TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnología de Información

Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR

Trabajo final de graduación para optar por el título de Licenciatura en Administración de Tecnología de Información

Elaborado por: Hellen Yazmin Cordero Robles

Profesor tutor: Laura Alpízar Chaves

Cartago, Noviembre 2021

II semestre, 2021

ÁREA ACADÉMICA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÒN

GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área Académica de Administración de Tecnologías de Información, recomendamos que el siguiente Trabajo Final de Graduación de la estudiante Hellen Cordero Robles sea aceptado como requisito parcial para optar al grado académico de Licenciatura en Administración de Tecnología de Información.

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.25 11:12:45 -06'00'

Laura Alpízar Chaves
Profesor tutor

LUIS CARLOS NARANJO ZELEDON (FIRMA)
Firmado digitalmente por LUIS CARLOS NARANJO ZELEDON (FIRMA)
Fecha: 2021.11.24 13:57:21 -06'00'

Luis Carlos Naranjo Zeledón
Lector académico

Herberth Torres
Lector externo

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2021.11.25 20:29:43 -06'00'

Yarima Sandoval Sánchez
Coordinadora de trabajo final de graduación

DEDICATORIA

A Dios y a la virgen de los Ángeles

Por darme salud, la sabiduría para poder llegar a este punto de mi vida y acompañarme siempre.

A mis padres

Por su esfuerzo y la motivación que me han dado para seguir adelante a pesar de las dificultades.

A mis hermanos y a mi tía Auxi

Por creer en mí y por todo el apoyo que me brindaron en toda esta etapa.

AGRADECIMIENTOS

A Dios y a la virgen de los Ángeles

Por darme la fuerza y la sabiduría para salir adelante.

A mi familia, padres, hermanos y abuelita

Por todo su apoyo y esfuerzo que me brindaron durante todos estos años para ayudarme a cumplir mis sueños, por guiarme por el buen sendero e inspirarme hacer una mejor persona.

A mi profesora tutora Laura Alpízar

Por ser una guía en este proceso, por la retroalimentación durante todo el proyecto y la carrera, la paciencia y motivación para realizar las cosas de la mejor manera.

A mis amigas

A las chiquis a Dani, Yara, Nati, Vale, Karen y Maribel, por ser de las mejores cosas que me dejo el TEC, por tan buenos momentos que me han hecho pasar y por todo el apoyo que me brindaron. A Nati por estar presente en esta etapa y apoyarme en mis momentos de crisis. A Caro, por su amistad, por todo el apoyo que me dio en estos años y por creer en mis capacidades para concluir esta etapa.

A Cata por ser la mejor amiga que pude encontrar, por estar siempre para mí, apoyarme y animarme hasta el final. A Kar porque a pesar de la distancia siempre me ha apoyado para seguir adelante.

Al equipo de IT Audit

Por la oportunidad que me dieron de poder realizar este trabajo con ellos y el apoyo brindado en todo momento.

RESUMEN

El objetivo de este estudio recae en proponer un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – *Cybersecurity Framework*, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras, mediante el análisis de la documentación actual del área de auditoría de TI y los componentes del marco NIST- *Cybersecurity Framework*, para posteriormente elaborar un conjunto de herramientas que cumplan con las necesidades de HCR y de sus clientes. Además de determinar el retorno de inversión y beneficios que se derivan de este estudio.

La propuesta del proyecto surge debido a que por directriz de la empresa en todas las auditorías se deben evaluar los riesgos cibernéticos, sin embargo, la evaluación realizada por el área de auditoría de TI no es suficiente ya que, se presenta de forma indagatoria y no cuenta con un estándar o herramientas establecidas para tomar de referencia, provocando falta de claridad en la evaluación.

La investigación está basada en una metodología con diseño de investigación-acción, donde se utiliza un enfoque cualitativo que permite analizar las necesidades de los sujetos de estudio y brindarles soluciones de acuerdo con las situaciones identificadas.

El resultado del estudio proporcionó los procedimientos que se deben evaluar para determinar los riesgos cibernéticos en los clientes, así como definir que el componente del marco NIST- *Cybersecurity Framework* más adecuado para la evaluación es el *Framework Core.* Con base a lo anterior se elaboró un conjunto de herramientas que permitirá al equipo de auditoría de TI identificar los riesgos cibernéticos de forma clara y puntual.

Palabras claves: riesgos cibernéticos, marco de trabajo, NIST, *Framework Core*

ABSTRACT

The objective of this study is to propose a set of cyber risk assessment tools, based on the NIST - Cybersecurity Framework for the improvement and standardization of technological evaluations of the IT audit area that supports financial audits, by analyzing the current documentation of the IT audit area and the components of the NIST-Cybersecurity Framework, to later develop a set of tools that meet the needs of HCR and its clients. In addition to determining the return on investment and benefits derived from this study.

The project proposal arises because by company guideline in all audits cyber risks must be evaluated, however, the evaluation carried out by the IT audit area is not enough since it is presented in an investigative way and not It has a standard or established tools to take as a reference, causing a lack of clarity in the evaluation.

The research is based on a methodology with an action-research design, where a qualitative approach is used that allows to analyze the needs of the study subjects and provide them with solutions according to the identified situations.

The result of the study provided the procedures to be evaluated to determine cyber risks in clients, as well as to define that the most suitable component of the NIST-Cybersecurity Framework for the evaluation is the Framework Core. Based on the above, a set of tools was developed that will allow the IT audit team to identify cyber risks in a clear and timely manner.

Keywords: Cyber risks, framework, NIST, Framework Core

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

NOTA ACLARATORIA

Género[1]**:**

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del "género inclusivo". Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

Nombre de la empresa:

La empresa donde se realizará el trabajo final de graduación ha solicitado que su nombre no aparezca en ningún apartado del presente documento, por razones de confidencialidad.

Por lo anterior, la empresa será denominada como "HCR", con el propósito de respetar las indicaciones solicitadas por la empresa.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

CAPÍTULO I

INTRODUCCIÓN

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

En el presente documento se desarrolla una propuesta de trabajo final de graduación (TFG) de la carrera de Administración de Tecnología de Información, del Instituto Tecnológico de Costa Rica. Se refiere a un conjunto de herramientas para la evaluación de los riesgos cibernéticos basado en el marco de trabajo NIST – Cybersecurity Framework, con el fin de estandarizar y mejorar la valoración de las implicaciones que tienen los riesgos en las empresas auditadas.

En las primeras secciones del estudio se contextualiza la organización y brinda un entendimiento de la problemática actual que está enfrentando el área de Auditoría de TI. A continuación, en las siguientes secciones se mencionan los objetivos que se desean cumplir para brindarle solución a la problemática establecida.

Asimismo, se aborda un enfoque teórico que ayuda a comprender la propuesta de solución. Seguidamente se encuentra el marco metodológico, donde se detallan las fuentes de información, los instrumentos y fases del proyecto.

Finalmente, se presenta un análisis de resultados y la explicación detallada de la propuesta de solución desarrollada para el equipo de auditoría de TI.

1.2. ANTECEDENTES

1.2.1. Descripción de la organización

En esta sección se detalla la información general de la organización donde se elaborará el trabajo final de graduación, contemplando la misión, visión, valores e información general de esta.

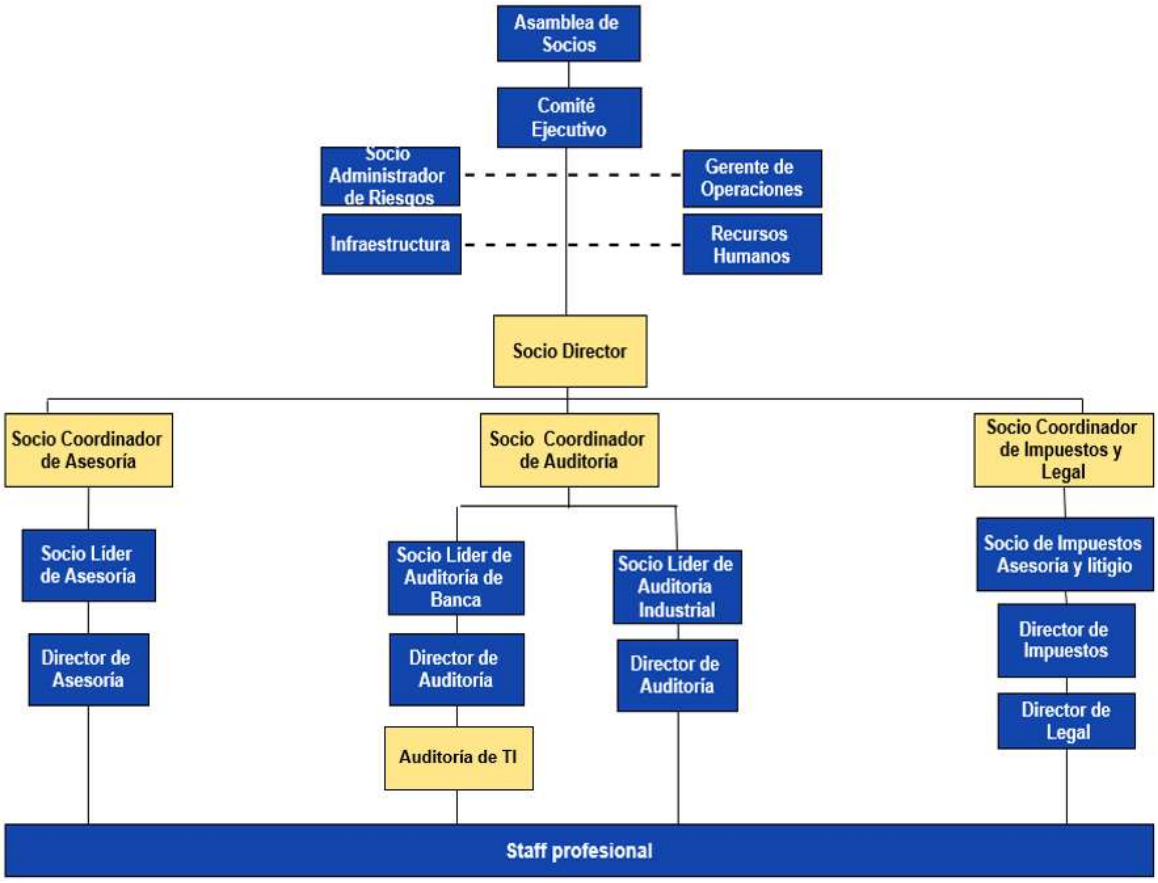
La empresa HCR forma parte de una red global de organizaciones a nivel internacional, con presencia en 165 países trabajando alrededor del mundo, y se especializa en atender necesidades de otras empresas clientes (HCR, 2021). Actualmente HCR cuenta con alrededor de 173 000 profesionales en diversos equipos disciplinarios, los cuales se encuentran distribuidos en los cinco departamentos existentes: Advisory, Tax, Legal, Infrastructure y Audit; nombrados en inglés según la red global. (HCR, 2021).

La empresa HCR cuenta con más de 60 años de experiencia en el país, durante el año 2005 se formó una integración con las Firmas miembros ubicadas en Centroamérica, las cuales se encuentran ubicadas en: Guatemala, El Salvador, Nicaragua, Panamá y República Dominicana. (HCR, 2021).

Esta organización, pertenece a una red global, por lo tanto, posee una estructura jerárquica utilizada por todas las firmas miembros a nivel mundial, donde las principales directrices empresariales son establecidas y comunicadas por un Director Ejecutivo y un Socio Director. En una escala laboral debajo de estos, se encuentran los socios empresariales, responsables de definir las metas y los objetivos para cada uno de los departamentos, en la Figura 1, se muestra una adaptación del organigrama actual de la empresa.

Figura 1.

Organigrama HCR



Nota: La figura muestra una adaptación del organigrama general de la empresa HCR.

Fuente: HCR (2021).

A continuación, se expone la misión, visión, valores y estructura de HCR.

1.2.1.1. Misión.

La misión de HCR es:

"Proveer servicios de auditoría con el más alto nivel de calidad, buscando siempre la máxima satisfacción de nuestros clientes dentro de un marco de ética, independencia y confidencialidad." (HCR, 2021).

1.2.1.2. Visión.

La visión de HCR es:

"Ser la mejor firma en dónde trabajar, para nuestros clientes, para nuestra gente y para nuestra comunidad." (HCR, 2021)

1.2.1.3. Valores.

Los valores bajos los cuales se rige HCR para crear un sentido de identidad compartida dentro de la organización son los siguientes (HCR, 2021):

- Lideramos con el ejemplo en todos los niveles actuando de manera que ejemplifique lo que queremos de cada uno de nosotros.
- Trabajamos en equipo tomando lo mejor de cada uno y creando relaciones fuertes y duraderas.
- Respetamos a los individuos respetando a las personas por lo que son y por su conocimiento, habilidades y experiencia como miembros individuales de un grupo.
- Investigamos los hechos y transmitimos conocimientos verificando los hechos y fortaleciendo nuestra reputación como asesores de negocios con credibilidad y objetividad.
- Nos comunicamos de forma abierta y honesta compartiendo información, conocimiento manejando situaciones difíciles con coraje y creatividad.
- Comprometidos con la Sociedad comportándonos como ciudadanos responsables y ampliando nuestras habilidades, experiencia y perspectiva de nuestras comunidades.
- Por encima de todo nos comportamos con integridad manteniendo elevados estándares profesionales en todo momento, proveyendo asesoría útil y conservando nuestra independencia con rigor.

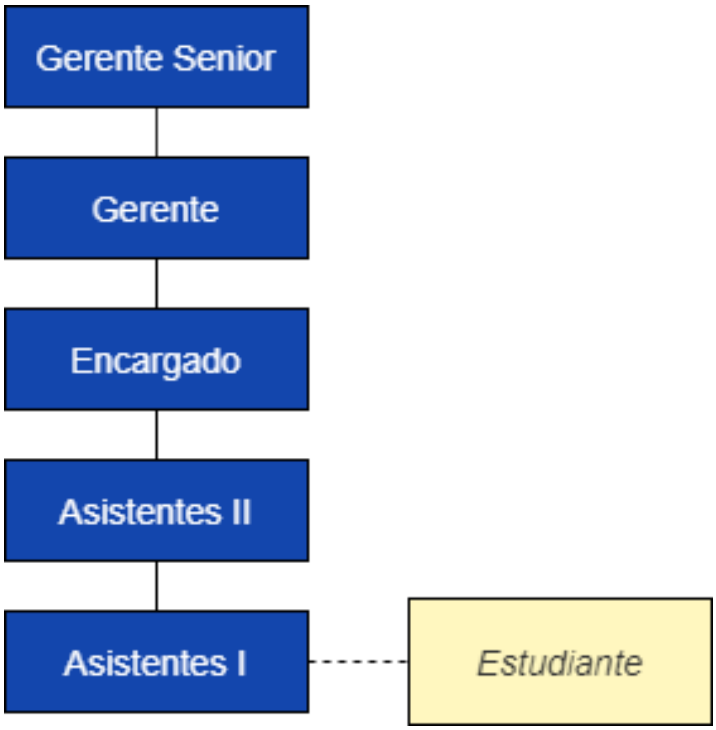
1.21.4. Equipo de trabajo.

El equipo de Auditoría de TI está conformado por especialistas de TI, responsables de brindar apoyo al grupo de auditoría financiera, en la evaluación de los sistemas de información e infraestructura tecnológica. En este proceso es donde se determinan posibles debilidades en las configuraciones de los sistemas que pueden provocar errores o cambios indebidos en los registros contables y estados financieros.

Actualmente, el equipo de Auditoría de TI está conformado por un Gerente Senior, un Gerente, un Encargado, y un conjunto de especialistas de TI, en carreras afines a tecnología de información. En la Figura 2 se muestra la jerarquía existente dentro del equipo de Auditoría de TI y la ubicación del estudiante que realiza el presente trabajo.

Figura 2.

Organigrama equipo Auditoría TI



Fuente: Elaboración propia, basada en información consultada en la empresa (2021)

1.2.2. Trabajos similares realizados dentro y fuera de la organización

En esta sección se describen proyectos realizados dentro y fuera de la organización, relacionados con el presente trabajo.

1.2.2.1. Proyectos Internos

Con el fin de identificar proyectos similares al proyecto por desarrollar, se recurrió a la red interna de la empresa HCR, la cual forma parte de la red de conocimiento International, la cual posee un repositorio de los diferentes proyectos realizados por HCR a nivel global.

Si bien, no existe ningún proyecto con un enfoque similar al presente estudio, a nivel global HCR ha desarrollado diversas metodologías que sirven de insumo para brindar servicios en temas de ciberseguridad en países como Estados Unidos y Canadá. A continuación, se presentan los proyectos similares llevados a cabo por HCR International:

1.2.2.1.1. *Cyber Security Framework* – HCR Canadá

La empresa HCR en Canadá ha desarrollado un marco de trabajo basado en buenas prácticas de ciberseguridad, tales como: NIST, OSFI, SANS, ISF e ISO27001. Este marco de trabajo ayuda a identificar la posición de defensa en cuanto a amenazas de ciberseguridad de los clientes. Este servicio consta de dos principales actividades: Evaluación General de Madurez en Ciberseguridad y Red Team Exercise (HCR Canadá, 2015)

Este marco de trabajo consta de cuatro fases: Proteger, Preparar, Integrar y Detectar, las cuales están alineadas a una constante fase de transformación cibernética, la cual busca implementar plataformas de lanzamientos de soluciones inteligentes ante posibles amenazas.

1.2.2.1.2. *Cyber Security Risk Assessment* – HCR Estados Unidos

HCR en Estados Unidos brinda un servicio de *Cyber Security Risk Assessment,* para brindar este servicio, Estados Unidos realizó una adaptación del marco de trabajo NIST-*Cybersecurity Framework* con el fin de identificar las capacidades reales de los clientes (HCR Estados Unidos, 2015)

1.2.2.1.3. Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información

Por otro lado, anterior a este proyecto se encuentra el trabajo final de graduación de Inces, C (2019) nombrado “Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información”.

En este proyecto se ejecutó un proceso de optimización de los controles generales de TI, a fin de responder con las exigencias definidas en el Reglamento General de Gestión de la Tecnología de Información, según el acuerdo 14-17, emitido por SUGEF en el 2017, que propone a las entidades del sector financiero costarricense, alinearse al marco de referencia de COBIT 5. (Inces C, 2019)

La ejecución del proceso de mejora de los controles generales abarca desde el fortalecimiento de los controles existentes, definición de nuevos y pruebas que permiten la revisión de la eficiencia de los procesos implementados en las organizaciones financieras; generando así un mecanismo que asegure la integridad, exactitud y confidencialidad de los datos e información utilizada por auditoría financiera. (Inces, 2019).

1.2.2.2. Proyectos Externos

De forma externa se encuentran proyectos académicos relacionados con el presente trabajo.

A partir de repositorios de material académico relacionados con trabajos finales de graduación o tesis, se encontró el trabajo realizado por Azofeifa, H (2019) denominado "Propuesta de Metodología para Determinar el Nivel de Madurez de la Atención riesgos cibernéticos según el Marco de Trabajo NIST".

En este estudio se elaboró una propuesta metodológica para determinar el nivel de madurez de la atención de riesgos de ciberseguridad. Se consideran aspectos como: matrices de evaluación, modelo de madurez, gestión de riesgos, guía de ayuda, presentación de resultados, entre otras relevantes. (Azofeifa, 2019)

Asimismo, la presente investigación se relaciona con la propuesta planteada en el párrafo anterior, pues para su desarrollo se utilizará el mismo marco de trabajo empleado por Azofeifa, H (2019).

1.3. PLANTEAMIENTO DEL PROBLEMA

En este apartado se describe la situación problemática hallada dentro del entorno de la organización, el cual motiva el desarrollo del proyecto, así como la mención de los beneficios esperados del producto.

1.3.1. Situación problemática

El equipo de Auditoría de TI es el encargado del proceso de auditoría de los departamentos o áreas de Tecnologías de Información de las organizaciones auditadas por HCR. Dichos equipos o departamentos son responsables de habilitar y mantener los sistemas

de información relacionados con las operaciones de contabilidad y reportes financieros de dichas organizaciones.

HCR utiliza como base una metodología propia que establece las reglas generales para el desarrollo de las auditorías. Además, en esta se definen las responsabilidades del equipo de Auditoría de TI en el proceso de auditoría financiera, las cuales corresponden a evaluar el entendimiento del entorno de TI de las organizaciones auditadas y la evaluación de los controles generales y de aplicación de TI.

Como parte de la evaluación, se realiza una revisión de los riesgos cibernéticos para conocer sus implicaciones, ya que, los clientes de HCR son entidades de mucho prestigio y poseen gran nivel de activos, y la exposición a este tipo de riesgos resulta preocupante, en tanto ocasionaría problemas muy graves en sus operaciones.

En este caso la evaluación realizada por el área de auditoría de TI no es suficiente al considerar los riesgos que las entidades auditadas enfrentan en la actualidad, ya que, se presenta de forma indagatoria y no cuenta con un estándar o herramientas establecidas para tomar como referencia.

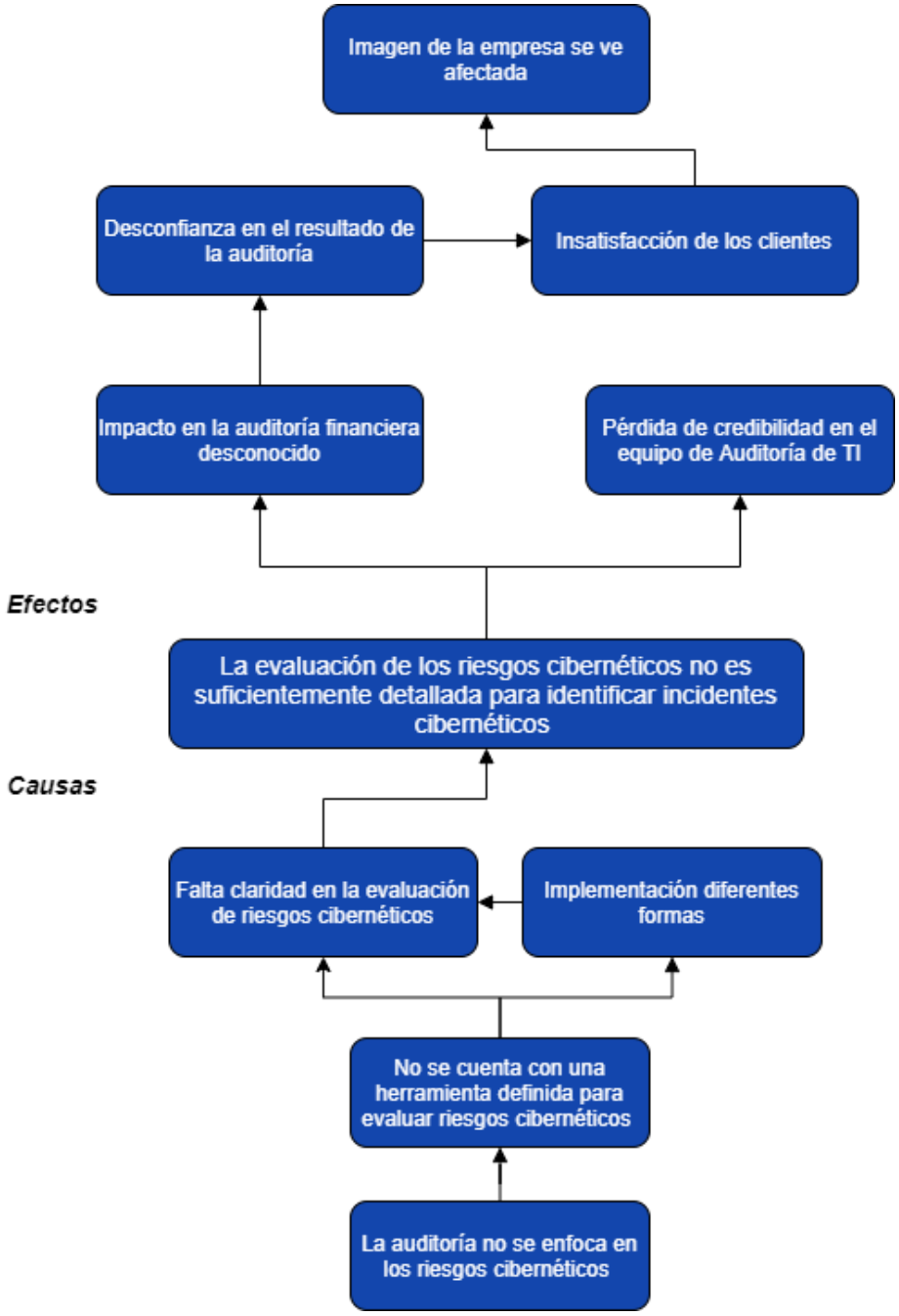
Esto a su vez, provoca que la evaluación se implemente de diferentes formas en cada proyecto, por ende, origina falta de claridad al evaluar los riesgos cibernéticos y dificulta que se identifiquen estos incidentes.

Asimismo, el enfoque se presenta en los sistemas y datos que son relevantes para la preparación de los estados financieros, y es poco probable que la evaluación realizada en la actualidad identifique un incidente cibernético, situación que pone en duda la confianza en dichos sistemas de información, tal como se muestra en la Figura 3, donde se identifica a través de un árbol de decisión, las causas y efectos de la problemática presente en HCR

La situación problemática descrita anteriormente, busca responder la siguiente pregunta: ¿La evaluación de los riesgos cibernéticos no es suficientemente detallada para identificar incidentes cibernéticos?

Figura 3.

Árbol de Problemas



Fuente: Elaboración propia (2021)

1.3.2. Justificación del proyecto

Los incidentes de ciberseguridad son ataques intencionales o eventos no intencionales mediante los cuales los usuarios no autorizados obtienen acceso a los sistemas digitales para interrumpir las operaciones, robar información confidencial o causar la denegación de servicio en los sitios web. (HCR, 2021)

El crecimiento en el uso de la tecnología, en todos los sectores de la industria y en la economía digital, ha traído consigo un incremento en los ataques cibernéticos en todo el mundo, ocasionando la preocupación de los individuos por asuntos de seguridad cibernética. Además, los inversores y los reguladores exigen, constantemente, a las entidades para que mejoren sus salvaguardas y solicitan una mayor transparencia en torno a los incidentes de ciberseguridad.

Asimismo, es transcendental mencionar que actualmente la empresa HCR tiene como directriz que en todos los proyectos de auditoría que se realicen, se deben revisar los riesgos cibernéticos.

Por ello, es importante que HCR cuente con programas formales para auditar las estrategias y procesos asociados con la gestión del riesgo cibernético, mediante el uso de marcos de referencia y mejores prácticas relacionadas con la ciberseguridad. En consecuencia, el equipo de Auditoría de TI, como entidad externa, debe considerar dichos aspectos para mantenerse alineado a las condiciones de la industria y brindar resultados relevantes en las auditorías.

Para el presente proyecto se elaboran un conjunto de herramientas para la evaluación de los riesgos cibernéticos en las auditorías, basadas en el marco de trabajo NIST – Cybersecurity Framework, ya que la empresa HCR eligió este marco al proporcionar un

lenguaje común y una metodología sistemática para gestionar el riesgo de ciberseguridad, además de adaptarse a cualquier organización. (National Institute of Standards and Technology, 2021)

El área de Auditoría de TI podrá minimizar el riesgo de detección con el conjunto de herramientas para la evaluación de los riesgos cibernéticos, ya que le brinda al equipo instrumentos para poder identificar, de manera más puntual, los riesgos cibernéticos que actualmente no se determinan.

Este es un proyecto novedoso para realizar la evaluación de riesgos cibernéticos de los clientes de HCR, ya que es una nueva forma de ejecutar dicha evaluación y brindarles a los clientes un servicio de auditoría más completo y confiable.

Asimismo, como estudiante de la carrera de Administración de Tecnología de Información y de acuerdo con el Reglamento Específico del Trabajo Final de Graduación en su Artículo 14 es trascendental que el estudiante desarrolle habilidades técnicas y blandas, en áreas como la investigación de tecnología de información y estudio de diferentes estándares, finalmente, se destaca que para la construcción de los instrumentos se debe indagar sobre temas relevantes como la Auditoría de TI, Infraestructura Tecnológica, entre otros.

1.3.3. Beneficios esperados o aportes del Trabajo Final de Graduación

En esta sección se mencionan los beneficios directos e indirectos obtenidos al resolver la problemática planteada con anterioridad.

1.3.3.1. Beneficios Directos.

Los beneficios directos son aquellos que se relacionan de forma inmediata con la ejecución del proyecto, de los cuales se obtienen los siguientes:

- Establecimiento de nuevas herramientas adaptadas al entorno para determinar las implicaciones que tienen los riesgos cibernéticos en las empresas auditadas, basándose en el marco de trabajo NIST – Cybersecurity Framework.
- Nuevas oportunidades de mejora en las organizaciones auditadas, al optimizar la evaluación de la auditoría por parte del equipo de Auditoría de TI.
- Mayor confiabilidad en las herramientas y sistemas tecnológicos de las empresas auditadas.
- Se presenta una mejora sobre las evaluaciones realizadas por el equipo Auditoría de TI.
- Mayor entendimiento en los temas relacionados con los riesgos cibernéticos, por parte del departamento de TI de la organización auditada.
- Contar con una evaluación de riesgos cibernéticos más específica, al demostrar el compromiso del área de Auditoría de TI a responder y cumplir con los cambios y necesidades actuales.

1.3.3.2. Beneficios Indirectos

Los beneficios indirectos son aquellos que obtiene la organización de forma involuntaria, de los cuales se identifican los siguientes:

- Aumenta la atracción de clientes, al brindar auditorías meticulosas que permitan la disminución de riesgos cibernéticos.
- Se da un aumento del valor agregado en los servicios brindados a los clientes, producto de la mejora en la evaluación de los riesgos cibernéticos, con ello también mejora así la imagen de HCR.

1.4. OBJETIVOS DEL TRABAJO FINAL DE GRADUACIÓN

1.4.1. Objetivo General

Proponer un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – *Cybersecurity Framework*, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR, en un periodo de 14 semanas.

1.4.2. Objetivos Específicos

1. Analizar los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR relacionados con la evaluación riesgos cibernéticos para el entendimiento de las necesidades actuales en materia de riesgos cibernéticos.

2. Determinar los componentes del marco de trabajo NIST – Cybersecurity Framework, para la elaboración de las herramientas para el área de auditoría de TI, según las necesidades de la empresa HCR

3. Elaborar un conjunto de herramientas basada en el marco de trabajo NIST – Cybersecurity Framework y en la documentación actual del área de auditoría de TI para que se cumpla con las necesidades de HCR y de sus clientes.

4. Determinar el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto.

1.5. ALCANCE

En esta sección se delimita el alcance del proyecto, donde se definen los aspectos que se realizan para cumplir con los objetivos establecidos.

El equipo de Auditoría de TI se encarga de evaluar los riesgos cibernéticos y las implicaciones que tienen estos últimos en la auditoría; sin embargo, esta evaluación se realiza de forma indagatoria, por lo tanto, no se puede confiar totalmente en la información que brinde la compañía auditada.

Es importante recalcar que el presente estudio busca definir una guía y ser un apoyo que permita obtener una mejor evaluación de los aspectos relacionados con los riesgos cibernéticos, asegurando que la valoración de los demás procesos de la auditoría tenga mayor confiabilidad.

Para lograr lo mencionado previamente, se busca elaborar una propuesta de un conjunto de herramientas para la evaluación de los riesgos cibernéticos en las auditorías financieras, basado en el marco de trabajo NIST – Cybersecurity Framework, a fin de estandarizar y mejorar la evaluación de las implicaciones que tienen los riesgos cibernéticos en las empresas auditadas.

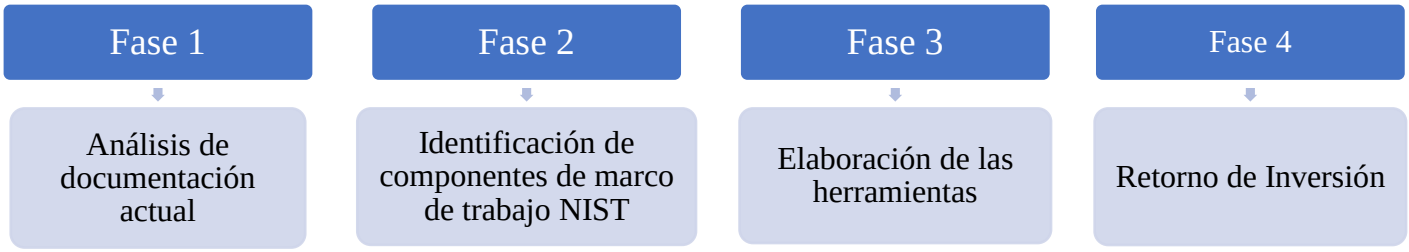
Por su parte, este marco de trabajo es una guía voluntaria, basada en estándares, pautas y prácticas existentes para que las organizaciones administren y reduzcan mejor el riesgo de ciberseguridad. Además de ayudar a las organizaciones a gestionar y reducir los riesgos, se diseñó para fomentar las comunicaciones de gestión de riesgos y ciberseguridad entre las partes interesadas de la organización, tanto internas como externas. (National Institute of Standards and Technology, 2021).

Como se menciona anteriormente, este marco de trabajo se enfoca en gestionar el riesgo de ciberseguridad y se compone de cinco funciones principales que forman parte del *Framework Core*, también se integra de los niveles de implementación (Tiers) y los perfiles del marco. Cada componente refuerza la conexión entre negocio y actividades de ciberseguridad.

Para cumplir el objetivo establecido, resulta necesario llevar a cabo una serie de actividades; para esto, en la Figura 4 se presentan las fases identificadas para el desarrollo de este proyecto:

Figura 4.

Fases del Proyecto



Fuente: Elaboración propia (2021)

A continuación, se indican las actividades por realizar en cada fase que compone el proyecto.

Fase 1: Análisis de documentación actual

En esta primera fase se efectúa un análisis de los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR, relacionados con la evaluación de riesgos cibernéticos para el entendimiento de las necesidades actuales.

Fase 2: Identificación de componentes de marco de trabajo NIST

Para la segunda fase, se procede a la identificación de los componentes del marco de trabajo NIST – Cybersecurity Framework, según las necesidades de la empresa HCR identificadas en la etapa anterior, con el fin de elaborar herramientas para el área de auditoría de TI.

Fase 3: Elaboración de las herramientas

En la tercera fase del proyecto se elabora el conjunto de herramientas basado en el marco de trabajo NIST – Cybersecurity Framework para que se cumplan las necesidades de HCR, según lo identificado en las fases anteriores.

Fase 4: Retorno de Inversión

Finalmente, en la última fase se determina el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto.

1.6. SUPUESTOS

En esta sección se describen los supuestos definidos para este proyecto, con la aclaración de que pueden variar o no llegar a darse, según sean los factores o condiciones planteadas.

- Se cuenta con el apoyo del equipo de Auditoría de TI para el cumplimiento de los objetivos y alcance del proyecto.
- Se tiene la mayor disposición para que la información solicitada sea entregada de manera oportuna y completa para la elaboración del informe.
- La metodología utilizada se encuentra actualizada y es clara.

1.7. ENTREGABLES

En esta sección se detallan los entregables considerados para este proyecto. Se toman en cuentan los productos entregables a HCR, los informes académicos y la gestión del proyecto.

1.7.1. Entregable académico

Este entregable corresponde al informe del Trabajo Final de Graduación requerido para optar por la Licenciatura en Administración de Tecnología de Información. En este se documentan todas las actividades realizadas con fines académicos, durante toda la ejecución del proyecto; se detallan secciones como: introducción, marco conceptual, desarrollo metodológico, análisis de resultados, propuesta de solución, conclusiones, recomendaciones, anexos, apéndices y referencias bibliográficas.

1.7.2. Entregables del producto

En este apartado se describen los entregables resultantes de la ejecución de este proyecto y que obtendrá el equipo de Auditoría de TI para agregar valor al área; cada entregable surge de los objetivos descritos en la sesión Objetivos del Trabajo Final de Graduación.

1.7.2.1. Informe de situación actual

En este informe se indican y describen los procedimientos y documentación actual del área de auditoría de TI, de la empresa HCR, relacionados con la evaluación de riesgos cibernéticos.

El objetivo de este entregable es tener un mejor entendimiento de las necesidades actuales en materia de riesgos cibernéticos.

1.7.2.2. Presentación de los componentes del marco de trabajo NIST

Una vez realizado el análisis de la situación actual del área de Auditoría de TI se procede a determinar los componentes del marco de trabajo NIST – Cybersecurity Framework, con el fin de elaborar las herramientas para el área de auditoría de TI, según las necesidades de la empresa HCR.

1.7.2.3. Herramientas para la evaluación de riesgos cibernéticos

Para este entregable se elaboran un conjunto de herramientas basadas en el marco de trabajo NIST – Cybersecurity Framework y en la documentación actual del área de auditoría de TI, con el fin de cumplir con las necesidades de HCR y de sus clientes.

1.7.2.4. Análisis Económico

Este entregable corresponde al análisis económico de este estudio, el cual, consiste en medir el impacto económico y la eficiencia en el uso de los recursos utilizados durante el desarrollo de este proyecto. Incluye lo siguiente:

- Estimar los costos y gastos que va a suponer la puesta en marcha del proyecto.
- Valorar los posibles ingresos para realizar un cálculo aproximado de los beneficios que puede otorgar el proyecto.

1.7.3. Gestión del proyecto

En esta sección se describen los artefactos asociados con la gestión del proyecto.

1.7.3.1. Cronograma

Se establece un cronograma con las actividades descritas anteriormente, como mecanismo de control sobre el avance de las acciones realizadas, para esto, se estima la duración de cada actividad. El cronograma se observa en APÉNDICE B. CRONOGRAMA.

1.7.3.2. Minutas

Como mecanismo de control, para el presente trabajo se hará uso de minutas para gestionar temas tratados durante reuniones y mantener evidencia sobre su desarrollo. Ver ANEXO A. PLANTILLA DE MINUTA

1.7.3.3. Gestión del Cambio

Para un correcto manejo de los entregables establecidos se requiere que los cambios se gestionen de manera adecuada, ya que ningún proyecto está exento de ellos. Para esto, se utilizará el APÉNDICE A. PLANTILLA DE SOLICITUD DE CAMBIOS para gestionar los cambios que puedan presentarse.

1.7.4. Exclusiones del proyecto

En esta sección se indican aquellos entregables o productos que no son tomados en cuenta durante el desarrollo de este trabajo, por factores como el tamaño, madurez o presupuesto de la organización.

Resulta importante aclarar que el desarrollo de este trabajo tiene como objetivo la elaboración de una propuesta que apoye la evaluación de riesgos cibernéticos y las implicaciones que tienen estos en la auditoría, por lo tanto, para el presente estudio se excluye lo siguiente:

- Propuesta para desarrollar planes de implementación para las actividades de mejora de la ciberseguridad.
- Realizar evaluaciones en alguno de los clientes de HCR

1.8. LIMITACIONES

En esta sección se describen las restricciones o limitaciones que pueden afectar el desarrollo del proyecto

- Disponibilidad de los colaboradores para atender consultas.
- Uso de material confidencial de la organización
- El apoyo que brinda la organización sobre el desarrollo del proyecto (se refiere únicamente al equipo de Auditoría de TI.)
- No se tiene acceso a los datos necesarios para definir el impacto económico de la propuesta.

CAPÍTULO II

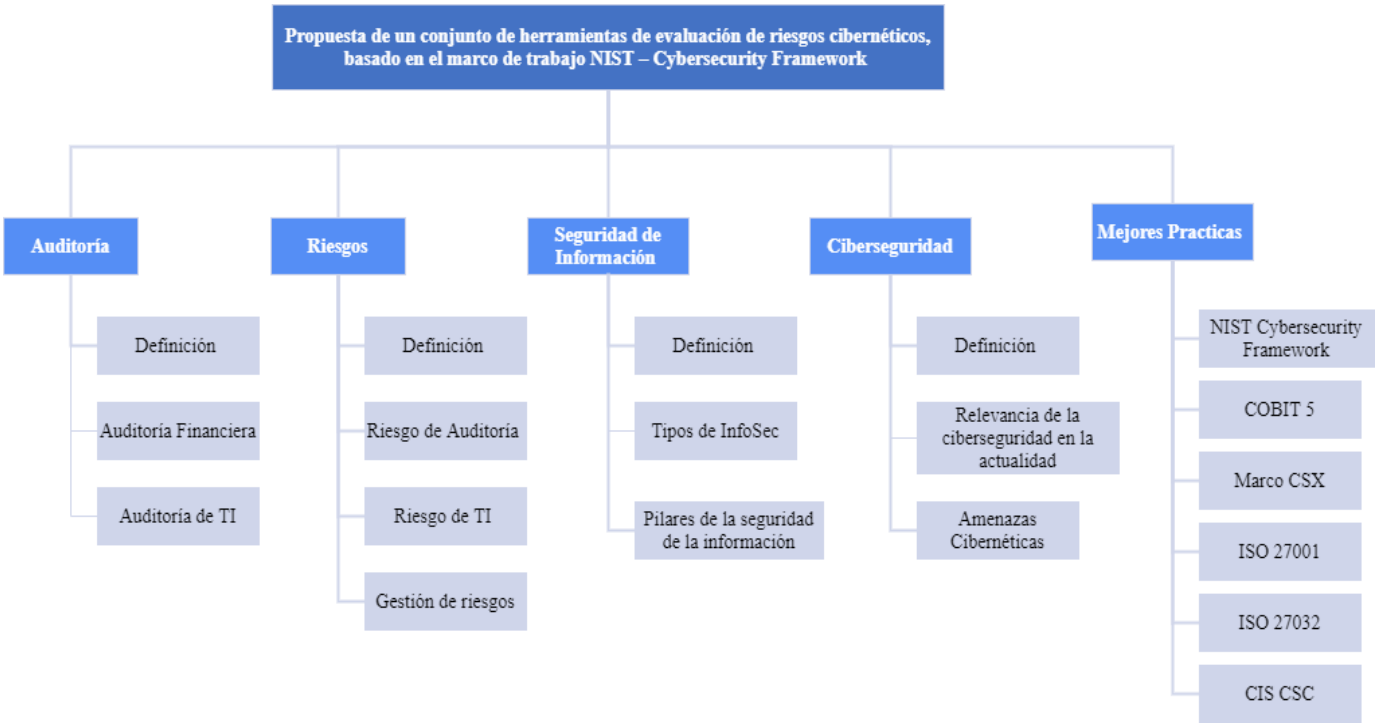
MARCO CONCEPTUAL

2. MARCO CONCEPTUAL

Para el segundo capítulo del presente documento se lleva a cabo una revisión literaria de conceptos y áreas relacionadas con el tema de estudio, cuyo fin es fundamentar y conformar la base teórica para el desarrollo del trabajo final de graduación. En la Figura 5 se muestra un mapa de conceptos que resume los temas planteados.

Figura 5.

Mapa de Conceptos



Fuente: Elaboración propia (2021)

Primeramente, se indica el concepto de auditoría; seguidamente, se tiene la definición de riesgos, seguridad de información y ciberseguridad; y, por último, se precisan términos relacionados con marcos de buenas prácticas, controles y estándares, afines con la seguridad de la información y ciberseguridad. Asimismo, se presenta el marco de trabajo NIST Cybersecurity Framework y los términos contenidos dentro de este..

2.1. AUDITORÍA

La Real Academia Española (2021), en su diccionario, define auditoría como "Revisión sistemática de una actividad o una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse." (párr. 1).

En su glosario de términos, la Asociación de Auditoría y Control de Sistemas de Información (ISACA, 2015) define a la palabra "auditoría" de la siguiente forma: "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).

A partir de las definiciones anteriores, se identifica que la auditoría se debe de respaldar de criterios que amparen el cumplimiento de reglas establecidas por órganos reguladores o mejores prácticas del mercado, por parte de la empresa u organización auditada.

Para una de las firmas de auditoría más importantes a nivel internacional, como lo es KPMG, la auditoría se debe enfocar en tres fundamentos: independencia, integridad y calidad (KPMG, 2021).

Adicionalmente, KPMG (2019) define que la auditoría debe ir más allá de una evaluación de la documentación de una empresa, donde se consideren aspectos como la cultura, sector de operación, competencia, entre otros elementos de la organización auditada. Además, se indica que la auditoría se debe enfocar en áreas claves de riesgo, basada en las características operativas del auditado.

2.1.1. Auditoría Financiera

Según Estupiñán (2012), la auditoría financiera, también conocida como auditoría contable, se trata de un método por el que se examina y analiza la información que una empresa

tiene reflejada en los estados de sus cuentas. Dicha auditoría podrá ser realizada por un auditor interno o externo a la empresa.

Tapia (2013), menciona que en una auditoría financiera el auditor revisará y emitirá una opinión, informando si los estados financieros han sido preparados en todos los aspectos materiales, de conformidad con el marco de información financiera aplicable.

Una auditoría de estados financieros es un trabajo de aseguramiento. El auditor está contratado para propósitos de expresar una opinión diseñada para mejorar el grado de confianza de los usuarios en los estados financieros. Como base para la opinión, el auditor obtiene una seguridad razonable sobre si los estados financieros en su conjunto están libres de incorrección material, debida a fraude o error. (IFAC, 2007 a, p. 12)

Asimismo, Tapia (2013) indica que el objeto de una auditoría consiste en proporcionar los elementos técnicos que puedan ser utilizados por el auditor, para obtener la información y la comprobación necesaria que fundamente su opinión profesional, sobre los aspectos de una entidad. Por su parte, la auditoría se enfoca en el análisis y estudio de los estados financieros, con la finalidad de emitir una opinión sobre dos aspectos fundamentales:

- La razonabilidad de los saldos.
- El cumplimiento con la normatividad contable aplicable.

Para emitir los informes mencionados previamente, según Tapia, (2013) el auditor financiero aplica los procedimientos de auditoría necesarios para determinar si los saldos son razonables; es decir, si están bien presentados y, libres de desviaciones relevantes que pueden ser producidas por error y/o fraude.

De acuerdo con la Norma Internacional de Auditoría (NIA) 240, en caso de detectar fraudes, el Auditor financiero se preocupa por establecer la incidencia que éstos tienen sobre

los Estados Financieros; por lo tanto, debe determinar si dichos fraudes afectan o no la razonabilidad de los saldos involucrados.

La auditoría financiera permite a las entidades detectar las áreas de mejora y alcanzar objetivos estratégicos mediante tres aspectos: la medición de resultados, el asesoramiento en gestión de riesgos y un profundo conocimiento.

2.1.2. Auditoría de TI

Las tecnologías de información son fundamentales para una serie de elementos, estos son: el éxito organizacional, la eficiencia operativa, la competitividad e incluso la supervivencia, entre otros. Para este contexto, es importante que los recursos se asignen de manera eficiente, así como que TI funcione a un nivel adecuado de desempeño y calidad para respaldar, eficazmente, el negocio y que los activos de información estén adecuadamente asegurados, de acuerdo con la tolerancia al riesgo de la organización.

Dichos activos también deben ser gobernados de manera efectiva, lo que significa que operan según lo previsto, funcionan correctamente y de una manera que cumplen con las regulaciones y estándares aplicables. Por este motivo, la auditoría de TI es de gran relevancia, ya que puede ayudar a las organizaciones a cumplir con estos objetivos.

Tapia (2013) define la auditoría informática como: la revisión y la evaluación de los controles, sistemas y procedimientos de informática de los equipos de cómputo, así como que permite la eficiencia y la seguridad en la compañía.

Cabe destacar que este tipo de auditoría participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información, que luego servirá para una adecuada toma de decisiones.

Por otro lado, Echenique (2001) en el libro Auditoría en Informática establece que la auditoría es “un examen crítico que se realiza con el objetivo de evaluar la eficacia y eficiencia de una organización y determinar acciones alternativas para la mejora de la misma” (p. 2).

Asimismo, el boletín C de normas de auditoría del Instituto Mexicano de Contadores (como se citó en Echenique, s.f) indica que la auditoría no es una actividad meramente mecánica que involucra la aplicación de ciertos procedimientos, cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los pasos que deben de seguirse y, finalmente, estimar los resultados obtenidos.

Según lo anterior, la auditoría es una ayuda que se le brinda a la organización, con el fin de evaluar oportunidades de mejora que le permitan ajustarse a lineamientos o estándares que buscan una mejor funcionalidad en sus operaciones.

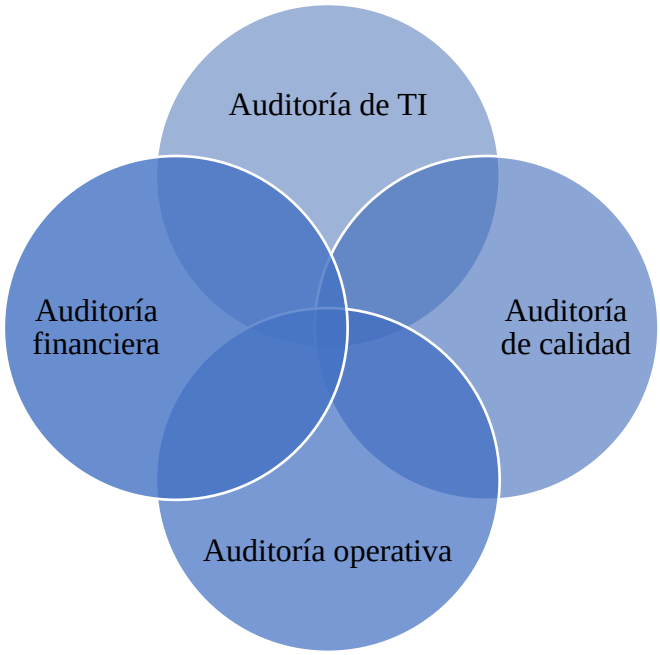
Por otro lado, Gómez Estupiñán (2014) afirma que la auditoría informática o auditoría de sistemas de información consiste en la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados y las interfaces correspondientes. (p. 40)

Stephen Gantz (2014), menciona en su libro *The Basics of IT Audit Purposes, Processes, and Practical Information,* que la auditoría de TI también es un componente de otros tipos importantes de auditoría, como se ilustra conceptualmente en la Figura 6. En la medida en que las prácticas financieras y contables de las organizaciones auditadas utilicen la tecnología de la información, las auditorías financieras deben abordar los controles basados en

la tecnología y su contribución para respaldar eficazmente los controles financieros internos. (p. 28).

Figura 6.

Auditoría de TI



Fuente: Adaptado al español de Gantz, S (2014)

Las auditorías internas y externas de TI comparten un factor en común, este consiste en la revisión de los controles internos implementados en las organizaciones para gestionar, de manera correcta, los procesos de TI. Como lo indica Gantz (2014), los controles son el elemento base para la gestión de TI, los cuales son definidos a través de estándares, guías, metodologías y marcos de trabajo que abordan los procesos de negocio, prestación de servicios y operación de los sistemas de información.

2.2. RIESGOS

La palabra riesgo es tan antigua como la propia existencia humana. Se puede decir que con ella se describe, desde el sentido común, la posibilidad de perder algo (o alguien) o de tener un resultado no deseado, negativo o peligroso. (Echemendía, 2011a, p. 471)

Igualmente, Echemendía, (2011) afirma que el riesgo de una actividad puede tener dos componentes: la posibilidad o probabilidad de que un resultado negativo ocurra y el tamaño de ese resultado. Por lo tanto, cuanto mayor sea la probabilidad y la pérdida potencial, mayor será el riesgo (p. 471).

Algunas características presentadas por Cienfuegos (2013) referentes al concepto de riesgos, son las siguientes:

- Riesgo es la probabilidad de un resultado adverso.
- Riesgo es una medida de la probabilidad y la severidad de los efectos adversos.
- Riesgo es la combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo está definido como un conjunto de escenarios, cada uno de los cuales tiene una probabilidad y una consecuencia.
- Riesgo es igual a la combinación bidimensional de eventos/consecuencias y sus incertidumbres asociadas.
- Riesgo se refiere a la incertidumbre del resultado de las acciones y eventos.

Según lo mencionado previamente, el riesgo se relaciona con el término de incertidumbre, sin embargo, de acuerdo con lo establecido por Cienfuegos (2013) este puede ser explicado como “no saber con seguridad qué va a ocurrir”, mientras que incertidumbre se refiere a “no saber ni siquiera las probabilidades de lo que va a ocurrir”. Por lo tanto, en ese

sentido, la incertidumbre sería inmedible e incalculable mientras que el riesgo se puede medir, utilizando la fórmula: riesgo = probabilidad x impacto.

2.2.1. Riesgo de Auditoría

Para Rivera (2015) el riesgo de auditoría es la posibilidad de que el auditor no detecte un error significativo que pudiera existir en la evidencia analizada, por lo tanto, el auditor no puede detectar errores, irregularidades o fraudes en las evidencias que examina, lo que impide hacer una evaluación adecuada y razonable de la situación existente. (p.12)

De acuerdo con la Guía 2202 (ISACA, 2014) existen tres componentes de riesgo en la auditoría, estos deben ser considerados antes y durante el proceso de evaluación; además, resulta importante tomar medidas preventivas que disminuyan la posibilidad de conclusiones erradas, estos riesgos se presentan a continuación en la Tabla 1.

Tabla 1.

Riesgos de auditoría

Riesgo	***Definición***
Riesgo de Control	El riesgo de que exista un error material que no se evite o detectado de forma oportuna por el sistema de control interno.
Riesgo de Detección	El riesgo de que los procedimientos sustantivos del profesional de auditoría y aseguramiento de SI no detectara un error que podría ser material, individual o en combinación con otros errores.
Riesgo Inherente	El nivel de riesgo o exposición, sin tener en cuenta las acciones que la gerencia ha tomado o ha podido tomar (ejemplo, implementar controles)

Fuente: Elaboración propia, con información de ISACA (2014)

2.2.2. Riesgos de TI

Para Kumsuprom (2010) el riesgo de TI se refiere al asociado con el uso de tecnología de información y comunicación en las organizaciones. Asimismo, los riesgos de TI resultan de la incertidumbre que rodea a las operaciones de tecnología de información, de la probabilidad de pérdidas en el negocio y de resultados negativos provenientes del entorno interno o externo (p. 16).

COBIT 5 presenta una categoría del Riesgo de TI (como se citó en Alvarado y Zumba, 2015) que considera tres tipos, los cuales se presentan en la Tabla 2

Tabla 2.

Categoria de riesgos de TI

Categoría Riesgo	***Descripción***
Riesgo de generación de valor de TI (estratégico)	Volver a enfocarse en los riesgos para consideraciones tales como cuan bien alineada está la capacidad de las TI con las estrategias de negocio y su aprovechamiento con el fin de mejorar la eficiencia o efectividad de los procesos del negocio
Riesgo en la entrega de programas y proyectos de TI (proyecto)	La administración de riesgos necesita enfocarse en la habilidad para comprender y gestionar proyectos complejos de manera que no exista una deficiente contribución de las TI para las nuevas soluciones o mejoras
Riesgo en la entrega de servicios y operaciones de TI (operacional)	Aquellos riesgos que podrían comprometer la efectividad de los servicios soportados por TI y la infraestructura de apoyo. Se debe recordar que el rendimiento y disponibilidad de los servicios de TI pueden influir directamente en el valor de la empresa llegando a reducirlo e inclusive destruirlo

Fuente: Elaboración propia, con información de Alvarado y Zumba (2015)

Asimismo, Kumsuprom (2010) indica que los riesgos de TI se pueden clasificar en estratégicos, técnicos y operativos. Por su parte, este autor propone una serie de fuentes de riesgo y factores clave para cada categoría de riesgos de TI (p. 18), en la Tabla 3 se presenta lo indicado:

Tabla 3.

Fuentes de riesgo y factores clave asociados

Tipo de riesgo TI	***Fuentes de riesgo***	***Factores clave***
Operacional y riesgos técnicos asociados	– Pérdida de activos informáticos. – Registro inexacto de datos. – Aumento del riesgo de fraude. – Pérdida o robo de datos. – Interrupción del negocio. – Violaciones de privacidad. – Brechas informáticas. – Protección insuficiente de la información o los sistemas. – Roles y responsabilidades pocos claros. – Faltas técnicas y humanas. – Vulnerabilidades de sistemas. – Fraude o eventos externos.	– Gestión de activos. – Gestión del recurso humano. – Gestión de seguridad de la información. – Gestión de tecnología de información.
Riesgo Estratégico	– Falta de estrategia. – Falta de gestión específica para riesgos de TI. – La naturaleza de la perspectiva de gestión. – Fallos en los procesos de gestión. – La responsabilidad de la auditoría y el control de las TI. – La complejidad de los sistemas.	– Estrategia organizacional. – Política organizacional. – Planificación en relación con planes estratégicos y planes operativos

Tipo de riesgo TI	*Fuentes de riesgo*	*Factores clave*
	– Plan estratégico poco claro. – Plan operativo poco claro. – Fallos en la gestión de proyectos de TI	

Fuente: Kumsuprom (2010)

2.2.3. Gestión de Riesgos

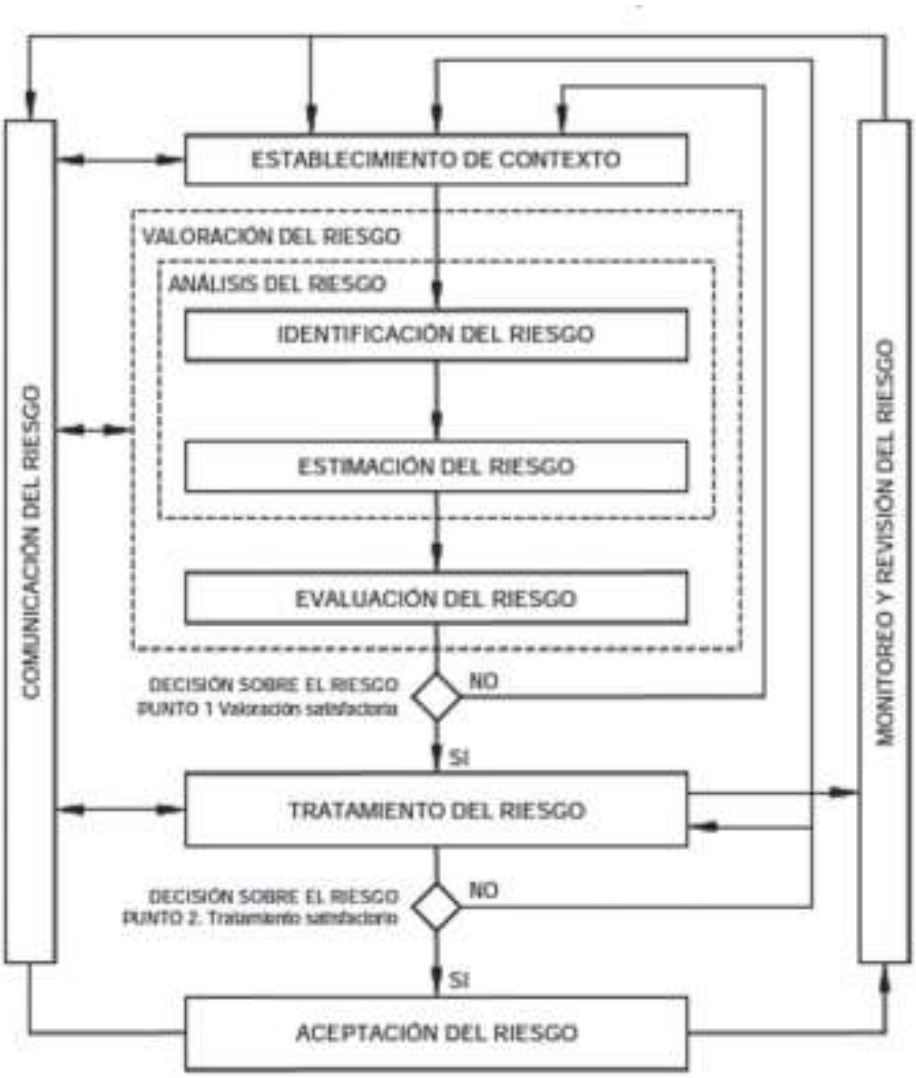
De acuerdo con Valencia et al, (2016) los riesgos de TIC han estado presentes en la evolución de los diferentes modelos de negocio y reglamentaciones que han surgido a través del tiempo, lo que pone de manifiesto que cualquier riesgo tecnológico no puede ser analizado al margen del contexto organizacional dado su efecto dominó sobre sus procesos, metas y objetivos. Esto conlleva a un proceso de articulación entre las actividades de riesgo organizacional y riesgo de TIC, y en particular, a desarrollar iniciativas de gobierno y gestión de riesgos de TI. (p. 67).

Valencia et al, (2016) agregan que la gestión de TI, por su parte, se centra en administrar e implementar la estrategia tecnológica del día a día, y su enfoque está más orientado al suministro interno de TI, definido de igual forma por la norma internacional como el sistema de controles y procesos requeridos para lograr los objetivos estratégicos, establecidos por la dirección de la organización, y está sujeta a la guía y monitoreo del gobierno de TI. (p. 67).

El proceso de gestión de riesgos de seguridad de la información, de acuerdo con la ISO/IEC 27005:2009, (como se citó en Valencia et al, 2016), se presenta en la Figura 7 (p.70).

Figura 7.

Proceso de gestión de riesgos



Fuente: Valencia et al (2016)

2.2.3.1. Aspectos clave en la gestión de riesgos de TI

Kumsuprom, (2010), describe algunos aspectos clave para la gestión de riesgos de TI, en la Tabla 4 se mencionan algunos aspectos indicados por el autor. (p. 43)

Tabla 4.

Aspectos clave para la gestión de riesgos de TI

Aspectos	***Descripción***
Gestión de recursos humanos	La gestión de riesgos de TI se encuentra inmersa en la estructura organizacional de la empresa o entidad en la que se desarrolle. Para garantizar una gestión de riesgos eficaz, la organización debe tener el conocimiento y establecer los procedimientos adecuados. Así mismo, la arquitectura organizacional debe permitir que los colaboradores desempeñen sus responsabilidades en la gestión de riesgos de TI.
Gestión de TI	La importancia de la gestión de TI para una adecuada gestión de riesgos radica en que la primera permite conocer los recursos y la capacidad de TI. Los recursos de TI están directamente ligados con el riesgo, pues pueden ser factores causantes de riesgo o bien, pueden verse afectados por la ocurrencia de riesgos. La capacidad de TI, por su parte, es un concepto al que se debe prestar atención en pro de disminuir el nivel de riesgo asociado.
Gestión de la seguridad de la información	La seguridad de la información, tanto física como lógica, es un aspecto relevante para la gestión de riesgos de TI. Permite asegurar que los datos y la información están protegidos con identificación/autenticación, autorización, confidencialidad, integridad y no repudio. Los controles de seguridad que establezca la organización son aliados importantes para la gestión de los riesgos; tanto aquellos asociados con vulnerabilidades propias de los activos como los que son causados por el hombre.
Controles para riesgos de TI	Tanto los controles que se haya establecido para los objetivos de negocio como los relacionados con los objetivos de TI, deben adaptarse al modelo de gestión de riesgos de TI, de manera que aseguren el diseño de políticas, procedimientos, prácticas y de una estructura organizacional que permita prevenir, detectar y corregir los riesgos de TI oportunamente.

Fuente: Elaboración propia con información proporcionada por Kumsuprom, (2010)

2.3. SEGURIDAD DE INFORMACIÓN

La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (SGSI, 2015)

De acuerdo con Soriano (s.f) la seguridad de la información 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. (p. 7).

Asimismo, según CISCO (2021) La seguridad de la información, a menudo denominada InfoSec, se refiere a los procesos y herramientas diseñados e implementados para proteger la información empresarial confidencial de modificaciones, interrupciones, destrucción e inspección.

Se destaca la existencia del sistema de gestión de seguridad de la información, el cual, de acuerdo con CISCO (2021) es un conjunto de pautas y procesos creados para ayudar a las organizaciones en un escenario de violación de datos. Al tener un conjunto formal de pautas, las empresas pueden minimizar el riesgo y garantizar la continuidad del trabajo, en caso de un cambio de personal, por ejemplo; el ISO 27001 es una especificación conocida para el SGSI de una empresa.

2.3.1. Tipos de InfoSec

De acuerdo con Cisco (2021) existen seis tipos de InfoSec que su aplicación conjunta ayudará a mantener un sistema de gestión de seguridad. La Tabla 5 indica los tipos de seguridad de información definidos por CISCO.

Tabla 5.

Tipos de InfoSec

Tipo	***Descripción***
Seguridad de la aplicación	La seguridad de las aplicaciones es un tema amplio que cubre las vulnerabilidades del software en las aplicaciones web y móviles y las interfaces de programación de aplicaciones (API). Estas vulnerabilidades se pueden encontrar en la autenticación o autorización de los usuarios, la integridad del código y las configuraciones, y las políticas y procedimientos maduros. Las vulnerabilidades de las aplicaciones pueden crear puntos de entrada para infracciones importantes de InfoSec. La seguridad de las aplicaciones es una parte importante de la defensa del perímetro de InfoSec.
Seguridad en la nube	La seguridad en la nube se centra en la creación y el alojamiento de aplicaciones seguras en entornos de nube y en el consumo seguro de aplicaciones en la nube de terceros. "Nube" simplemente significa que la aplicación se ejecuta en un entorno compartido. Las empresas deben asegurarse de que exista un aislamiento adecuado entre los diferentes procesos en entornos compartidos.
Criptografía	Cifrar los datos en tránsito y los datos en reposo ayuda a garantizar la confidencialidad e integridad de los datos. Las firmas digitales se utilizan comúnmente en criptografía para validar la autenticidad de los datos. La criptografía y el cifrado se han vuelto cada vez más importantes. Un buen ejemplo de uso de la criptografía es el Estándar de cifrado avanzado (AES). El AES es un algoritmo de clave simétrica que se utiliza para proteger información gubernamental clasificada.
Seguridad de la infraestructura	La seguridad de la infraestructura se ocupa de la protección de redes internas y extranet, laboratorios, centros de datos, servidores, computadoras de escritorio y dispositivos móviles.

Tipo	*Descripción*
Respuesta al incidente	La respuesta a incidentes es la función que monitorea e investiga el comportamiento potencialmente malicioso. En preparación para las infracciones, el personal de TI debe tener un plan de respuesta a incidentes para contener la amenaza y restaurar la red. Además, el plan debe crear un sistema para preservar las pruebas para el análisis forense y el posible enjuiciamiento. Estos datos pueden ayudar a prevenir más infracciones y ayudar al personal a descubrir al atacante.
Gestión de vulnerabilidades	La gestión de vulnerabilidades es el proceso de escanear un entorno en busca de puntos débiles (como software sin parches) y priorizar la corrección en función del riesgo. En muchas redes, las empresas agregan constantemente aplicaciones, usuarios, infraestructura, etc. Por esta razón, es importante escanear constantemente la red en busca de posibles vulnerabilidades. Encontrar una vulnerabilidad de antemano puede ahorrarle a su empresa los costos catastróficos de una infracción.

Fuente: Elaboración propia (2021)(2021)con información de CISCO (2019)

2.3.2. Pilares de la seguridad de la información

El Sistema de Gestión de Seguridad de la Información, según la norma ISO-27001 genera un proceso de mejora continua y de gran flexibilidad frente a los cambios que se pueden producir en la compañía, refiriéndose a los procesos de negocio y a la tecnología. El SGSI se basa en tres pilares fundamentales, según Beltran (2012) son: la confidencialidad, integridad, disponibilidad y autenticidad, los cuales se describen a continuación en la Tabla 6.

Tabla 6.

Pilares de la seguridad de información

Pilares	***Descripción***
Confidencialidad	La información es confiable cuando está protegida ante individuos o sistemas no autorizados. Garantiza que solo aquellos que tengan los derechos y privilegios de acceso puedan acceder a la información.
Integridad	La información es íntegra cuando es completa y no corrupta. Este aspecto se ve comprometido cuando no hay seguridad suficiente y expuesta a daños, destrucción o algún tipo de disrupción en su estado original.
Disponibilidad	Habilita a los usuarios, personas o sistemas autorizados a acceder información sin obstrucciones o interferencias y recibirla en el formato requerido
Autenticidad	Es la cualidad o estado de que sea genuina u original, en vez de una replicación de información. La información es auténtica cuando está en el mismo estado en el cual fue creado, almacenado o transferido.

Fuente: Elaboración propia con información de Whitman & Mattord (2017)

Por otro lado, según CISCO (2021) la seguridad de la información y la ciberseguridad a menudo se confunden. InfoSec es una parte crucial de la ciberseguridad, pero se refiere exclusivamente a los procesos diseñados para la seguridad de los datos. Por su parte, la ciberseguridad es un término más general que incluye InfoSec, el cual se detallara más adelante.

2.4. CIBERSEGURIDAD

De acuerdo con Kaspersky, (2021), el concepto de ciberseguridad hace referencia a la práctica de defender computadoras, ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. También es conocido como seguridad de tecnologías de información o seguridad electrónica de información.

De igual forma, Kaspersky (2021) menciona algunas categorías en las que se puede dividir la ciberseguridad

Tabla 7.

Categorías ciberseguridad

Seguridad de red	Es la práctica para proteger la red computacional de intrusos, ya sean hackers o malwares.
Seguridad de aplicación	Busca liberar de amenazas al software y dispositivos. Una aplicación comprometida puede acceder a los datos almacenados, los cuales estaban destinados a ser protegidos.
Seguridad de información	Protege la integridad y privacidad de los datos, ya sea en su almacenamiento o en tránsito.
Seguridad operacional	Incluye los procesos y decisiones para manejar y proteger los activos de datos. Se estudia los controles de acceso a la red y los procedimientos para determinar cómo y dónde los datos van a ser almacenados o compartidos.
Continuidad del negocio y recuperación de desastres	Define la respuesta de la organización ante un incidente de ciberseguridad o cualquier otro evento que cause la pérdida en las operaciones regulares de las organizaciones o bien, pérdida de datos.
Educación de usuario final	Busca enseñar a las personas y colaboradores de la empresa, la importancia de la seguridad de la información. Esto mediante programas de capacitación sobre virus, malwares, entre otros tipos de ataques.

Fuente: Elaboración propia con información de Kaspersky (2021)

2.4.1. Relevancia de la ciberseguridad en la actualidad

Actualmente, el mundo atraviesa un escenario en donde se vio obligado a aumentar el uso de la tecnología, con ello la palabra “Ciberseguridad” se escucha más a menudo, pero realmente ¿hasta qué punto puede afectar este término tanto a nivel personal como profesional?

El *World Economic Forum* (2020) afirma que a medida en que la pandemia del COVID -19 continúa perturbando los sistemas sociales, políticos, económicos y de salud mundial, existe otra 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

El *World Economic Forum* (2020) también menciona tres razones por las que las medidas sólidas de ciberseguridad son más importantes que nunca, las cuales se señalan a continuación:

1- **Una mayor dependencia de la infraestructura digital aumenta el costo de las fallas.**

En una pandemia de esta escala, con casos de coronavirus reportados en más de 150 países, la dependencia de las comunicaciones digitales se multiplica. Internet se ha convertido casi instantáneamente en el canal para la interacción humana efectiva y en la forma principal en que las personas trabajan, se contactan y se apoyan unos a otros. *(World Economic Forum*, 2020)

El *World Economic Forum* (2020) afirma que las empresas y las organizaciones del sector público ofrecen o imponen cada vez más políticas de "trabajo desde casa", y las interacciones sociales se están limitando rápidamente a las videollamadas, las publicaciones en las redes sociales y los programas de chat. También, muchos gobiernos están difundiendo información a través de medios digitales.

2- **El ciberdelito explota el miedo y la incertidumbre**

Los ciberdelincuentes aprovechan la debilidad humana para penetrar las defensas de los sistemas. En una situación de crisis, especialmente si es prolongada, las

personas tienden a cometer errores que no hubiesen efectuado de otro modo. En línea, cometer un error, en cuanto a un enlace en el cual se hace “clic” o en quién confía sus datos, puede costarle caro. *(World Economic Forum*, 2020).

3- Más tiempo en línea podría conducir a comportamientos más riesgosos.

El comportamiento inadvertido de riesgo en Internet aumenta a medida que se pasa más tiempo en línea. Por ejemplo, los usuarios podrían caer en el acceso "gratuito" a sitios web oscuros o programas pirateados, abriendo la puerta a posibles ataques y malware. (World Economic Forum, 2020).

2.4.2. Amenazas cibernéticas

Como se mencionó con anterioridad, el uso de la tecnología ha aumentado considerablemente, lo que ha provocado que los ataques y amenazas cibernéticas también hayan aumentado, a continuación, en la Tabla 8 se presentan los diferentes tipos de amenazas de ciberseguridad más comunes, según CISCO (2021).

Tabla 8.

Tipos de amenazas de ciberseguridad

Tipo	***Descripción***
Ransomware	Está diseñado para extorsionar a los individuos a cambio de dinero, bloqueando el acceso a los archivos o al sistema informático hasta que se pague el rescate. Pagar no garantiza que los archivos se recuperarán o que se restaurará el sistema.
Malware	Es un tipo de software diseñado para obtener acceso no autorizado o causar daños a una computadora.
Ingeniería social	Es una táctica que usan para engañar y revelar información confidencial. Pueden solicitar un pago monetario u obtener

Tipo	*Descripción*
	acceso a datos confidenciales. La ingeniería social se puede combinar con cualquiera de las amenazas enumeradas anteriormente para que sea más probable que el sujeto haga "clic" en enlaces, descargue malware o confiar en una fuente maliciosa.
Phishing	Es la práctica de enviar correos electrónicos fraudulentos que se parecen a correos electrónicos de fuentes confiables. El objetivo es robar datos confidenciales como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque y puede ayudar a protegerse a través de la educación o una solución tecnológica que filtra los correos electrónicos maliciosos.

Fuente: Elaboración propia con información de CISCO (2021).

2.5. MEJORES PRÁCTICAS

Mundialmente, existen diferentes marcos de referencia y mejores prácticas que guían el accionar de las empresas en temas de TI. Osores (2014) define una mejor práctica como: "Una forma de hacer las cosas o una serie de principios generalmente aceptados en un ámbito profesional, y que sirven para aportar valor de negocio; en el caso de las TI, a través del manejo de la información".

En este apartado se desarrollan algunas de esas mejores prácticas y marcos de referencia relacionados con el presente trabajo final de graduación

2.5.1. NIST Cybersecurity Framework

El marco de trabajo y de buenas prácticas NIST CSF (Cybersecurity Framework), es de un enfoque flexible, priorizado, repetible, basado en el desempeño y costo – efectivo, que incluye medidas de seguridad de la información y controles que los propietarios y operadores

de los procesos, datos e infraestructura crítica puedan adoptar para ayudar a identificar, evaluar y gestionar los riesgos cibernéticos. (NIST, 2018).

El marco incluye una metodología para la protección de la privacidad y protección individual de los componentes de infraestructura crítica y procesos organizacionales. Se hace referencia a una variedad de normas, directrices y prácticas existentes que evolucionan con los años y se adaptan a la tecnología existente. Además, al basarse en prácticas globales, directrices y estándares desarrollados, administrados y actualizados por la industria, las herramientas y los métodos disponibles para alcanzar los resultados del marco brindarán también los resultados esperados según las necesidades del negocio. Estas soluciones reconocerán la naturaleza global de los riesgos de seguridad de información y cibernética, de esa forma evolucionarán con los requisitos empresariales (NIST, 2018).

NIST (2018), define que, a partir de la integración de los estándares, directrices y prácticas, el marco de trabajo proporciona una serie de actividades cotidianas y relacionadas entre sí para establecer patrones comunes que se han visto emerger:

- El liderazgo ha aprendido el vocabulario del marco y puede tener conversaciones informadas sobre el riesgo de ciberseguridad.
- Las organizaciones han utilizado los niveles para determinar los óptimos de gestión de riesgos.
- Las organizaciones han concluido que el proceso de creación de perfiles es extremadamente efectivo para comprender las prácticas actuales de ciberseguridad en su entorno empresarial.
- Los perfiles y los planes de implementación se están aprovechando para priorizar y presupuestar las actividades de mejora de la ciberseguridad.

Por otro lado, el marco de ciberseguridad consta de tres componentes principales: el núcleo, los niveles de implementación y los perfiles, los cuales se detallarán posteriormente.

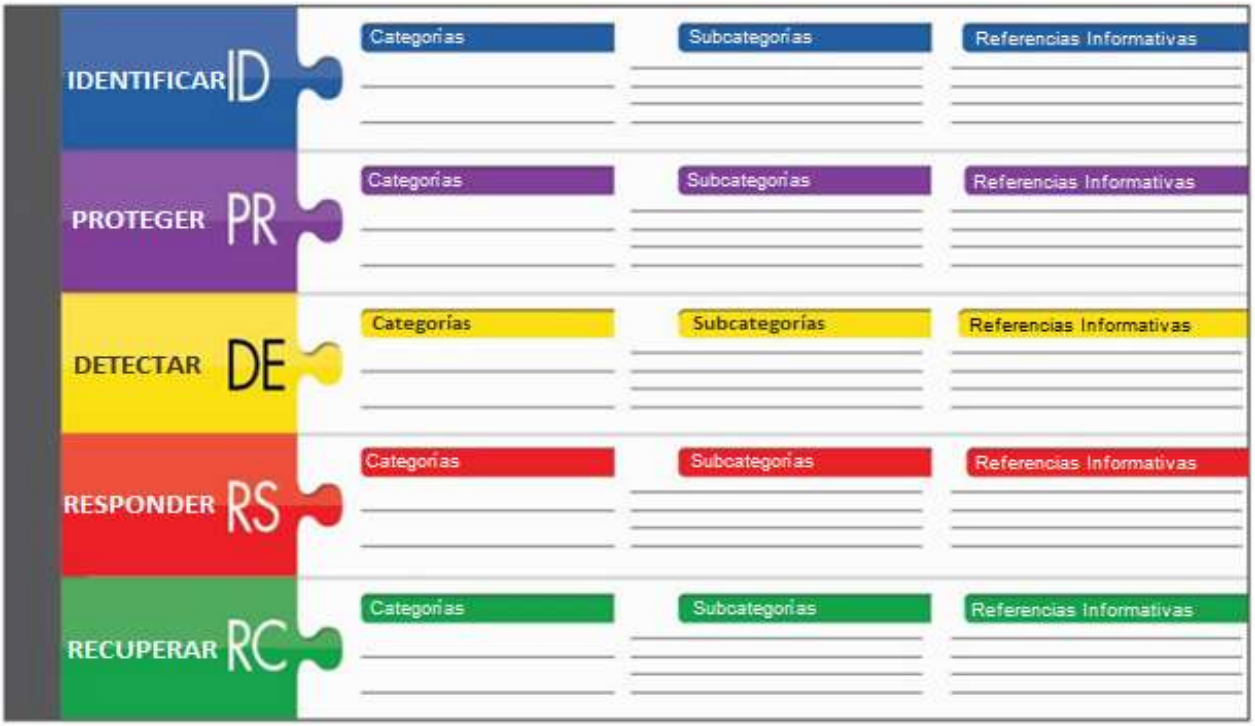
2.5.1.1. Framework Core

Según NIST, (2018) el *Framework Core* proporciona un conjunto de actividades y resultados de ciberseguridad deseados, utilizando un lenguaje común que es fácil de entender. El Core guía a las organizaciones en la gestión y reducción de sus riesgos de ciberseguridad, de manera que complementa los procesos de ciberseguridad y gestión de riesgos existentes de una organización.

El núcleo del marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El núcleo no es una lista de verificación de las acciones por realizar, este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo de seguridad cibernética. Además, el núcleo consta de cuatro elementos: funciones, categorías, subcategorías y referencias informativas, como se muestra en la Figura 8. (NIST CSF, 2018).

Figura 8.

Estructura del Núcleo del Marco



Fuente: Adaptado al español de NIST (2018).

En la Tabla 9 se describe la forma en que trabajan juntos los elementos del núcleo del Marco.

Tabla 9.

Elementos del Núcleo del Marco

Elementos	Descripción
Funciones	Organizan actividades básicas de seguridad cibernética en su nivel más alto. Las Funciones se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en seguridad cibernética.

Elementos	Descripción
Categorías	Son las subdivisiones de una función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares. Los ejemplos de categorías incluyen "Administración de activos", "Control de acceso" y "Tecnología de protección"
Subcategorías	Estas dividen aún más una categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada categoría.
Referencias Informativas	Son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría. Las referencias informativas presentadas en el Núcleo del Marco son ilustrativas y no exhaustivas. Se basan en la orientación intersectorial a la que se hace referencia con más frecuencia durante el proceso de desarrollo del Marco

Fuente: Elaboración propia, se base en NIST (2018)

De acuerdo con NIST (2018), las funciones proporcionan el nivel más alto de estructura para organizar actividades básicas de seguridad cibernética en categorías y subcategorías. Las cinco funciones son: identificar, proteger, detectar, responder y recuperar.

Estas cinco funciones fueron seleccionadas pues representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico. Además, ayudan a las organizaciones a expresar fácilmente su gestión del riesgo de ciberseguridad a un alto nivel y posibilitan decisiones de gestión de riesgos. (NIST CSF, 2018).

A continuación, se definen cada una de las funciones que componen el núcleo del marco de trabajo, así como las categorías y subcategorías que las integran.

Para facilitar el uso, a cada elemento del Núcleo del Marco se lo asigna un identificador único. Las funciones y las categorías tienen cada una un identificador alfabético único, y las subcategorías dentro de cada categoría se referencian numéricamente. En la descripción de cada función se muestran las categorías y subcategorías correspondientes.

2.5.1.1.1. Identificar

Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales. (NIST CSF, 2018).

En la Tabla 10 se muestran las categorías y subcategorías para esta función, además de indicar la referencia informativa.

Tabla 10.

Categorías y subcategorías de la función Identificar

Categoría	Subcategoría	Referencias Informativas
Administración de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados**.**	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-

Categoría	Subcategoría	Referencias Informativas
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-2:** Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
	ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
	ID.AM-4: Los sistemas de información externos están catalogados.	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
	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.	COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
	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.	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Categoría	Subcategoría	Referencias Informativas
Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes 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-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
	ID.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
	ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
	ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
	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).	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

Categoría	Subcategoría	Referencias Informativas
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	COBIT 5 APO01.03, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1
	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7
	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.	COBIT 5 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1 NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
	ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 NIST SP 800-53 Rev. 4 PM-9, PM-11

Categoría	Subcategoría	Referencias Informativas
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.	CCS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
	ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
	ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

Categoría	Subcategoría	Referencias Informativas
	ID.RA-6: Se identifican y priorizan las respuestas al riesgo	COBIT 5 APO12.05, APO13.02 NIST SP 800-53 Rev. 4 PM-4, PM-9
Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos	COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 NIST SP 800-53 Rev. 4 PM-9
	ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 NIST SP 800-53 Rev. 4 PM-9
	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	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
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	**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.	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9

Categoría	Subcategoría	Referencias Informativas
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-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	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
	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	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
	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	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1,

Categoría	Subcategoría	Referencias Informativas
	confirmar que cumplen con sus obligaciones contractuales	A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
	ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR8, IR-9

Fuente: Elaboración propia, basada en NIST (2018).

2.5.1.1.2. Proteger

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad. (NIST CSF, 2018).

En la Tabla 11 se muestran las categorías y subcategorías para esta función, además de indicar la referencia informativa.

Tabla 11.

Categorías y subcategorías de la función Proteger

Categoría	Subcategoría	Referencias informativas
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 coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**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.	CCS CSC 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2
	PR.AC-2: Se gestiona y se protege el acceso físico a los activos	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
	PR.AC-3: Se gestiona el acceso remoto.	COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

Categoría	Subcategoría	Referencias informativas
	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	CCS CSC 12, 15 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, SC-7
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.	CCS CSC 9 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-2, PM-13
	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	CCS CSC 9 COBIT 5 APO07.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	CCS CSC 9 COBIT 5 APO07.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9

Categoría	Subcategoría	Referencias informativas
	PR.AT-4: Los ejecutivos superiorescomprenden sus roles y responsabilidades	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13
	PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13
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.	CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 SC-28
	PR.DS-2: Los datos en tránsito están protegidos	CCS CSC 17 COBIT 5 APO01.06, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8
	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4. 4.3.3.3.9 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7

Categoría	Subcategoría	Referencias informativas
		NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	COBIT 5 APO13.01 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.3.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	CCS CSC 17 COBIT 5 APO01.06 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información	ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SI-7
	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción	COBIT 5 BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2

Categoría	Subcategoría	Referencias informativas
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 procedimientos para gestionar la protección de los sistemas de información y los activos.	**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)	CCS CSC 3, 10 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
	PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	COBIT 5 BAI06.01, BAI01.06 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Categoría	Subcategoría	Referencias informativas
	PR.IP-4: Se encuentran establecidos procesos de control de cambio de la configuración.	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6
	PR.IP-7: Se mejoran los procesos de protección.	COBIT 5 APO11.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
	PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA 7, SI-4

Categoría	Subcategoría	Referencias informativas
	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).	COBIT 5 DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 NIST SP 800-53 Rev. 4 CP-2, IR-8
	PR.IP-10: Se prueban los planes de respuesta y recuperación	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, des aprovisionamiento, selección del personal)	COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS Family
	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

Categoría	Subcategoría	Referencias informativas
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.	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 NIST SP 800-53 Rev. 4 MA-2, MA 3, MA-5
	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.	COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
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	CCS CSC 14 COBIT 5 APO11.04 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4
	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7

Categoría	Subcategoría	Referencias informativas
	PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
	PR.PT-4: Las redes de comunicaciones y control están protegidas.	CCS CSC 7 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, AC 17, AC-18, CP-8, SC-7

Fuente: Elaboración propia, basada en NIST (2018).

2.5.1.1.3. Detectar

Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos. (NIST CSF, 2018).

En la Tabla 12 se muestran las categorías y subcategorías para esta función, además de indicar la referencia informativa.

Tabla 12.

Categorías y subcategorías de la función Detectar

Categoría	Subcategoría	Referencias informativas
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.	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
	DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	DE.AE-4: Se determina el impacto de los eventos.	COBIT 5 APO12.06 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
	DE.AE-5: Se establecen umbrales de alerta de incidentes	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.2.3.10

Categoría	Subcategoría	Referencias informativas
		NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
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.	CCS CSC 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU 12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	ISA 62443-2-1:2009 4.3.3.3.8 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1 NIST SP 800-53 Rev. 4 AC-2, AU 12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Se detecta el código malicioso.	CCS CSC 5 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3
	DE.CM-5: Se detecta el código móvil no autorizado.	ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1 NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	COBIT 5 APO07.06 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4

Categoría	Subcategoría	Referencias informativas
	DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Se realizan escaneos de vulnerabilidades	COBIT 5 BAI03.10 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5
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	CCS CSC 5 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
	DE.DP-3: Se prueban los procesos de detección	COBIT 5 APO13.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
	DE.DP-4: Se comunica la información de la detección de eventos.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

Categoría	Subcategoría	Referencias informativas
	DE.DP-5: Los procesos de detección se mejoran continuamente.	COBIT 5 APO11.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Fuente: Elaboración propia, basada en NIST (2018).

2.5.1.1.4. Responder

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente. (NIST CSF, 2018).

En la Tabla 13 se muestran las categorías y subcategorías para esta función, además de indicar la referencia informativa.

Tabla 13.

Categorías y subcategorías de la función Responder

Categoría	Subcategoría	Referencias informativas
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.	COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

Categoría	Subcategoría	Referencias informativas
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.	COBIT 5 EDM03.02, APO01.02, APO12.03 ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
	RS.CO-2: : Los incidentes se informan de acuerdo con los criterios establecidos.	COBIT 5 DSS01.03 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta	COBIT 5 DSS03.04 ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
	RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	COBIT 5 DSS03.04 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética	COBIT 5 BAI08.04 NIST SP 800-53 Rev. 4 PM-15, SI-5

Categoría	Subcategoría	Referencias informativas
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.	COBIT 5 DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	RS.AN-2: Se comprende el impacto del incidente.	COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
	RS.AN-3: Se realizan análisis forenses	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
	RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta	COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
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.	COBIT 5 APO12.06 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
	RS.MI-2: Los incidentes son mitigados	COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4

Categoría	Subcategoría	Referencias informativas
	RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
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.	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RS.IM-2: Se actualizan las estrategias de respuesta.	COBIT 5 BAI01.13, DSS04.08 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Fuente: Elaboración propia, basada en NIST (2018).

2.5.1.1.5. Recuperar

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad. (NIST CSF, 2018).

En la Tabla 14 se muestran las categorías y subcategorías para esta función, además de indicar la referencia informativa.

Tabla 14.

Categorías y subcategorías de la función Recuperar

Categoría	Subcategoría	Referencias informativas
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.	CCS CSC 8 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
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	COBIT 5 BAI05.07 ISA 62443-2-1 4.4.3.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RC.IM-2: Se actualizan las estrategias de recuperación.	COBIT 5 BAI07.08 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
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	COBIT 5 EDM03.02
	RC.CO-2: La reputación se repara después de un incidente.	COBIT 5 MEA03.02
	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.	NIST SP 800-53 Rev. 4 CP-2, IR-4

Fuente: Elaboración propia, basada en NIST (2018).

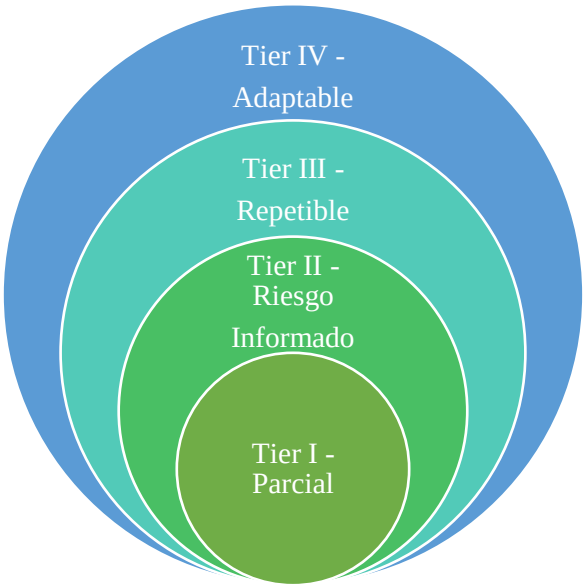
2.5.1.2. Niveles de Implementación

En cuanto a los niveles de implementación del marco, según NIST CSF, (2018), ayudan a las organizaciones al proporcionar un contexto sobre cómo una compañía ve la gestión de riesgos de ciberseguridad. Los niveles guían a las organizaciones a considerar el grado apropiado de rigor para su programa de ciberseguridad y, a menudo, se utilizan como una herramienta de comunicación para discutir el apetito por el riesgo, la prioridad de la misión y el presupuesto.

La división de los niveles de implementación del marco de trabajo se presenta en cuatro estados, cada uno con diferentes componentes de diseño y niveles de cumplimiento. La Figura 9, presenta los niveles de implementación propuestos por *NIST Cybersecurity Framework.*

Figura 9.

Niveles de Implementación de NIST Cybersecurity Framework



Fuente: Elaboración propia con información de NIST CSF (2018).

2.5.1.3. Perfiles de marco

Según NIST CSF (2018) los perfiles de marco son la alineación única de una organización de sus requisitos y objetivos organizacionales, apetito por el riesgo y recursos con los resultados deseados del núcleo del marco. Asimismo, los perfiles se utilizan principalmente para identificar y priorizar oportunidades para mejorar la ciberseguridad en una organización.

Estos perfiles indican el estado actual (Current Profile) y una proyección hacia un estado objetivo (Target Profile), esto mediante la identificación de las actividades de ciberseguridad gestionadas en las organizaciones. Para efectos de este último componente del marco de trabajo, se analizan los posibles planes de acción basados en el nivel de implementación actual (perfil actual) y la posible definición de un estado objetivo.

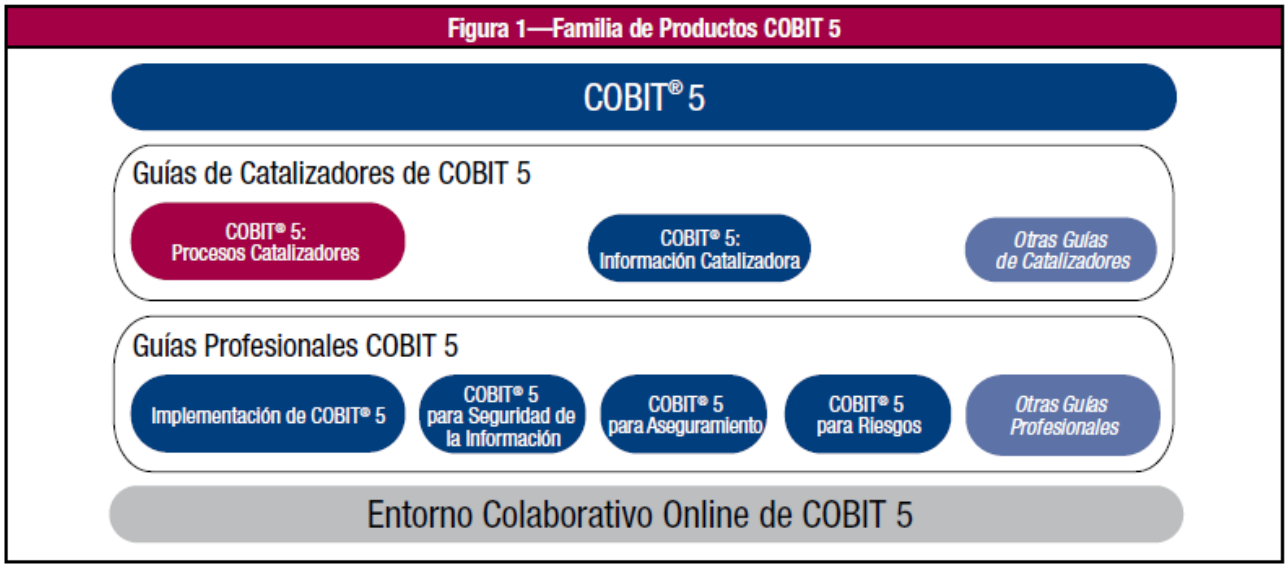
2.5.2. COBIT 5

Según lo mencionado en ISACA (2015), COBIT 5 proporciona un marco de referencia exhaustivo que asiste a las compañías para alcanzar sus objetivos de gobierno y gestión de las TI de la empresa (GEIT). Puede ser implementado de forma gradual, comenzando con un alcance pequeño y creciendo sobre la base de los éxitos obtenidos, o ser gestionado de forma holística en toda la empresa, incorporando el negocio en su totalidad y la responsabilidad de las áreas funcionales TI.

Cualquiera que sea el enfoque, COBIT ayuda a las empresas a crear un valor óptimo de las TI manteniendo un equilibrio entre la obtención de beneficios, la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 es genérico y útil para empresas de todos los tamaños: comerciales, empresas sin ánimo de lucro o administraciones públicas. La familia de productos COBIT 5 se muestra en la Figura 10. (p.11)

Figura 10.

Familia de Productos COBIT 5



Fuente: (ISACA, 2012)

Según ISACA (2012) el marco COBIT 5 se basa en cinco principios clave para GEIT:

- Principio 1: satisfacción de las Necesidades de las Partes Interesadas.
- Principio 2: cubrir la empresa de extremo a extremo, a través de los procesos de negocio.
- Principio 3: aplicar un solo marco integrado de gestión.
- Principio 4: habilitar un enfoque holístico (enfoque global de gestión).
- Principio 5: separar la gobernanza de la administración.

De forma conjunta, estos cinco principios permiten que la empresa construya un marco efectivo de gobierno y gestión que optimice la inversión, y el uso de la información y tecnología en beneficio de las partes interesadas (ISACA, 2014a, p. 15)

El marco de referencia COBIT 5 ayuda a las empresas a generar y obtener el valor óptimo para la gestión de las tecnologías de información, manteniendo así un balance entre los beneficios, riesgos y recursos. Mediante el enfoque holístico se administran y gestiona la información y tecnologías de todas las empresas que apliquen las prácticas contenidas dentro del marco. En la Figura 11 se indican los elementos necesarios para la generación del valor.

Figura 11.

Creación de Valor

Fuente: (ISACA, 2012)

Actualmente existe una versión más actualizada del marco COBIT 5, llamada COBIT 2019, sin embargo, para este proyecto no se utilizó la versión actualizada, porque el marco de trabajo *NIST-Cybersecurity Framework*, hace referencia a ciertos procesos de gestión del COBIT 5, asimismo el marco CSX que se detalla a continuación, también se basa en el marco de trabajo COBIT 5.

2.5.3. Marco CSX

Las amenazas a los sistemas de seguridad de la información no son nuevas; ISACA se constituyó hace casi cincuenta años para hacer frente a la necesidad de una fuente centralizada de información y que a su vez orientara sobre la seguridad de los sistemas informáticos.

Ahora bien, los atacantes están organizados y cuentan con un apoyo adecuado, haciendo uso de métodos sofisticados que dejan muy atrás las acciones de los hackers de principios del siglo XXI. Al mismo tiempo, la sociedad es altamente dependiente de la tecnología, y la conectividad y el intercambio de información son cada vez más vitales. Mientras que los dispositivos móviles continúan proliferando y el Internet de las Cosas sigue evolucionando, la necesidad de protegerse de los ataques de ciberseguridad es cada vez más importante. (ISACA, 2014a, p. 11)

Para ayudar a atender estas necesidades, ISACA ha desarrollado una nueva plataforma de conocimiento de seguridad y un programa profesional de ciberseguridad. El Cybersecurity Nexus (CSX), desarrollado en colaboración con expertos de ciberseguridad de las compañías líderes en todo el mundo, proporciona programas innovadores de liderazgo de pensamiento, capacitación y certificación para profesionales que impulsan la ciberseguridad hacia el futuro. Como parte del conocimiento, de las herramientas y de la orientación que CSX proporciona, ISACA ha desarrollado esta guía para la implementación del Marco para Mejorar la Ciberseguridad de la Infraestructura Crítica (el Marco de Ciberseguridad, Cybersecurity Framework, o MCS) de NIST. (ISACA, 2014a, p. 11)

Esta guía de implementación aborda los requerimientos técnicos y de negocio para aplicar el MCS (el Marco de Ciberseguridad, Cybersecurity Framework), y emplea prácticas, principios y documentos seleccionados, como los desarrollados por el IT Governance Institute2

(ITGI). El público previsto abarca desde el consejo y la dirección ejecutiva hasta los operadores técnicos y personal de mantenimiento. (ISACA, 2014a, p. 11)

Los criterios de éxito para el MCS fueron proporcionados en la sección 7 de la OE 13636. Estos requieren que el MCS: (ISACA, 2014a, p. 15)

- Ofrezca un enfoque priorizado, flexible, repetible, basado en el rendimiento y la eficiencia, que incluya medidas y controles de seguridad de la información que ayuden a los propietarios y operadores de la infraestructura crítica por identificar, evaluar y gestionar los ciberriesgos.
- Se centre en la identificación de las normas y directrices de seguridad transversales a todos los sectores que son aplicables a la infraestructura crítica.
- Identifique las áreas de mejora que deberían abordarse a través de la futura colaboración con sectores particulares y organizaciones que desarrollan normas.
- Proporcione orientación tecnológicamente neutral que permita a los sectores de infraestructura crítica beneficiarse de un mercado competitivo de productos y servicios que cumplan con las normas, metodologías, procedimientos y procesos desarrollados para hacer frente al ciberriesgos.
- Incluyan orientación para medir el rendimiento de una entidad en la implementación del Marco de Ciberseguridad.

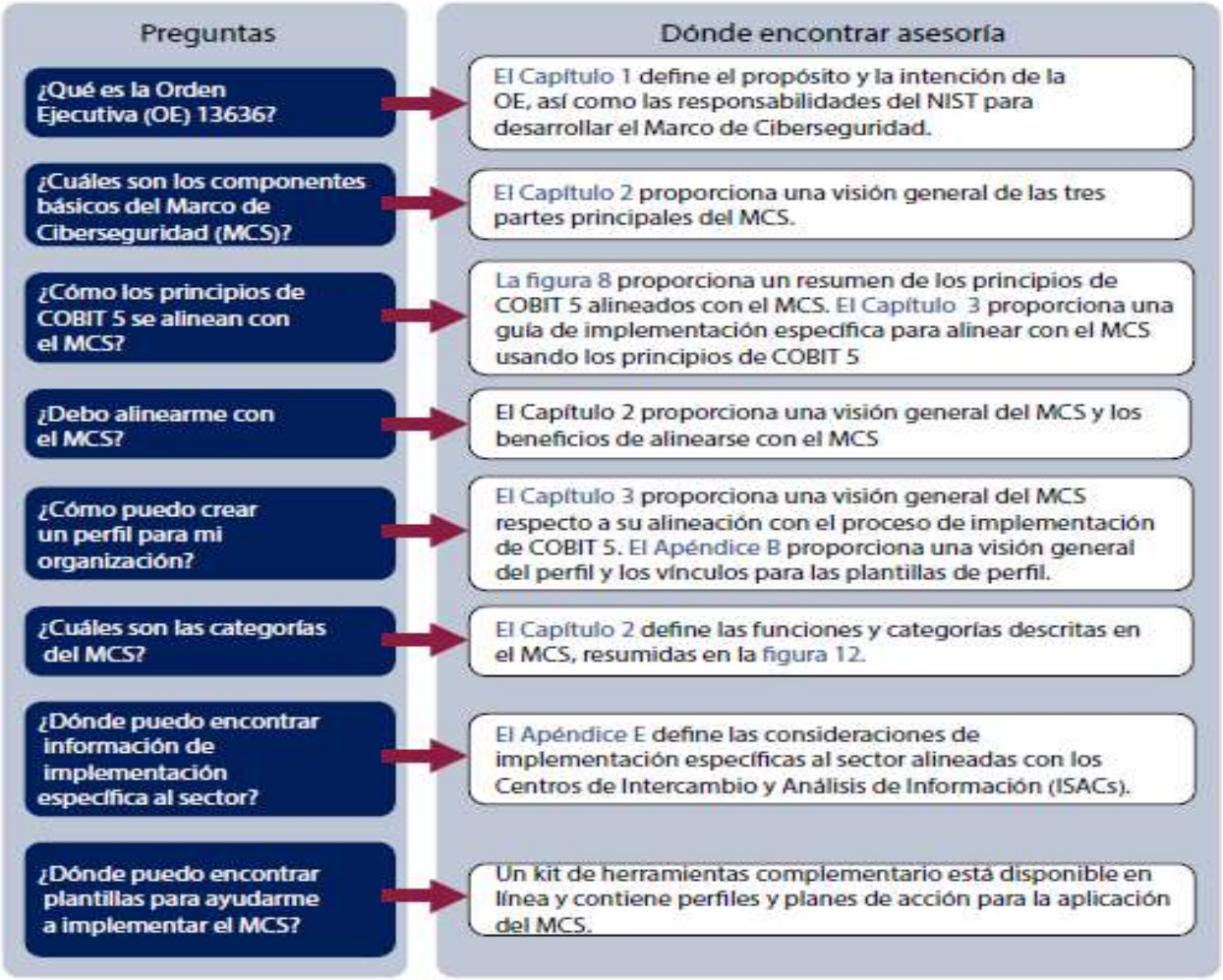
El NIST publicó la versión 1.0 del Marco de Ciberseguridad5 el 12 de febrero de 2014. El MCS 1.0 identifica tres componentes: Marco Básico, Niveles de Implementación del Marco y Perfiles del Marco. (ISACA, 2014a, p. 15).

2.5.3.1. Alcance y Enfoque

ISACA (2014) pretende ayudar a las organizaciones a través de pasos comprensibles para la implementación del MCS, mediante su enfoque y sus métodos de ISACA. La guía proporciona procesos, plantillas de ejemplo y orientación para utilizar el MCS, con el fin de identificar y alcanzar los objetivos de la empresa y la organización, para el gobierno y la gestión de TI. En la Figura 12 se presenta un resumen de la visión General de la Implementación del Marco de Ciberseguridad. (p.21)

Figura 12.

Visión General de la Implementación del Marco de Ciberseguridad



Fuente: ISACA, (2014)

Según ISACA, (2014) el MCS es un enfoque basado en el riesgo para la gestión riesgos cibernéticos y se compone de tres partes: Marco Básico, los Niveles de Implementación del Marco y los Perfiles del Marco, que se detallan a continuación (p. 24)

- El Marco Básico es un conjunto de actividades de ciberseguridad, resultados deseados y referencias aplicables que son comunes a los sectores de infraestructura crítica. Los Niveles de Implementación del Marco proveen el contexto de una organización para analizar los riesgos de ciberseguridad, así como los procesos establecidos para gestionarlos.
- Los Niveles describen el grado en el que las prácticas de gestión de riesgo de la organización exhiben las características definidas en el Marco (por ejemplo, concienciación de riesgo y amenaza, repetible y adaptativa). Los Niveles caracterizan las prácticas de la organización dentro de un rango, desde Parcial (nivel 1) hasta Adaptativo (nivel 4). El Perfil del Marco representa los resultados de acuerdo con las necesidades del negocio que una organización ha seleccionado de las Categorías y Subcategorías del Marco.
- El Perfil puede ser caracterizado como la alineación de normas, guías y prácticas con el Marco Básico, en un escenario particular de implementación. Los Perfiles pueden usarse para identificar las oportunidades de mejora de la postura de ciberseguridad, al comparar el Perfil Actual (el estado "como está") con el Perfil Objetivo (el estado "a estar").

ISACA (2014), indica que un componente importante tanto del MCS como del marco de COBIT 5 implica el gobierno y la gestión de proveedores y socios de negocio. Un único sistema de negocio puede implicar a decenas de partes interesadas externas y proveedores de servicios/cadena de suministros. Cada una de estas partes interesadas proporciona

oportunidades para cumplir con la empresa y objetivos relacionados con TI; también añaden vulnerabilidades adicionales y riesgos potenciales por considerar. La implementación del MCS utilizando procesos y principios de COBIT proporciona un lenguaje común para comunicar las necesidades y los requisitos de las partes interesadas. (p. 60)

La implementación del Marco ayudará a alinear y comunicar su postura ante el riesgo de ciberseguridad con sus socios y a comunicar las expectativas, para que la gestión de los riesgos de ciberseguridad sea consistente con las necesidades del negocio. (ISACA, 2014a, p. 101).

2.5.4. ISO 27001

Las normas ISO consisten en un conjunto de normas estandarizadas y aceptadas a nivel internacional, estas tienen como enfoque la mejora de la gestión empresarial mediante las prácticas que permite la eficiencia y eficacia de procedimientos.

Dentro del conjunto de las normas ISO, se encuentra el ISO 27001 que describe la seguridad de la información como la protección de la información de un rango amplio de amenazas, que permite asegurar la continuidad del negocio, minimizar riesgos comerciales y maximizar el retorno de las inversiones y oportunidades comerciales de las organizaciones. (ISO, 2013)

Asimismo, la norma ISO/IEC 27001 posee controles para la gestión de un sistema de seguridad de la información. Esta hace referencia a tecnologías de información, técnicas de seguridad y sistemas de gestión de la seguridad de la información, entre otros elementos. La norma ISO/IEC 27001 fue elaborada para suministrar una serie de requisitos para el establecimiento, implementación, mantenimiento y procesos de mejora continua hacia un sistema de gestión de seguridad de la información (ISO, 2013).

Según ISO (2013), la decisión de adoptar un sistema de gestión de seguridad debe ser formulada a partir de una necesidad estratégica para la organización. En este caso, el alineamiento estratégico, las necesidades y objetivos de la organización deben ser considerados para influenciar y potenciar una implementación de un sistema de gestión de seguridad de la información. Una vez analizado dicho alineamiento, es necesario conocer los requisitos de seguridad, los procesos organizacionales actuales o por implementar, el tamaño y estructura de la organización.

NIST –Cybersecurity Framework, hace referencia a ISO/IEC 27001 en su totalidad de controles, a los cuales NIST CSF se refiere en la norma ISO/IEC 27001, estos son:

1- Políticas de seguridad de la información.

2- Organización de la seguridad de la información.

3- Seguridad de los recursos humanos.

4- Gestión de activos.

5- Controles de acceso.

6- Criptografía – Cifrado y gestión de claves.

7- Seguridad física y ambiental.

8- Seguridad operacional.

9- Seguridad de las comunicaciones.

10- Adquisición, desarrollo y mantenimiento del sistema.

11- Gestión de incidentes de seguridad de la información.

12- Cumplimiento.

2.5.5. ISO 27032

La seguridad en Internet y en el ciberespacio preocupa a los seres humanos (partes interesadas). Cada vez hay más presencia en el ciberespacio, sitios web y otras aplicaciones que tienden a aprovechar este nuevo mundo virtual. (ISACA, 2012).

El ciberespacio es un entorno complejo entre los diferentes activos de información (personas, Software, internet, entre otros), generando brechas de seguridad para las organizaciones, debido a que los servicios brindados en el ciberespacio no son soportados por el mismo proveedor, regulaciones, u otros aspectos que hacen que no se tengan en cuenta las brechas de seguridad en torno a las organizaciones, exponiendo la información sensible. (Guzmán, 2019a, p.20)

La Ciberseguridad, consiste en la seguridad en el Ciberespacio, ahora bien, para abordar sus retos surge la norma ISO/IEC 27032, que define las Guías en este ámbito y se centra en dos áreas: por un lado, en cubrir los espacios o vacíos no protegidos por normas anteriores de seguridad, en este ámbito conceptual más amplio, en el que aparecen nuevos ataques y los riesgos asociados a éstos; y, por otro lado, el proceso de colaboración entre los agentes que operan en el entorno actual, en lo que se denomina comúnmente un Marco de Ciberseguridad o CSF, CyberSecurity Framework.(Internet Security Auditors, 2021)

ISO / IEC 27032 proporciona una guía para mejorar el estado de la ciberseguridad, destacando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular: (ISACA, 2012)

- Seguridad de información.
- Seguridad de la red.
- Seguridad en internet.

2.5.6. Protección de la infraestructura de información crítica (CIIP)CIS CSC

El Centro de Seguridad para Internet (*Center for Internet Security*) es una organización sin fines de lucro ante amenazas cibernéticas, que busca fortalecer las entidades públicas y privadas dentro de la comunidad de tecnologías de información. Esta es una organización global reconocida por elaborar prácticas para la seguridad de los sistemas de tecnologías de información ante ataques cibernéticos. Las guías y estándares elaborados por CIS están en constante actualización y verificados por voluntarios, miembros de una comunidad de profesionales en tecnologías de información, los cuales cuentan con amplia experiencia en este ámbito. (CIS, 2021)

Según CIS (2021), dentro de los estándares y controles que esta organización elabora se encuentran los controles CSC – Controles Críticos de Seguridad (Critical Security Controls). Estos fueron iniciados como un proyecto en el año 2009 y ha estado en constante actualización. Consiste en una guía para las mejores prácticas en seguridad computacional.

Dicha guía fue actualizada a su versión 8, la cual considera 18 acciones claves. Los controles CIS son un conjunto de acciones recomendadas para la defensa cibernética que proporcionan formas específicas y viables para detener los ataques más generalizados y peligrosos de la actualidad.

Para finalizar, *NIST – Cybersecurity Framework* hace referencia a CIS CSC en la totalidad de los controles, en la siguiente Figura 13 se muestran los controles de la última versión de CIS CSC.

Figura 13.

Controles CIS CSS

Controles CIS Versión 8	
01	Inventario y control de los activos empresariales
02	Inventario y control de activos de software
03	Protección de datos
04	Configuración segura de activos y software
05	Gestión de cuentas
06	Gestión del control de acceso
07	Gestión continua de vulnerabilidades
08	Gestión de registros de auditoría
09	Protecciones de correo electrónico y navegador web
10	Defensas contra el malware
11	Recuperación de datos
12	Gestión de la infraestructura de red
13	Supervisión y defensa de la red
14	Concientización y capacitación en materia de seguridad
15	Gestión de proveedores de servicios
16	Seguridad del software de aplicación
17	Gestión de respuesta a incidentes
18	Pruebas de penetración

Fuente: SANS (2021)

CAPÍTULO III

MARCO METODOLÓGICO

3. MARCO METODOLÓGICO

En el siguiente capítulo se describen los aspectos relacionados al marco metodológico del presente trabajo final de graduación, tales como el tipo de investigación, diseño, fuentes, sujetos de investigación, variables por estudiar, instrumentos, herramientas y técnicas de recolección de información, con el propósito de cumplir con los objetivos definidos en el capítulo 1.

3.1. TIPO DE INVESTIGACIÓN

La investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema con el resultado (o el objetivo) de ampliar su conocimiento. Esta concepción se aplica por igual a los enfoques cuantitativo, cualitativo y mixto. (Hernández et al, 2018, p. 4).

El tipo de investigación hace referencia a la ruta que el investigador sigue para realizar el estudio. Hernández et al. (2018) señalan que existen tres rutas fundamentales: la cuantitativa, la cualitativa y la mixta.

Asimismo, Hernández et al. (2014) indican que ambos enfoques emplean procesos cuidadosos, metódicos y empíricos en su esfuerzo para generar conocimiento, por lo que la definición previa de investigación se aplica a los dos por igual (p. 4).

De igual manera, Hernández et al. (2018) explican los enfoques de la siguiente manera:

- **Investigación Cuantitativa:** la ruta cuantitativa es apropiada cuando queremos estimar las magnitudes u ocurrencia de los fenómenos y probar hipótesis (p. 6).
- **Investigación Cualitativa:** las investigaciones cualitativas suelen producir preguntas antes, durante o después de la recolección y análisis de los datos. La

> acción indagatoria se mueve de manera dinámica entre los hechos y su interpretación, y resulta un proceso más bien "circular" en el que la secuencia no siempre es la misma, puede variar en cada estudio (p. 8).

- **Investigación Mixta:** los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio (p.10).

Al considerar las definiciones anteriores y por medio de un análisis concienzudo acerca del trabajo realizado, se decide que el enfoque más adecuado para desarrollar el proyecto es el **cualitativo**. Asimismo, se deben resaltar las siguientes características que plantean Hernández et al. (2018) y que se presentan en la investigación:

- El investigador plantea un problema, pero no sigue un proceso preestablecido con claridad.
- En la ruta cualitativa predomina la lógica o razonamiento inductivo, dirigiéndose de lo particular a lo general. Primero explorar y describir individualidades, para posteriormente generar teoría.
- En la mayoría de los estudios cualitativos no se prueban hipótesis,
- La investigación cualitativa resulta interpretativa, pues pretende encontrar sentido a los fenómenos y hechos en función de los significados que las personas les otorguen.
- El enfoque se basa en métodos de recolección de datos no estandarizados ni completamente predeterminados.

- Se utilizan técnicas para recolectar datos, como la observación no estructurada, entrevistas abiertas, revisión de documentos, discusión en grupo, entre otras.

3.2. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación varía según su tipo, por lo tanto, es importante mencionar que este estudio es cualitativo. Asimismo, Ñaupas et al. (2014) menciona que el diseño de investigación es una estructura que determina las variables que van a ser estudiadas y cómo deben ser controladas, manipuladas, observadas y medidas. Implica analizar e interpretar las diferencias de los resultados obtenidos y finalmente, indicar qué conclusiones se deben establecer (p. 327).

Hernández et al. (2018) plantean que existen diversos tipos de diseño cualitativo, pero las más significativas se presentan en la Tabla 15, vinculadas con preguntas de investigación e información que se proporciona en el estudio.

Tabla 15.

Diseños de la investigación cualitativa

Pregunta de investigación	Diseño, marco o abordaje	Información que proporciona
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	Descripcion y explicación de los elementos y categorías que integran al sistema social: historia y evolución, estructura (social, política, económica, etc.), interacciones, lenguaje,

Pregunta de investigación	Diseño, marco o abordaje	Información que proporciona
		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, etcétera	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, etc., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones.

Fuente: Elaboración propia basada en la Metodología de la Investigación por Hernández et al. (2018)

A partir de las explicaciones y características principales de los diseños mencionados en la Tabla 15, se determina que para el presente proyecto el diseño de investigación cualitativa que más se ajusta es la investigación/acción, ya que se pretende resolver una problemática que afecta a los colaboradores de la organización donde se desarrolla el estudio.

Hernández et al. (2018) mencionan que, durante este ciclo, el investigador recolecta continuamente datos para evaluar cada tarea realizada y el desarrollo de la implementación (p.

556). Por lo tanto, desde el contexto del presente trabajo se permite definir las condiciones y aspectos requeridos para cumplir con los objetivos del proyecto.

Según Pavlish y Pharris (2011, citados por Hernández et al., 2018) se plantean los siguientes ciclos:

- Detectar el problema de investigación, clarificarlo y diagnosticarlo (ya sea un problema social, la necesidad de un cambio, una mejora, etcétera).
- Formular un plan o programa para resolver el problema o introducir el cambio.
- Implementar el plan o programa y evaluar resultados.
- Realimentación, la cual conduce a un nuevo diagnóstico y a una nueva espiral de reflexión y acción.

3.3. FUENTES DE INVESTIGACIÓN

De acuerdo con Hernández et al. (2014), las fuentes que se consultan para recolectar datos e información a la hora de realizar una investigación se dividen en dos categorías: las fuentes primarias y las fuentes secundarias. Asimismo, señalan que la revisión de la literatura puede iniciarse directamente con el acopio de las referencias o fuentes primaria (p. 61).

A continuación, se detallan las fuentes de información primarias y secundarias.

3.3.1. Fuentes primarias

Según Gómez (2016) el término fuente primaria se refiere a la institución (pública, privada o sin fines de lucro) o, si es el caso, a la persona que recogió primero los datos y produjo la estadística (p.37).

Por otro lado, Hernández et al. (2014) explican que las referencias o fuentes primarias proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes. (p. 61).

Las fuentes primarias correspondientes a este proyecto se detallan a continuación:

- Marco de referencia de las mejores prácticas, como las siguientes:
    - NIST Cybersecurity Framework.
- Juicio de experto del equipo de trabajo del área de auditoría de TI, a través de reuniones virtuales.
- Sitios web de Internet con información relativa al tema

3.3.2. Fuentes secundarias

De acuerdo con Gómez (2016) las fuentes secundarias son las que contienen información recogida por otros (p.40).

Las fuentes secundarias utilizadas en la presente investigación funcionaron como complemento para fortalecer el estudio y analizar con mayor claridad y profundidad lo indicado en las fuentes primarias. A continuación, se plantean las fuentes secundarias consultadas:

- Bases de datos otorgadas por la biblioteca del Instituto Tecnológico de Costa Rica.
- Proyectos de graduación referentes a temas de similares.
- Documentación interna de la organización: marcos de trabajo, metodologías establecidas, guías de trabajo, etc.
- Marco de referencia de las mejores prácticas, como las siguientes:
    - Norma ISO/IEC 27001.
    - Norma ISO/IEC 27032.
    - Marco de referencia COBIT 5

- Marco CSX.
- Controles CIS CSC.

3.4. SUJETOS DE INVESTIGACIÓN

Según Mata (2021) Los sujetos de investigación son aquellas personas o grupos de personas que forman parte de los colectivos, cuyas características, opiniones, experiencias, condiciones de vida, entre otros rasgos y atributos cobran interés particular para investigaciones con enfoque cuantitativo o cualitativo. (s.p)

Por otro lado, Hernández et al. (2014) definen como "muestra" a los sujetos de investigación, es decir a las personas, procesos u otros a quienes se les aplican las técnicas o instrumentos de evaluación para recolectar información.

Se debe resaltar que según Neuman (2009, citado por Hernández et al., 2014) en la indagación cualitativa el tamaño de muestra no se fija a priori (antes de la recolección de los datos), sino que se establece un tipo de unidad de análisis y a veces se perfila un número aproximado de casos, pero la muestra final se conoce cuando las nuevas unidades que se añaden ya no aportan información o datos novedosos (p. 385).

Para la investigación realizada, los sujetos de investigación corresponden a colaboradores del área de auditoría de TI de la empresa HCR, los cuales se definen en la Tabla 16 a continuación:

Tabla 16.

Sujetos de investigación

Puesto	Rol en la empresa	Cantidad
Gerente	Debe contar con al menos 6 años de experiencia, algunas de sus responsabilidades corresponden a las siguientes: • Planificar y crear la estrategia de la auditoría, identificación de riesgos y diseño de las pruebas de control. • Administrar la ejecución de los proyectos a cargo de acuerdo con las normas de la firma con respecto a calidad y servicio al cliente. • Controlar financieramente los presupuestos de los proyectos a cargo. • Supervisar el personal a cargo en los proyectos, respecto a la calidad y ejecución de los proyecto a cargo.	1
Encargado	Profesional con participación en el proceso de planificación de la auditoría y realizar evaluaciones de control interno en los clientes, debe contar con al menos dos años de experiencia en labores de auditoría externa o interna.	1
Asistente II	Responsable de realizar evaluaciones de control interno en los clientes, analizando el diseño e implementación del mismo, con el fin de determinar la eficacia operativa. Cuenta con al menos un año de experiencia en labores de auditoría.	1

Puesto	Rol en la empresa	Cantidad
Asistente I	Responsable de realizar evaluaciones de control interno en los clientes, analizando el diseño e implementación del mismo, con el fin de determinar la eficacia operativa.	3

Fuente: Elaboración propia, con información proporcionada por la empresa.(2021)

3.5. VARIABLES DE LA INVESTIGACIÓN

Según Hernández (2014), la variable es una propiedad que puede fluctuar y cuya variación es susceptible a medirse u observarse. Asimismo, las variables pueden ser encontradas e incluidas indirectamente en cada objetivo específico de la investigación porque identifican los elementos que se desean estudiar.

Seguidamente, se plantea que al momento de estructurar las variables se tomen en cuenta los siguientes elementos (Ulate y Vargas, 2014):

- ***Objetivos específicos***: los definidos en la sección Objetivos Específicos de este proyecto.
- ***Variables de estudio:*** el aspecto por medir.
- ***Definición conceptual:*** definición del significado de la variable en la investigación.
- ***Indicadores:*** lo que se desea conocer de la variable.
- ***Definición instrumental:*** los instrumentos que se utilizarán para obtener la información.

En la Tabla 17 describe las variables del estudio, según los objetivos específicos definidos para el presente proyecto.

Tabla 17.

Variables de investigación

Objetivo específico	Variables de investigación	Definición conceptual	Indicadores	Definición instrumental
Analizar los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR relacionados con la evaluación riesgos cibernéticos para el entendimiento de las necesidades actuales en materia de riesgos cibernéticos.	Análisis de la situación actual de la empresa relacionada con la evaluación de riesgos cibernéticos	Documentación de apoyo que actualmente la empresa tiene para realizar la evaluación de los riesgos cibernéticos en los proyectos de auditoría.	Cantidad de documentación que se utiliza actualmente en la evaluación de riesgos cibernéticos	• Encuesta • Revisión documental
Identificar los componentes del marco de trabajo NIST – Cybersecurity Framework, según las necesidades de la empresa HCR para la elaboración de las	Recomendaciones a la situación y componentes por incluir en la elaboración de las herramientas	Oportunidades de mejora encontradas en el análisis de la situación actual y seleccionar los componentes del marco de trabajo NIST faltantes para	Listado de oportunidades de mejora de la documentación y herramientas actuales	• Entrevista • Revisión documental

Objetivo específico	Variables de investigación	Definición conceptual	Indicadores	Definición instrumental
herramientas para el área de auditoría de TI.		una evaluación de riesgos cibernéticos más completa.		
Elaborar un conjunto de herramientas basada en el marco de trabajo NIST – Cybersecurity Framework para que se cumplan las necesidades de HCR y de sus clientes	Herramientas para la evaluación de riesgos cibernéticos basado en el marco de trabajo NIST- Cybersecurity Framework	Construcción de las herramientas basada en el marco de trabajo NIST – Cybersecurity Framework para la evaluación de riesgos cibernéticos en diferentes proyectos.	Diseño de herramientas	• Entrevistas • Revisión documental
Determinar el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto	Retorno de inversión derivados del proyecto.	Se realizan los cálculos del retorno de inversión del presente proyecto.	Cálculo del retorno de inversión	• Revisión documental

Fuente: Elaboración propia (2021)

3.6. INSTRUMENTOS DE INVESTIGACIÓN

Los instrumentos de investigación son un conjunto de procedimientos que le permiten al investigador establecer una relación con el sujeto de estudio, por otra parte, estos constituyen mecanismos para recolectar información. Para la recolección de los datos de la investigación se utilizaron las siguientes técnicas: la revisión de documental, la entrevista y la encuesta.

3.6.1. Entrevista

Hernández et al. (2014) definen la entrevista como una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) (p. 403).

Según Ryen (2013) y Grinnell y Unrau (2011, citados por Hernández et al., 2014) las entrevistas se dividen en estructuradas, semiestructuradas y no estructuradas o abiertas. En las primeras, el entrevistador realiza su labor siguiendo una guía de preguntas específicas y se sujeta exclusivamente a ésta (el instrumento prescribe qué cuestiones se preguntarán y en qué orden). Seguidamente las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir interrogantes adicionales para precisar conceptos u obtener más información. Finalmente, las entrevistas abiertas se fundamentan en una guía general de contenido y el entrevistador posee toda la flexibilidad para manejarla (p. 403).

En la investigación realizada se utilizaron entrevistas semiestructuradas y estructuradas, en el APÉNDICE D. PLANTILLA ENTREVISTA SITUACIÓN ACTUAL se observa la plantilla para documentar la entrevista de la situación actual de la empresa HCR, y en el APÉNDICE E. PLANTILLA DE ENTREVISTA DE HERRAMIENTAS la plantilla para documentar la entrevista referente a lo esperado por el presente proyecto.

3.6.2. Revisión documental

De acuerdo con Hernández et al. (2014) los documentos son una fuente de datos muy importante al momento de realizar una investigación cualitativa, ya que pueden ayudar a entender el fenómeno central que se está estudiando (p. 396).

La revisión documental, según Hernández et al. (2014) incluye la consulta de libros, revistas, artículos, documentos de la organización, imágenes, grabaciones de audio y video, bitácoras, cartas, artefactos artísticos como, por ejemplo, vasijas, esculturas, grafitis, entre otros.

Algunos de los documentos consultados para realizar la investigación fueron libros y artículos sobre la temática del proyecto, imágenes, páginas web, documentación de sistemas de información, diversos marcos de referencia, estándares, marcos de trabajo, entre otras mejores prácticas y normativas. Se utilizó el APÉNDICE F. PLANTILLA PARA DOCUMENTAR LA REVISIÓN DOCUMENTAL como plantilla para describir las fuentes consultadas.

3.6.3. Encuestas

Según Ulate y Vargas (2014), la encuesta es la técnica utilizada para conocer la opinión de las personas sobre una situación o un problema (p. 73).

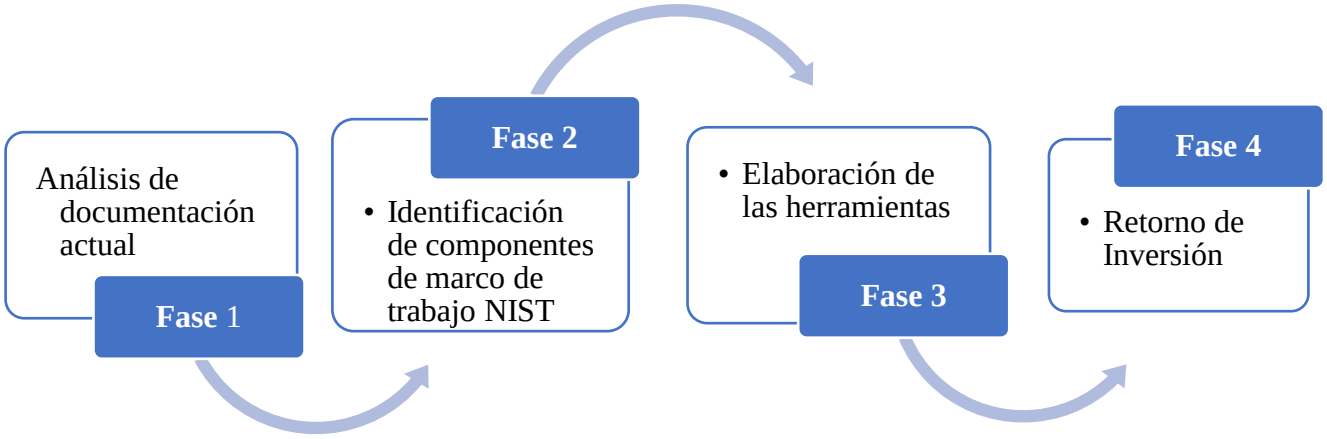
Para el presente proyecto se realizó una encuesta para conocer la situación actual del área de Auditoría de TI referente a la forma en la cual se evalúan los riesgos cibernéticos; por su parte, en el APÉNDICE C. PLANTILLA ENCUESTA SITUACIÓN ACTUAL se encuentra la plantilla del instrumento.

3.7. PROCEDIMIENTO METODOLÓGICO DE LA INVESTIGACIÓN

Con el fin de alcanzar los objetivos establecidos, con la ayuda de las técnicas e instrumentos mencionados, se determinaron las etapas y actividades por seguir. A continuación, en la Figura 14 se definen las fases que se ejecutaran en el proyecto.

Figura 14.

Fases de la metodología



Fuente: Elaboración propia (2021)

A continuación, se indican las actividades por realizar en cada fase mencionada previamente:

3.7.1. Fase 1: Análisis de documentación actual

En esta primera fase se efectuó un análisis de los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR, relacionados con la evaluación de riesgos cibernéticos para el entendimiento de las necesidades actuales en cuanto a estos.

Se desarrollaron actividades de recolección y análisis de información que permitan comprender la forma en que trabaja el área de auditoría de TI, específicamente en la evaluación

de riesgos cibernéticos, además de la documentación y herramientas que tienen a disposición para realizar dicha evaluación.

Para esta fase se detallan las siguientes actividades:

- Recolección y análisis de información interna sobre la evaluación de riesgos cibernéticos.
- Aplicación de una encuesta a los colaboradores para análisis de información.

Estas actividades se basaron en las necesidades de HCR específicamente del área de auditoría de TI y lo que se desea resolver mediante la elaboración de esta propuesta, el resultado de estas actividades se observa en el Capítulo 4: ANÁLISIS DE RESULTADOS.

3.7.2. Fase 2: Identificación de componentes de marco de trabajo NIST

Para la segunda fase, se procedió a la identificación de los componentes del marco de trabajo NIST – Cybersecurity Framework, según las necesidades de la empresa HCR específicamente del área de auditoría de TI, que se identificaron en la etapa anterior para la elaboración de las herramientas.

Con el análisis realizado en la fase anterior, se buscó investigar los componentes del marco de trabajo NIST que se ajusten a las necesidades del equipo y de los clientes. A continuación, se detallan las actividades correspondientes a esta fase:

- Análisis de la información recolectada en la fase anterior, mediante la aplicación de los instrumentos de investigación definidos previamente. Dicho análisis se puede observar en el capítulo 4 ANÁLISIS DE RESULTADOS
- Una vez realizado el análisis de la información recolectada con el equipo de Auditoría de TI de HCR, se procedió mediante la revisión documental a identificar

los componentes del marco de trabajo NIST, que más se adecuen a las necesidades del área de Auditoría de TI de la empresa HCR. De igual forma, esta actividad se puede visualizar en el Capítulo 4 ANÁLISIS DE RESULTADOS.

3.7.3. Fase 3: Elaboración de las herramientas

En la tercera fase del proyecto, se elaboró el conjunto de herramientas basadas en el marco de trabajo NIST – Cybersecurity Framework que cumplan con las necesidades de HCR y de sus clientes, según lo identificado en las fases anteriores.

Para esta fase se detallan las siguientes actividades:

- Una vez utilizadas las fuentes de información y los resultados de los instrumentos de investigación aplicados en las fases anteriores se identificaron una serie de herramientas que ayudaron a solucionar el problema planteado y con esto, satisfacer las necesidades del área de Auditoría de TI.
- Después de identificar las herramientas adecuadas para satisfacer las necesidades del área se realizó la construcción de dichas herramientas.

El resultado de estas actividades se puede observar en el Capítulo 5 PROPUESTA DE SOLUCIÓN.

3.7.4. Fase 4: Retorno de Inversión

Por último, en la última fase se determinó el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto.

Las actividades que se realizaran en esta fase corresponden a las siguientes:

- Se revisaron los costos y datos del mercado para el cálculo del retorno de inversión.

- Según los costos del mercado se procedió a calcular el ROI (retorno de inversión) del presente proyecto.
- Asimismo, se realizó el cálculo del valor actual neto y la tasa interna de retorno.

El resultado de estas actividades se puede observar en el Capítulo 5: PROPUESTA DE SOLUCIÓN.

3.8. OPERALIZACIÓN DEL MARCO METODOLÓGICO

A continuación, en la Tabla 18 se muestra un resumen del procedimiento metodológico y su interacción con los demás elementos definidos en la metodología que se siguió para realizar la investigación.

Tabla 18.

Resumen del procedimiento metodológico

Objetivo específico	Fase	Variable	Indicadores	Instrumento	Sujeto
Analizar los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR relacionados con la evaluación riesgos cibernéticos para el entendimiento de las necesidades actuales en materia de riesgos cibernéticos.	Fase 1: Análisis de documentación actual	Análisis de la situación actual de la empresa relacionada con la evaluación de riesgos cibernéticos	• Cantidad de documentación que se utiliza actualmente en la evaluación de riesgos cibernéticos	• Entrevista • Encuesta • Revisión documental	Gerente Encargado Asistente I y II
Determinar los componentes del marco de trabajo NIST – Cybersecurity Framework, para la elaboración de las herramientas para el área de auditoría de TI, según las necesidades de la empresa HCR	Fase 2: Identificación de componentes de marco de trabajo NIST	Recomendaciones a la situación y componentes por incluir en la elaboración de las herramientas	• Listado de oportunidades de mejora de la documentación y herramientas actuales	• Entrevista • Revisión documental	Gerente Encargado Asistente I y II

Objetivo específico	Fase	Variable	Indicadores	Instrumento	Sujeto
Elaborar un conjunto de herramientas basada en el marco de trabajo NIST – Cybersecurity Framework y en la documentación actual del área de auditoría de TI para que se cumplan las necesidades de HCR y de sus clientes	Fase 3: Elaboración de las herramientas	Herramientas para la evaluación de riesgos cibernéticos basado en el marco de trabajo NIST-Cybersecurity Framework	• Diseño de herramientas	• Entrevistas • Revisión documental	Gerente Encargado
Determinar el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto	Fase 4: Retorno de Inversión	Retorno de inversión derivados del proyecto.	• Cálculo del retorno de inversión	• Revisión documental	No aplica

Fuente: Elaboración propia (2021)

CAPÍTULO IV

ANÁLISIS DE RESULTADO

4. ANÁLISIS DE RESULTADOS

En el presente capítulo se analizan los resultados de la aplicación de los instrumentos de investigación descritos en el apartado anterior.

Cabe destacar que se llevó a cabo un análisis por cada una de las fases planteadas en el apartado 3.7 Procedimiento metodológico de la Investigación; a continuación, se presenta.

4.1. FASE 1: ANÁLISIS DE DOCUMENTACIÓN ACTUAL

En esta primera fase se realizó un análisis de los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR, relacionados con la evaluación riesgos cibernéticos para el entendimiento de las necesidades actuales. Esto se efectuó mediante la aplicación de los instrumentos definidos en el capítulo anterior

A continuación, se describen los datos obtenidos al aplicar, específicamente los instrumentos sobre la situación actual.

4.1.1. Procedimientos y documentación utilizada

Como se describió en el "Planteamiento del problema" del presente proyecto, el área de Auditoría de TI es responsable de auditar el entorno de TI de las organizaciones como apoyo de la auditoría financiera, asimismo como parte de sus responsabilidades se destaca la revisión de los riesgos cibernéticos, esta se da de forma indagatoria y no cuenta con un estándar o herramientas establecidas para tomar de referencia.

Sin embargo, HCR posee una metodología propia que establece las reglas generales en el desarrollo de las auditorías, además de contar con diferentes guías que funcionan como alertas que complementan y abordan las revisiones de los estándares de auditoría aplicables y acciones adicionales que no se han incluido en el marco de referencia.

Entre estas alertas se encuentran las consideraciones sobre riesgos cibernéticos, se indica que para la evaluación de dichos riesgos se debe tomar en cuenta lo siguiente: (Ver APÉNDICE P. BITÁCORA DE REVISIÓN DOCUMENTAL)

- Considerar que, si un incidente de ciberseguridad ocurre, este, impactaría el enfoque de auditoría.
- Consultar con las organizaciones qué se debe de hacer para obtener una comprensión del proceso de evaluación de riesgos cibernéticos de la administración.
- Ejemplos de algunos de los procesos de la entidad que se pueden considerar al comprender la evaluación de riesgos cibernéticos de la administración.
- Procedimientos que se pueden realizar si un incidente de ciberseguridad surge durante el curso de la auditoría.
- Un documento de trabajo se utiliza en todos los flujos de trabajo, para las consideraciones de riesgos cibernéticos.

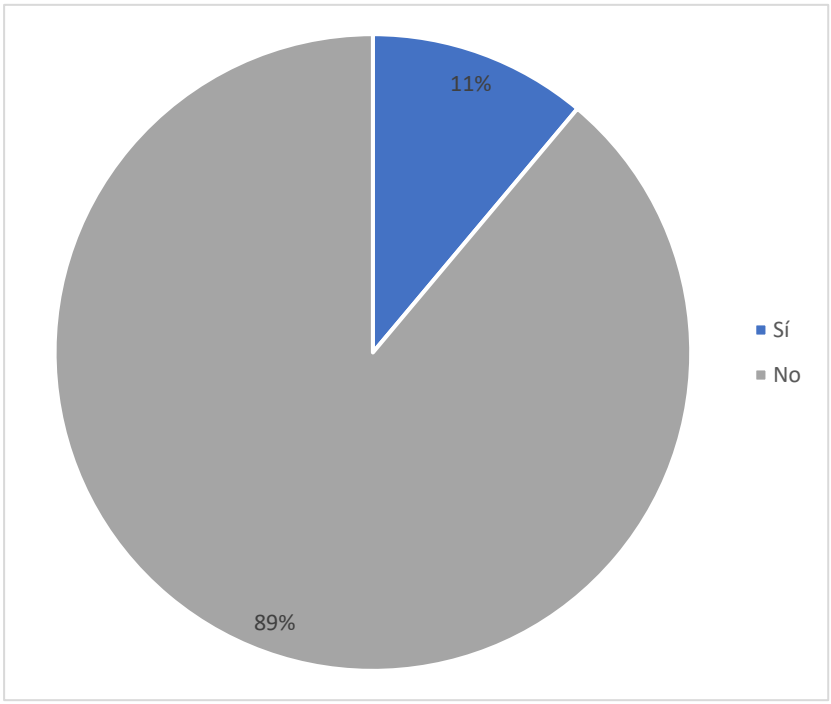
El documento de trabajo sobre consideraciones de riesgos cibernéticos mencionado previamente, ayuda al equipo de Auditoría de TI a documentar lo siguiente:

- Consultas sobre la evaluación de riesgos cibernéticos de la entidad, las consideraciones de la administración sobre el impacto potencial que esos riesgos plantean a los estados financieros.
- Cuando se ha producido un incidente de ciberseguridad o si el equipo encargado identifica riesgos cibernéticos, qué procedimientos se realizaron para evaluar el impacto del incidente en la auditoría y sobre los estados financieros de la entidad.

Según la encuesta realizada a la totalidad del equipo de Auditoría de TI, ubicada en el APÉNDICE G. RESPUESTA DE LA ENCUESTA SOBRE LA SITUACIÓN ACTUAL, se concluye que un 89% de los participantes indica que la metodología y las guías actuales no son lo suficientemente claras para la evaluación de los riesgos cibernéticos, se plantea en la Figura 15.

Figura 15.

Existe claridad en las guías

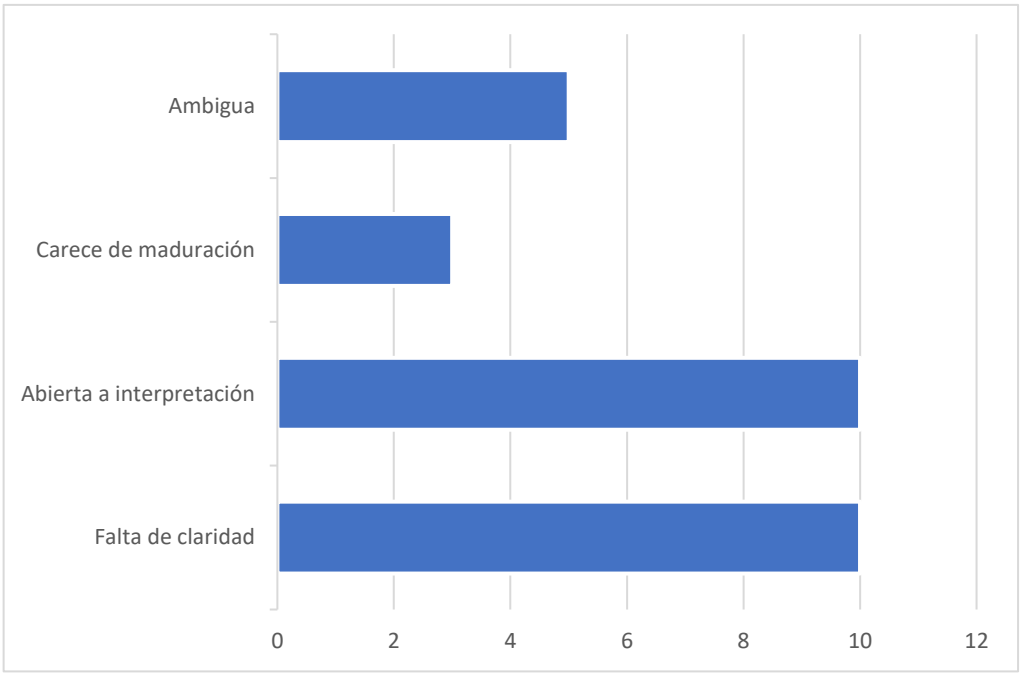


Fuente: Elaboración propia (2021)

Asimismo, algunas de las opiniones que brindan las personas encuestadas sobre estas guías se refieren a que están abiertas a interpretaciones, carecen de maduración y son ambiguas, al obtener únicamente un entendimiento superficial sobre la evaluación de riesgos cibernéticos. En la Figura 16, se muestran las opiniones mencionadas previamente.

Figura 16.

Opinión sobre guía actual



Fuente: Elaboración propia (2021)

Seguidamente, se efectuó una entrevista a diferentes miembros del equipo, entre estos el gerente del área, encargado, asistente II y asistente, dicho instrumento se observa en el APÉNDICE H. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL GERENTE DEL ÁREA DE AUDITORÍA DE TI, APÉNDICE I. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ENCARGADO DEL ÁREA DE AUDITORÍA DE TI, APÉNDICE J. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ASISTENTE II DEL ÁREA DE AUDITORÍA DE TI y APÉNDICE K. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ASISTENTE I DEL ÁREA DE AUDITORÍA DE TI. A raíz de los resultados obtenidos, se confirmó que la guía empleada en la actualidad no es suficiente para realizar la evaluación de riesgos cibernéticos, sobre todo al considerar que ningún miembro del equipo de Auditoría de TI tiene conocimientos profundos sobre el tema de ciberseguridad.

De igual forma, mediante la aplicación de la encuesta, en el APÉNDICE G. RESPUESTA DE LA ENCUESTA SOBRE LA SITUACIÓN ACTUAL y en las entrevistas al equipo de Auditoría de TI, en el APÉNDICE H. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL GERENTE DEL ÁREA DE AUDITORÍA DE TI, APÉNDICE I. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ENCARGADO DEL ÁREA DE AUDITORÍA DE TI, APÉNDICE J. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ASISTENTE II DEL ÁREA DE AUDITORÍA DE TI y APÉNDICE K. RESPUESTA ENTREVISTA SOBRE SITUACIÓN ACTUAL ASISTENTE I DEL ÁREA DE AUDITORÍA DE TI, se indica la importancia actual de realizar una adecuada evaluación de riesgos cibernéticos con los clientes, así como la necesidad de un conjunto de herramientas que apoye esta evaluación, pues sería de gran utilidad para brindar una base sólida, sustentada y estandarizada.

4.1.2. Necesidades actuales

A partir de la aplicación de la encuesta, las entrevistas realizadas al área de Auditoría de TI y la revisión documental, se pretende conocer las necesidades actuales del equipo, en materia de riesgos cibernéticos.

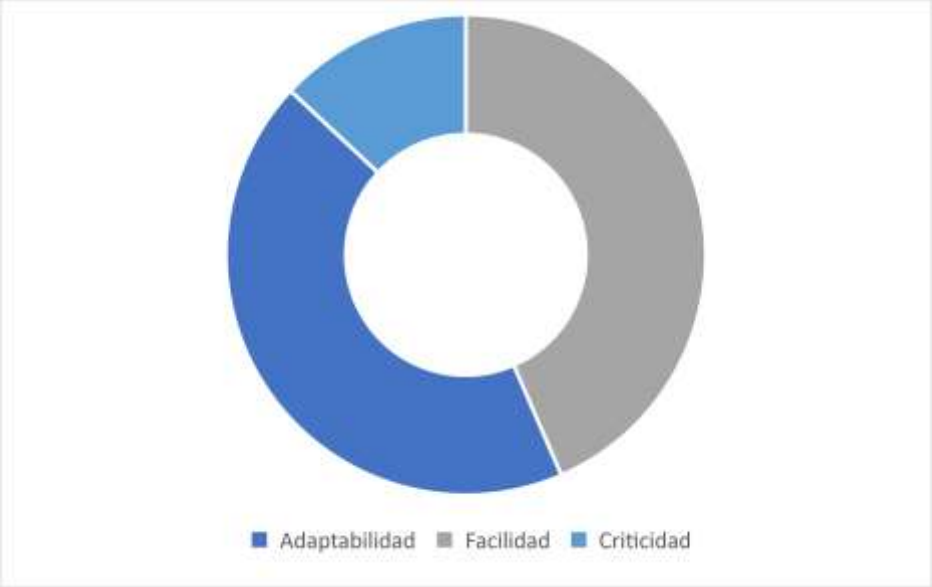
Según las entrevistas y la revisión documental de la guía utilizada para esta evaluación se obtiene lo siguiente:

4.1.2.1. Aspectos estratégicos

Para la elaboración del conjunto de herramientas que apoyan la evaluación de riesgos cibernéticos es importante tomar en cuenta aspectos estratégicos, que también los miembros del equipo consideran relevantes para la construcción de dichas herramientas, estos son: la adaptabilidad, facilidad y criticidad, como se representa en la Figura 17

Figura 17.

Aspectos estratégicos



Fuente: Elaboración propia (2021)

4.1.2.1.1. Adaptabilidad

Mediante la entrevista realizada a la encargada del área de Auditoría de TI (2021), se indica que las herramientas deberían adaptarse a los diferentes clientes, sin importar las actividades a las que se dedica, el tamaño de la empresa y la complejidad de sus procesos.

4.1.2.1.2. Facilidad

La facilidad de la herramienta es un aspecto estratégico por considerar para la elaboración de las herramientas, como indica la encargada y los asistentes I y II del área de Auditoría de TI (2021), ya que, al pretender que sean una ayuda para la evaluación de riesgos cibernéticos es de gran importancia que sea fácil de entender y utilizar por todos los miembros del equipo.

4.1.2.1.3. Criticidad

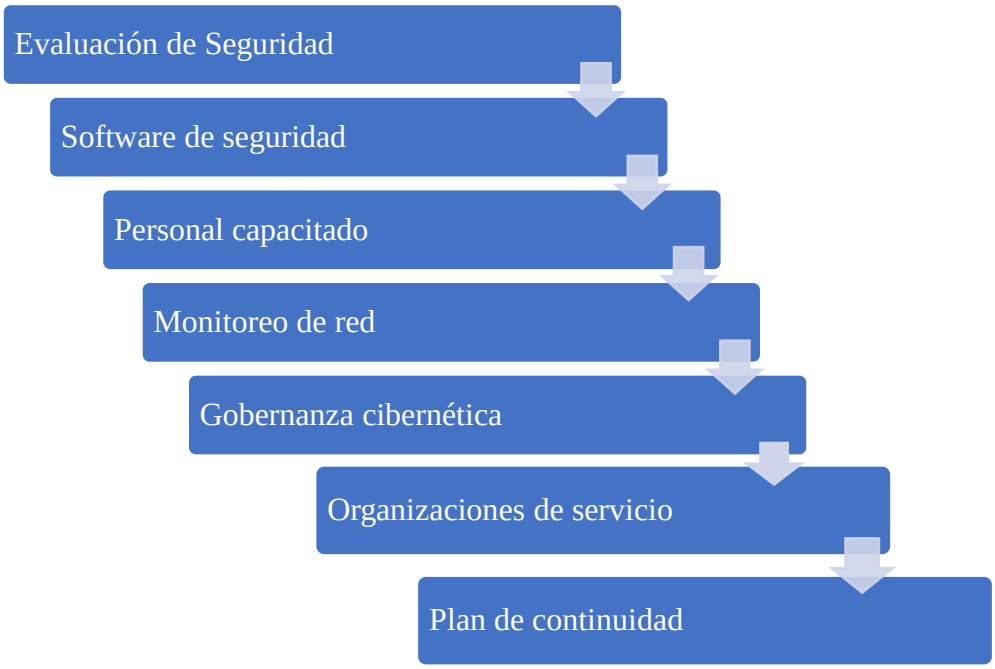
Como se ha mencionado previamente, no todas las empresas tienen mismas características, por lo tanto, es importante que las herramientas permitan identificar los aspectos más críticos, según la empresa que se está evaluando. (Guzmán V, comunicación personal, 2021)

4.1.2.2. Procesos para comprender

De igual forma, mediante las entrevistas realizadas a algunos miembros de área de Auditoría de TI, se indicó que las actividades efectuadas para evaluar los riesgos de ciberseguridad son indagatorias y corresponden a las indicadas en el documento de trabajo sobre las consideraciones de riesgos cibernéticos, por lo tanto, se procedió a realizar la revisión documental de dicho documento (Ver APÉNDICE P. BITÁCORA DE REVISIÓN DOCUMENTAL) y se obtuvo que los procesos más relevantes para la evaluación corresponden a los expuestos en la Figura 18.

Figura 18.

Procesos relevantes para la evaluación



Fuente: Elaboración propia (2021)

4.1.2.2.1. Evaluaciones de seguridad

Las evaluaciones de seguridad son necesarias para escanear, investigar, analizar e informar sobre cualquier vulnerabilidad de seguridad descubierta en el público, dispositivos orientados a internet y para proporcionar, a la administración de la entidad, estrategias de mitigación adecuadas para abordar esas vulnerabilidades descubiertas. (HCR, 2021, p.7).

4.1.2.2.2. Software de seguridad

El software de seguridad se instala para ayudar a proteger a la entidad de las amenazas basadas en la web, incluidos el spyware, los virus y los ataques de phishing. Además, la entidad utiliza redes privadas virtuales y cifrado de correo electrónico para evitar la divulgación no autorizada de información. (HCR, 2021, p.7).

4.1.2.2.3. Personal capacitado

El personal debe completar la capacitación en seguridad al momento de la contratación, este se centra en la seguridad y el acceso a TI, las amenazas de compromiso del correo electrónico comercial, las comunicaciones, etc. Contar con las políticas y procedimientos de seguridad, disponibles durante todo el año, resulta una práctica obligatoria. (HCR, 2021, p.7).

4.1.2.2.4. Monitoreo de Red

Las entidades buscan monitorear el acceso a la red en toda la organización, mediante herramientas de software. Estos incluyen escáneres de vulnerabilidades, rastreadores de empaquetadores, sistema de detección de intrusiones (IDS), dispositivos de explotación de vulnerabilidades, herramientas de creación de paquetes y dispositivos de monitoreo de firewall. (HCR, 2021, p.5).

4.1.2.2.5. Gobernanza cibernética

La entidad incorpora el ciber gobierno en su régimen de gobernanza, que vele por recibir periódicamente un informe sobre las actividades de ciberseguridad. (HCR, 2021, p.5).

4.1.2.2.6. Organizaciones de servicio

La entidad tiene un proceso para considerar el impacto de los riesgos de ciberseguridad en las organizaciones de servicios.(HCR, 2021, p.5).

4.1.2.2.7. Plan de continuidad

La entidad cuenta con un plan documentado y probado para hacer frente a los incidentes de ciberseguridad. (HCR, 2021, p.5).

4.1.2.3. Limitaciones de la evaluación

Por otro lado, mediante la entrevista realizada al gerente del área de Auditoría de TI (2021) se indicó que existen varios factores que limitan la adecuada evaluación de riesgos cibernéticos, en la Tabla 19 se describen dos que, según la gerencia, limitan en gran medida la evaluación de los riesgos cibernéticos en los clientes, producto de la adaptabilidad y la ausencia de recurso humano con formación profesional específica en ciberseguridad. Sin embargo, se considera que la propuesta sobre el conjunto de herramientas de evaluación de riesgos cibernéticos es un inicio y una guía para mejorar dicha evaluación.

Tabla 19.

Limitaciones de la evaluación

Factor limitante	Detalle
Adaptabilidad	La adaptabilidad es un factor limitante porque como se ha mencionado previamente, no todas las organizaciones tienen las mismas características, lo que puede dificultar al, momento de alinear la evaluación con las necesidades y recursos de los clientes.
Recurso humano	El equipo que conforma el área de Auditoría de TI está formado por ingenieros en computación, administración de tecnología de información y carreras similares, sin embargo, no se cuenta con expertos en temas de ciberseguridad que comprendan y realicen la evaluación de la forma correcta.

Fuente: Elaboración propia con información tomada de las entrevistas (2021)

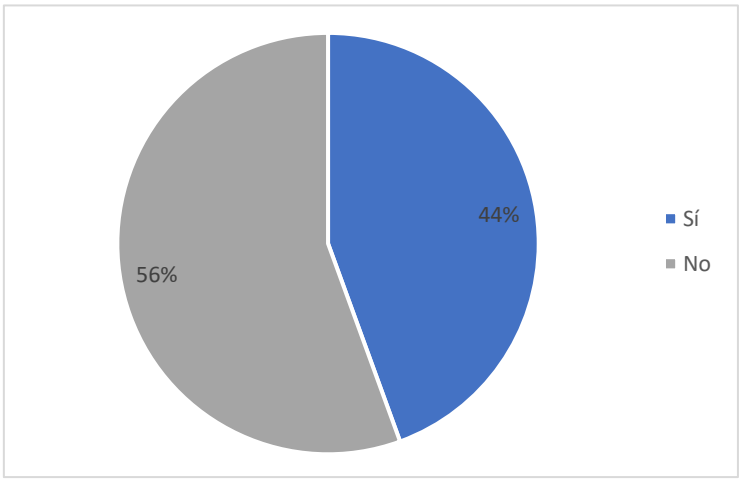
4.2. FASE 2: IDENTIFICACIÓN DE COMPONENTES DE MARCO DE TRABAJO NIST

Para la segunda fase se determinaron los componentes del marco de trabajo NIST – Cybersecurity Framework más adecuados para la elaboración de las herramientas según los resultados obtenidos en la fase anterior.

Como se ha mencionado previamente, se realizó una encuesta donde participaron todos los miembros del área de Auditoría de TI, en dicho instrumento se les consultó si conocían sobre el marco de trabajo NIST – Cybersecurity Framework, los resultados se evidencian en la Figura 19, donde se indica que solo el 44% están al tanto dicho marco. (APÉNDICE G. RESPUESTA DE LA ENCUESTA SOBRE LA SITUACIÓN ACTUAL)

Figura 19.

Conocimiento del marco de trabajo NIST- Cybersecurity Framework

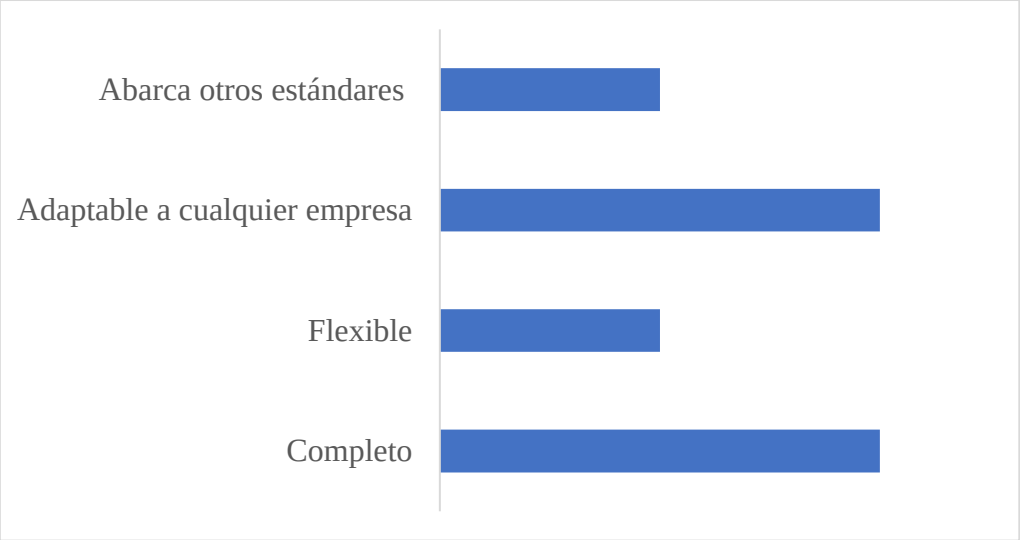


Fuente: Elaboración propia (2021)

Considerando lo anterior, se le consultó a ese 44% su opinión sobre el marco de trabajo NIST – Cybersecurity Framework, por su parte, en la **Figura 20** se muestran las opiniones brindadas acerca de este, especificándole como: completo, flexible, adaptable a cualquier empresa y muy útil al momento de abarcar otros estándares de la industria.

Figura 20.

Opinión sobre el marco de trabajo NIST- Cybersecurity Framework



Fuente: Elaboración propia (2021)

Asimismo, se les consultó sobre la propuesta de un conjunto de herramientas basado en este marco y se obtuvo una reacción positiva, al considerar que al ser fácil de adaptar a cualquier compañía ayudaría a realizar una mejor evaluación.

4.2.1. Componentes del marco de trabajo NIST

Esta propuesta se basa en el marco de trabajo NIST *Cybersecurity Framework*, sin embargo, según las necesidades identificadas en la fase anterior "Necesidades " y la revisión documental, se determinan los componentes para la elaboración de las herramientas que apoyan al área de auditoría de TI, en la evaluación de riesgos cibernéticos, corresponden a las siguientes:

4.2.1.1. Framework Core

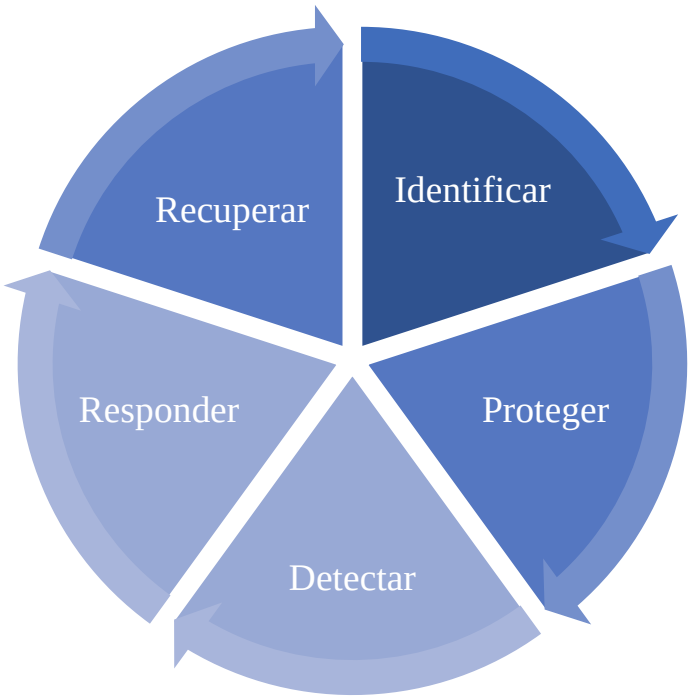
Según NIST (2021) el Framework Core proporciona un conjunto de actividades y resultados de ciberseguridad deseados, utilizando un lenguaje común que es fácil de entender. El Core guía a las organizaciones en la gestión y reducción de sus riesgos de ciberseguridad,

de una manera que complementa los procesos de ciberseguridad y gestión de riesgos existentes de una organización.

El núcleo del marco de trabajo propone cinco funciones que ayudan a una empresa en la estructuración de su programa de gestión del riesgo cibernético, esto facilita la toma de decisiones, al identificar y abordar amenazas y propiciar el mejoramiento de la capacidad de aprendizaje de actividades previas. Estas funciones corresponden a las definidas en la Figura 21, se detallan a continuación:

Figura 21.

Funciones Framework Core



Fuente: Elaboración propia con información, NIST CSF (2018).

El núcleo del marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética, este consta de tres elementos: funciones, categorías y Subcategorías, a continuación, se mencionan los elementos que se utilizaron en la construcción de las herramientas propuestas.

4.2.1.1.1. Identificar:

Esta función permite desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. Las actividades que engloban esta función son fundamentales para el uso efectivo del marco.

En la Tabla 20 se definen las categorías y subcategorías, correspondientes a esta función, empleadas para la elaboración de las herramientas.

Tabla 20.

Categorías y Subcategorías de la función identificar

Categoría	ID	Subcategoría
Administración de Activos ID.BE	ID.BE.3	El flujo de la comunicación organizacional y de datos está mapeado.
	ID.BE.5	Los recursos (p.ej., hardware, dispositivos, datos y software) están priorizados de acuerdo con su clasificación, criticidad y valor para el negocio.
Entorno del Negocio ID.BE	ID.BE.3	Las prioridades para la misión, objetivos y actividades de la organización están establecidas y comunicadas.
	ID.BE.4	Las dependencias y funciones críticas para la prestación de servicios críticos están establecidas
	ID.BE.5	Los requerimientos de resiliencia para soportar la prestación de servicios críticos están establecidos.
Gobierno ID.GV	ID.GV.1	La política de seguridad de la información de la organización está establecida.
	ID.GV.2	Los roles y responsabilidades de seguridad de la información están coordinados y alineados con las funciones internas y socios externos
	ID.GV.4	Los procesos de Gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.

Categoría	ID	Subcategoría
Evaluación de riesgos ID.RA	ID.RA.1	Las vulnerabilidades de los activos están identificadas y documentadas.
	ID.RA.3	Amenazas, tanto internas como externas, están identificadas y documentadas.
	ID.RA.4	Impactos potenciales al negocio y sus probabilidades están identificados.
	ID.RA.5	Las amenazas, vulnerabilidades, probabilidades e impactos son usados para la determinación de riesgos
	ID.RA.6	Las respuestas a los riesgos están identificadas y priorizadas.
Estrategia de gestión de riesgos ID.RM	ID.RM.2	La tolerancia al riesgo organizacional está determinada y claramente expresada.
	ID.RM.3	La determinación de la organización frente a la tolerancia al riesgo se basa en su papel en la infraestructura crítica y el análisis de riesgos específicos del sector.

Fuente: Elaboración propia, basado en NIST (2018).

4.2.1.1.2. Proteger:

La función de proteger describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta contempla la capacidad de limitar o contener el impacto de un potencial evento que atente contra la ciberseguridad.

En la Tabla 21 se definen las categorías y subcategorías correspondientes a esta función, empleadas para la elaboración de las herramientas.

Tabla 21.

Categorías y Subcategorías de la función proteger

Categoría	ID	Subcategoría
Control de accesos PR.AC	PR.AC.1	Las identidades y credenciales están administradas para dispositivos y usuarios autorizados.

Categoría	ID	Subcategoría
	PR.AC.2	El acceso físico a los activos está administrado y protegido.
	PR.AC.3	El acceso remoto está administrado.
	PR.AC.4	Los permisos de acceso se manejan, incorporando los principios de mínimos privilegios y separación de deberes.
	PR.AC.5	La integridad de la red es protegida, e incorpora la segregación de la red donde es apropiado.
Entrenamiento de conciencia PR.AT	PR.AT.1	Todos los usuarios están informados y capacitados
	PR.AT.2	Los usuarios privilegiados entienden sus roles y responsabilidades.
	PR.AT.4	Los altos ejecutivos entienden sus roles y responsabilidades.
	PR.AT.5	El personal de seguridad física y de la información entiende sus roles y responsabilidades
Seguridad de 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.
	PR.DS.4	Existe una adecuada capacidad para garantizar que la disponibilidad se mantenga.
	PR.DS.5	Protecciones en contra de la fuga de datos está implementadas.
Procesos y procedimientos de protección de la información PR.IP	PR.IP.4	Las copias de seguridad de la información se realizan, se les hace mantenimiento y se prueban periódicamente.
	PR.IP.5	Las políticas y regulaciones respecto al entorno físico de operación para que los activos organizacionales se cumplen.
	PR.IP.6	Los datos son destruidos 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

Categoría	ID	Subcategoría
	PR.IP.9	Los planes de respuesta (respuesta a incidentes y continuidad del negocio) y los planes de recuperación (recuperación ante incidentes y desastres) están en orden y se encuentran administrados.
	PR.IP.11	La ciberseguridad está incluida en las prácticas de recursos humanos. (p.ej., des aprovisionamiento, selección de personal).
	PR.IP.12	Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
Mantenimiento PR.MA	PR.MA.2	El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se impide el acceso no autorizado.
Tecnología de protección PR.PT	PR.PT.2	Los medios extraíbles están protegidos, y su uso está restringido de acuerdo con las políticas.
	PR.PT.3	Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales

Fuente: Elaboración propia, basado en NIST (2018).

4.2.1.1.3. Detectar

Esta función define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, pues permite un descubrimiento oportuno.

En la Tabla 22 se definen las categorías y subcategorías, correspondientes a esta función, empleadas para la elaboración de las herramientas.

Tabla 22.

Categorías y Subcategorías de la función detectar

Categoría	ID	Subcategoría
Anomalías y eventos DE.AE	DE.AE.5	Los límites de alertas ante incidentes están establecidos.
Monitoreo continuo de seguridad DE.CM	DE.CM.1	La red está monitoreada para detectar eventos potenciales de ciberseguridad.
	DE.CM.2	El entorno físico es monitoreado para detectar eventos potenciales de ciberseguridad.
	DE.CM.3	La actividad del personal es monitoreada para detectar eventos potenciales de ciberseguridad.
	DE.CM.4	Los códigos maliciosos son detectados.
	DE.CM.7	Se realiza monitoreo en busca de personal, conexiones, dispositivos y software no autorizados.
	DE.CM.8	Se realizan escaneos de vulnerabilidad.
Procesos de detección DE.DP	DE.DP.3	Los procesos de detección están probados.
	DE.DP.3	La información de detección de eventos es comunicada a las partes apropiadas.

Fuente: Elaboración propia, basado en NIST (2018).

4.2.1.1.4. Responder

Para esta función se incluyen actividades necesarias con el fin de tomar medidas frente a un incidente de ciberseguridad detectado, se desarrolla la capacidad de contener el impacto de un potencial ataque.

En la Tabla 23 se definen las categorías y subcategorías de esta función, empleadas en la elaboración de las herramientas.

Tabla 23.

Categorías y Subcategorías de la función responder

Categoría	ID	Subcategoría
Planeación de respuesta RS.RP	RS.RP.1	El plan de respuesta se ejecuta durante o después de un evento.
Comunicaciones RS.CO	RS.CO.1	El personal conoce su rol y el orden de las operaciones cuando una respuesta es requerida
	RS.CO.3	La información se comparte consistentemente con los planes de respuesta.
	RS.CO.4	La coordinación con las partes interesadas ocurre en consistencia con los planes de respuesta.
Análisis RS.AN	RS.AN.1	Las notificaciones de sistemas de detección son investigadas.
	RS.AN.2	El impacto del incidente se comprende.
	RS.AN.3	Los incidentes son categorizados consistentemente con los planes de respuesta.
Mitigación RS.MI	RS.MI.1	Los incidentes son contenidos, mitigados y documentados
Mejoras RC.IM	RC.IM.1	Los planes de respuesta incorporan las lecciones aprendidas.
	RC.IM.2	Las estrategias de respuesta se actualizan

Fuente: Elaboración propia, basado en NIST (2018).

4.2.1.1.5. Recuperar

Por último, esta función permite identificar las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado como consecuencia de un incidente de ciberseguridad.

En la Tabla 24 se definen las categorías y subcategorías correspondientes es esta función, que se utilizarán en la elaboración de las herramientas.

Tabla 24.

Categorías y Subcategorías de la función recuperar

Categoría	ID	Subcategoría
Mejoras RC.IM	RC.IM.1	Los planes de respuesta incorporan las lecciones aprendidas.
	RC.IM.2	Las estrategias de respuesta se actualizan
Comunicaciones RC.CO	RC.CO.3	Las actividades de recuperación son comunicadas a las partes interesadas internas y los equipos ejecutivos y de gestión.

Fuente: Elaboración propia, basado en NIST (2018).

El componente *Framework Core* mediante las cinco funciones mencionadas previamente, permite conocer la realidad de la empresa en temas de ciberseguridad. Por su parte, en la PROPUESTA DE SOLUCIÓN se utilizan las categorías y subcategorías expuestas en cada función para la revisión de cada uno de los procesos determinados en el apartado "Necesidades actuales"

4.3. FASE 3: ELABORACIÓN DE LAS HERRAMIENTAS

En esta tercera fase se define lo esperado de la propuesta, según los miembros del equipo de auditoría de TI. Esto mediante la aplicación de las entrevistas y la encuesta, las cuales se pueden consultar en: el APÉNDICE G. RESPUESTA DE LA ENCUESTA SOBRE LA SITUACIÓN ACTUAL APÉNDICE L. RESPUESTA ENTREVISTA SOBRE HERRAMIENTAS ESPERADAS AL GERENTE DEL ÁREA DE AUDITORÍA DE TI, APÉNDICE M. RESPUESTA ENTREVISTA SOBRE HERRAMIENTAS ESPERADAS AL ENCARGADO DEL ÁREA DE AUDITORÍA DE TI APÉNDICE N. RESPUESTA ENTREVISTA SOBRE HERRAMIENTAS ESPERADAS A ASISTENTE II DEL ÁREA DE

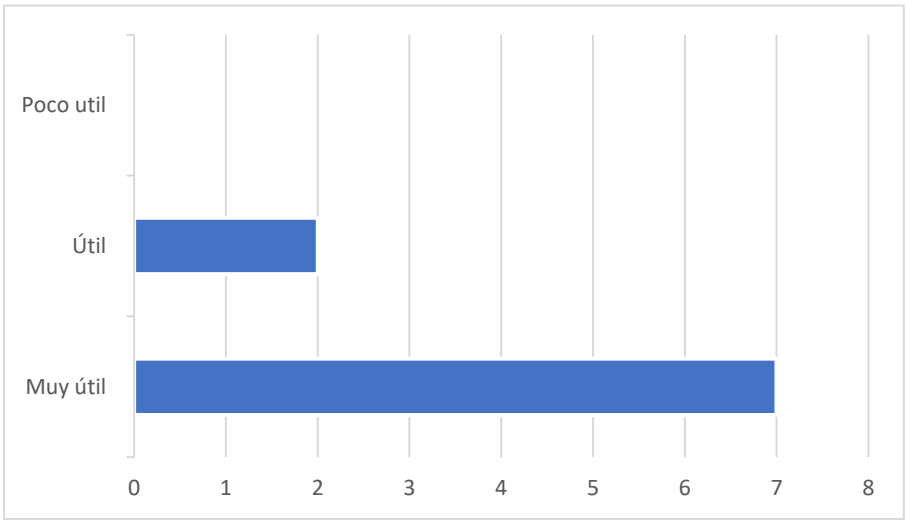
AUDITORÍA DE TI y el APÉNDICE O. RESPUESTA ENTREVISTA SOBRE HERRAMIENTAS ESPERADAS A ASISTENTE I DEL ÁREA DE AUDITORÍA DE .

4.3.1. Utilidad de las herramientas

Para obtener un insumo de parte de las personas del área que están en constante evaluación con los clientes, se procedió a valorar la utilidad de las herramientas que son vistas por los clientes y para ello, mediante la encuesta realizada se les consultó a los miembros del equipo de Auditoría de TI si un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación realizada en los proyectos y se obtuvo que las herramientas serían muy útiles para la elaboración de esta evaluación, tal como se muestra en la Figura 22.

Figura 22.

Utilidad de las herramientas



Fuente: Elaboración propia (2021)

Asimismo, una vez que se les comentó a los participantes de las entrevistas sobre las herramientas y los componentes que se decidieron utilizar para la construcción de estas,

también se obtuvo una respuesta positiva ya que las 4 personas entrevistadas consideran útil las herramientas propuestas en este proyecto.

4.3.2. Expectativas de la herramienta

Para identificar las expectativas esperadas de las herramientas de evaluación de riesgos cibernéticos, se requiere conocer la opinión de las personas que utilizarán dichas herramientas y mediante la aplicación de las entrevistas de la herramienta, se determinó que los involucrados indican cuadro características críticas que las herramientas deben tener, las cuales corresponden a las siguientes:

- Las herramientas sean intuitivas y fáciles de usar
- Facilita la evaluación de los riesgos cibernéticos
- Permita identificar si las organizaciones tienen riesgos cibernéticos que afecten la auditoría
- El proceso sea estandarizado y defina las actividades que se deban realizar para la evaluación

4.4. FASE 4: RETORNO DE INVERSIÓN

Para la fase 4 de este proyecto se realizó una revisión documental sobre las estimaciones del mercado necesarios para el cálculo del retorno de inversión de la elaboración de este proyecto debido a la confidencialidad de la organización.

Así como la revisión de las estimaciones del mercado también se tomó como referencia los conocimientos del estudiante para definir las horas estimadas de esta evaluación y realizar los cálculos necesarios para determinar el retorno de inversión, el valor actual neto y la tasa interna de retorno del presente proyecto, esto con el objetivo de conocer la rentabilidad de implementar este proyecto en las auditorías realizadas por HCR.

4.4.1. Costo de la auditoría

El Colegio de Contadores Públicos de Costa Rica (2021) indica que los honorarios mínimos para una Auditoría Financiera, Informática u Operacional, debe ser efectuado tomando en cuenta los siguientes parámetros: (p.5)

- Independientemente del tipo, naturaleza, tamaño de la empresa contratante y de la naturaleza simple o compleja del programa de una auditoría, la tarifa mínima para esta es de ¢22.695,71 (veintidós mil seiscientos noventa y cinco colones con setenta y un céntimos) por hora profesional.

Tiempo estimado

En caso del tiempo que dura un proyecto varía según el tipo de auditoría y el tamaño del cliente, para este ejercicio tomaron en cuenta la cantidad de horas aproximadas que duraría esta evaluación.

En la Tabla 25 se resumen los datos mencionados anteriormente y se muestra el costo aproximado de la evaluación de riesgos cibernéticos, para dos proyectos, ya que se parte del supuesto de iniciar la evaluación en dos proyectos diferentes.

Tabla 25.

Honorarios mínimos para una Auditoría Financiera, Informática u Operacional

	Por hora	**Horas mínimas para la evaluación**	**Cantidad de proyectos**	**Total**
Auditoría	₡22 695,71	12	2	₡544 697,04

Fuente: Elaboración propia (2021)

4.4.2. Salarios Colaboradores

Por otro lado, para efectos de los salarios correspondientes al personal involucrado en el desarrollo de este proyecto se consultaron fuentes como INFOCOOP (2021) para obtener una estimación del salario de un gerente de área y se utilizó un promedio del salario de los colaboradores del área de Auditoría de TI, en la Tabla 26 se presentan las estimaciones de dichos salarios y la cantidad de horas que se utilizaron durante las 14 semanas que duró la elaboración del proyecto; cabe mencionar que el salario por hora se sacó dividiendo el salario mensual entre 160 horas.

Tabla 26.

Salarios colaboradores

	Mensual	**Por horas**	**Horas utilizadas por semana**
Estudiante	₡ 600 000,00	₡3 750,00	40
Gerente de área	₡ 1 148 523,14	₡ 7 178,27	1
Auditores	₡ 670 000,00	₡ 4 187,50	-

Fuente: Elaboración propia (2021)

4.4.3. Otros datos

Según la Información jurídica inteligente (2021) se realiza un incremento de 0,5562880%, durante 6 años consecutivos, siendo el primer ajuste a partir de 01 de enero de 2021 y posteriormente en enero de cada año, finalizando en enero de 2026.

Por lo tanto, se utilizó este porcentaje para el aumento de los salarios en los próximos tres años, obteniendo como resultado los datos presentados en la Tabla 30, cabe recalcar que estos montos son los salarios mensuales, la estimación de los salarios por hora se pueden visualizar en la Tabla 28

Tabla 27.

Salarios mensual para 3 años

	Año 1	Año 2	Año 3
Gerente de área	₡ 1 148 523,14	₡1 154 912,24	₡1 161 336,87
Auditores	₡ 670 000,00	₡673 727,13	₡677 474,99

Fuente: Elaboración propia (2021)

Tabla 28.

Salarios por hora para 3 años

	Año 1	Año 2	Año 3
Gerente de área	₡ 7 178,27	₡7 218,20	₡7 258,36
Auditores	₡ 4 187,50	₡4 210,79	₡4 234,22

Fuente: Elaboración propia (2021)

Por otro lado, para estimar la tarifa anual de esta evaluación por tres años, se hace la suposición de realizar un plan piloto para implementarlo en diferentes clientes. En la Tabla 29 se presentan la cantidad de clientes en los que se implementaría este proyecto, para los tres años que se toman en cuenta, y en la Tabla 30 se puede observar la estimación del ingreso anual de los tres años.

Tabla 29.

Cantidad de clientes para implementar

	Cantidad clientes
Año 1	2
Año 2	3
Año 3	5

Fuente: Elaboración propia (2021)

Tabla 30.

Ingresos anuales

	Año 1	**Año 2**	**Año 3**	**Total**
Ingreso anual	₡544 697,04	₡817 045,56	₡1 361 742,60	₡2 723 485,20

Fuente: Elaboración propia. (2021)

Los datos indicados, previamente son utilizados para el cálculo el retorno de inversión, el valor actual neto y la tasa interna de retorno, los cuales se pueden visualizar en el capítulo 5 PROPUESTA DE SOLUCIÓN.

Finalmente, en este capítulo, se concretaron las necesidades y procesos necesarios para realizar la evaluación de riesgos cibernéticos, y se definieron los componentes del marco de trabajo NIST – *Cybersecurity Framework* en el que se basara la propuesta descrita el siguiente capitulo, la cual consiste en un conjunto de herramientas que ayude a realizar dicha evaluación a los miembros del equipo de auditoría de TI.

Asimismo, se presentaron los costos para realizar los cálculos necesarios y conocer el retorno de inversión de la implementación de este proyecto.

CAPÍTULO V

PROPUESTA DE SOLUCIÓN

5. PROPUESTA DE SOLUCIÓN

En este capítulo se plantea la propuesta de solución diseñada para solventar el problema descrito en el apartado Situación problemática.

Como parte de la propuesta de solución para el mejoramiento y estandarización de las evaluaciones de riesgos cibernéticos del área de auditoría de TI, se desarrolla un conjunto de herramientas desde la plataforma Microsoft Excel. Lo anterior se basa en los diferentes instrumentos aplicados y analizados en el capítulo anterior.

5.1. ASPECTOS PARA CONSIDERAR EN LA ELABORACIÓN DE LAS HERRAMIENTAS

Como se mencionó en el capítulo anterior el componente del marco de trabajo NIST-Cybersecurity Framework que se tomó en cuenta para la elaboración de las herramientas corresponde al Framework Core, el cual se detalla a continuación.

5.1.1. Framework Core

Como se ha mencionado en capítulos anteriores el Framework Core contine cinco funciones que pueden ayudar a una organización en la administración de los riesgos cibernéticos, lo que facilita la toma de decisiones, identificando y abordando amenazas.

Basándose en estas cinco funciones y de acuerdo con lo indicado en el marco de trabajo NIST- Cybersecurity Framework, se establecen actividades para realizar evaluaciones de auditoría de ciberseguridad, apoyados en las categorías y subcategorías definidas en este marco de trabajo.

En el apartado Esta propuesta se basa en el marco de trabajo NIST *Cybersecurity Framework*, sin embargo, según las necesidades identificadas en la fase anterior “Necesidades

” y la revisión documental, se determinan los componentes para la elaboración de las herramientas que apoyan al área de auditoría de TI, en la evaluación de riesgos cibernéticos, corresponden a las siguientes:

4.2.1.1. Framework Core, se presenta las categorías y subcategorías asociadas a cada una de las funciones del Marco de Ciberseguridad de NIST, cabe indicar que para la construcción de las herramientas se adaptaron las funciones a las necesidades de la empresa.

5.2. PROCESOS EVALUADOS

Los procesos evaluados surgen de las Necesidades actuales identificados en el capítulo anterior. A continuación, se describen cada uno de los procesos definidos y el mapeo de las subcategorías para cada una de estas.

5.2.1. Gestión de seguridad

Este proceso contiene aquellas actividades que buscan evaluar y conocer la situación actual en términos de gestión de seguridad, es decir se busca identificar cualquier vulnerabilidad de seguridad que pueda afectar la organización. Este proceso comprende las 4.1.2.2.1. Evaluaciones de seguridad, el 4.1.2.2.2. Software de seguridad, el 4.1.2.2.4. Monitoreo de Red y las 4.1.2.2.6. Organizaciones de servicio descritos en el apartado de Necesidades actuales. Para esta se alinearon 39 subcategorías del marco de trabajo NIST-Cybersecurity Framework, según a la categoría que pertenecen, en la Tabla 31 se indican las categorías y subcategorías correspondientes a este primer proceso.

Tabla 31.

Categorías y subcategorías para la gestión de seguridad

Función	Categoría	ID	Subcategoría
Identificar	Administración de Activos ID.AM	ID.AM.5	Los recursos (p.ej., hardware, dispositivos, datos y software) están priorizados de acuerdo con su clasificación, criticidad y valor para el negocio.
	Gobierno ID.GV	ID.GV.1	La política de seguridad cibernética de la organización está establecida.
		ID.GV.2	Los roles y responsabilidades de seguridad de la información están coordinados y alineados con las funciones internas y socios externos
		ID.GV.4	Los procesos de Gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.
	Evaluación de Riesgos ID.RA	ID.RA.1	Las vulnerabilidades de los activos están identificadas y documentadas.
		ID.RA.3	Amenazas, tanto internas como externas, están identificadas y documentadas.
		ID.RA.4	Impactos potenciales al negocio y sus probabilidades están identificados.
		ID.RA.5	Las amenazas, vulnerabilidades, probabilidades e impactos son usados para la determinación de riesgos
		ID.RA.6	Las respuestas a los riesgos están identificadas y priorizadas.
	Estrategia de gestión de riesgos ID.RM	ID.RM.2	La tolerancia al riesgo organizacional está determinada y claramente expresada.
		ID.RM.3	La determinación de la organización frente a la tolerancia al riesgo se basa en su papel en la infraestructura crítica y el análisis de riesgos específicos del sector.

Función	Categoría	ID	Subcategoría
Proteger	Control de accesos PR.AC	PR.AC.1	Las identidades y credenciales están administradas para dispositivos y usuarios autorizados.
		PR.AC.2	El acceso físico a los activos está administrado y protegido.
		PR.AC.3	El acceso remoto está administrado.
		PR.AC.4	Los permisos de acceso se manejan, incorporando los principios de mínimos privilegios y separación de funciones
		PR.AC.5	La integridad de la red es protegida e incorpora la segregación de la red donde es apropiado.
	Seguridad de 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.
		PR.DS.4	Se mantiene una capacidad adecuada para asegurar la disponibilidad
		PR.DS.5	Se implementan protecciones contra las filtraciones de datos.
	Procesos y procedimientos de protección de la información PR.IP	PR.IP.4	Las copias de seguridad de la información se realizan, se les hace mantenimiento y se prueban periódicamente.
		PR.IP.6	Los datos son destruidos de acuerdo con las políticas.
		PR.IP.7	Se mejoran los procesos de protección.
		PR.IP.12	Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
	Tecnología de protección PR.PT	PR.PT.2	Los medios extraíbles están protegidos, y su uso está restringido de acuerdo con las políticas.
		PR.PT.3	Se incorpora el principio de menor funcionalidad mediante la configuración de los

Función	Categoría	ID	Subcategoría
			sistemas para proporcionar solo las capacidades esenciales.
Detectar	Monitoreo continuo de seguridad DE.CM	DE.CM.1	La red está monitoreada para detectar eventos potenciales de ciberseguridad.
		DE.CM.2	El entorno físico es monitoreado para detectar eventos potenciales de ciberseguridad.
		DE.CM.4	Los códigos maliciosos son detectados.
		DE.CM.7	Se realiza monitoreo en busca de personal, conexiones, dispositivos y software no autorizados.
		DE.CM.8	Se realizan escaneos de vulnerabilidad.
Responder	Planeación de respuesta RS.RP	RS.RP.1	El plan de respuesta se ejecuta durante o después de un evento.
	Análisis RS.AN	RS.AN.1	Las notificaciones de sistemas de detección son investigadas.
		RS.AN.2	El impacto del incidente se comprende.
		RS.AN.3	Los incidentes son categorizados consistentemente con los planes de respuesta.
	Mitigación RS.MI	RS.MI.1	Los incidentes son contenidos, mitigados y documentados
Recuperar	Mejoras RC.IM	RC.IM.1	Los planes de respuesta incorporan las lecciones aprendidas.
		RC.IM.2	Las estrategias de respuesta se actualizan

Fuente: Elaboración propia, basado en NIST (2018)

5.2.2. Personal capacitado

Para este proceso se definen las actividades que buscan asegurar que el personal de la organización esté debidamente capacitado y comprenda la naturaleza de las amenazas de ciberseguridad y conozca su papel en la protección de los activos de la organización. Este

proceso comprende el criterio de evaluación 4.1.2.2.3. Personal capacitado mencionado en el apartado de Necesidades actuales. En este caso se alinearon 8 subcategorías del marco de trabajo NIST- Cybersecurity Framework, según a la categoría que pertenecen, en la Tabla 32 se indican las categorías y subcategorías correspondientes a este proceso.

Tabla 32.

Categorías y subcategorías para el personal capacitado

Función	Categoría	ID	Subcategoría
Identificar	Evaluación de Riesgos ID.RA	ID.RA.2	La información sobre amenazas y vulnerabilidad se recibe de fórums y fuentes de intercambio de información
Proteger	Entrenamiento de conciencia PR.AT	PR.AT.1	Todos los usuarios están informados y capacitados
		PR.AT.2	Los usuarios privilegiados entienden sus roles y responsabilidades.
		PR.AT.4	Los altos ejecutivos entienden sus roles y responsabilidades.
		PR.AT.5	El personal de seguridad física y de la información entiende sus roles y responsabilidades
	Procesos y procedimientos de protección de la información PR.IP	PR.IP.11	La ciberseguridad está incluida en las prácticas de recursos humanos. (p.ej., des aprovisionamiento, selección de personal).
Detectar	Monitoreo continuo de seguridad DE.CM	DE.CM.3	La actividad del personal es monitoreada para detectar eventos potenciales de ciberseguridad.

Función	Categoría	ID	Subcategoría
Responder	Comunicaciones RS.CO	RS.CO.1	El personal conoce su rol y el orden de las operaciones cuando una respuesta es requerida

Fuente: Elaboración propia, basada en el NIST, (2018)

5.2.3. Gobernanza cibernética

El proceso de gobernanza cibernética contiene las actividades que buscan asegurar que la entidad incorpora el ciber gobierno en su régimen de gobernanza, este proceso comprende la 4.1.2.2.5. Gobernanza cibernética, mencionado en el apartado de Necesidades actuales. En este caso se alinearon 14 subcategorías del marco de trabajo NIST- Cybersecurity Framework, según a la categoría que pertenecen, en la Tabla 33 se indican estas categorías y subcategorías.

Tabla 33.

Categorías y subcategorías para la gobernanza cibernética

Función	Categoría	ID	Subcategoría
Identificar	Administración de Activos ID.AM	ID.AM.3	El flujo de la comunicación organizacional y de datos está mapeado.
	Entorno del Negocio ID.BE	ID.BE.3	Las prioridades para la misión, objetivos y actividades de la organización están establecidas y comunicadas.
		ID.BE.4	Las dependencias y funciones críticas para la prestación de servicios críticos están establecidas.
	Gobierno ID.GV	ID.GV.4	Los procesos de Gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.
Proteger	Procesos y procedimientos de protección de	PR.IP.5	Las políticas y regulaciones respecto al entorno físico de operación para que los activos organizacionales se cumplen.

Función	Categoría	ID	Subcategoría
	la información PR.IP	PR.IP.8	Se comparte la efectividad de las tecnologías de protección.
	Mantenimiento PR.MA	PR.MA.2	El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se impide el acceso no autorizado.
	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.
Detectar	Anomalías y eventos DE.AE	DE.AE.5	Los límites de alertas ante incidentes están establecidos.
	Procesos de detección DE.DP	DE.DP.3	Los procesos de detección están probados.
		DE.DP.4	La información de detección de eventos es comunicada a las partes apropiadas.
Responder	Comunicaciones RS.CO	RS.CO.3	La información se comparte consistentemente con los planes de respuesta.
		RS.CO.4	La coordinación con las partes interesadas ocurre en consistencia con los planes de respuesta.
Recuperar	Comunicaciones RC.CO	RC.CO.3	Las actividades de recuperación son comunicadas a las partes interesadas internas y los equipos ejecutivos y de gestión.

Fuente: Elaboración propia, basada en el NIST, (2018)

5.2.4. Continuidad

´Por último, este proceso contiene aquellas actividades que buscan asegurar que la entidad cuenta con un plan documentado y aprobado para ejecutar frente a los incidentes de ciberseguridad, este proceso comprende el 4.1.2.2.7. Plan de continuidad, mencionado en el apartado de Necesidades actuales. Para este proceso se alinearon 10 subcategorías del marco

de trabajo NIST- Cybersecurity Framework, según a la categoría que pertenecen, tal como se muestra en la Tabla 34.

Tabla 34.

Categorías y subcategorías para la continuidad

Función	Categoría	ID	Subcategoría
Identificar	Administración de Activos ID.AM	ID.AM.3	El flujo de la comunicación organizacional y de datos está mapeado
	Entorno del Negocio ID.BE	ID.BE.3	Las prioridades para la misión, objetivos y actividades de la organización están establecidas y comunicadas.
		ID.BE.4	Las dependencias y funciones críticas para la prestación de servicios críticos están establecidas
	Gobierno ID.GV	ID.GV.4	Los procesos de Gobierno y gestión de riesgos abordan los riesgos de ciberseguridad.
Proteger	Procesos y procedimientos de protección de la información PR.IP	PR.IP.5	Las políticas y regulaciones respecto al entorno físico de operación para que los activos organizacionales se cumplen
		PR.IP.8	Se comparte la efectividad de las tecnologías de protección
	Mantenimiento PR.MA	PR.MA.2	El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se impide el acceso no autorizado.
	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

Función	Categoría	ID	Subcategoría
Detectar	Anomalías y eventos DE.AE	DE.AE.5	Los límites de alertas ante incidentes están establecidos
	Procesos de detección DE.DP	DE.DP.3	Los procesos de detección están probados.
		DE.DP.4	La información de detección de eventos es comunicada a las partes apropiadas.
Responder	Comunicaciones RS.CO	RS.CO.3	La información se comparte consistentemente con los planes de respuesta
		RS.CO.4	La coordinación con las partes interesadas ocurre en consistencia con los planes de respuesta.
Recuperar	Comunicaciones RC.CO	RC.CO.3	Las actividades de recuperación son comunicadas a las partes interesadas internas y los equipos ejecutivos y de gestión.

Fuente: Elaboración propia, basada en el NIST, (2018)

El mapeo de cada proceso anterior fue presentado y revisado por el Supervisor del proyecto, mediante una entrevista, la cual se puede observar en el APÉNDICE Z: MINUTA REVISIÓN PRELIMINAR DE LAS HERRAMIENTAS CON EL GERENTE DEL ÁREA DE AUDITORÍA DE TI. Según lo indicado por el supervisor, estos procesos y el mapeo correspondiente permiten realizar una adecuada evaluación de los riesgos cibernéticos.

5.3. ACTIVIDADES PARA REALIZAR

En la construcción de las herramientas se indicaron algunas actividades a tomar en cuenta para realizar la evaluación de riesgos cibernéticos, con el fin de brindarle al personal que utilizará las herramientas una guía de lo que se debe realizar y pedir para completar la evaluación.

5.3.1. Actividades para el proceso gestión de seguridad

A continuación, en la Tabla 35, se muestran las actividades a realizar para cada subcategoría del proceso gestión de seguridad, estas se presentan de acuerdo con el proceso al que pertenecen y al ID de cada subcategoría.

Tabla 35.

Actividades para la gestión de seguridad

ID	Actividades para realizar
ID.AM.5	1. Obtener clasificación de datos de la organización 2. Revisar el programa para determinar si los recursos clave (p.ej., hardware, dispositivos, datos, software) están clasificados y priorizados con base en criticidad y valor comercial
ID.GV.1	1. Obtener una copia de la política de seguridad de la información. 2. Determinar si la política está completa y si ha sido aprobada por la estructura de gobierno al interior de la organización. 3. Determinar si la política está comunicada a los empleados.
ID.GV.2	1. Determinar si los roles y responsabilidades de seguridad de la información están definidos. Los roles y responsabilidades pueden definirse en políticas, descripciones de trabajo, acuerdos, matriz RACI, cuadros jerárquicos y/o contratos. 2. Determinar si hay suficiente independencia al interior de los roles de seguridad de la información para proporcionar una adecuada separación de las funciones críticas. 3. Revisar contratos, acuerdos de confidencialidad y de nivel de servicio con proveedores críticos para determinar si los controles y la notificación de incidentes de ciberseguridad se abordan adecuadamente.
ID.GV.4	1. Determinar la idoneidad de la supervisión ejecutiva o de la junta y la comprensión de ciberseguridad. Considere lo siguiente: a. Gestión de riesgos. b. Estructuras de Gobierno.

ID	Actividades para realizar
	c. Supervisión de seguridad. d. Entrenamiento/formación. e. Responsabilidad. f. Reporte.
ID.RA.1	1. Determinar si las pruebas de vulnerabilidad son conducidas y analizadas en activos organizacionales críticos (p. ej., activos importantes para los objetivos empresariales y la estrategia de riesgo de la organización
ID.RA.3	1. Revisar las evaluaciones de riesgo para determinar si amenazas internas y externas están identificadas y documentadas. 2. Determinar si la organización ha desarrollado procesos para monitorear y reportar activamente potenciales amenazas.
ID.RA.4	1. Revisar las evaluaciones de riesgos y el análisis de impacto al negocio para determinar si impactos probables y potenciales están identificados y analizados en busca de amenazas
ID.RA.5	1. Determinar si el proceso de evaluación de riesgos identifica amenazas y vulnerabilidades internas y externas razonablemente predecibles, el probable y potencial daño de dichas amenazas, y la suficiencia de los controles para mitigar el riesgo asociado a dichas amenazas. 2. Revisar los resultados relacionados con los tiempos tolerables por la organización para recuperar sus procesos de negocio, productos y servicios críticos.
ID.RA.6	1. Obtener el plan de gestión de riesgos de la organización y/o otra documentación que muestre su respuesta a los niveles de riesgo identificados en la evaluación de riesgos. 2. Determinar si el plan de gestión de riesgos está diseñando para aceptar o reducir el nivel de riesgo de acuerdo con el apetito de riesgo de la organización. 3. Obtener copias de las respuestas de gestión a recientes auditorías y evaluaciones relacionadas con ciberseguridad para determinar si excepciones observadas en auditorías y evaluaciones están identificadas y priorizadas.
ID.RM.2	1. Determinar si la organización ha definido y aprobado un estatuto de apetito al riesgo cibernético.

ID	Actividades para realizar
ID.RM.3	1. Obtener una copia de la estrategia de gestión de riesgo y estatuto de apetito al riesgo de la organización para determinar si están alineados con su rol en la infraestructura crítica (como está definido por el plan nacional de protección de infraestructura [NIPP] y planes específicos del sector).
PR.AC.1	1. Determinar si el acceso a dispositivos de red (p.ej., servidores, estaciones de trabajo, dispositivos móviles, firewalls) está restringido por: a. Único ID de usuario para inicio de sesión. b. Contraseñas complejas. c. Autenticación de múltiples factores. d. Cierre automático si se deja desatendido. e. Bloqueo automático después de repetidos intentos fallidos de acceso. f. Cambio de nombre y contraseña predeterminados para cuentas administrativas. 2. Determinar si los parámetros de contraseña cumplen con la política de la organización y/o los requisitos aplicables de la industria. Considere lo siguiente: a. Longitud, complejidad, requisitos de cambio, historia b. ¿Se suprimen las contraseñas de todos los resultados? c. ¿Los archivos de contraseña están encriptados y restringidos? 3. Revisar los procedimientos de terminación para garantizar que las credenciales se revoquen o cambien cuando un empleado se va. a. Verifique las cuentas para garantizar que el acceso del usuario se revoque después de la terminación y que las cuentas se eliminen de acuerdo con las políticas.
PR.AC.2	1. Determinar si el acceso físico a activos clave está físicamente restringido: a. Puertas cerradas. b. Vigilancia. c. Cercas o muros. d. Registros. e. Acompañamiento al visitante. 2. Determinar si las políticas y procedimientos permiten el acceso únicamente a personal autorizado a áreas sensibles.

ID	Actividades para realizar
	3. Revisar los procedimientos de terminación para asegurar que el acceso físico se remueve cuando el empleado se va de la organización.
PR.AC.3	1. Determinar si las políticas y los procedimientos relacionados con las capacidades de acceso de los usuarios remotos están formalizados. Considere lo siguiente: a. Usuarios remotos (p.ej., empleados, contratistas, terceros) con acceso a los sistemas críticos están aprobados y documentados. b. Conexiones remotas son solo abiertas según sea requerido. c. Conexiones remotas están registradas y monitoreadas. d. Conexiones remotas están encriptadas. e. Existe una autenticación fuerte (p.ej., múltiples factores, parámetros de contraseña fuertes). f. La capacidad para borrar datos de forma remota en dispositivos móviles cuando faltan datos o son robados está habilitada. g. Los controles de seguridad de la institución (p.ej., antivirus, patch management) son requeridos en dispositivos remotos que se conectan a la red.
PR.AC.4	1. Revisar los derechos y permisos de acceso a la red y a cualquier aplicación crítica. 2. Determinar si los perfiles de acceso del usuario son consistentes con sus funciones de trabajo (con base en el mínimo privilegio). 3. Comparar una muestra de la autoridad de acceso de los usuarios con sus deberes y responsabilidades asignadas. 4. Determinar si el acceso está otorgado para funciones de misión crítica y funciones de soporte de sistemas de información para reducir el riesgo de actividad maliciosa sin conclusión (p.ej. procesos críticos que requieren que dos personas realicen una función). 5. Determinar si los usuarios con privilegios de administrador local en estaciones de trabajo requieren este nivel de acceso. 6. Revisar cómo la organización restringe y/o monitorea el acceso a datos sensibles por parte de usuarios con altos privilegios en la red. 7. Determinar si los controles de acceso basados en roles están implementados

ID	Actividades para realizar
	(p.ej., roles vs. usuarios que tienen asignados derechos de acceso). 8. Determinar si hay revisiones regulares al acceso
PR.AC.5	1. Revisar los diagramas de red y de flujo de datos. 2. Determinar si los sistemas de alto costo/críticos están separados de los sistemas de alto riesgo cuando es posible. 3. Determinar si la organización tiene un proceso formal para aprobar el flujo de datos y/o conexiones entre redes y/o sistemas
PR.DS.1	1. Determinar si los datos confidenciales o sensibles están identificados en la red de la organización (p.ej., clasificación de datos, evaluación de riesgo). 2. Determinar si la información confidencial está segura (p.ej., encriptación fuerte según está definida por las mejores prácticas de la industria) en reposo. 3. Determinar si los dispositivos móviles (p.ej., laptops, tablets, medios removibles) que son usados para almacenar información confidencial están encriptados. 4. Revisar contratos con terceros que almacenan información confidencial para garantizar que existen controles de seguridad apropiados para datos sensibles en reposo.
PR.DS.2	1. Determinar si los datos sensibles están seguros (p.ej., encriptación fuerte según definida por las mejores prácticas de la industria) cuando son transmitidos a través de redes de acceso público. 2. Determinar si existen políticas adecuadas en relación con la transmisión de información confidencial o sensible vía email. 3. Revisar el material de capacitación y/o políticas de uso aceptable para determinar si los empleados están instruidos en las políticas de la organización sobre la transmisión de datos. 4. Revisar contratos con terceros que transmiten información confidencial para garantizar que existen controles de seguridad apropiados para la transmisión de datos sensibles.
PR.DS.3	1. Revisar las políticas y los procedimientos de inventario de activos. Considere lo siguiente: a. Existen procesos formalizados.

ID	Actividades para realizar
	b. Exactitud en el seguimiento de activos. c. Eliminación o destrucción segura de información confidencial de activos desmantelados
PR.DS.4	1. Revisar una muestra de informes de monitoreo de la administración de capacidad usados para monitorear recursos críticos como el ancho de banda, CPU, utilización del disco, disponibilidad de red, intercambio de paquetes, etc. 2. Determinar si los recursos tienen capacidad adecuada. 3. Determinar si el riesgo de ataque de denegación de servicio distribuido (DDoS) se ha abordado y está en línea con el apetito de riesgo de la organización.
PR.DS.5	1. Revisar las evaluaciones de riesgo, las actas de reuniones de seguridad de la información y las estrategias de seguridad de la información para determinar si la prevención al riesgo de pérdida de datos o exfiltración de datos confidenciales se está considerando. 2. Asegurar que existen controles y herramientas (p.ej., prevención de pérdida de datos) para detectar o bloquear una potencial transmisión o eliminación de datos confidenciales (p.ej., email, dispositivos USB).
PR.IP.4	1. Determinar si existe un plan formal para copias de seguridad y restauración. 2. Revisar los procedimientos de copias de seguridad. Asegurar que se realizan pruebas periódicas de copias de seguridad para verificar que los datos son accesibles y leíbles.
PR.IP.6	1. Revisar las políticas de desinfección de medios (destrucción de datos). 2. Asegurar que las técnicas y procedimientos de desinfección son proporcionales con la categoría o clasificación de seguridad de la información o evaluación, y están de acuerdo con políticas federales y organizacionales y estándares de la organización que apliquen. 3. Verificar basureras, contenedores de basura, basura triturada y/o trituradores para garantizar el cumplimento de las políticas. 4. Obtener pruebas (p.ej., certificados de destrucción) de que la desinfección de medios ocurre de acuerdo con las políticas.
PR.IP.7	1. Revisar las políticas y los procedimientos de la organización relacionados con el mejoramiento continuo de los procesos de protección. Considere lo siguiente:

ID	Actividades para realizar
	a. Auditorías, evaluaciones y escaneos de vulnerabilidades en curso son realizados, revisados y respondidos. b. Los planes, procesos y políticas están actualizados con base a lecciones aprendidas de pruebas (p.ej., continuidad del negocio, recuperación de desastres, respuesta a incidentes c. Posición designada y/o responsable del comité para la evaluación continua de las necesidades y postura de la seguridad de la información de la compañía. d. Recopilación de la información de amenazas y respuestas a cambios en el entorno de amenaza
PR.IP.12	1. Obtener el plan de gestión de vulnerabilidades de la organización y garantizar que incluya lo siguiente: a. Frecuencia de escaneo de vulnerabilidades. b. Métodos para medir el impacto de las vulnerabilidades identificadas (p.ej., sistema de puntaje de vulnerabilidades comunes [CVSS]). c. Incorporación de las vulnerabilidades identificadas en otras evaluaciones de control de seguridad (p.ej., auditorías externas, pruebas de penetración). d. Procedimientos para el desarrollo de reparación de vulnerabilidades identificadas. 2. Obtener una copia de la evaluación de riesgos de la organización para garantizar que las vulnerabilidades identificadas durante el proceso de gestión de vulnerabilidades están incluidas
PR.PT.2	1. Obtener una copia de la política de medios removibles. Los controles deben incluir: a. Capacitación al usuario. b. Encriptación de medios removibles. c. Acceso restringido a medios removibles (p.ej., restricciones a USB). d. Procedimientos de desinfección para medios desmantelados. 2. Realización de verificación a sistemas con restricciones de medios removibles para garantizar que las restricciones estén funcionando como se espera y cumplan con las políticas de la organización

ID	Actividades para realizar
PR.PT.3	1. Revisar los sistemas de información para determinar si las funciones, los puertos, los protocolos y los servicios innecesarios y/o no seguros están deshabilitados. 2. Donde sea factible, la organización limita las funcionalidades de un componente a una sola función por dispositivo (p.ej., servidor dedicado a email).
DE.CM.1	1. Obtener una lista del control de monitoreo implementado por la organización a los siguientes niveles: a. Red (p.ej., firewall, router, interruptor). b. Sistema operativo (p.ej., plataformas de servidores, plataformas de estaciones de trabajo, electrodomésticos). c. Aplicaciones (p.ej., administración de cuentas, acceso a archivos y bases de datos). 2. Determinar si el monitoreo en cada nivel incluye detección de eventos de ciberseguridad (p.ej., ataques de negación de servicio, acceso no autorizado a cuentas, acceso no autorizado a archivos/sistemas, ataques de escalada de privilegios, ataques de inyección SQL).
DE.CM.2	1. Obtener un inventario de instalaciones críticas (p.ej., centros de datos, armarios de red, centros de operaciones, centros de control crítico). 2. Determinar si los controles de monitoreo de seguridad física están implementados y son apropiados para detectar eventos potenciales de ciberseguridad (p.ej., registros de entrada/salida, detectores de movimiento, cámaras de seguridad, iluminación de seguridad, guardias de seguridad, cerraduras de puertas/ventanas, bloqueo automático del sistema cuando está inactivo, acceso físico restringido a servidores, estaciones de trabajo, dispositivos de red, puertos de red).
DE.CM.4	1. Obtener una copia de los procesos y procedimientos usados para detectar código malicioso en la red y servidores/puestos de trabajo (p.ej., anti-malware software en servidores y estaciones de trabajo, filtros de phishing en sistemas de email, sistemas de prevención/detección de intrusión en la red, productos de seguridad de punto final en estaciones de trabajo y/o servidores). 2. Determinar si los controles de código malicioso están:

ID	Actividades para realizar
	a. Instalados en todos los sistemas y puntos de control de la red en los que aplique. b. Actualizados de manera regular. c. Configurados para realizar escaneo en tiempo real o escaneos periódicos en intervalos regulares. 3. Inspeccionar estaciones de trabajo y otros dispositivos de punto final de usuario para verificar lo siguiente: a. Los controles de código malicioso están instalados. b. Los controles de código malicioso están actualizados. c. Los controles de código malicioso son capaces de detectar códigos de prueba
DE.CM.7	1. Obtener una copia de los procesos y procedimientos diseñados para detectar acceso no autorizado a las instalaciones y sistemas de la organización (p.ej., registros de inicio/cierre de sesión o de entrada/salida, videos de vigilancia, alarmas de intrusión, bloqueo de puertos de red, restricciones de dispositivos USB en estaciones de trabajo y dispositivos de usuario, monitoreo de inicios de sesión fallidos excesivos indicando un ataque de adivinación de contraseña). 2. Verificación de los controles de acceso no autorizado accediendo a las instalaciones y sistemas con permiso para probar, pero no con autorización estándar. Pedir a la organización que provea las notificaciones de alerta generadas por el acceso no autorizado simulado.
DE.CM.8	1. Obtener una copia de la programación de la organización para realizar escaneos de vulnerabilidad interna y externa, y los resultados de los escaneos de vulnerabilidad interna y externa más recientes. 2. Revisar la programación y los resultados en busca de lo siguiente: a. Frecuencia. b. Finalización exitosa. c. Solución o mitigación documentada de las vulnerabilidades identificadas. d. El alcance de las pruebas incluye a todos los sistemas críticos. 3. Determinar si los resultados de los escaneos de vulnerabilidad fueron reportados a individuos o grupos con autoridad apropiada para asegurar su solución

ID	Actividades para realizar
RS.RP.1	1. Determinar si la organización ha aprobado respuestas a incidentes y planes de continuidad del negocio. 2. Obtener las copias de reportes de incidentes recientes para validar que los planes son ejecutados. 3. Identificar la estructura establecida para responder ante eventos de ciber resiliencia
RS.AN.1	1. Obtener evidencia de notificaciones de eventos (p.ej., alertas de detección, reportes) de sistemas de información (p.ej., uso de la cuenta, acceso remoto, conectividad wireless, conexión de dispositivos móviles, ajustes de configuración, inventarios de componentes de los sistemas, uso de las herramientas de mantenimiento, acceso físico, temperatura y humedad, actividad anómala, uso de código móvil). 2. Determinar quién recibe las alertas o reportes de los sistemas de detección y qué acciones son tomadas al recibir los reportes. 3. Revisar el plan de respuesta ante incidentes para determinar si las acciones tomadas siguen el plan.
RS.AN.2	1. Revisar el plan de respuesta ante incidentes para determinar si hay un proceso para analizar y clasificar formalmente los incidentes según su impacto potencial. 2. Revisar el currículum y la capacitación de los miembros del equipo de respuesta a incidentes responsables de determinar su impacto para identificar si ellos tienen el conocimiento y la experiencia para comprender el impacto potencial
RS.AN.3	1. Revisar el plan de respuesta ante incidentes para determinar si está diseñado para priorizarlos, permitiendo una rápida respuesta para incidentes o vulnerabilidades significativas. 2. Obtener copias de los reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan
RS.MI.1	1. Revisar el plan de respuesta ante incidentes para determinar si existen los pasos apropiados para mitigar el impacto de un incidente. Considere lo siguiente: a. Pasos para mitigar el incidente para prevenir daños adicionales. b. Procedimientos para notificar a terceros potencialmente impactados. c. Estrategias para mitigar el impacto de diferentes tipos de incidentes (p.ej.,

ID	Actividades para realizar
	denegación de servicio distribuido [DDoS], malware, etc.). 2. Revisar cualquier incidente documentado para determinar si los esfuerzos de mitigación fueron implementados y efectivos.
RC.IM.1	1. Obtener una copia de los resultados de recientes eventos o pruebas de eventos de Ciberseguridad. 2. Evaluar la documentación en busca de lo siguiente: a. Lecciones aprendidas y análisis documentados de controles fallidos o faltantes. b. Ítems de acción diseñados para mejorar los planes y procedimientos de recuperación con base en las lecciones aprendidas y los análisis.
RC.IM.2	1. Obtener una copia de los planes y procedimientos de recuperación (p.ej., el plan de continuidad del negocio, el plan de respuesta ante incidentes, el plan de recuperación ante desastres, el plan ante incidentes de ciberseguridad) y los resultados documentados de eventos o pruebas de eventos recientes. 2. Determinar si los planes y procedimientos de recuperación están revisados, actualizados y aprobados regularmente o al hacer cambios a sistemas y controles. 3. Revisar los planes y los procedimientos de recuperación para determinar si los ítems de acción que son el resultado de lecciones aprendidas durante eventos o pruebas de eventos de ciberseguridad han sido implementados.

Fuente: Elaboración propia, basado en Asobancaria, (2020)

5.3.2. Actividades para la personal capacitado

Seguidamente, en la Tabla 36, se muestran las actividades a realizar para cada subcategoría del proceso personal capacitado.

Tabla 36.

Actividades para la personal capacitado

ID	Actividades para realizar
ID.RA.2	1.Determinar si la organización tiene un proceso formal para difundir información sobre amenazas y vulnerabilidad a individuos con la experticia para revisar la información y la autoridad para mitigar el riesgo que representan para la organización
PR.AT.1	1. Revisar las políticas de uso aceptable y/o material de capacitación para garantizar que el contenido es adecuado. 2. Revisar los reportes y/o documentación de capacitación del usuario para garantizar que los usuarios son capacitados de acuerdo con la política, orientación, y/o requisito aplicable (p.ej., capacitación anual sobre ciberseguridad de todos los empleados). 3. Determinar si los materiales de capacitación están actualizados con base a cambios en el entorno de amenazas cibernéticas
PR.AT.2	1. Determinar si la organización tiene un procedimiento para identificar usuarios privilegiados. 2. Determinar si los roles de los usuarios privilegiados están bien definidos y si los usuarios privilegiados están capacitados de acuerdo con sus responsabilidades. 3. Revisar el material de capacitación y/o acuerdos de usuario para asegurar que los usuarios con altos privilegios se les ha enseñado sobre los roles y responsabilidades de seguridad asociados a altos privilegios.
PR.AT.4	Revisar los programas de capacitación y educación continua para altos ejecutivos. Considerar lo siguiente: a. Los conocimientos de ciberseguridad y niveles de habilidad para realizar sus deberes están definidos. b. Capacitación específica según roles es asignada teniendo en cuenta los roles y responsabilidades de ciberseguridad. c. Existe un método para medir conocimientos y comprensión de la
PR.AT.5	

ID	Actividades para realizar
	ciberseguridad de los altos ejecutivos con respecto a los requisitos de la organización. d. Materiales de capacitación y educación están actualizados para reflejar los cambios en el entorno de amenaza
PR.IP.11	1. Revisar los procesos de contratación para determinar si la verificación de antecedentes se realiza a todos los empleados. 2. Revisar los procesos de contratación para posiciones con acceso a información sensible para determinar si ellos son proporcionales a un nivel alto de riesgo. 3. Revisar los procesos de terminación para determinar si cuentas/accesos son deshabilitados de manera oportuna.
DE.CM.3	1. Obtener una lista de los controles de monitoreo implementados por la organización a nivel de aplicación/cuenta de usuario (p.ej., administración de cuentas, roles de acceso de usuarios, monitoreo de actividad de usuarios, acceso a archivos y bases de datos) 2. Determinar si el monitoreo incluye detección y alertas de eventos de ciberseguridad (p.ej., acceso no autorizado a cuentas, acceso no autorizado a archivos/sistemas, acceso fuera de horario, acceso a datos sensibles, acceso inusual, acceso físico no autorizado, ataques de escalada de privilegios
RS.CO.1	1. Revisar los planes de respuesta ante incidentes para determinar si los roles y responsabilidades están definidas para empleados. 2. Entrevistar a los empleados para determinar si ellos conocen sus roles y responsabilidades según lo definido en el plan. 3. Revisar cualquier prueba de respuesta ante accidentes o capacitación dada a los empleados para determinar si ayudan a educar a los empleados en sus roles y responsabilidades

Fuente: Elaboración propia, basado en Asobancaria, (2020)

5.3.3. Actividades para el proceso gobernanza cibernética

Para el proceso que evalúa la gobernanza cibernética, se definen las actividades de cada subcategoría en la Tabla 37

Tabla 37.

Actividades para el proceso gobernanza cibernética

ID	Actividades para realizar
ID.AM.3	Garantizar que la organización mantenga copias adecuadas y actuales de los diagramas de flujo de los datos (DFD), diagramas de red lógica (LND), y/u otros diagramas que muestren el flujo de datos y comunicación organizacional.
ID.BE.3	1. Determinar si la organización tiene un plan estratégico que define los objetivos de la empresa. Se debe asegurar que los objetivos de la empresa están alineados con los intereses de las partes interesadas. 2. Determinar si el estatuto de la misión y los objetivos están claramente publicados, de tal forma que los trabajadores puedan verlos y acceder a ellos fácilmente. 3. Determinar si un plan estratégico de IT está documentado, define funciones y está mapeado a los objetivos de la empresa. 4. Determinar si los trabajadores saben sobre la misión y los objetivos de la organización.
ID.BE.4	Obtener el plan de continuidad del negocio, el plan de recuperación ante desastres, el análisis del impacto del negocio y las evaluaciones de riesgos, y revisar lo siguiente
ID.GV.4	Determinar la idoneidad de la supervisión ejecutiva o de la junta y la comprensión de ciberseguridad. Considere lo siguiente: a. Gestión de riesgos. b. Estructuras de Gobierno. c. Supervisión de seguridad. d. Entrenamiento/formación. e. Responsabilidad. f. Reporte.

ID	Actividades para realizar
PR.IP.5	Revisar las políticas, los procedimientos y los planes del entorno operativo de seguridad física. Asegurarse que lo siguiente se aborde: a. Interruptor de emergencia. b. Iluminación de emergencia. c. Planta de emergencia. d. Protección contra el fuego. e. Control de temperatura y humedad. f. Protección contra daño por agua. g. Ubicación de los componentes de sistemas de información (para minimizar daños).
PR.IP.8	1. Determinar si la organización participa en grupos de intercambio y análisis de la información. 2. Determinar si la organización facilita el intercambio de información permitiendo la autorización de usuarios para compartir información autorizada con socios de intercambio
PR.MA.2	Determinar si el mantenimiento remoto en servidores, estaciones de trabajo y otros sistemas es realizado. Considere lo siguiente: a. ¿A quién se le permite conectarse a los sistemas (p.ej. trabajadores internos, terceros)? b. ¿Qué software/versión o servicios son usados para conectarse? c. Si los usuarios finales deben realizar alguna acción previa a permitir el control remoto de su estación de trabajo y/o si el acceso se registra y monitorea. d. Requerimientos de autentificación adecuados (p.ej., autentificación multifactorial).
PR.PT.3	1. Revisar los sistemas de información para determinar si las funciones, los puertos, los protocolos y los servicios innecesarios y/o no seguros están deshabilitados. 2. Donde sea factible, la organización limita las funcionalidades de un componente a una sola función por dispositivo (p.ej., servidor dedicado a email). 3. Determinar si la organización revisa funciones y servicios prestados por

ID	Actividades para realizar
	sistemas de información o componentes individuales de sistemas de información para determinar cuáles funciones y servicios son candidatos para eliminar
DE.AE.5	1. Obtener una copia de mensajes de alerta, actas de reuniones, reportes y otra documentación donde eventos detectados fueron escalados. 2. Revisar la documentación y determinar lo siguiente: a. Los eventos detectados son reportados de manera oportuna a alguien con el conocimiento y experticia para resolver o escalar el evento. b. Los eventos escalados son reportados a individuos o grupos con la autoridad apropiada para tomar decisiones acerca de la respuesta de la organización. c. Los límites están definidos tal que un evento desencadena la respuesta apropiada (p.ej., respuesta de continuidad del negocio, respuesta de recuperación de desastres, respuesta de incidentes, respuesta legal).
DE.DP.3	1. Obtener una copia de la programación de la organización para realizar pruebas de respuesta a incidentes, los resultados de pruebas recientes a respuesta a incidentes, y los procesos y procedimientos documentados que requieren pruebas de control de actividad anómala (p.ej., pruebas periódicas de sistemas de detección/prevención de intrusión, anti-malware software de punto final). 2. Revisar la documentación en busca de lo siguiente: a. Completitud en la prueba de controles implementados de detección de actividad anómala. b. Frecuencia de la prueba. c. Solución o mitigación documentada de resultados de prueba negativos.
DE.DP.4	1. Obtener una copia de las actas de reuniones donde las actividades físicas y electrónicas anómalas están reportadas (p.ej., reuniones del comité de seguridad de la información, reuniones de la junta/gerencia, reuniones de gestión del riesgo). 2. Obtener una copia de las respuestas documentadas a incidentes recientes de actividad física y electrónica anómala. 3. Comparar las actas de reuniones con incidentes documentados y determinar si los eventos detectados están consistentemente reportados y apropiadamente manejados.

ID	Actividades para realizar
RS.CO.3	1. Revisar el plan de respuesta ante incidentes para determinar si el intercambio de información está claramente definido dado que relaciona lo siguiente (si corresponde): a. Clientes. b. Fuerzas del orden público. c. Reguladores. d. Medios. e. Organizaciones de intercambio de información. 2. Obtener las copias de los reportes de incidentes recientes para validar que el intercambio es consistente y sigue el plan.
RS.CO.4	1. Revisar el plan de respuesta ante incidentes para determinar si existe un proceso para comunicarse con las partes interesadas internas y externas durante y/o prosiguiendo a un incidente. 2. Obtener las copias de reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan.
RC.CO.3	1. Obtener una copia de las actas de reunión donde estén reportados eventos de ciberseguridad (p.ej. reuniones del Comité de Seguridad de la Información, reuniones de la junta/gerencia, reuniones de gestión del riesgo, reuniones del Comité de Cumplimento). 2. Obtener una copia de los resultados documentados sobre eventos de ciberseguridad. 3. Comparar las actas de reuniones con los eventos documentados de ciberseguridad y determinar si en las actividades de recuperación se notificaron a las partes interesadas y miembros de la gerencia pertinentes (p.ej. miembros de la junta, accionistas, ejecutivos de nivel C, gerentes de gestión de riesgos, gerentes de departamentos afectados).

Fuente: Elaboración propia, basado en Asobancaria, (2020)

5.3.4. Actividades para el proceso de continuidad

Finalmente, para el proceso de continuidad se definió una serie de actividades, las cuales son mencionadas en la Tabla 38.

Tabla 38.

Actividades para el proceso de continuidad

ID	Actividades para realizar
ID.BE.5	1. Determinar si los planes de continuidad y recuperación ante desastres de la organización (incluyendo el análisis de impacto al negocio) respaldan la capacidad de recuperación de los servicios críticos. 2. Determinar si existe información apropiada para realizar una debida diligencia (p.ej., plan de continuidad del negocio, acuerdos de nivel de servicio, reportes de control de servicio de la organización) y si está revisada para garantizar que los requisitos de recuperación de la organización puedan cumplirse para los servicios críticos de terceros.
PR.DS.4	1. Revisar una muestra de informes de monitoreo de la administración de capacidad usados para monitorear recursos críticos como el ancho de banda, CPU, utilización del disco, disponibilidad de red, intercambio de paquetes, etc. 2. Determinar si los recursos tienen capacidad adecuada (p.ej., espacio en el disco, CPU). 3. Determinar si el riesgo de ataque de denegación de servicio distribuido (DDoS) se ha abordado y está en línea con el apetito de riesgo de la organización.
PR.IP.4	1. Determinar si existe un plan formal para copias de seguridad y restauración. 2. Revisar los procedimientos de copias de seguridad. Asegurar que se realizan pruebas periódicas de copias de seguridad para verificar que los datos son accesibles y leíbles.
PR.IP.9	1. Revisar la respuesta a incidentes y el plan de continuidad del negocio para determinar si la institución tiene documentado cómo responderá a un incidente cibernético. 2. Evaluar los planes para determinar qué tan frecuente se actualizan y aprueban. 3. Validar que la estrategia de ciber resiliencia definida se encuentre alineada a los objetivos del negocio y la estrategia de ciberseguridad. 4. Identificar las soluciones establecidas orientadas a la ciber resiliencia, y cómo

ID	Actividades para realizar
	estas están incluidas y desarrolladas en las soluciones de ciberseguridad y continuidad del negocio.
RS.RP.1	1. Determinar si la organización ha aprobado respuestas a incidentes y planes de continuidad del negocio. 2. Obtener las copias de reportes de incidentes recientes para validar que los planes son ejecutados. 3. Identificar la estructura establecida para responder ante eventos de ciber resiliencia
RS.AN.2	1. Revisar el plan de respuesta ante incidentes para determinar si hay un proceso para analizar y clasificar formalmente los incidentes según su impacto potencial. 2. Revisar el currículum y la capacitación de los miembros del equipo de respuesta a incidentes responsables de determinar su impacto para identificar si ellos tienen el conocimiento y la experiencia para comprender el impacto potencial.
RS.AN.3	1. Revisar el plan de respuesta ante incidentes para determinar si está diseñado para priorizarlos, permitiendo una rápida respuesta para incidentes o vulnerabilidades significativas. 2. Obtener copias de los reportes de incidentes recientes para validar que el reporte es consistente y sigue el plan.
RS.MI.1	Determinar si los procesos de monitoreo continuo de la organización (p.ej., evaluación de riesgos, escaneo de vulnerabilidades) facilitan el conocimiento continuo de amenazas, vulnerabilidades y seguridad de la información para respaldar las decisiones de gestión de riesgos organizacionales. Considere lo siguiente: a. ¿Es el proceso continuo (a una frecuencia suficiente para respaldar las decisiones organizacionales relacionadas con los riesgos)? b. Los resultados generan una respuesta apropiada al riesgo (p.ej., estrategia de mitigación, aceptación) con base en el apetito al riesgo de la organización

ID	Actividades para realizar
RC.IM.1	1. Obtener una copia de los resultados de recientes eventos o pruebas de eventos de Ciberseguridad. 2. Evaluar la documentación en busca de lo siguiente: a. Lecciones aprendidas y análisis documentados de controles fallidos o faltantes. b. Ítems de acción diseñados para mejorar los planes y procedimientos de recuperación con base en las lecciones aprendidas y los análisis.
RC.IM.2	1. Obtener una copia de los planes y procedimientos de recuperación (p.ej., el plan de continuidad del negocio, el plan de respuesta ante incidentes, el plan de recuperación ante desastres, el plan ante incidentes de ciberseguridad) y los resultados documentados de eventos o pruebas de eventos recientes. 2. Determinar si los planes y procedimientos de recuperación están revisados, actualizados y aprobados regularmente o al hacer cambios a sistemas y controles. 3. Revisar los planes y los procedimientos de recuperación para determinar si los ítems de acción que son el resultado de lecciones aprendidas durante eventos o pruebas de eventos de ciberseguridad han sido implementados.

Fuente: Elaboración propia, basado en Asobancaria, (2020)

5.4. HERRAMIENTAS

De acuerdo con lo mencionado previamente y a lo analizado en el capítulo 4, como parte de la propuesta de solución se diseñaron las siguientes herramientas para la evaluación de riesgos cibernéticos.

5.4.1. Herramienta evaluación de riesgos

Esta herramienta busca validar el estado actual de las organizaciones, mediante la evaluación de diferentes subcategorías para así determinar si existen riesgos cibernéticos considerables que alteren el enfoque de la auditoría.

La herramienta consiste en cuatro matrices (una por cada proceso definido anteriormente) que describe las categorías y subcategorías del marco de trabajo NIST-*Cybersecurity Framework* según sus funciones, además incluyen las actividades que se mencionan en el apartado 5.3. Actividades para realizar. En la Tabla 39, se describen las columnas que se incluyeron en esta herramienta.

Tabla 39.

Descripción de las columnas

Columna	Descripción
Función	Corresponde a la función incluida en el componente framework Core del marco de trabajo NIST – Cybersecurity Framework
Categoría	Es la subdivisión de una función en grupos de resultados de seguridad cibernética
ID	Es un identificar único alfanumérico para cada subcategoría, este se compone por las primeras letras de la función, seguida de las letras que representan la categoría y el número correspondiente a la subcategoría.
Subcategoría	La subcategoría divide la categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada categoría.
Actividades por realizar	Requerimientos de información que se le debe solicitar al cliente para realizar cada la evaluación.
Observaciones	Apartado para documentar las observaciones del resultado de cada subcategoría
Resultado	Resultado final de cada prueba, la cual puede ser “Cumple” o “No cumple”. Tambien se incluye la opción de “N/A” en caso de que no aplique para la empresa evaluada.

Fuente: Elaboración propia (2021)

En la Figura 23 se muestra un ejemplo de la matriz correspondiente al proceso de personal capacitado, en esta se incluyó la función, categorías y subcategorías necesarias para la evaluación de este.

Figura 23.

Ejemplo de la herramienta

Función	Categoría	ID	Subcategoría	Actividades a realizar	Resultado		Observaciones
Proteger	Entrenamiento de conciencia PR.AT	PR.AT.1	Todos los usuarios están informados y capacitados	1. Revisar las políticas de uso aceptable y/o material de capacitación para garantizar que el contenido es adecuado. 2. Revisar los reportes y/o documentación de capacitación del usuario para garantizar que los usuarios son capacitados de acuerdo con la política, orientación, y/o requisito aplicable (p.ej., capacitación anual sobre ciberseguridad de todos los empleados). 3. Determinar si los materiales de capacitación están actualizados con base a cambios en el entorno de amenazas cibernéticas	No cumple	●	
		PR.AT.2	Los usuarios privilegiados entienden sus roles y responsabilidades.	1. Determinar si la organización tiene un procedimiento para identificar usuarios privilegiados. 2. Determinar si los roles de los usuarios privilegiados están bien definidos y si los usuarios privilegiados están capacitados de acuerdo con sus responsabilidades. 3. Revisar el material de capacitación y/o acuerdos de usuario para asegurar que los usuarios con altos privilegios se les ha enseñado sobre los roles y responsabilidades de seguridad asociados a altos privilegios.	Cumple	●	
		PR.AT.4	Los altos ejecutivos entienden sus roles y responsabilidades.	Revisar los programas de capacitación y educación continua para altos ejecutivos. Considerar lo siguiente: a. Los conocimientos de ciberseguridad y niveles de habilidad para realizar sus deberes están definidos. b. Capacitación específica según roles es asignada teniendo en cuenta los roles y responsabilidades de ciberseguridad. c. Existe un método para medir conocimientos y comprensión de la ciberseguridad de los altos ejecutivos con respecto a los requisitos de la organización. d. Materiales de capacitación y educación están actualizados para reflejar los cambios en el entorno de amenaza	N/A	●	
		PR.AT.5	El personal de seguridad física y de la información entiende sus roles y responsabilidades				

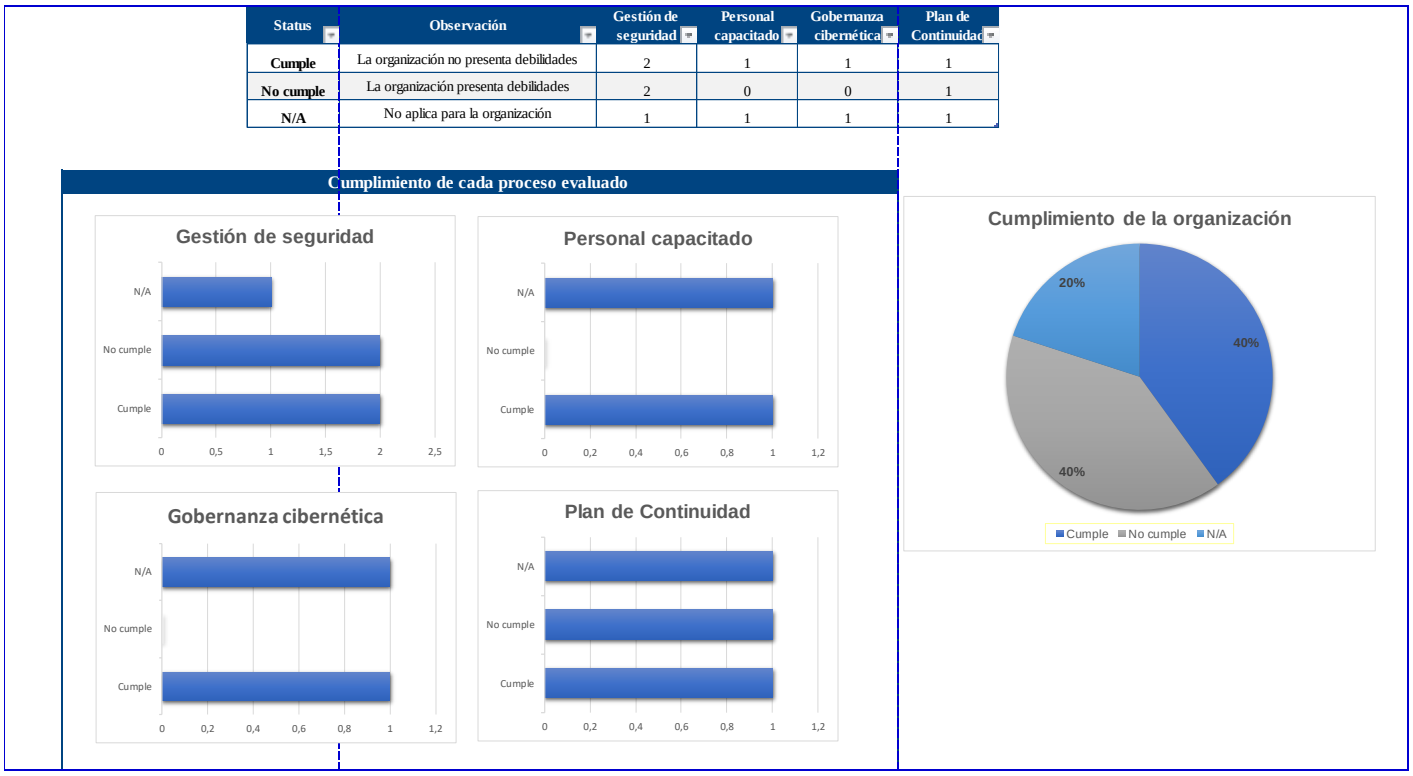
Fuente: Elaboración propia (2021)

5.3.1.1. Resumen de resultados

Una vez que se realice la evaluación utilizando las cuatro matrices definidas anteriormente, el resumen de los resultados se puede observar de forma gráfica, tal como se muestra en la Figura 24, donde se pueden visualizar los resultados por proceso y de forma completa.

Figura 24.

Resumen de resultados



Fuente: Elaboración propia (2021)

5.4.2. Debilidades identificadas

Según el resultado expuesto en la Herramienta evaluación de riesgos, se documentan las debilidades para cada proceso definido anteriormente, utilizando la plantilla presentada en la Figura 25.

Figura 25.

Debilidades identificadas

Documentación de Debilidades
El objetivo de esta herramienta es documentar las debilidades identificadas en los procesos anteriores, a continuación se define cada proceso y en el espacio correspondiente, se deben explicar las observaciones identificadas en cada uno de los procesos, para posteriormente evaluar el impacto de los riesgos.
Gestión de seguridad
Este proceso contiene aquellas actividades que buscan evaluar y conocer la situación actual en términos de gestión de seguridad, es decir se busca identificar cualquier vulnerabilidad de seguridad que pueda afectar la organización
- - -
Personal capacitado
Este proceso contiene aquellas actividades que buscan asegurar que el personal de la organización esté debidamente capacitado y comprenda la naturaleza de las amenazas de ciberseguridad y conozca su papel en la protección de los activos de la organización
- - -
Gobernanza cibernética
Este proceso contiene aquellas actividades que buscan asegurar que la entidad incorpora el ciber gobierno en su régimen de gobernanza
- - -
Continuidad
Este proceso contiene aquellas actividades que buscan asegurar que la entidad cuenta con un plan documentado y aprobado para hacer frente a los incidentes de ciberseguridad
- - -

Fuente: Elaboración propia (2021)

5.4.3. Matriz de Riesgos

La matriz de riesgos corresponde a una matriz para registrar los riesgos que se derivan de las Debilidades identificadas, en esta se debe indicar el impacto y la probabilidad que tiene cada riesgo registrado, con el fin de definir el nivel del riesgo y tomar una decisión sobre el enfoque de la auditoría según el resultado de esta evaluación. En la Figura 26, se muestra un ejemplo de esta herramienta.

Figura 26.

Matriz de Riesgos

Matriz Riesgos						
ID Riesgo	Proceso	Riesgos	Probabilidad	Impacto	Probabilidad*Impacto	Nivel de riesgo
RI-001	Gestión de seguridad	La política de seguridad cibernética de la organización esta desactualizada y no se encuentra aprobada	Poco probable	Medio	2	***Bajo***
			Muy probable	Medio	6	***Medio***
					0	
			Muy probable	Alto	9	***Alto***
					0	
					0	
					0	
					0	

Fuente: Elaboración propia (2021)

5.3.3.1. Impacto de los riesgos

A continuación, en la Tabla 40 se definen el impacto para evaluar el nivel del riesgo utilizados en esta herramienta.

Tabla 40.

Impacto de los riesgos

Valor	Impacto	Descripción
3	**Alto**	Incidentes mayores de ciberseguridad que afectan los estados financieros y que pueden resultar en fraude financiero
2	**Medio**	Incidentes leves que se solucionan de manera oportuna
1	**Bajo**	Se presentan errores leves, que no representan problemas en los estados financieros.

Fuente: Elaboración propia (2021)

5.3.3.2. Probabilidad de los riesgos

En la Tabla 41 se define la probabilidad para evaluar el nivel del riesgo utilizada en esta herramienta.

Tabla 41.

Probabilidad de los riesgos

Valor	Probabilidad	Descripción
3	**Muy probable**	La probabilidad de que ocurra el incidente va entre 1% al 32%
2	**Probable**	La probabilidad de que ocurra el incidente va entre 33% al 65%
1	**Poco probable**	La probabilidad de que ocurra el incidente va entre 66% al 99%

Fuente: Elaboración propia (2021)

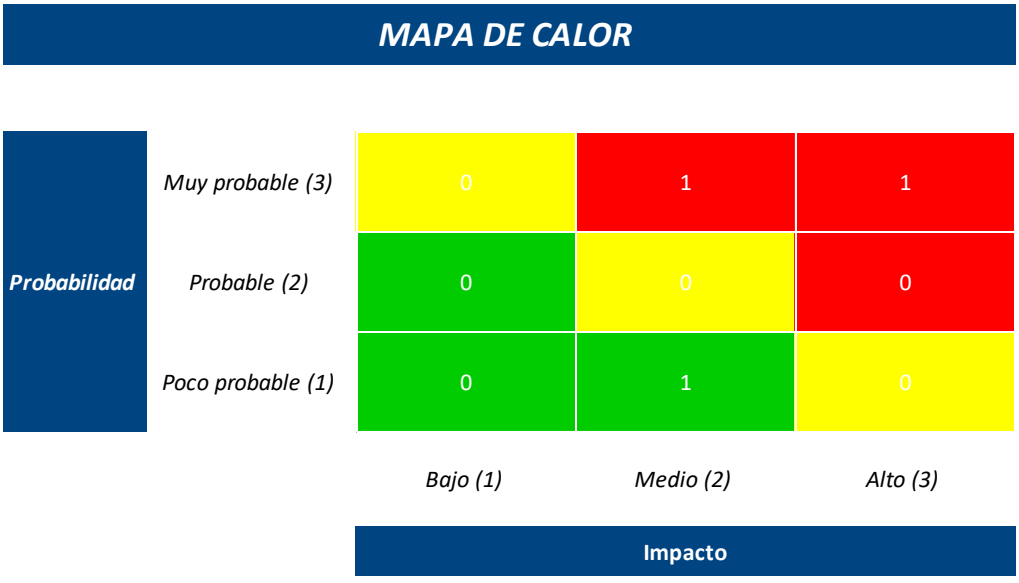
5.4.4. Mapa de Calor

A partir del impacto y la probabilidad definidos previamente se utiliza un mapa de calor para tener una mejor visualización de los riesgos y de esa forma identificar las acciones que se deben tomar a partir del resultado.

A continuación, en la Figura 27 se muestra el mapa de calor donde se indica como se clasifican los riesgos según su impacto y probabilidad.

Figura 27.

Mapa de calor



Fuente: Elaboración propia (2021)

Los niveles de riesgos resultantes de esta evaluación corresponden a los riesgos bajos, riesgos medios y riesgos altos, según el tipo de riesgo se define la acción que se debe tomar, la cual se detalla en la Tabla 42.

Tabla 42.

Acciones a tomar

Riesgos	Acción
Riesgos bajos	Los riesgos identificados no presentan un error material por lo tanto no se debe alterar el enfoque de la auditoría
Riesgos medios	Los riesgos identificados no tienen mayor implicación en los estados financieros por lo tanto no es necesario alterar el enfoque de la auditoría, sin embargo, es punto de mejora
Riesgos altos	Los riesgos identificados afectan los estados financieros, por lo tanto, se debe valorar cambiar el enfoque de la auditoría.

Fuente: Elaboración propia (2021)

5.5. RETORNO DE INVERSIÓN

En este apartado se contemplaron los aspectos financieros relacionados con la elaboración de este proyecto.

5.5.1. Inversión inicial

Los costos que se tomaron en cuenta para la inversión inicial del proyecto son los siguientes:

- **Elaboración del proyecto:** para este rubro se tomaron en cuenta las horas de trabajo del estudiante y las horas de revisión del supervisor del proyecto, los cuales se pueden visualizar en la Tabla 43

Tabla 43.

Costos de la elaboración del proyecto.

	Salario por horas	Horas por semana	Duración del proyecto en semanas	Costo
Estudiante	₡3 750,00	40	14	₡2 100 000,00
Supervisor	₡7 178,27	1	14	₡100 495,77

Fuente: Elaboración propia (2021)

- **Capacitación al área de Auditoría de TI:** para este rubro se toma 1 hora de todos los miembros del equipo de auditoría de TI para realizar una capacitación sobre el funcionamiento de las herramientas propuestas.

En la Tabla 44, se presentan los rubros definidos previamente y el total de la inversión inicial de este proyecto.

Tabla 44.

Inversión Inicial

Rubro	Inversión inicial
Elaboración del proyecto	₡2 200 495,77
Capacitación a Auditoría de TI	₡44 553,27
Total	**₡2 244 924,04**

Fuente: Elaboración propia (2021)

5.5.2. Flujo de efectivo

Para flujo de efectivo se tomó en cuenta la inversión inicial y el costo de operación para tres años; los rubros utilizados para el cálculo de este costo se definen a continuación:

- **Costo de operación:** para el costo de operación se toma en cuenta el salario del auditor que vaya a utilizar las herramientas, el salario de una hora del gerente

encargado de revisar el proyecto, las horas estimadas que se dura en la evaluación y la cantidad de clientes en el que se aplicara esta evaluación; los costos utilizados se definieron en el capítulo anterior específicamente en la Fase 4: Retorno de inversión, sin embargo, en la Tabla 45 se resumen los datos tomados para el cálculo del costo de operación, cabe mencionar que el rubro del auditor ya incluye el aumento salarial anual.

Tabla 45.

Costo de operación

Rubro	Año 1	Año 2	Año 3
Auditor	₡4 187,50	₡4 210,79	₡4 234,22
Horas	15	12	12
Clientes	2	3	5
Gerente proyecto	₡7 178,27	₡7 218,20	₡7 258,36
Total	₡139 981,54	₡173 243,21	₡290 344,90

Fuente: Elaboración propia (2021)

Como se mencionó anteriormente para flujo de efectivo se tomó en cuenta la inversión inicial y el costo de operación los cuales se resumen en la Tabla 46.

Tabla 46.

Flujo de efectivo

Concepto	Año 1	Año 2	Año 3	Total
Elaboración				
Desarrollo	₡1 185 495,77			
Capacitación	₡44 553,27			
Operación				

Concepto	Año 1	Año 2	Año 3	Total
Costos de operación	₡139 981,54	₡173 243,21	₡290 344,90	
Total	₡2 384 905,58	₡173 243,21	₡290 344,90	₡2 848 493,69

Fuente: Elaboración propia (2021)

5.5.3. Retorno de Inversión ROI

Para el cálculo del retorno de inversión se utilizó la inversión inicial y el ingreso correspondiente a la evaluación de riesgos cibernéticos. La fórmula utilizada para este cálculo es la siguiente:

$$ROI = \frac{(Ingreso - Inversión)}{Inversión}$$

En la Tabla 47 se muestra el resultado del ROI del presente proyecto, el cual corresponde a un 21% lo que nos indica que el retorno de inversión del proyecto es positivo.

Tabla 47.

Cálculo del ROI

Concepto	Valores
Ingreso	₡2 723 485,20
Inversión	₡2 244 924,04
ROI	**21%**

Fuente: Elaboración propia (2021)

5.5.4. Valor actual neto y Tasa interna de retorno

Otros de los cálculos realizados para el conocer la rentabilidad del proyecto consisten en el valor actual neto y la tasa interna de retorno, para estos se utilizó la inversión inicial y el flujo de efectivo para los tres años que se valoraron. En la Tabla 48 se muestra el cálculo del

VAN y del TIR, donde se obtuvo un resultado positivo que indica que el proyecto podría generar ganancias a futuro.

Tabla 48.

Factores de valoración

Concepto	Valor
Inversión inicial	-₡2 244 924,04
Año 1	₡2 384 905,58
Año 2	₡173 243,21
Año 3	₡290 344,90
Tasa de interés	0,211890814
VAN	**₡4 081,82**
TIR	**21%**

Fuente: Elaboración propia.(2021)

Según los resultados obtenidos por el ROI, VAN y TIR, se puede decir que el proyecto es rentable y su implementación podría traerle beneficios a la empresa, sin embargo, es importante mencionar que para estos cálculos se utilizaron costos estimados del mercado.

Finalmente, en este capítulo, se describió la propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – *Cybersecurity Framework,* con esta propuesta se espera que el área de auditoría de TI pueda realizar una evaluación más completa y clara.

CAPÍTULO VI

CONCLUSIONES

6. CONCLUSIONES

En este capítulo se presentan las conclusiones que se derivan al desarrollar el presente proyecto, las cuales están asociadas a cada uno de los objetivos específicos planteados

6.1. OBJETIVO ESPECÍFICO 1

En relación con el Objetivo Específico 1: Analizar los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR relacionados con la evaluación de riesgos de ciberseguridad para el entendimiento de las necesidades actuales en materia de riesgos cibernéticos, se concluye lo siguiente:

1- Se logró determinar, mediante la revisión documental, que la empresa cuenta con una metodología propia, que establece las reglas generales en el desarrollo de las auditorías; además de poseer diferentes guías que funcionan como alertas que complementan dicha metodología, entre estas se indican las consideraciones sobre riesgos cibernéticos que utiliza actualmente el área para evaluarlos.

2- Mediante la revisión documental de la guía de consideraciones de riesgos cibernéticos se determinó los procesos relevantes para la evaluación que realiza el área de auditoría de TI a las empresas clientes.

3- Mediante la aplicación de una encuesta y cuatro entrevistas se determinó que el 89% de los colaboradores del área de Auditoría de TI considera que la metodología y las guías empleadas para la evaluación de riesgos cibernéticos no son lo suficientemente claras ni completas para realizar esta evaluación, ya que existen aspectos que no son cubiertos al realizarse de forma indagatoria.

6.2. OBJETIVO ESPECÍFICO 2

En relación con el Objetivo Específico 2: Determinar los componentes del marco de trabajo NIST – Cybersecurity Framework, para la elaboración de las herramientas para el área de auditoría de TI, según las necesidades de la empresa HCR, se concluye lo siguiente:

1- Se determinó que del marco de trabajo NIST–Cybersecurity Framework se utilizó para la elaboración de las herramientas propuestas el Framework Core.
2- De acuerdo con la revisión documental del marco de trabajo NIST–Cybersecurity Framework, específicamente del componente Framework Core, se determinó que este propone cinco funciones: identificar, proteger, detectar, responder y recuperar, las cuales permiten conocer la gestión de riesgos cibernéticos de los clientes, por lo que se tomó como base para la elaboración de las herramientas propuestas.
3- Mediante la revisión documental y las entrevistas realizadas se determinaron las categorías y subcategorías de las funciones del Framework Core, adecuadas para realizar la evaluación de los riesgos cibernéticos.

6.3. OBJETIVO ESPECÍFICO 3

En relación con el Objetivo Específico 3: Elaborar un conjunto de herramientas basada en el marco de trabajo NIST – Cybersecurity Framework y en la documentación actual del área de auditoría de TI para que se cumpla con las necesidades de HCR, se concluye lo siguiente:

1- El uso de este marco permite diseñar una base sólida para la evaluación de riesgos cibernéticos en las auditorías realizadas por HCR. De acuerdo con el análisis de resultados, la elaboración de un conjunto de herramientas, basado en el marco NIST

Cybersecurity Framework, considera aspectos como: adaptabilidad, facilidad y criticidad.

2- La herramienta de evaluación permite definir las actividades que se deben realizar para evaluar los procesos relevantes definidos por HCR y ayuda a identificar debilidades de los clientes, en temas de ciberseguridad, para posteriormente determinar los riesgos cibernéticos que estos presentan.
3- El registro de riesgos funciona como una base para identificar aquellos que pueden afectar el enfoque de la auditoría, mediante un mapa de calor, según su probabilidad y su impacto.

6.4. OBJETIVO ESPECÍFICO 4

En relación con el Objetivo Específico 4: Determinar el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto, se concluye lo siguiente:

1- Se determinó mediante la realización de un análisis financiero que el retorno de inversión de este proyecto corresponde a un 21%, lo que significa que la elaboración de este proyecto es rentable en base a los datos que se utilizaron
2- Por otro lado, se determinó que el valor actual neto es de ₡4 081,82 colones y la tasa de rendimiento interna es del 21% lo que nos indica que el proyecto tiene una rentabilidad positiva para ser implementado según los datos utilizados para el análisis.

CAPÍTULO VII

RECOMENDACIONES

7. RECOMENDACIONES

En este capítulo se describen las recomendaciones que se le brindarán al área de auditoría de TI obtenidas con base en los objetivos específicos considerados en el proyecto.

7.1. OBJETIVO ESPECÍFICO 1

En relación con el Objetivo específico 1: Analizar los procedimientos y documentación actual del área de auditoría de TI de la empresa HCR relacionados con la evaluación de riesgos de ciberseguridad para el entendimiento de las necesidades actuales en materia de riesgos cibernéticos, se recomienda lo siguiente:

1- La empresa debe valorar la posibilidad de contratar a un experto en ciberseguridad para el área de auditoría de TI que garantice la aplicación de la herramienta propuesta potenciando los resultados con criterio técnico especializado.
2- La empresa debe definir una metodología formal para la evaluación de riesgos cibernéticos en las auditorías financieras, que se adecue a las necesidades actuales de los clientes y que sirva como guía para el equipo de auditoría de TI en la ejecución de esta evaluación.

7.2. OBJETIVO ESPECÍFICO 2

En relación con el Objetivo específico 2: Determinar los componentes del marco de trabajo NIST – Cybersecurity Framework, para la elaboración de las herramientas para el área de auditoría de TI, según las necesidades de la empresa HCR, se recomienda lo siguiente:

1- Realizar capacitaciones sobre la implementación de las actividades descritas en el marco de trabajo NIST – Cybersecurity Framework para fomentar el conocimiento y el aprendizaje continuo en temas relacionados con ciberseguridad.

7.3. OBJETIVO ESPECÍFICO 3

En relación con el Objetivo Específico 3: Elaborar un conjunto de herramientas basada en el marco de trabajo NIST – Cybersecurity Framework y en la documentación actual del área de auditoría de TI para que se cumpla con las necesidades de HCR y de sus clientes, se recomienda lo siguiente:

1- Ejecutar un plan piloto, con al menos dos clientes, para implementar las herramientas propuestas y analizar las lecciones aprendidas para su adecuada incorporación.

7.4. OBJETIVO ESPECÍFICO 4

En relación con el Objetivo Específico 4: Determinar el retorno de inversión para el esclarecimiento de los costos y beneficios que se derivan de este proyecto, se recomienda lo siguiente:

1- La organización debe generar nuevos valores del retorno de inversión, posterior a la ejecución del plan piloto con los clientes, con la finalidad de actualizar las variables que muestren información estimada con información real obtenida en el plan piloto.

CAPÍTULO 8

REFERENCIAS BIBLIOGRÁFICAS

8. REFERENCIAS BIBLIOGRÁFICAS

Alvarado, D., & Zumba, L. (2015). Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca. http://dspace.ucuenca.edu.ec/handle/123456789/22342

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

Carbajal Romero, J. (2013). Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del sistema nacional de control peruano https://pirhua.udep.edu.pe/bitstream/handle/11042/2022/MAS_DET_009.pdf?sequen

Cienfuegos, I. (2013). Risk management theory the integrated perspective and its application in the public sector., 89-126. https://dialnet.unirioja.es/servlet/articulo?codigo=5604762

CIS. (2019). Cybersercurity Best Practices. https://www.cisecurity.org/cybersecurity-bestpractices/

CISCO. (2021). What is information security? https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Colegio de Contadores Públicos de Costa Rica. (2021) https://contador.co.cr/salario-del-contador/

Comisión Técnica de los, OCEX. (2018). Guía práctica de fiscalización de los OCEX. https://asocex.es/wp-content/uploads/2018/11/GPF-OCEX-5340-Controles-de-aplicacion-v20181112.pdf

Echemendía, B. (2011). Definiciones acerca del riesgo y sus implicaciones., 470-481. http://scielo.sld.cu/pdf/hie/v49n3/hie14311.pdf

Echenique, J. A. (s.f). Auditoría en Informática. México: McGraw-Hill.

Estupiñán Gaitán, R. (2012). Estados financieros básicos bajo NIC/NIIF (Segunda Edición ed.). ECOE.

Estupiñán Gaitán, R. (2014). Estados financieros básicos bajo NIC/NIIF (Tercera Edición ed.). ECOE.

FAO. (2019). Good Practices. www.fao.org/capacitydevelopment/goodpractices/gphome/es/

Gantz, S. D. (2014). The Basics of IT Audit Purposes, Processes, and Practical Information. Wyman Street, Waltham, USA: Syngress.

Gómez, M. (2016). Elementos de Estadística Descriptiva. (5ª. ed.), EUNED

HCR, (2021). Alerts. Intranet de la empresa

HCR, (2021). Audit Execution Guide. Intranet de la empresa

HCR, (2021). Audit Execution Guide. Intranet de la empresa

HCR, (2021) HCR en Costa Rica. Sitio Web de la empresa

HCR, (2021)¿Quiénes somos?. Sitio Web de la empresa

HCR, (2021)¿ Nuestros Valores?. Sitio Web de la empresa

HCR Canada. (2015). Cyber Security Assessment [Diapositivas de PowerPoint].

HCR Estados Unidos. (2015). Cyber Security Risk Assessment [Diapositivas de PowerPoint]

Hernández, R., Fernández, C. y Baptista, L. (2014). *Metodología de la investigación*. México, D. F.: McGraw Hill/Interamericana Editores, S. A. de C.V.

Hernández, R., Mendoza, C. (2018). *Metodología de la investigación*. México, D. F.: McGraw Hill/Interamericana Editores, S. A. de C.V.

Inces, F. (2019). Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información

INFOCOOP. (2021) Escala salarial. https://www.infocoop.go.cr/node/176

Información jurídica inteligente (2021) Decreto No. 42923-MTSS. https://vlex.co.cr/vid/decreto-no-42923-mtss-869545125

International Federation of Accountants. (2007). ISA 200, Overall Objective of the Independent Auditor, and the Conduct of an Audit in Accordance with International Standards on Auditing

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

International Organization for Standardization. (2012). ISO/IEC 27032:2012 Guidelines for cybersecurity

ISACA. (2014). Guía de Auditoría y Aseguramiento de SI 2202 Análisis de Riesgos en la Planificación.

ISACA. (2015). Glossary of Terms

ISACA. (2018). COBIT 2019 Objetivos de gobierno y gestión.

ISACA. (2018b). COBIT 2019 Marco de Referencia Introducción y metodología

ISACA (2012). Information technology — Security techniques — Guidelines for cybersecurity. Genova: ISO/IEC 27032

ISACA. (2014). IS Audit and Assurance Standard. https://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205-Evidence_gui_Eng_0614.pdf

Kaspesky. (2019). What is Cybersecurity? https://www.kaspersky.com/resourcecenter/definitions/what-is-cyber-security.

KPMG. (2019). Auditoría & Co el portal de la auditoría. http://auditoria-auditores.com/directorio/auditores-kpmg

Kumsuprom, S. (2010). Structured approach to organisational ICT risk management: An empirical study in Thai businesses https://researchrepository.rmit.edu.au/esploro/outputs/doctoral/Structured-approach-to-organisational-ICT-risk/9921861468101341#file-0

Mata, L. (2021) Los sujetos de estudio. https://investigaliacr.com/investigacion/los-sujetos-de-estudio/

Minguillón, A. (2010). La revisión de los controles generales en un entorno informatizado., 125-136. https://asocex.es/wp-content/uploads/PDF/PAG%20PAG%20125-136.pdf

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2011). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

National Institute of Standards and Technology. (2013). NIST Special Publication (SP) 800-53 Revision 4. https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf

National Institute of Standards and Technology. (2016). Guide for Cybersecurity Event Recovery 4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework

NIAS. (2009). *Norma Internacional de Auditoría 500.* Obtenido de http://www.aplicaciones-mcit.gov.co/adjuntos/niif/20%20-%20NIA%20500.pdf

Norton. (2020). What is cybersecurity, what you need to know. https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html

Ñaupas, H., Mejía, E., Novoa, E y Villagómez, A. (2014). Metodología de la investigación cuantitativa - cualitativa y redacción de la tesis.

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

Real Academia Española. (2021). Auditoría. https://dle.rae.es/auditor%C3%ADa

Rivera Peñafiel, M. (2015). Auditoría informática, centros de datos principal de la EP - Petroecuador, dominio supervisar, evaluar y valorar, Cobit 5 http://repositorio.espe.edu.ec/handle/21000/12368

SANS (2021) Controles CIS v8. https://www.sans.org/blog/cis-controls-v8/

Saucedo Mendoza, M. (2006). Planeación de la auditoría en un ambiente de sistemas de información por computadoras en una distribuidora de repuestos http://biblioteca.usac.edu.gt/tesis/03/03_0480.pdf

SGSI. (2015). ISO 27001: ¿Qué significa la Seguridad de la Información? https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Soriano, M.Seguridad en redes y seguridad de la información https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n

Tapia Iturriaga, K. (2013). Handbook of International Quality Control, Auditing, Re-view, Other Assurance, and Related Services Pronouncements. IFAC.

Tapia (2013), Fundamentos de auditoría. Aplicación práctica de las Normas Internacionales de Auditoría. Instituto Mexicano de Contadores Públicos.

Ulate, Vargas, (2014, reimpresión 2019). Metodología para Elaborar una Tesis (1ª. ed.), EUNED

Valencia, F., Marulanda, C., & López, M. (2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. https://www.researchgate.net/publication/311206737_Gobierno_y_gestion_de_riesgos_de_tecnologias_de_informacion_y_aspectos_diferenciadores_con_el_riesgo_organizacional/link/583f334c08ae61f75dc78af8/download

Whitman, M., & Mattord, H. (2017). Principles of information security (6th ed ed.). Cengage Learning.

World Economic Forum (2020) https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

APÉNDICES

APÉNDICES

Apéndice A. Plantilla de solicitud de cambios

Minuta de Reunión #			
Fecha:		**Hora de inicio:**	
Medio:		**Hora Finalización:**	
Objetivo:			

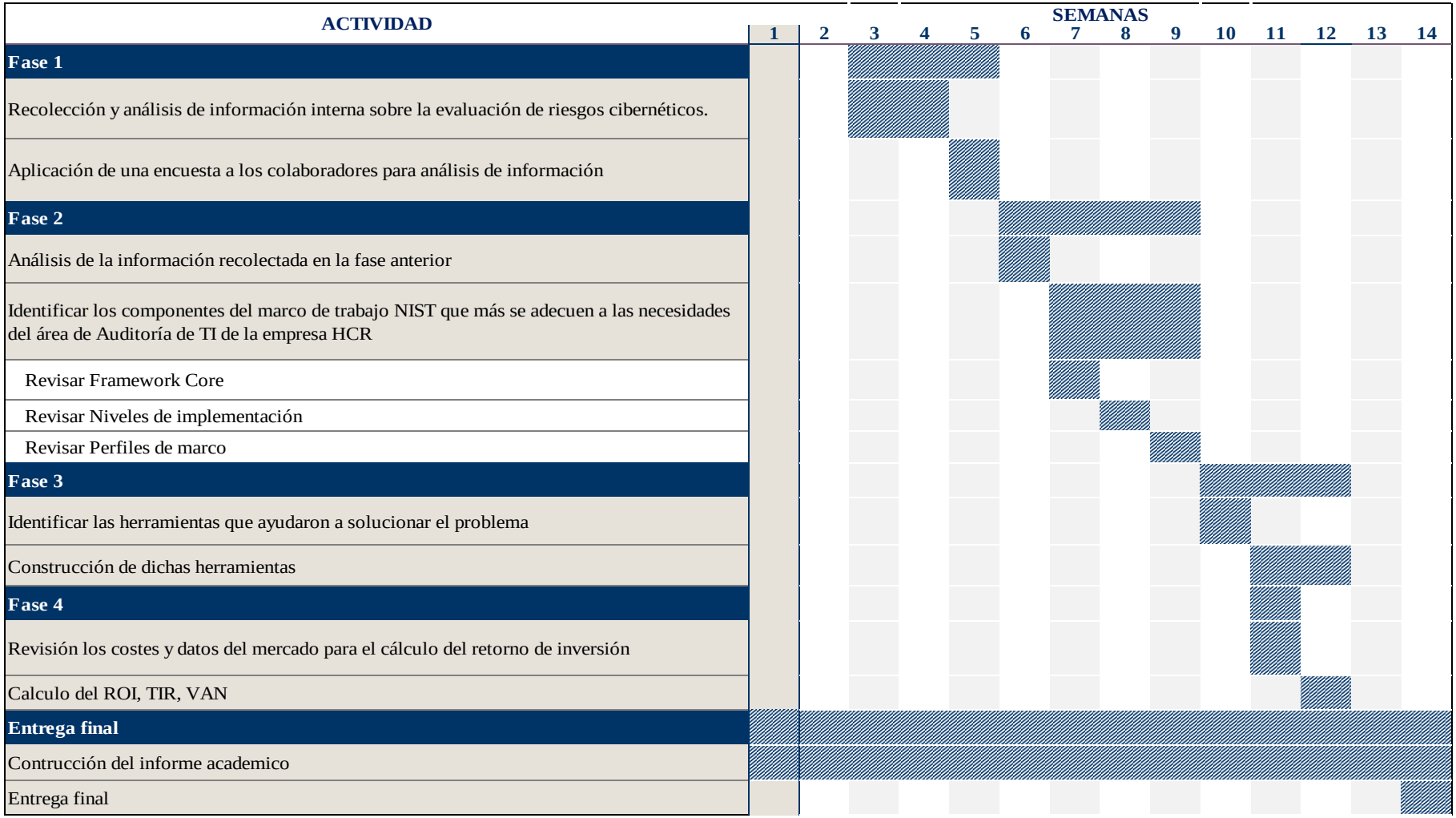
Participantes	Empresa	Rol

Temas a Discutidos	Acuerdos

Temas Pendientes	Responsable

Próxima reunión	Fecha y hora

Apéndice B. Cronograma



Apéndice C. Plantilla encuesta situación actual

Encuesta de situación actual	
Encuesta	
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Preguntas	
1. ¿Cuánto tiempo tiene laborando en el área de auditoría de TI?	
	Menos de 1 año
	Entre 2 y 3 años
	Más de 3 años
2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado?	
	Sí
	No
3. ¿Conoce el procedimiento o metodología para realizar la evaluación brindado por la firma?	
	Sí
	No
4. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente?	
5. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes?	
	Sí
	No
6. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework?	
	Sí
	No
7. ¿Qué opina sobre una propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, según el marco de trabajo NIST?	
8. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?	
	Sí
	No
9. ¿Por qué?	
10. Comentario adicional	

Apéndice D. Plantilla entrevista situación actual

Entrevista Situación actual evaluación riesgos cibernéticos	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:**
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Entrevistado:	
Puesto:	
Años de Experiencia:	
1. ¿Cuáles son las actividades que usted realiza para efectuar esta evaluación?	
2. ¿Considera que la forma en la que actualmente se realiza esta evaluación es adecuada?	
3. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
4. ¿Esa evaluación esta estandarizada, es decir todos los proyectos evaluan los riesgos cibernéticos de la misma forma?	
5. ¿Cómo se realiza la recolección de información?	
6. ¿Qué necesidades tiene la firma para realizar adecuadamente la evaluación de riesgos cibernéticos?	
7. ¿Cuáles oportunidades de mejora considera que se pueden hacer en esta evaluación?	
8. ¿Cuáles considera sean las principales debilidades de la evaluación que se realiza actualmente?	

Apéndice E. Plantilla de entrevista de herramientas

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:**
Objetivo: El objetivo de la entrevista es conocer las expectativas del conjunto de herramientas	
Entrevistado:	
Puesto:	
Años de Experiencia:	
1. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? ¿Por qué?	
2. ¿Cuál es la expectativa general de estas herramientas?	
2. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
3. ¿Qué aspectos se deben tomar en consideración en una herramienta para evaluar los procesos que consideren riesgos de ciberseguridad?	
4. ¿Cómo le gustaría que se presenten los resultados del análisis de información?	
5. Comentarios adicionales a cerca de la propuesta	

Apéndice F. Plantilla para documentar la revisión documental

No	Fecha	Fuente	Nombre del documento	Descripción	Observaciones
001					
002					
003					
00k					

Apéndice G. Respuesta de la encuesta sobre la situación actual

Respuesta 1

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts
   Calificada de forma automática
   - (•) Menos de 1 año
   - ( ) Entre 1 y 3 años
   - ( ) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts
   Calificada de forma automática
   - (•) Si
   - ( ) No

3. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts
   Calificada de forma automática

   Conocer bien cómo manejan manejan dichos riesgos, si cuentan con los recursos necesarios para detectarlos y posteriormente corregirlos en caso de que se materialice alguno

4. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts
   Calificada de forma automática
   - ( ) Si
   - (•) No

5. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? 0 / 0 pts
   Calificada de forma automática
   - ( ) Si
   - (•) No

6. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- (•) Si
- ( ) No

7. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Porque no soy una experta en ciberseguridad y puede que al momento de hacer la evaluación no esté cubriendo ciertos aspectos que puedan ser relevantes

8. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

Me parece que estas herramientas le resultarían muy útiles a todos los miembros del equipo, sobretodo a los que venimos entrando al área y no tenemos suficiente experiencia ni un conocimiento amplio en el tema

Respuesta 2

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts

Calificada de forma automática

- (•) Menos de 1 año
- ( ) Entre 1 y 3 años
- ( ) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

3. ¿Conoce el procedimiento o metodología para realizar la evaluación brindado por la firma? 0 / 0 pts

Calificada de forma automática

- (•) Si
- ( ) No

4. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts

Calificada de forma automática

lo más importante del análisis de riesgos es la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto

5. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts

Calificada de forma automática

- (•) Si
- ( ) No

6. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? — 0 / 0 pts — *Calificada de forma automática*

- (•) Si
- ( ) No

7. ¿Qué opina sobre una propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, según el marco de trabajo NIST? — 0 / 0 pts — *Calificada de forma automática*

Puede utilizarse como referencia para establecer un programa o sistema de seguridad cibernética.

8. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? — 0 / 0 pts — *Calificada de forma automática*

- (•) Si
- ( ) No

9. ¿Por qué? — 0 / 0 pts — *Calificada de forma automática*

Porque se evalúa las vulnerabilidades de una organización o empresa, se puede categorizar estas deficiencias de acuerdo al riesgo, incluso proporcionar reportes continuos, datos estadísticos y también apoya a la organización en el cumplimiento de estándares regulatorios

10. Comentarios u observaciones — 0 / 0 pts — *Calificada de forma automática*

No se proporciona ninguna respuesta.

Respuesta 3

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts

Calificada de forma automática

- (•) Menos de 1 año
- ( ) Entre 1 y 3 años
- ( ) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts

Calificada de forma automática

- (•) Si
- ( ) No

3. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts

Calificada de forma automática

Para determinar si las medidas por el cliente son suficientes para evitar que materialice un riesgo cibernético o puedan minimizar su impacto

4. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

5. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

6. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- (•) Si
- ( ) No

7. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Habría una guía más clara y espero que sencilla para realizar la evaluación.

8. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

No se proporciona ninguna respuesta.

Respuesta 4

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts

Calificada de forma automática

- (•) Menos de 1 año
- ( ) Entre 1 y 3 años
- ( ) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

3. ¿Conoce el procedimiento o metodología para realizar la evaluación brindado por la firma? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

4. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts

Calificada de forma automática

Actualmente con la crisis sanitaria muchas empresas han adoptado la modalidad de teletrabajo y consigo vienen riesgos cibernéticos que pueden afectar a las empresas, por eso importante está evaluando para dar mayor seguridad que se está realizando un buen trabajo

5. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts

Calificada de forma automática

- ( ) Si
- (•) No

6. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? — 0 / 0 pts — *Calificada de forma automática*

- (•) Si
- ( ) No

7. ¿Qué opina sobre una propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, según el marco de trabajo NIST? — 0 / 0 pts — *Calificada de forma automática*

El marco me parece que es muy completo y se ayudaría hacer una mejor evaluación

8. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? — 0 / 0 pts — *Calificada de forma automática*

- (•) Si
- ( ) No

9. ¿Por qué? — 0 / 0 pts — *Calificada de forma automática*

Porque si bien, hay una guía para hacer está evaluación, no es del todo clara y se puede prestar a la interpretación de cada persona, por lo tanto establecer herramientas apoyaría mucho este trabajo

10. Comentarios u observaciones — 0 / 0 pts — *Calificada de forma automática*

Esperaría que las herramientas fueran claras, fáciles de interpretar.

Respuesta 5

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts
Calificada de forma automática

- ○ Menos de 1 año
- ○ Entre 1 y 3 años
- ◉ Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts
Calificada de forma automática

- ◉ Si
- ○ No

3. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts
Calificada de forma automática

Para identificar los riesgos correctamente

4. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts
Calificada de forma automática

- ○ Si
- ◉ No

5. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? 0 / 0 pts
Calificada de forma automática

- ◉ Si
- ○ No

6. ¿Qué opina sobre una propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, según el marco de trabajo NIST?

0 / 0 pts
Calificada de forma automática

My útil, el marco NIST es bastante completo y flexible para adaptarlo a cualquier tipo de empresa

7. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- (•) Si
- ( ) No

8. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Para tener un apoyo y estandarizar el proceso

9. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

No se proporciona ninguna respuesta.

Respuesta 6

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts

Calificada de forma automática

- ○ Menos de 1 año
- ○ Entre 1 y 3 años
- ◉ Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts

Calificada de forma automática

- ◉ Sí
- ○ No

3. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts

Calificada de forma automática

Identificar los riesgos cibernéticos que pueden afectar el resultados de los estados financieros

4. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts

Calificada de forma automática

- ○ Sí
- ◉ No

5. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? 0 / 0 pts

Calificada de forma automática

- ◉ Sí
- ○ No

6. ¿Qué opina sobre una propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, según el marco de trabajo NIST?

0 / 0 pts
Calificada de forma automática

Es interesante, es un marco que abarca otros estándares y se puede adaptar a cualquier empresa

7. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- (•) Si
- ( ) No

8. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Porque la forma en que se realiza la evaluación actualmente es un poco ambigua y nos quedamos solo con la indagación que realizamos con los colaboradores que se encargan de este tema en las empresas

9. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

Esperaría que las herramientas sean fáciles de interpretar y ayuden a realizar una mejor evaluación

Respuesta 7

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts
Calificada de forma automática

- ○ Menos de 1 año
- ◉ Entre 1 y 3 años
- ○ Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts
Calificada de forma automática

- ○ Si
- ◉ No

3. ¿Conoce el procedimiento o metodología para realizar la evaluación brindado por la firma? 0 / 0 pts
Calificada de forma automática

- ◉ Si
- ○ No

4. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts
Calificada de forma automática

Identificar brechas que puedan explotarse y generar afectación de alguna forma en los estados financieros

5. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts
Calificada de forma automática

- ○ Si
- ◉ No

6. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework?

0 / 0 pts
Calificada de forma automática

- Si
- No

7. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- Si
- No

8. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Porque brindaría una base sólida, sustentable y estandarizada para abordar la evaluación de riesgos. Asimismo se tendría claridad y todos los integrantes de IT Audit aplicarían la misma evaluación en todos los proyectos y no sería tan subjetivo como lo es actualmente, por lo tanto habría un incremento sustancial en la calidad de dichas evaluaciones

9. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

No se proporciona ninguna respuesta.

Respuesta 8

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts
Calificada de forma automática

- (○) Menos de 1 año
- (◉) Entre 1 y 3 años
- (○) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts
Calificada de forma automática

- (◉) Si
- (○) No

3. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts
Calificada de forma automática

Identificar incidentes cibernéticos que puedan afectar la auditoria

4. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts
Calificada de forma automática

- (○) Si
- (◉) No

5. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework? 0 / 0 pts
Calificada de forma automática

- (○) Si
- (◉) No

6. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- (•) Si
- ( ) No

7. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Porque facilitaría la evaluación, además de completar lo que se hace actualmente

8. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

No se proporciona ninguna respuesta.

Respuesta 9

1. ¿Cuánto tiempo tiene laborando en el área de IT Audit? 0 / 0 pts
Calificada de forma automática

- (○) Menos de 1 año
- (◉) Entre 1 y 3 años
- (○) Más de 3 años

2. ¿A realizado la evaluación de riesgos cibernéticos en los proyectos que a participado? 0 / 0 pts
Calificada de forma automática

- (○) Si
- (◉) No

3. ¿Conoce el procedimiento o metodología para realizar la evaluación brindado por la firma? 0 / 0 pts
Calificada de forma automática

- (◉) Si
- (○) No

4. ¿Cuál considera que es la importancia de realizar una adecuada evaluación de riesgos cibernéticos en los clientes actualmente? 0 / 0 pts
Calificada de forma automática

Para verificar que no existan incidentes que afecten o afectaron los estados financieros y así poder confiar en la auditoría

5. ¿Considera que la metodología y las guías actuales son claras para poder realizar la evaluación de los riesgos cibernéticos de los clientes? 0 / 0 pts
Calificada de forma automática

- (○) Si
- (◉) No

6. ¿Conoce sobre el marco de trabajo NIST-Cybersecurity Framework?

0 / 0 pts
Calificada de forma automática

- ○ Si
- ◉ No

7. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos?

0 / 0 pts
Calificada de forma automática

- ◉ Si
- ○ No

8. ¿Por qué?

0 / 0 pts
Calificada de forma automática

Porque actualmente la evaluación se hace completando un documento y al no tener mucha experiencia en el tema se puede pasar algo por algo y puede afectar la auditoría, y con las herramientas habría una guía que nos oriente a realizar mejor está evaluancion

9. Comentarios u observaciones

0 / 0 pts
Calificada de forma automática

No se proporciona ninguna respuesta.

Apéndice H. Respuesta entrevista sobre situación actual gerente del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha: 15/10/2021**
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Puesto: Gerente	
Años de Experiencia: 24 años	
1. ¿Cuáles son las actividades que usted realiza para efectuar esta evaluación?	
Mi función es revisar lo que hacen los muchachos, por lo tanto, yo reviso que la evaluación que se realizó cumpla con lo que se pide en la guía establecida para la evaluación de este tema. Sin embargo, si sé que esta evaluación se realiza de forma indagatoria por medio de entrevistas a la gerencia encargada de los clientes.	
2. ¿Considera que la forma en la que actualmente se realiza esta evaluación es adecuada?	
No, esta es una evaluación muy importante actualmente y lo que se hace es totalmente indagatoria y así no se puede tener la certeza de lo que se revisa sea correcto	
3. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Políticas y documentación relacionada con el proceso. Informes presentados a la gerencia. Listado de incidentes de ciberseguridad. Capturas de pantalla a nivel de las herramientas utilizadas para el proceso	
4. ¿Esa evaluación esta estandarizada, es decir todos los proyectos evalúan los riesgos cibernéticos de la misma forma?	
Se tiene que evaluar lo establecido por la firma mediante las alertas que brindan, sin embargo, la evaluación como tal se hace diferente en cada proyecto, siempre que al final se complete un memo con el resultado de esta.	

5. ¿Cómo se realiza la recolección de información?
Como ya he mencionado se realiza de forma indagatoria entonces la información se tiene mediante entrevistas principalmente.
6. ¿Qué necesidades tiene la firma para realizar adecuadamente la evaluación de riesgos cibernéticos?
-Hacer un mejor trabajo -Dar mayor seguridad a los estados financieros para poder confiar en ellos -Asegurarse si los clientes han tenido incidentes cibernéticos, y si los han tenido revisar el impacto que tuvieron en los estados financieros y pueden tener en la auditoría.
7. ¿Cuáles oportunidades de mejora considera que se pueden hacer en esta evaluación?
-Hacer una revisión más profunda - Tener algún experto en el tema que sustente lo evaluado.
8. ¿Cuáles considera sean las principales debilidades de la evaluación que se realiza actualmente?
Solamente nos quedamos con la indagación, y no es suficiente para esta evaluación
9. Comentarios adicionales a cerca de la propuesta
Esta evaluación tiene muchas limitaciones, sin embargo, la más importante es que ningún miembro del equipo es experto en ciberseguridad y es algo necesario para realizar una evaluación adecuada.

Apéndice I. Respuesta entrevista sobre situación actual encargado del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha: 11/10/2021**
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Entrevistado: Verónica Guzmán	
Puesto: Encargado 1	
Años de Experiencia: 4 años	
1. ¿Cuáles son las actividades que usted realiza para efectuar esta evaluación?	
Se realiza una entrevista con el área de negocio y de TI de la empresa para observar e indagar su posición en el tema de acuerdo con lo que dice la guía de la firma	
2. ¿Considera que la forma en la que actualmente se realiza esta evaluación es adecuada?	
No, porque me parece que solamente indagamos y no probamos si realmente la información es correcta	
3. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Información orientada a incidencias y resolución de problemas	
4. ¿Esa evaluación esta estandarizada, es decir todos los proyectos evalúan los riesgos cibernéticos de la misma forma?	
Me parece que no, cada compañero lo hace diferente porque está abierta a interpretaciones	
5. ¿Cómo se realiza la recolección de información?	
Mediante entrevistas con la empresa	

6. ¿Qué necesidades tiene la firma para realizar adecuadamente la evaluación de riesgos cibernéticos?
Para saber cómo la empresa maneja los riesgos de ciberseguridad en caso de un ataque más ahora con la situación actual del Covid 19, porque puede afectar los resultados de la auditoría
7. ¿Cuáles oportunidades de mejora considera que se pueden hacer en esta evaluación?
-Estandarizar -mejora de consultas, -Herramientas o guías -Expertos
8. ¿Cuáles considera sean las principales debilidades de la evaluación que se realiza actualmente?
Solamente nos quedamos con la indagación, con lo que nos dicen en las entrevistas, entonces no nos podemos asegurar que lo que se está haciendo sea correcto

Apéndice J. Respuesta entrevista sobre situación actual asistente ii del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha: 13/10/2021**
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Entrevistado: Deiber Ureña González	
Puesto: Asistente II	
Años de Experiencia: 2 años	
1. ¿Cuáles son las actividades que usted realiza para efectuar esta evaluación?	
Indagar sobre el proceso de evaluación y respuesta ante riesgos cibernéticos, y si se encuentra documentado y aprobado. Extraer y observar la lista de incidentes de seguridad cibernética. Indagar sobre la evaluación de la seguridad y pruebas periódicas de vulnerabilidad. Indagar sobre la concientización en temas de seguridad para usuarios finales, así como, procedimientos/políticas de seguridad y su disponibilidad para ser consultadas por estos usuarios. Indagar y observar las herramientas de monitoreo de red. Identificar el software utilizado para detectar y proteger de las amenazas. Indagar sobre la generación de informes a la gerencia, e inspeccionar esta documentación.	
2. ¿Considera que la forma en la que actualmente se realiza esta evaluación es adecuada?	
Actualmente el proceso carece de maduración, ya que solo se obtiene un entendimiento superficial sobre la evaluación de ciberseguridad. Y el personal no cuenta con conocimientos profundos sobre este tema.	

3. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?
Políticas y documentación relacionada con el proceso. Informes presentados a la gerencia. Listado de incidentes de ciberseguridad. Capturas de pantalla a nivel de las herramientas utilizadas para el proceso
4. ¿Esa evaluación esta estandarizada, es decir todos los proyectos evalúan los riesgos cibernéticos de la misma forma?
Me parece que no, aunque son los procedimientos que se indican seguir en el sitio de calidad, se pueden interpretar diferente
5. ¿Cómo se realiza la recolección de información?
Se realiza mediante una sesión con el personal encargado, y se genera una minuta. Además, se envía al equipo auditor la evidencia generada durante la reunión vía correo electrónico.
6. ¿Qué necesidades tiene la firma para realizar adecuadamente la evaluación de riesgos cibernéticos?
Podría apoyar el proceso en algún marco de trabajo o norma, que ayude a profundizar la evaluación, así como brindar una orientación al personal para que realicen la evaluación apegados a estas mejoras.
7. ¿Cuáles oportunidades de mejora considera que se pueden hacer en esta evaluación?
Incluir algún frameworks que sustente la evaluación y orientar con mayor conocimiento del tema al personal encargado que realiza la evaluación.
8. ¿Cuáles considera sean las principales debilidades de la evaluación que se realiza actualmente?
Carece de madurez, es decir que no es claro

Apéndice K. Respuesta entrevista sobre situación actual asistente i del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha: 11/10/2021**
Objetivo: El objetivo de la entrevista es conocer sobre la situación actual referente a la evaluación de riesgos cibernéticos realizada en los proyectos	
Entrevistado: Natalia Bonilla Quirós	
Puesto: Asistente I	
Años de Experiencia: 1 año	
1. ¿Cuáles son las actividades que usted realiza para efectuar esta evaluación?	
Inspección de documentos e indagación con los encargados de ciberseguridad	
2. ¿Considera que la forma en la que actualmente se realiza esta evaluación es adecuada?	
No, solamente indagamos y no probamos si realmente la información es correcta	
3. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Organigrama del área de ciberseguridad, manuales de puestos, políticas y procedimientos relacionadas con ciberseguridad, herramientas para incidentes de seguridad, monitoreo de red y aplicaciones para prevenir ataques. También reportes de incidentes que hayan tenido en el periodo y reportes de evaluación que haya hecho algún tercero	
4. ¿Esa evaluación esta estandarizada, es decir todos los proyectos evalúan los riesgos cibernéticos de la misma forma?	
No, porque he visto que hay muchas interpretaciones	
5. ¿Cómo se realiza la recolección de información?	
Se realiza mediante una sesión con el personal encargado, y se genera una minuta. Además, se envía al equipo auditor la evidencia generada durante la reunión vía correo electrónico.	

6. ¿Qué necesidades tiene la firma para realizar adecuadamente la evaluación de riesgos cibernéticos?
Identificar el nivel de riesgo que hay para saber si afecta la auditoría
7. ¿Cuáles oportunidades de mejora considera que se pueden hacer en esta evaluación?
Primeramente, estandarizar el proceso, esto debido a que no todos realizamos la evaluación de la misma forma
8. ¿Cuáles considera sean las principales debilidades de la evaluación que se realiza actualmente?
Actualmente todos realizamos la evaluación de forma diferente. No tenemos el conocimiento suficiente para saber si la evaluación realizada es efectiva

Apéndice L. Respuesta entrevista sobre herramientas esperadas al gerente del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:** 15/10/201
Objetivo: El objetivo de la entrevista es conocer las expectativas del conjunto de herramientas	
Puesto: Gerente	
Años de Experiencia: 24 años	
1. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? ¿Por qué?	
Sí, sería útil ya que le brindaría al equipo recursos para mejorar la evaluación que se hace actualmente	
2. ¿Cuál es la expectativa general de estas herramientas?	
Que sean intuitivas y faciliten la evaluación de alguna manera	
2. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Lo que se indica en la alertas que da firma	
3. ¿Qué aspectos se deben tomar en consideración en una herramienta para evaluar los procesos que consideren riesgos de ciberseguridad?	
-Que cumpla con lo que pide la firma -Guía de lo que se tiene que hacer	
4. ¿Cómo le gustaría que se presenten los resultados del análisis de información?	
Tal vez con una matriz fácil de usar por cualquier miembro del equipo.	
5. Comentarios adicionales a cerca de la propuesta	
Lo que se hace actualmente no es suficiente, y espero que estas herramientas sean un mapa para ir mejorando la forma en la que se hace esta evaluación	

Apéndice M. Respuesta entrevista sobre herramientas esperadas al encargado del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:** 14/10/201
Objetivo: El objetivo de la entrevista es conocer las expectativas del conjunto de herramientas	
Entrevistado: Verónica Guzmán	
Puesto: Encargado 1	
Años de Experiencia: 4 años	
1. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? ¿Por qué?	
Sí, sería muy útil, porque serviría como guía y facilitaría hacer esta revisión.	
2. ¿Cuál es la expectativa general de estas herramientas?	
Que sean intuitivas y faciliten la evaluación de alguna manera y que haya una mejora en la identificación de riesgos en cuanto a la información obtenida	
2. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Lo que pide la metodología y en la guía que tiene la firma	
3. ¿Qué aspectos se deben tomar en consideración en una herramienta para evaluar los procesos que consideren riesgos de ciberseguridad?	
-Actividades	
4. ¿Cómo le gustaría que se presenten los resultados del análisis de información?	
-Gráficas -Matriz	
5. Comentarios adicionales a cerca de la propuesta	
No, lo mismo pienso que puede ser de mucha ayuda para el equipo.	

Apéndice N. Respuesta entrevista sobre herramientas esperadas a asistente ii del área de auditoría de TI

Detalles de la entrevistaA1:F15A19A1:F13A1:F17A1:F15	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:** 14/10/201
Objetivo: El objetivo de la entrevista es conocer las expectativas del conjunto de herramientas	
Entrevistado: Deiber Ureña González	
Puesto: Asistente II	
Años de Experiencia: 2 años	
1. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? ¿Por qué?	
Sí, sería muy útil podrían facilitar la revisión del proceso, así como la estandarización del mismo.	
2. ¿Cuál es la expectativa general de estas herramientas?	
Que sean intuitivas y faciliten la evaluación de alguna manera	
2. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Lo que pide la metodología y en la guía que tiene la firma	
3. ¿Qué aspectos se deben tomar en consideración en una herramienta para evaluar los procesos que consideren riesgos de ciberseguridad?	
Se podría considerar un conjunto de riesgos para considerados durante las revisiones, que el auditor elija los que determina son potenciales o cubiertos por la organización auditada. Sin embargo, hay que tener en cuenta que todos los clientes son diferentes y tenemos que revisar lo que el cliente tiene implementado. Entonces, los riesgos podrían variar, por eso, un set de controles que permita asignar a cada cliente los que apliquen.	
4. ¿Cómo le gustaría que se presenten los resultados del análisis de información?	
-Un Excel que muestre el análisis y resultado	
5. Comentarios adicionales a cerca de la propuesta	
No, igual esperar que la herramienta ayude con esta evaluación.	

Apéndice O. Respuesta entrevista sobre herramientas esperadas a asistente i del área de auditoría de TI

Detalles de la entrevista	
Detalles de la entrevista	
Tipo de entrevista: Estructurada	**Fecha:** 14/10/201
Objetivo: El objetivo de la entrevista es conocer las expectativas del conjunto de herramientas	
Entrevistado: Natalia Bonilla Quirós	
Puesto: Asistente I	
Años de Experiencia: 1 años	
1. ¿Considera que un conjunto de herramientas para la evaluación de riesgos cibernéticos ayudaría a la evaluación de riesgos cibernéticos realizada en los proyectos? ¿Por qué?	
Sí, sería muy útil porque actualmente cada quien tiene las suyas propias.	
2. ¿Cuál es la expectativa general de estas herramientas?	
Que el proceso sea estandarizado y cubra todos los riesgos	
2. ¿Qué información se solicita generalmente a las empresas para realizar esta evaluación?	
Lo que pide la metodología y en la guía que tiene la firma	
3. ¿Qué aspectos se deben tomar en consideración en una herramienta para evaluar los procesos que consideren riesgos de ciberseguridad?	
Que se adapte a cualquier tipo de empresa	
4. ¿Cómo le gustaría que se presenten los resultados del análisis de información?	
-En una matriz	
5. Comentarios adicionales a cerca de la propuesta	
No, como lo dije antes pueden ayudar a dejar mucho más clara como se hace esta evaluación	

Apéndice P. Bitácora de revisión documental

No	Fecha	Fuente	Nombre
001	Julio-Agosto	Sitio Web HCR	¿Quiénes somos?
002	Julio-Agosto	Sitio Web HCR	Nuestros Valores
003	Julio-Agosto	Sitio Web HCR	Servicios
004	Agosto-Setiembre	Intranet HCR	Cyber security and the financial statement audit
005	Agosto-Setiembre	Intranet HCR	Metodologías HCR
006	Agosto-Setiembre	Intranet HCR	HCR Audit Execution Guide
007	Agosto-Setiembre	Intranet HCR	HCR Alerts
008	Agosto-Setiembre	Intranet HCR	Attachment 1 –New activity -Understand cybersecurity risks and incidents
009	Agosto-Setiembre	Intranet HCR	Attachment 2 –Revisions to activity - Understand cybersecurity risks and incidents
010	Agosto-Setiembre	Intranet HCR	Attachment 3 –Revisions to activity - Understand cybersecurity risks and incidents
011	Agosto-Setiembre	Intranet HCR	Attachment 4 –Cybersecurity Risk Considerations work paper
012	Setiembre-Octubre	Intranet HCR	Cybersecurity risk considerations – new required work paper and revised methodology
013	Setiembre-Octubre	NIST	CYBERSECURITY FRAMEWORK
014	Setiembre-Octubre	NIST	An Introduction to the Components of the Framework
015	Setiembre-Octubre	NIST	Uses and Benefits of the Framework
016	Setiembre-Octubre	NIST	Informative References: What are they, and how are they used?
017	Setiembre-Octubre	NIST	NIST SP 800-53 Rev. 4
018	Setiembre-Octubre	NIST	National Online Informative References Program
019	Setiembre-Octubre	NIST	The Five Functions Share

No	Fecha	Fuente	Nombre
020	Setiembre-Octubre	NIST	Framework for Improving Critical Infrastructure Cybersecurity V1.0
021	Setiembre-Octubre	NIST	Framework for Improving Critical Infrastructure Cybersecurity V1,1
022	Setiembre-Octubre	NIST	Framework V1.0 Core (Excel)
023	Setiembre-Octubre	NIST	Framework V1.1 Core (Excel)
024	Setiembre-Octubre	ISO	ISO / IEC 27001: 2013
025	Setiembre-Octubre	ISACA	COBIT 5
026	Setiembre-Octubre	CIS CSC	CIS Critical Security Controls
027	Setiembre-Octubre	ISA	ISA 62443-2-1:2010
028	Setiembre-Octubre	ISA	ISA 62443-3-3:2013

Apéndice Q: Minuta con la organización de inicio del proyecto

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	02/08/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00 pm. / 4:30 pm
Objetivo de la reunión:	Inicio del proyecto		
Participantes:	Presentes: -Eric Mora -Hellen Cordero		

Temas Tratados	
No.	**Temas discutidos**
1	Se comentan generalidades del proyecto: -Nombre del proyecto -Presentación del anteproyecto -Cronograma del proyecto

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**
Por definir	Por definir	Por definir

Apéndice R: Minuta entrevista - situación actual gerente

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	04	**Fecha:**	15/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00 pm. / 4:30 pm
Objetivo de la reunión:	Situación actual referente a la evaluación de riesgos cibernéticos		
Participantes:	Presentes: -Eric Mora -Hellen Cordero		

Temas Tratados

No.	Temas discutidos
1	Descripción del proyecto
2	Como se realiza actualmente la evaluación de riesgos cibernéticos
3	Comentarios sobre la forma y los recursos de la empresa para realizar la evaluación de riesgos cibernéticos.
4	Limitaciones de la evaluación de riesgos cibernéticos actual

Próxima reunión

Temas por tratar	Fecha	Convocados
Herramientas para la evaluación de riesgos cibernéticos	Por definir	Eric Mora

Apéndice S: Minuta entrevista - situación actual encargado

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	11/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	8:00 am. / 8:30 am
Objetivo de la reunión:	Situación actual referente a la evaluación de riesgos cibernéticos		
Participantes:	Presentes: -Verónica Guzmán -Hellen Cordero		

Temas Tratados

No.	Temas discutidos
1	Descripción del proyecto
2	Como realiza el entrevistado actualmente la evaluación de riesgos cibernéticos
3	Comentarios sobre la forma y los recursos de la empresa para realizar la evaluación de riesgos cibernéticos.

Próxima reunión

Temas por tratar	Fecha	Convocados
Herramientas para la evaluación de riesgos cibernéticos	Por definir	Verónica Guzmán

Apéndice T: Minuta entrevista - situación actual asistente II

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	03	**Fecha:**	13/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:30 pm. / 5:00 pm
Objetivo de la reunión:	Situación actual referente a la evaluación de riesgos cibernéticos		
Participantes:	Presentes: -Deiber Ureña González -Hellen Cordero		

Temas Tratados

No.	Temas discutidos
1	Descripción del proyecto
2	Como realiza el entrevistado actualmente la evaluación de riesgos cibernéticos
3	Comentarios sobre la forma y los recursos de la empresa para realizar la evaluación de riesgos cibernéticos.

Próxima reunión

Temas por tratar	Fecha	Convocados
Herramientas para la evaluación de riesgos cibernéticos	Por definir	Deiber Ureña González

Apéndice U: Minuta entrevista - situación actual asistente I

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	02	**Fecha:**	11/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:30 pm. / 5:00 pm
Objetivo de la reunión:	Situación actual referente a la evaluación de riesgos cibernéticos		
Participantes:	Presentes: -Natalia Bonilla Quirós -Hellen Cordero		

Temas Tratados

No.	Temas discutidos
1	Descripción del proyecto
2	Como realiza el entrevistado actualmente la evaluación de riesgos cibernéticos
3	Comentarios sobre la forma y los recursos de la empresa para realizar la evaluación de riesgos cibernéticos.

Próxima reunión

Temas por tratar	Fecha	Convocados
Herramientas para la evaluación de riesgos cibernéticos	Por definir	Natalia Bonilla Quirós

Apéndice V: Minuta entrevista herramientas esperadas -gerente

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	04	**Fecha:**	15/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00 pm. / 4:30 pm
Objetivo de la reunión:	Conocer expectativas de la herramienta		
Participantes:	Presentes: -Eric Mora -Hellen Cordero		

Temas Tratados	
No.	**Temas discutidos**
1	Se comenta lo tratado en la reunión pasada
2	Opinión sobre la utilidad de las herramientas
3	Expectativas del proyecto

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**
Presentación de la herramienta	Por definir	Eric Mora

Apéndice W: Minuta entrevista herramientas esperadas - encargado

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	03	**Fecha:**	14/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00 pm. / 4:30 pm
Objetivo de la reunión:	Conocer expectativas de la herramienta		
Participantes:	Presentes: -Verónica Guzmán -Hellen Cordero		

Temas Tratados	
No.	**Temas discutidos**
1	Se comenta lo tratado en la reunión pasada
2	Opinión sobre la utilidad de las herramientas
3	Expectativas del proyecto

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**

Apéndice X: Minuta entrevista herramientas esperadas - asistente II

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	17/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	8:00 am. / 8:30 am
Objetivo de la reunión:	Conocer expectativas de la herramienta		
Participantes:	Presentes: -Deiber Ureña González -Hellen Cordero		

Temas Tratados	
No.	**Temas discutidos**
1	Se comenta lo tratado en la reunión pasada
2	Opinión sobre la utilidad de las herramientas
3	Expectativas del proyecto

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**

Uso Confidencial Pág. 1/1

Apéndice Y: Minuta entrevista herramientas esperadas - asistente I

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	02	**Fecha:**	14/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	8:00 am. / 8:30 am
Objetivo de la reunión:	Conocer expectativas de la herramienta		
Participantes:	Presentes: -Natalia Bonilla Quirós -Hellen Cordero		

Temas Tratados

No.	Temas discutidos
1	Se comenta lo tratado en la reunión pasada
2	Opinión sobre la utilidad de las herramientas
3	Expectativas del proyecto

Próxima reunión

Temas por tratar	Fecha	Convocados

Apéndice Z: Minuta revisión preliminar de las herramientas con el gerente del área de auditoría de TI

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	27/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00 pm. / 4:30 pm
Objetivo de la reunión:	Presentación preliminar de las herramientas		
Participantes:	Presentes: -Eric Mora -Hellen Cordero		

Temas Tratados	
No.	**Temas discutidos**
1	Criterios que se tomaron en cuenta para las herramientas
2	Procesos que se van a evaluar
3	Funciones, categorías, subcategorías y actividades contempladas para evaluar cada proceso

Próxima reunión		
Temas por tratar	**Fecha**	**Convocados**

Apéndice AA. Minuta reunión 1 con la organización y profesor tutor

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	06-08-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:30pm-5:15pm
Objetivo de la reunión:	Reunión inicial con la organización por parte del profesor tutor		
Participantes:	Presentes: Eric Mora, Laura Alpizar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de los trabajos de graduación**	Se presento el nombre del proyecto que va a realizar cada estudiante.	
2	**Responsabilidades de las partes**	Se presentaron las responsabilidades que debe cumplir cada parte durante el desarrollo del trabajo final de graduación (Estudiante y Organización)	
3	**Evaluación del trabajo final de graduación**	Se presento la evaluación correspondiente al trabajo final de graduación	
4	**Rubrica de la organización**	Se presenta la rúbrica de calificación de la organización	• Enviar rúbrica a la empresa en las semanas correspondiente a las evaluaciones. • Consultar con la coordinadora de trabajo de graduación por el formato de la rúbrica de la empresa ***Responsable: Hellen Cordero***
5	**Cronograma del proyecto**	Se presenta el cronograma del proyecto y se plantean las fechas tentativas para las próximas reuniones.	• Recordar evaluaciones • Fechas tentativas próximas reuniones: -Viernes 17 septiembre 2021, 4:30pm -Viernes 22 de octubre 2021, 4:30pm ***Responsable: Hellen Cordero***

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Próxima reunión		
Temas para tratar	**Fecha**	**Convocados**
Avance del proyecto de graduación	Viernes 17 septiembre 2021 Hora: 4:30pm	Laura Alpizar Eric Mora Hellen Cordero

Eric Mora Rugama — Digitally signed by Eric Mora Rugama Date: 2021.11.05 15:11:12 -06'00'

Firma del responsable de la organización Eric Mora Rugama

Deiber Ureña González — Digitally signed by Deiber Ureña González Date: 2021.11.05 17:42:58 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

LAURA CRISTINA ALPIZAR CHAVES (FIRMA) — Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA) Fecha: 2021.11.05 19:00:35 -06'00'

Firma de profesor Tutor
Laura Alpizar Chávez

Hellen Cordero Robles — Digitally signed by Hellen Cordero Robles Date: 2021.11.05 17:56:57 -06'00'

Firma del estudiante
Hellen Cordero Robles

Apéndice BB. Minuta reunión 2 con la organización y profesor tutor

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	02	**Fecha:**	08-10-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00pm-5:00pm
Objetivo de la reunión:	Reunió inicial de seguimiento con la empresa.		
Participantes:	Presentes: Eric Mora, Laura Alpízar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de la reunión**	Profesora indica el objetivo de la reunión y se menciona el orden en que presentaran los estudiantes.	
2	**Presentación de Avance Hellen Cordero**	Se realizó una pequeña presentación por parte de la estudiante Hellen Cordero donde se indica el trabajo realizado hasta el momento y el trabajo pendiente. También se indica el tiempo que falta para concluir con el TFG	
3	**Presentación de Avance Deiber Ureña**	Se realizó una pequeña presentación por parte del estudiante Deiber Ureña donde se indica el trabajo realizado hasta el momento y el trabajo pendiente.	
4	**Comentarios finales**	Se comenta que no se han presentado problemas con la empresa y los estudiantes tienen el apoyo de esta.	

Próxima reunión

Temas para tratar	Fecha	Convocados
Reunión final con la organización	Por definir	Laura Alpízar Eric Mora Hellen Cordero

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Eric Mora Rugama
Digitally signed by Eric Mora Rugama
Date: 2021.11.05 15:11:56 -06'00'

Firma del responsable de la organización
Eric Mora Rugama

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.05 19:01:44 -06'00'

Firma de profesor Tutor
Laura Alpizar Chávez

Deiber Ureña González
Digitally signed by Deiber Ureña González
Date: 2021.11.05 17:41:18 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

Hellen Cordero Robles
Digitally signed by Hellen Cordero Robles
Date: 2021.11.05 18:00:32 -06'00'

Firma del estudiante
Hellen Cordero Robles

Apéndice CC. Minuta reunión 3 con la organización y profesor tutor

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	03	**Fecha:**	03-11-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	9:30am-10:30am
Objetivo de la reunión:	Reunió inicial con la organización por parte del profesor tutor		
Participantes:	Presentes: Eric Mora, Laura Alpízar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de los resultados por parte de Hellen Cordero**	Se presentaron los resultados obtenidos, y se explicaron las herramientas realizadas por la estudiante Hellen Cordero	
2	**Presentación de los resultados por parte de Deiber Ureña**	Se presentaron los resultados obtenidos, y se explicó el set de herramientas realizadas por el estudiante Deiber Ureña	
3	**Comentarios finales**	• Agradecimiento a ambas partes por el apoyo brindado • Comentarios sobre la utilidad de las herramientas presentadas	

Eric Mora Rugama — Digitally signed by Eric Mora Rugama Date: 2021.11.05 15:12:39 -06'00'

Firma del responsable de la organización
Eric Mora Rugama

Hellen Cordero Robles — Digitally signed by Hellen Cordero Robles Date: 2021.11.05 17:53:34 -06'00'

Firma del estudiante
Hellen Cordero Robles

LAURA CRISTINA ALPIZAR CHAVES (FIRMA) — Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA) Fecha: 2021.11.05 19:01:07 -06'00'

Firma de profesor Tutor
Laura Alpízar Chávez

Deiber Ureña González — Digitally signed by Deiber Ureña González Date: 2021.11.05 17:45:30 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

Apéndice DD. Carta de aceptación de minutas entre el profesor y el estudiante

TEC | Tecnológico de Costa Rica

ati
Área Académica de Administración de Tecnologías de Información
Licenciatura en Administración de Tecnología de Información

Cartago, Costa Rica, 5 de noviembre 2021

Asunto: Aceptación de las minutas de reunión del TFG

Mediante la presente yo Hellen Cordero Robles carnet universitario 2015183067, estudiante de la carrera Administración de Tecnología de Información, solicita a aprobación de las minutas realizadas durante el trabajo final de graduación (TFG) durante el II Semestre 2021.

Esta aprobación incluye las siguientes minutas:

- Minuta#1: 31/07/2021
- Minuta#2:30/08/2021
- Minuta#3:24/09/2021
- Minuta#4: 07/10/2021
- Minuta#5: 22/10/2021
- Minuta#6: 29/10/2021
- Minuta#:04/11/2021

Sin más que agregar me despido

Muchas gracias de antemano

Atentamente

Hellen Cordero Robles
Digitally signed by Hellen Cordero Robles
Date: 2021.11.05 17:53:34 -06'00'

Hellen Cordero Robles
Carné 2015183067

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.04 19:04:31 -06'00'

Laura Alpizar Chaves
Profesora tutora

Apéndice EE. Minuta reunión 1 con la tutora

MINUTA DE REUNIÓN

Proyecto: Elaboración de una propuesta de un conjunto de herramientas para la evaluación de los riesgos cibernéticos en las auditorías financieras, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	01	**Fecha:**	31-07-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	1:45pm-2:45pm
Objetivo de la reunión:	Reunió inicial para contacto con el profesor tutor y ver aspectos generales para la elaboración del trabajo final de graduación		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero, Deiber Ureña, Sebastián Grossberger		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Capítulos de Investigación**	La profesora explica cada capítulo del contenido en el trabajo final de graduación.	Elaborar documentos desde 0 con los títulos correspondientes a cada capítulo. Encargado: cada estudiante (Hellen Cordero)
2	**Método para la elaboración del TFG**	Se evaluaron las dos formas para la elaboración del TFG: - Tradicional: por capítulos - Por objetivos	Se decide trabajar con el método tradicional Encargado: estudiante (Hellen Cordero)
3	**Aspectos generales sobre las reuniones con las empresas**	Profesora explica que se vera en cada reunión con la empresa	- Confirmar agenda para organizar reunión con la contraparte. Encargado: profesor tutor - Solicitar y organizar reunión con contraparte organización Encargado: estudiante (Hellen Cordero)
4	**Aspectos generales sobre las reuniones con profesora tutora**	Profesora explica las consideraciones generales sobre las reuniones con la tutora	- Se firmará una única carta que aprueba las minutas de todas las reuniones - Las reuniones de seguimiento se realizan de acuerdo con la necesidad del estudiante para resolver consultas

Próxima reunión

Temas para tratar	Fecha	Convocados
Ajuste del anteproyecto hacia el TFG	Por definir	Laura Alpizar Hellen Cordero

Apéndice FF. Minuta reunión 2 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	02	**Fecha:**	30/08/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	7:00 pm. / 8:30 pm
Objetivo de la reunión:	Revisión y seguimiento Avance I y Avance II		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Revisión del avance I**	Se realizo una revisión general del avance I	- Modificar formato del documento
2	**Revisión de objetivos**	Se revisaron los objetivos del proyecto	- Modificar objetivo general - Modificar objetivos específicos - Agregar objetivo específico para calcular el retorno de inversión
3	**Temas para incorporar en el Marco Conceptual**	Se revisaron los temas que se incorporaron en el marco conceptual	Se debe agregar temas como: - Definición de riesgo - Importancia de ciberseguridad en la actualidad - Marco CSX

Próxima reunión

Temas a tratar	Fecha	Convocados
Reunión de seguimiento	Por definir	Laura Alpizar Hellen Cordero

Apéndice GG. Minuta reunión 3 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	03	**Fecha:**	24/09/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:45 pm. / 5:30 pm
Objetivo de la reunión:	Revisión y seguimiento del proyecto		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Revisión de los cambios solicitados en la reunión anterior**	Se revisaron los objetivos modificados y el formato del documento	
2	**Revisión del avance II**	Se realizó la revisión del avance II, conceptos y temas incluidos	- Se acuerda con la profesora, consultar con la empresa si se puede utilizar COBIT 5

Próxima reunión

Temas a tratar	Fecha	Convocados
Reunión de seguimiento	Por definir	Laura Alpizar Hellen Cordero

Apéndice HH. Minuta reunión 4 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	03	**Fecha:**	07/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	2:00 pm. / 2:30 pm
Objetivo de la reunión:	Revisión y seguimiento del proyecto		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Explicación de la metodología**	Se revisó el marco metodológico	- Referenciar anexos durante el documento. - Definir actividades que se realizaran en cada fase del proyecto - Agregar indicador en la tabla de procedimiento metodológico
2	**Acuerdos reunión anterior**	Se indica a la profesora que la empresa permite usar COBIT 5	

Próxima reunión

Temas a tratar	Fecha	Convocados
Reunión de seguimiento	Por definir	Laura Alpizar Hellen Cordero

Apéndice II. Minuta reunión 5 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	05	**Fecha:**	07/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	11:00 am. / 12:30 am
Objetivo de la reunión:	Revisión y seguimiento del proyecto		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Revisión Metodología**	Se revisaron las modificaciones realizadas al marco metodológico	
2	**Revisión capítulo 4**	Se revisó el análisis de resultados	- Agregar material visual (gráficos y tabla), para visualizar los resultados de los instrumentos - Explicar más cada apartado y no solo comentar los resultados de los instrumentos
3	**Revisión capítulo 5**	Se inicia la revisión del capítulo 5	- Se acuerda no ser redundante con lo que se puso en el capítulo 4
5	**Retorno de inversión**	Se consulta a la profesora sobre los datos que se deben utilizar para el retorno de inversión	- Se acuerda que se deben utilizar las horas del desarrollo del proyecto, horas de revisión por el supervisor del proyecto y las necesarias para los cálculos.

Próxima reunión

Temas a tratar	Fecha	Convocados
Reunión de seguimiento	Por definir	Laura Alpizar Hellen Cordero

Apéndice JJ. Minuta reunión 6 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	06	**Fecha:**	29/10/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	1:00 pm. / 2:00 pm
Objetivo de la reunión:	Revisión y seguimiento del proyecto		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Revisión capítulo 4**	Se revisó el análisis de resultados	- Agregar un párrafo de conclusión al final del capítulo.
2	**Revisión capítulo 5**	Se realiza la revisión del capítulo 5	- Agregar las actividades de cada subcategoría de la herramienta con viñetas - Agregar un párrafo de conclusión al final del capítulo.
3	**Revisión de la herramienta**	Se revisa la herramienta	- Cambiar columna de observaciones después de la de resultados
4	**Retorno de inversión**	Se consulta a la profesora sobre los datos que se deben utilizar para el retorno de inversión	- Se acuerda que se deben utilizar las horas del desarrollo del proyecto, horas de revisión por el supervisor del proyecto y las necesarias para los cálculos.

Próxima reunión

Temas a tratar	Fecha	Convocados
Reunión de seguimiento	Por definir	Laura Alpizar Hellen Cordero

Apéndice KK. Minuta reunión 7 con la tutora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Reunión No.	07	**Fecha:**	04/11/2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	5:30 pm. / 7:00 pm
Objetivo de la reunión:	Revisión final del proyecto		
Participantes:	Presentes: Laura Alpizar, Hellen Cordero		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Revisión análisis financiero**	Se revisó el cálculo y los datos utilizados para el cálculo del TIR, VAN y ROI	
2	**Revisión capítulos 6 y 7**	Se realiza la revisión de conclusiones y recomendaciones.	
3	**Revisión final**	Se revisan modificaciones pendientes	
4	**Firma de documentos**	Se firman las minutas de las reuniones	
5	**Documento finalizado**	Se aprueba el documento académico	

Próxima reunión

Temas para tratar	Fecha	Convocados
Presentación defensa	Por definir	Laura Alpizar Hellen Cordero

ANEXOS

ANEXOS

Anexo A. Plantilla de minuta

Reunión No.	Es un núm. consecutivo para este proyecto	**Fecha:**	Indicar la fecha exacta de la reunión
Lugar:	Indicar dónde fue la reunión	**Hora Inicio/Finalización:**	xx:00 am. / yy:00 am
Objetivo de la reunión:			
Participantes:	Presentes:		
	Ausentes:		

Temas Tratados			
No.	**Asunto**	**Comentarios**	**Acuerdos**
1	**Debe ser detallado, explícito**	**Debe ser detallado, explícito**	**Debe ser detallado, explícito**
2	**Debe ser detallado, explícito**	**Debe ser detallado, explícito**	**Debe ser detallado, explícito**

Próxima reunión		
Temas para tratar	**Fecha**	**Convocados**
En la próxima reunión	indicar	Nombre de quiénes asistirán a esta próxima reunión.

Anexo B. Carta de aprobación filológica

Alajuela, 06 de noviembre de 2021

A quien interese:

Yo, Gisela Alfaro Chaves, cédula de identidad 2-0701-0506 profesional en Filología Española y en Enseñanza del Castellano y la Literatura, perteneciente al Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Artes; leí y corregí el proyecto final de graduación:

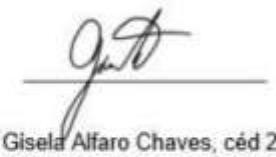
Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR

Documento realizado por el estudiante Hellen Yazmin Cordero Robles, con el número de cédula 3-0496-0873, con el fin de optar por el grado de Licenciatura en Administración de Tecnología de Información, del Tecnológico de Costa Rica.

Por este motivo, se revisaron y corrigieron aspectos como la construcción de párrafos, organización discursiva, vicios del lenguaje trasladados al campo escrito, ortografía, puntuación, barbarismos, coherencia, cohesión y otros elementos relacionados con el campo filológico.

Realizadas las correcciones, doy fe de que el documento está listo para ser presentado.

Se suscribe de ustedes cordialmente,



Gisela Alfaro Chaves, céd 207010506
Carné de colegiada 67138