisitos de Ciberseguridad para participar en el SINPE.* https://www.bccr.fi.cr/sistema-de-pagos/DocNormasSinpe/Norma_Tecnica-Requisitos_Ciberseguridad_para_participar_SINPE.pdf

Center for Internet Security . (2024). *CIS Critical Security Controls.* https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf

Cerdas., C. A. (2018). *Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho.*

Despacho. (2024). *Firma de Contadores Públicos en Costa Rica | Despacho*.

Galarza, C. (2020). Los alcances de una investigación. *CienciAmérica*, 1-5.

Gantz, S. D. (2014). *The Basics of IT Audit Purposes, Processes, and Practical Information.* Elsevier.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.*

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Security Management.*

International Organization for Standardization. (2015). *Quality management systems — Fundamentals and vocabulary* (ISO 9000). ISO.

International Organization for Standardization. (2018). *Guidelines for auditing management systems* (ISO 19011). INTECO.

IAASB. (2021). *NIA 500*. Obtenido de Ministerio de Ciencia, Innovación Tecnología y Telecomunicaciones: https://www.aplicaciones-mcit.gov.co/adjuntos/niif/20%20-%20NIA%20500.pdf

ISACA. (2015). *Glossary of Terms.*

ISACA. (2016). *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*. ISACA

Lucidchart. (s.f.). *Qué es la notación de modelado de procesos de negocio.* Lucidchart.

Martínez, H. (2012). *Metodología de la investigación.* Cengage.

Ministerio de Trabajo y Seguridad Social. (2024). *Lista de Salarios Mínimos por ocupación, año 2024*. Obtenido de https://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/lista_salarios_2024.pdf

MINTIC. (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Recuperado de https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes#:~:text=Un%20incidente%20de%20seguridad%20de,de%20la%20Informaci%C3%B3n%20de%20la

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations.*

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Organización Internacional de Normalización y Foro Internacional de Acreditación. (2016a). *ISO 9001 Auditing Practices Group Guidance on: Nonconformity – Documenting*.

Organización Internacional de Normalización y Foro Internacional de Acreditación. (2016b). *Grupo de Prácticas de Auditoría ISO 9001*.

Organization for Standardization. (2021). *Quality management systems — Guidance for documented information* (ISO 10013). ISO.

Osores, M. (2014). *Mejores prácticas de TI: Más valor para el negocio.* Recuperado de https://searchdatacenter.techtarget.com/es/cronica/Mejores-practicas-de-TI-Masvalor-para-el-negocio

Real Academia Española. (s.f.). Herramienta. En *Diccionario de la lengua española*. Recuperado en 20 de octubre de 2024, de https://dle.rae.es/herramienta?m=form

Robles, H. J. (2021). *Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework.*

SYDLE. (2024). *Procesos empresariales: ¿Qué son y cuáles son los más utilizados?* SYDLE. Recuperado de https://www.sydle.com/es/blog/procesos-empresariales-62686abc355bcb08dcbe06ec

Ulate, I., & Vargas, E. (2016). *Metodología para elaborar una tesis.* EUNED.

9. Apéndices

Esta sección reúne todos los elementos que facilitan la comprensión de este trabajo, los cuales fueron elaborados como parte del desarrollo del proyecto.

Apéndice A. Formato minuta grupo focal

Minuta del grupo focal		
Número de sesión:		
Tema del grupo focal:		
Fecha:	**Hora:**	**Lugar:**
Moderador:		
Participantes:		**Rol:**
Preguntas		
Pregunta 1		
Pregunta 2		
Pregunta n		
Firmas participantes		

Apéndice B. Formato grupo focal situación actual de auditoría en ciberseguridad

Minuta del grupo focal		
Número de sesión: 1		
Tema del grupo focal: Situación actual – Realización de auditorías en ciberseguridad		
Fecha:	**Hora:**	**Lugar:**
Moderador:		
Participantes:		**Rol:**
Preguntas		
1. ¿Cómo describirían la experiencia con respecto a la realización de auditorías en ciberseguridad para participación en SINPE en comparación con otros tipos de auditorías?		
2. ¿Qué problemas encuentran en seguir el procedimiento actual para realizar auditorías en ciberseguridad para participación en el SINPE?		
3. ¿Cómo describiría la consistencia de los procedimientos de auditoría realizados por diferentes auditores al evaluar un mismo control?		
4. ¿Qué hacen cuando tienen dudas sobre qué deben evaluar o cómo deben evaluar un control, a qué o quién recurren?		
5. ¿Han existido situaciones donde han sentido que requirieron más capacitación o documentación que les haya dificultado realizar las auditorías en ciberseguridad?		
6. ¿Qué cambios o mejoras sugieren que logren optimizar el procedimiento para realizar auditorías en ciberseguridad?		
Firmas participantes		

Apéndice C. Minuta grupo focal situación actual de auditoría en ciberseguridad

Minuta del grupo focal				
Número de sesión: 1				
Tema del grupo focal: Situación actual – Realización de auditorías en ciberseguridad				
Fecha: 11-09-2024	**Hora:** 4:00 p.m.		**Lugar:** Virtual	
Moderador: Jennifer Paola Lobo Quirós				
Participantes:	Elena Morera Monge	**Rol:**	Auditora asistente - encargada	
	Fernando Corrales Quirós		Auditor asistente - encargado	
	Hellen Cordero Robles		Auditora asistente	
	Juan Marín Aguilar		Auditor asistente	
Preguntas				
1. ¿Cómo describirían la experiencia con respecto a la realización de auditorías en ciberseguridad para participación en SINPE en comparación con otros tipos de auditorías?				
2. ¿Qué problemas encuentran en seguir el procedimiento actual para realizar auditorías en ciberseguridad para participación en el SINPE?				
3. ¿Cómo describiría la consistencia de los procedimientos de auditoría realizados por diferentes auditores al evaluar un mismo control?				
4. ¿Qué hacen cuando tienen dudas sobre qué deben evaluar o cómo deben evaluar un control, a qué o quién recurren?				
5. ¿Han existido situaciones donde han sentido que requirieron más capacitación o documentación que les haya dificultado realizar las auditorías en ciberseguridad?				
6. ¿Qué cambios o mejoras sugieren que logren optimizar el procedimiento para realizar auditorías en ciberseguridad?				
Firmas participantes	Elena Morera Monge	ELENA GABRIELA MORERA MONGE (FIRMA)	Firmado digitalmente por ELENA GABRIELA MORERA MONGE (FIRMA) Fecha: 2024.11.01 17:04:54 -06'00'	
	Fernando Corrales Quirós	FERNANDO STEVEN CORRALES QUIROS (FIRMA)	Firmado digitalmente por FERNANDO STEVEN CORRALES QUIROS (FIRMA) Fecha: 2024.10.30 16:17:29 -06'00'	
	Hellen Cordero Robles	HELLEN YAZMIN CORDERO ROBLES (FIRMA)	Firmado digitalmente por HELLEN YAZMIN CORDERO ROBLES (FIRMA) Fecha: 2024.10.31 09:19:57 -06'00'	
	Juan Marín Aguilar	JUAN PABLO MARIN AGUILAR (FIRMA)	Firmado digitalmente por JUAN PABLO MARIN AGUILAR (FIRMA) Fecha: 2024.10.30 16:24:29 -06'00'	

Apéndice D. Formato guía de entrevista

Tema de la entrevista:		
Número de entrevista:		
Fecha:	**Hora:**	**Lugar:**
Entrevistador:		
Entrevistado:	**Rol:**	
Introducción:		
Preguntas		
Pregunta 1		
Respuesta:		
Pregunta 2		
Respuesta:		
Pregunta n		
Respuesta:		

Apéndice E. Formato entrevista proceso actual de auditoría al gerente de auditoría de TI

Tema de la entrevista: Situación actual - ciclo de auditoría en ciberseguridad		
Número de entrevista: 1		
Fecha:	**Hora:**	**Lugar:**
Entrevistador:		
Entrevistado:	**Rol:**	
Introducción:		
Preguntas		
1. ¿Puede describir paso a paso cómo ejecutan el proceso de auditorías en ciberseguridad?		
Respuesta:		
2. ¿Quiénes son los responsables de las diferentes actividades dentro de este proceso de auditoría en ciberseguridad?		
Respuesta:		
3. ¿Cuáles son los insumos clave que necesita para comenzar el proceso de auditoría en ciberseguridad y qué resultados produce?		
Respuesta:		
4. ¿Qué herramientas o sistemas utiliza para completar el proceso de auditoría en ciberseguridad?		
Respuesta:		
5. ¿Cuáles son las principales dificultades que encuentra al llevar a cabo este proceso?		
Respuesta:		
Aunque se cumple con las fechas pactadas de entrega de avances o informes finales al cliente: 6. ¿Considera que hay procesos internos que podrían ser más eficientes? ¿Cuáles?		
Respuesta:		
7. ¿Cuáles son las actividades que consumen más tiempo o recursos?		
Respuesta:		
8. ¿Existen picos de trabajo que podrían evitarse con una mejor planificación o recursos?		

Tema de la entrevista: Situación actual - ciclo de auditoría en ciberseguridad	
Respuesta:	
9. ¿Hay informes que deban rehacerse más de una vez antes de ser aprobados?	
Respuesta:	
10. ¿Considera que la falta de estandarización en los procedimientos afecta la consistencia o calidad de las auditorías? ¿Por qué?	
Respuesta:	

Apéndice F. Entrevista proceso actual de auditoría al gerente de auditoría de TI

Tema de la entrevista: Situación actual - ciclo de auditoría en ciberseguridad		
Número de entrevista: 1		
Fecha: 12-09-2024	**Hora:** 2:30 p.m.	**Lugar:** Virtual
Entrevistador: Jennifer Paola Lobo Quirós		
Entrevistado: Fabián Cordero Navarro	**Rol:** Socio auditor de TI	
Introducción: Esta entrevista tiene como objetivo recopilar información sobre el ciclo de auditoría en ciberseguridad, sus distintas actividades y los principales desafíos, desde la perspectiva del socio auditor de TI, quien es responsable de velar por el cumplimiento del plan de auditoría.		
Preguntas		
1. ¿Puede describir paso a paso cómo ejecutan el proceso de auditorías en ciberseguridad?		
Respuesta:	La auditoría se realiza para quienes necesitan la participación en el SINPE y se dividen en 2 categorías, estas son la categoría uno y la categoría dos. La categoría uno son básicamente aquellas entidades que utilizan la plataforma provista por el Banco Central para hacer las transacciones del SINPE, es decir, que se conectan directamente a la plataforma y deben cumplir con todos los requisitos o todas las actividades que mencionan la normativa. Por el lado de la entidad 2, son los que tienen o crearon su propia plataforma para poder hacer los pagos con SINPE y únicamente utilizan web service para conectarse con la interfaz o con la plataforma del Banco Central. A partir de eso, las entidades crean sus necesidades de auditoría, elaboran un cartel inicial que llega a los diferentes oferentes, en este caso llegan al Despacho y nosotros lo analizamos, creamos la oferta, se le envía al cliente por parte de mercadeo, el cliente la analiza y posteriormente, indica si está de acuerdo o no. Si está de acuerdo, se realiza la contratación y se firma el contrato respectivo, ese sería como la prefase antes de empezar ya el proceso auditoría. Posteriormente, ya con el contrato, se establecen las fechas de visita con el cliente que no pueden pasar del 31 de julio porque es la fecha máxima de entrega de los informes de todas las entidades. Si hay 5 o 6 clientes, debemos avanzar en paralelo o ir adelantando para que el cliente no incumpla con el requisito de enviar el informe antes de esta fecha. Después, viene la fase de planeación donde se elabora el cronograma o el plan de auditoría, ese es donde viene el objetivo, el alcance, las actividades con fechas que debemos de cumplir en el proceso de auditoría y se solicitan los	

	requerimientos iniciales para que cuando iniciemos la fase de ejecución que es donde se inicia el proceso de auditoría, ya tengamos como insumo estos requerimientos iniciales que serán en función o están alineados a si el cliente es categoría uno o dos pero con las actividades propiamente que establezca la norma. Para la fase de ejecución, se ejecutan todos los procesos y actividades de revisión, si hay reuniones con el cliente, se realizan pruebas sustantivas y de cumplimiento al auditado y posteriormente, se van realizando reuniones de seguimiento para ir mostrando los avances, si el cliente tiene información adicional la puede suministrar para que el informe final salga depurado. En la etapa de cierre se envía el informe final, se presentan los resultados y las entidades envían el informe al banco central, posteriormente, si hay entidades que no cumplieron al 100 % (porque deben cumplir al 100% para obtener la certificación) deben realizar un plan de acción para a más tardar el 31 de octubre tenerlo listo. Debemos realizar los controles que no cumplieron, en función del plan de acción (los que ya estaban ya no se revisan) y se le envía al cliente el informe para que estos puedan enviarlo antes del 31 de octubre y que puedan cumplir con la fecha establecida por el banco central. En la fase de evaluación, una vez terminada la auditoría, el Socio Auditor de TI utiliza la herramienta de evaluación establecida para evaluar el proyecto de auditoría. Envía los resultados a los auditores y posteriormente se realiza una reunión para comentar los resultados y así identificar fortalezas y oportunidades de mejora.
2. ¿Quiénes son los responsables de las diferentes actividades dentro de este proceso de auditoría en ciberseguridad?	
Respuesta:	- Elaborar plan de auditoría - Socio encargado de TI - Reuniones con el cliente en la fase de planeación - Socio encargado de TI - Solicitar requerimientos iniciales - Socio encargado de TI - Elaborar pruebas sustantivas y de cumplimiento – auditor encargado, auditores asistentes - Revisar resultado de pruebas sustantivas - Socio encargado de TI - Elaborar el informe (sin las conclusiones de la revisión de los controles) – Socio encargado de TI - Dar formato al informe – Mercadeo - Reunión para comunicar resultados del informe - auditor encargado, auditores asistentes y socio encargado de TI
3. ¿Cuáles son los insumos clave que necesita para comenzar el proceso de auditoría en ciberseguridad y qué resultados produce?	
Respuesta:	Insumo inicial, el contacto que el cliente asigne para la comunicación con nosotros para validar las distintas actividades y que sea el responsable de enviarnos los requerimientos de auditoría. En la planeación: • El plan de auditoría tiene como resultado las actividades por realizar para llegar a la entrega del informe de auditoría. • Los requerimientos iniciales, tienen como resultado la elaboración de los procedimientos de auditoría.

	En la ejecución: • Requerimientos adicionales, tienen como resultado la elaboración de los procedimientos de auditoría. • Procedimientos de auditoría, tienen como resultado la elaboración del informe En etapa de cierre: • Reunión con el contacto definido por el cliente para la entrega de resultados del informe, tiene como resultado la aceptación del informe para ser enviado en su versión final al cliente o la realización de observaciones por parte del cliente para aplicar correcciones al mismo por parte del equipo de auditores.
4. ¿Qué herramientas o sistemas utiliza para completar el proceso de auditoría en ciberseguridad?	
Respuesta:	Actualmente solo se cuenta con la plantilla en Word para procedimientos de auditoría que se utiliza en los demás tipos de auditorías, específicamente para auditorías de COBIT y del MICITT. Excel para evaluar basado en la NIST que le da una guía al auditor según el estándar NIST qué se puede revisar.
5. ¿Cuáles son las principales dificultades que encuentra al llevar a cabo este proceso?	
Respuesta:	Los clientes no tienen claro lo que debían incluir los procedimientos o no los tenían hechos, no tenían claro qué se iba a revisar o con qué deben cumplir exactamente. Estos problemas afectan los tiempos de entrega del informe tanto para el Despacho al cliente, como para el cliente al Banco Central.
Aunque se cumple con las fechas pactadas de entrega de avances o informes finales al cliente: 6. ¿Considera que hay procesos internos que podrían ser más eficientes? ¿Cuáles?	
Respuesta:	Comunicar si hay alguna discrepancia con el cliente (por ejemplo, problemas con el envío de información del cliente al equipo auditor o lo enviado no fue lo solicitado) tal vez no me avisan con tiempo, entonces cuando yo pregunto ya ha pasado mucho tiempo. Otra situación es que tal vez no entiendan alguna prueba y no me preguntan en su momento entonces pueden atrasar los tiempos de la auditoría. O el equipo auditor no envían los requerimientos adicionales con antelación para que el cliente tenga tiempo para recolectar la información y enviarnos la evidencia.
7. ¿Cuáles son las actividades que consumen más tiempo o recursos?	
Respuesta:	1. La realización de pruebas sustantivas y de cumplimiento. 2. La realización de entrevistas para revisar la plataforma porque la normativa incluye sistemas, plataforma, red, activos y todo eso se debe revisar. 3. La revisión para solicitud de requerimientos adicionales.
8. ¿Existen picos de trabajo que podrían evitarse con una mejor planificación o recursos?	
Respuesta:	Teniendo una mejora en las herramientas para realizar la auditoría puede haber una mejora en el tiempo, el problema de picos de trabajo con estas auditorías es que dependiendo de cuantas ofertas se concluyan exitosas (es decir, el cliente

	nos elija y se realice la contratación) por normativa del Banco Central todas deben entregar sus informes en la misma fecha.
9. ¿Hay informes que deban rehacerse más de una vez antes de ser aprobados?	
Respuesta:	Sí, si son de fondo se le devuelve al equipo auditor para realizar correcciones.
10. ¿Considera que la falta de estandarización en los procedimientos afecta la consistencia o calidad de las auditorías? ¿Por qué?	
Respuesta:	A nivel del proceso completo de la auditoría, el plan de auditoría provee una estandarización al estar todo delimitado por actividades y fechas. Pero a nivel de realización de los procedimientos de auditoría si existe una desestandarización que puede ser atendida indicándole al auditor qué revisar en cada actividad según la NIST y la Norma Técnica del BCCR, esto puede ayudar a la hora de realizar los procedimientos y de redactar los requerimientos iniciales y adicionales.

Apéndice G. Formato minuta de reunión

Minuta de reunión		
Número de reunión:		
Objetivo de la reunión:		
Fecha:	**Hora:**	**Lugar:**
Participantes:		
Temas tratados		
Número	**Comentarios**	**Acuerdos**

Apéndice H. Formato instrumento Análisis de Brecha

Situación actual	Situación deseada	Plan de acción
Situación actual 1	Situación deseada 1	Plan de acción 1
Situación actual 2	Situación deseada 2	Plan de acción 2
Situación actual n	Situación deseada n	Plan de acción n

Apéndice I. Formato instrumento revisión documental

Revisión documental	
Objetivo:	
Fuente:	
Principales hallazgos	

Apéndice J. Resultados revisión documental 01

Revisión documental	
Objetivo:	Identificar las secciones requeridas para un manual de auditoría
Fuente:	ISO 10013
Principales hallazgos	
La ISO 10013 sugiere que la información documentada contenga las siguientes secciones: • Información sobre la organización. • Términos y definiciones. • Procesos de la organización (incluyendo el flujo o mapa de procesos). • Procedimientos documentados o una referencia a ellos.	
La fuente indica que todos los procesos de la organización deben estar documentados. Además, que los colaboradores de la institución deben ser capacitados sobre la información que se documente sobre los distintos procesos de negocio.	

Apéndice K. Resultados revisión documental 02

Revisión documental	
Objetivo:	Identificar las fases de una auditoría y sus requerimientos.
Fuente:	ISO 190011
Principales hallazgos	
Según la fuente consultada, se identificó que una auditoría debería contar con las siguientes fases: • Planificar • Hacer • Verificar • Actuar	
La fuente indica que las auditorías deben tener establecido un Plan de Auditoría que guíe toda la ejecución de esta. También establece la necesidad de contar con un equipo de auditores capacitado, que tengan las competencias necesarias para realizar las evaluaciones de auditoría.	

Apéndice L. Resultados revisión documental 03

Revisión documental	
Objetivo:	Identificar los requisitos obligatorios en ciberseguridad para participar en SINPE según normativa costarricense.
Fuente:	Norma Técnica – Requisitos de Ciberseguridad
Principales hallazgos	
La norma proporciona: • Categorización de clientes. • Los plazos. • Los tipos de controles. • Los 16 controles con sus respectivos objetivos y descripciones. • El formato mínimo requerido para la redacción del informe que se debe enviar al Banco Central de Costa Rica: o Resumen ejecutivo, Introducción, Marco Organizacional, Equipo de auditores, Alcance de la auditoría, Metodología, Hallazgos de la auditoría, Conclusión de la auditoría, Plan de Mitigación, Anexos.	

Apéndice M. Resultados revisión documental 04

Revisión documental	
Objetivo:	Identificar documentación existente sobre auditorías en ciberseguridad en el Despacho.
Fuente:	Documentación interna del Despacho.
Principales hallazgos	
El Manual de Auditorías existente es para las basadas en COBIT 19, no existe ninguna documentación interna para auditorías en ciberseguridad.	
Cuentan con una herramienta de auditoría específica para auditorías basadas en COBIT 19 o el MICITT. Sus secciones incluyen: • Información de la empresa auditada. • Información de los auditores y sus roles de participación. • Tipo de prueba realizada. • Criterio de auditoría utilizado. • Procedimiento de la prueba. • Atributos, conclusiones y papeles de trabajo. • Seguimiento de hallazgos previos.	

Apéndice N Minuta de reunión 01

Minuta de reunión		
Número de reunión: 01		
Objetivo de la reunión: Primera reunión tutor-estudiante-contraparte		
Fecha: 09/08/2024	**Hora:** 10:30	**Lugar:** Virtual
Participantes:	Fabián Cordero Navarro	
	Agustín Francesa Alfaro	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se realiza una presentación de los participantes y se le comunica a la contraparte de la empresa que serán requeridas dos sesiones más: tutor-estudiante-contraparte	Realizar dos sesiones más de seguimiento según cronograma de TFG.	Jennifer Paola Lobo Quirós Agustín Francesa Alfaro Fabián Cordero Navarro
Se consulta a don Fabián la necesidad de negocio para basar el manual en la NIST – Cybersecurity Framework	Se indica que es necesario agregarla como marco de referencia para que sirva como valor agregado a la evaluación para el cliente y para que sirva de guía extra a los auditores a la hora de realizar la evaluación de auditoría.	Jennifer Paola Lobo Quirós
Se comentó comprender la problemática y los entregables requeridos por la empresa, don Fabián también confirmó que se está claros con el trabajo por realizar.	Iniciar el desarrollo del proyecto y comentar avances en el documento académico y en el producto para la empresa.	Jennifer Paola Lobo Quirós

Apéndice Ñ. Minuta de reunión 02

Minuta de reunión		
Número de reunión: 02		
Objetivo de la reunión: Presentar avances sobre el desarrollo del TFG		
Fecha: 05/09/2024	**Hora:** 10:00 a.m.	**Lugar:** Virtual.
Participantes:	Fabián Cordero Navarro	
	Jennifer Paola Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se le presentaron los avances en el documento académico a don Fabián, se explicó que los primeros capítulos son teóricos, por ese motivo aún no existían avances sobre la realización del manual.	Continuar con la elaboración del documento académico y comunicar cuando existan dudas o avances sobre la elaboración del manual.	Jennifer Paola Lobo Quirós
Don Fabián solicita el documento del TFG para realizar una revisión y retroalimentación.	Enviar documento del TFG a don Fabián.	Jennifer Paola Lobo Quirós

Apéndice O. Minuta de reunión 03

Minuta de reunión		
Número de reunión: 03		
Objetivo de la reunión: Realizar segunda reunión de seguimiento tutor-empresa-estudiante.		
Fecha: 30/09/2024	**Hora:** 11:00 a.m.	**Lugar:** Virtual
Participantes:	Fabián Cordero Navarro	
	Agustín Francesa Alfaro	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se presentan avances sobre el documento del TFG, se mencionan los ajustes requeridos a la metodología	Se debe incluir el diagrama de cada fase del ciclo de auditoría, no como mejora del proceso	Jennifer Paola Lobo Quirós

para basarla en ISO 19011 debido a que el proyecto no es una mejora de procesos, por tanto, no aplica basarlo en Dumas como se tenía anteriormente.	sino para apoyo visual y porque deben estar documentados los procesos de negocio. Se deben incluir los diagramas en el manual de auditoría.	
Se realiza consulta al tutor sobre el análisis de brecha, si el plan de acción es el manual o una referencia al Manual de Auditoría.	Describir la sección general del manual que solventa la brecha.	Jennifer Paola Lobo Quirós
Se le consulta a don Fabián si no existe una metodología de evaluación al proyecto de auditoría, él indica que sí existe y se implementa.	Fabián Cordero enviará la herramienta de evaluación utilizada.	Fabián Navarro Cordero
Se consulta si en la herramienta de auditoría se deben incluir ambos controles, el que indica la Norma Técnica y lo que indica la NIST Se aclara, además, que a nivel de hallazgos solamente se utiliza como criterio la Norma Técnica.	Se acuerda agregar en la herramienta de auditoría los componentes de la NIST y también el control de la Norma Técnica. También, coordinar sesión para revisar propuesta de estructura del manual.	Jennifer Paola Lobo Quirós
El tutor consulta si con el avance presentado, se logrará sacar el proyecto a tiempo. Don Fabián indicó que está definido lo requerido para los productos finales, por tanto, considera que no existirán atrasos en el proyecto.	No se solicitará prórroga.	No aplica.

Apéndice P. Minuta de reunión 04

Minuta de reunión		
Número de reunión: 04		
Objetivo de la reunión: Presentar propuesta de herramienta de auditoría y de estructura del manual.		
Fecha: 03/10/2024	**Hora:** 9:15 a.m.	**Lugar:** Virtual
Participantes:	Fabián Navarro Cordero	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se presenta la propuesta de estructura de manual, don Fabián la aprueba con la salvedad de revisar si hay suficientes recomendaciones para agregar una sección específica para esto.	Implementar el manual con la estructura aprobada, revisar si aporta valor agregar recomendaciones.	Jennifer Lobo Quirós
Se presenta propuesta de herramienta de auditoría, pero don Fabián indica que, para mantener un formato con las herramientas utilizadas para auditorías de TI, se realice en Word manteniendo el estilo de la herramienta para auditorías de COBIT 19 y añadir lo que requiere la norma técnica para redactar los informes. De esta manera, la información quede centralizada y solamente se deba pasar de la herramienta a rellenar la plantilla de informe.	Cambiar herramienta ofimática para realizar la herramienta de auditoría, utilizar Excel.	Jennifer Lobo Quirós

Apéndice Q. Minuta de reunión 05

Minuta de reunión		
Número de reunión: 05		
Objetivo de la reunión: Solicitar aprobación sobre los atributos definidos		
Fecha: 23/10/2024	**Hora:** 10:30 a.m.	**Lugar:** Virtual
Participantes:	Fabián Cordero Navarro	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se presentan los atributos propuestos y la evidencia requerida definida, por cada uno de los 16 controles, para agregar al manual en la sección de fase de ejecución del ciclo de auditoría. Don Fabián solicita un ajuste, que se agregue una columna extra de manera que queden las siguientes columnas: atributo, evidencia requerida y ¿cómo revisar el control?	Agregar una tercera columna a la tabla de atributos por evaluar por control llamada "¿Cómo revisar el control?".	Jennifer Lobo Quirós

Apéndice R. Minuta de reunión 06

Minuta de reunión		
Número de reunión: 06		
Objetivo de la reunión: Realizar tercera reunión de seguimiento tutor-empresa-estudiante.		
Fecha: 30/10/2024	**Hora:** 10:30 a.m.	**Lugar:** Virtual
Participantes:	Fabián Cordero Navarro	
	Agustín Francesa Alfaro	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se indica que el documento TFG está listo, solamente queda atender los últimos	Enviar Manual de Auditoría a Fabián Cordero.	Jennifer Lobo Quirós

comentarios del tutor. Sobre los productos se comenta que se están terminando de atender los ajustes solicitados el 23 de octubre.		
Fabián Cordero indica que están claros los productos finales, que se han realizado sesiones para aclarar dudas y definir los entregables, los cuáles se han desarrollado en cumplimiento con la normativa vigente y lo esperado por la empresa.	Enviar nota de minutas para el firmado por parte de don Agustín y don Fabián.	Jennifer Lobo Quirós Agustín Francesa Alfaro Fabián Cordero Navarro

Apéndice S. Minuta de reunión 07

Minuta de reunión		
Número de reunión: 07		
Objetivo de la reunión: Solicitar aprobación de producto final.		
Fecha: 30/10/2024	**Hora:** 15:11	**Lugar:** Virtual
Participantes:	Fabián Cordero Navarro	
	Jennifer Lobo Quirós	
Temas tratados		
Comentarios	**Acuerdos**	**Responsable**
Se presenta Manual de Auditoría y herramienta de auditoría, los cuales son aprobados como versión final del producto.	Enviar a la empresa Manual de Auditoría creado en su versión final.	Jennifer Lobo Quirós

Apéndice T. Aceptación de minutas por parte de la contraparte de la empresa

Aceptación de minutas profesor contraparte de la empresa

Yo Fabián Cordero Navarro confirmo la veracidad de las siguientes minutas correspondientes al trabajo final de graduación de la estudiante Jennifer Paola Lobo Quirós, el cual lleva como nombre "Propuesta de manual de auditoría en ciberseguridad basado en el marco de trabajo NIST - Cybersecurity Framework y la Norma Técnica de Ciberseguridad del BCCR".

Minuta	Fecha
Minuta 01	09/08/2024
Minuta 02	05/09/2024
Minuta 03	30/09/2024
Minuta 04	03/10/2024
Minuta 05	23/10/2024
Minuta 06	30/10/2024
Minuta 07	30/10/2024
Entrevista número 01	12-09-2024

Firma: FABIAN EDUARDO CORDERO NAVARRO (FIRMA) Firmado digitalmente por FABIAN EDUARDO CORDERO NAVARRO (FIRMA) Fecha: 2024.10.31 15:41:16 -06'00'

Apéndice U. Aceptación de minutas por parte del profesor tutor

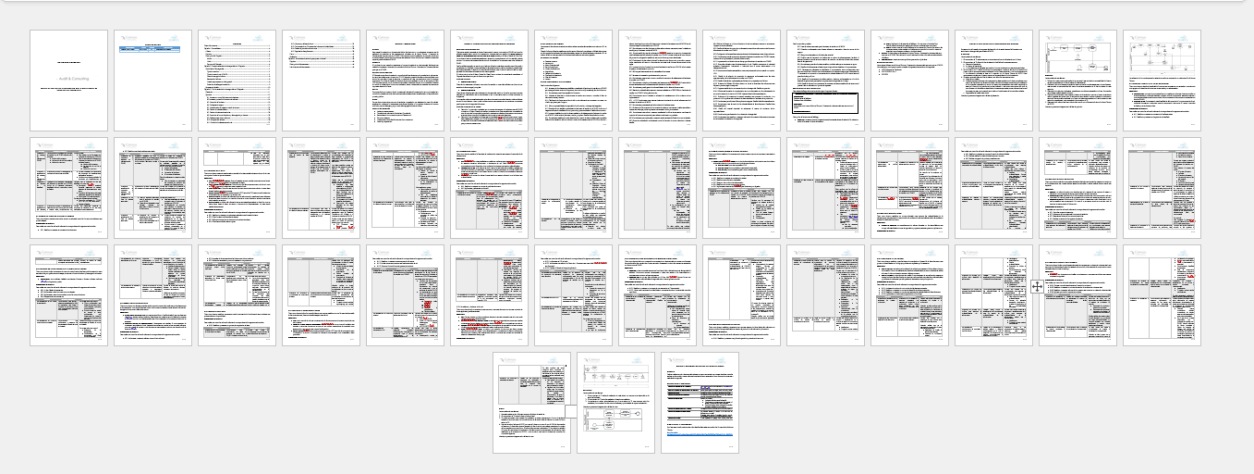
Aceptación de minutas profesor tutor

Yo Agustín Francesa Alfaro confirmo la veracidad de las siguientes minutas correspondientes al trabajo final de graduación de la estudiante Jennifer Paola Lobo Quirós, el cual lleva como nombre "Propuesta de manual de auditoría en ciberseguridad basado en el marco de trabajo NIST - Cybersecurity Framework y la Norma Técnica de Ciberseguridad del BCCR".

Minuta	Fecha
Minuta 01	09/08/2024
Minuta 03	30/09/2024
Minuta 06	30/10/2024

Firma: JOSE AGUSTIN FRANCESA ALFARO (FIRMA) 2024.10.30 16:07:19-06'00'

Apéndice V. Manual de auditoría



10.Anexos

Anexo I: Carta de revisión filológica

CARTA DE REVISIÓN FILOLÓGICA

Cartago, 02 de noviembre de 2024

Instituto Tecnológico de Costa Rica

Escuela de Administración de

Tecnologías de Información

Respetables señores:

Leí y di sugerencias filológicas al Proyecto de Graduación titulado: **"Propuesta de Manual de Auditoría en ciberseguridad basado en el marco de trabajo NIST-Cybersecurity Framework y la Norma Técnica de Ciberseguridad del BCCR".** Elaborado por Jennifer Paola Lobo Quirós, cédula 207880685. Se dieron sugerencias en aspectos como: construcción de párrafos, vicios del lenguaje que se trasladan al escrito, ortografía, puntuación y otros relacionados con el campo filológico. Considero que está listo para ser presentada como Trabajo Final de Graduación para optar por el grado y título de Licenciatura en Administración de Tecnología de Información

Atentamente.

MSc. Dinorah Sánchez Fallas

Cédula 105770564

Incorporada a COLYPRO

Carné No. 004821

Filóloga UCR

DINORAH MARIA DE LA CONCEPCION SANCHEZ FALLAS (FIRMA)

Firmado digitalmente por DINORAH MARIA DE LA CONCEPCION SANCHEZ FALLAS (FIRMA)
Fecha: 2024.11.02 12:27:44 -06'00'