Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas

Torres Ruiz, Herberth

Diciembre, 2021

Declaratoria de derechos de autor

Se declara que el presente proyecto de investigación fue realizado por el autor Herberth Torres Ruiz, fundamentando los diferentes capítulos del trabajo en diferentes fuentes bibliográficas, literatura citada, las cuales tienen su respectiva referencia, respetando los derechos de autor de dichos trabajos.

Se autoriza la reproducción total o parcial de este trabajo, para ser usados como referencia de trabajos futuros de tipo académico y científico, en este caso, se solicita incorporar la referencia de este trabajo respetando los derechos de autor.

Dedicatoria

A mis padres, por todos los sacrificios necesarios y por demostrarme su apoyo incondicional todos estos años.

A Rudi por compartir conmigo los últimos cinco años e impulsarme a iniciar esta maestría estando hoy a punto de cumplir con este sueño.

Finalmente, a mis hermanas, por su cariño y por estar dispuestas a ayudarme en cualquier momento a lo largo de este camino.

Agradecimientos

Primeramente, le agradezco a mi familia porque sin ellos no estaría aquí en este momento, en especial a mis papás por brindarme el regalo de una excelente educación y por ser un ejemplo a seguir.

Le agradezco a Rudi por ser mi compañero y apoyarme para seguir desarrollándome como persona y profesional.

Agradecerle al profesorado de la maestría por haberme brindado la oportunidad de aprender juntos y otorgarme las herramientas necesarias para realizar esta investigación.

A mi profesor tutor Dennis Durán, por su guía a lo largo de la realización de este proyecto, por su compromiso con la excelencia y por compartir sus conocimientos.

A mis amigos y compañeros de carrera por haber trabajado conmigo a lo largo de todos estos años.

Hoja de aprobación del proyecto

Universidad CENFOTEC
SOMOS LO QUE SABEMOS

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Torres Ruiz Herberth Antonio.**

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Digitally signed by DENNIS ALONSO DURAN CESPEDES (FIRMA)
DN: SERIALNUMBER=CPF-01-1029-0075, SN=DURAN CESPEDES, G=DENNIS ALONSO, C=CR, O=PERSONA FISICA, OU=CIUDADANO, CN=DENNIS ALONSO DURAN CESPEDES (FIRMA)
Reason: I am the author of this document
Location:
Date: 2022.07.07 09:36:05-06'00'
Foxit PDF Reader Version: 12.0.0

M. Sc. Dennis Durán Céspedes
Tutor

PAULA GARRON FALLAS (FIRMA)
Digitally signed by PAULA GARRON FALLAS (FIRMA)
Date: 2022.07.07 11:51:37 -06'00'

M. Sc. Paula Garrón Fallas
Lector 1

MIGUEL PEREZ MONTERO (FIRMA)
Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2022.07.07 14:46:41 -06'00'

M. Sc. Miguel Pérez Montero
Lector 2

San José, Costa Rica, 06 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Índice General

Página

Índice de Tablas

Tabla No. **Descripción** **Página**

Índice de Figuras

Figura No. **Descripción** **Página**

Resumen

Contexto

Existen diversos marcos de buenas prácticas en materia de seguridad informática que se utilizan para auditoría. La idea del presente proyecto es la revisión de estos marcos de buenas prácticas con el objetivo de proponer una metodología para auditoría de seguridad de sistemas y aplicaciones.

Objetivo

Este proyecto busca proponer una metodología para auditoría de seguridad tomando como base marcos de buenas prácticas. Esto con el objetivo de mantener un nivel aceptable de riesgo a nivel organizacional y minimizar el impacto en la confidencialidad, integridad y disponibilidad de los datos.

Método

Se realizó una revisión documental con el fin de identificar marcos de buenas prácticas. Posteriormente se compararon los marcos identificados, se seleccionaron controles y creó un papel de trabajo. Finalmente, se realizó un diagrama de flujo del proceso para facilitar la comunicación de la metodología.

Resultados

Se desarrolló una metodología con base en cuatro marcos de buenas prácticas: ISO 27001, COBIT 2019, CIS CSC v8 y el marco de ciberseguridad de NIST. La metodología incluye un proceso que toma en cuenta los puntos clave de los cuatro marcos, una herramienta de Excel para la ejecución de la auditoría y un diagrama de proceso en notación BPM para la comunicación de la metodología.

Conclusión

La metodología propuesta permite realizar auditorías de seguridad de sistemas y aplicaciones con base en marcos de buenas prácticas ampliamente aceptados por la industria. Adicionalmente, el proceso diseñado permite la adaptación al contexto organizacional y la optimización del proceso de auditoría de seguridad, pues toma en cuenta el ciclo de mejora continua.

Palabras clave: auditoría, seguridad, buenas prácticas, NIST, ISO 27001, COBIT 2019, CIS controles

Abstract

Context

There are several good practice frameworks at the IT security level that are used for auditing. The idea of this project is to review these best practice frameworks with the aim of proposing a methodology for systems and applications security auditing.

Objective

This project seeks to propose a methodology for security auditing based on good practice frameworks, this with the aim of maintaining an acceptable level of risk at the organizational level and minimizing the impact on the confidentiality, integrity, and availability of the data.

Method

A documentary review was carried out to identify good practice frameworks, then the identified frameworks were compared, controls were selected, and a working paper was created, finally a process flow diagram was made to facilitate the communication of the methodology.

Results

A methodology was developed based on four good practice frameworks: ISO 27001, COBIT 2019, CIS CSC v8, and the NIST cybersecurity framework. The methodology includes a process that considers the key points of the four frameworks, an Excel tool for the execution of the audit and a process diagram in BPM notation for the communication of the methodology.

Conclusion

The proposed methodology allows to carry out security audits of systems and applications based on good practice frameworks widely accepted by the industry, additionally the designed process allows adaptation to the organizational context and optimization of the security audit process as it considers the cycle of continuous improvement.

Key words: audit, security, good practices, NIST, ISO 27001, COBIT 2019, CIS controls

1. Capítulo 1: Introducción

1.1. Generalidades

El presente documento constituye el informe final del proyecto de graduación para optar por el grado de Máster en Ciberseguridad de la Universidad Cenfotec. El objetivo principal de este proyecto es proponer una metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas.

En el Capítulo 1: Introducción se describen los aspectos generales del proyecto, considerando los antecedentes y el contexto donde se desarrolla. Se explica en este capítulo la problemática que se resuelve y los beneficios esperados de la realización del proyecto. Asimismo, se establecen cuáles son los objetivos de la investigación y se describe el alcance detallado con los entregables que serán realizados y el estado de la cuestión.

En el Capítulo 2: Marco Conceptual se desarrollan y explican los conceptos que sirven para fundamentar el desarrollo de la solución que se propone en el proyecto según la problemática. Para esto se describen los resultados de la investigación documental en los siguientes temas: auditoría de sistemas, metodologías de auditoría de seguridad y marcos de buenas prácticas de seguridad informática.

En el Capítulo 3: Marco Metodológico se describe el tipo y diseño de la investigación. Se incluyen rasgos característicos de este tipo de estudio para justificar la metodología de trabajo utilizada. Se detallan también las fuentes de información, tanto primarias como secundarias y se hace referencia a las técnicas de recopilación empleadas. Finalmente, se hace una explicación de la metodología para obtener los resultados del proyecto.

En el Capítulo 4: Análisis del Diagnóstico, se presentan los resultados de la revisión documental de marcos de buenas prácticas, así como su selección, descripción, análisis y comparación con el objetivo de seleccionar los insumos que serán tomados en cuenta en la propuesta.

En el Capítulo 5: Propuesta de Solución, se detallan los pasos de la metodología propuesta, así como la descripción de los pasos y de los instrumentos elaborados para la realización de una auditoría de sistemas y aplicaciones, antes de la implementación.

En el Capítulo 6: Conclusiones y Recomendaciones, se muestran las conclusiones y recomendaciones del proyecto haciendo hincapié en los beneficios obtenidos y acciones a ejecutar en el futuro para dar seguimiento a los resultados presentados.

1.2. Antecedentes del problema

Existen varios marcos de buenas prácticas en materia de seguridad informática, que se utilizan para diversos objetivos. Específicamente, para realizar una auditoría en caso de implementaciones de sistemas y aplicaciones se pueden referenciar. Por ejemplo, la familia de normas ISO 27000, la NIST 800-115, COBIT en sus diferentes versiones, la última de las cuales es la 2019, CIC Controles, entre otros.

La idea del presente proyecto es la revisión de estos y otros marcos de buenas prácticas con el objetivo de proponer una metodología para auditar la seguridad de sistemas y aplicaciones, que permita mantener un nivel de seguridad mínimo a la hora de autorizar la implementación de esta en los proyectos productivos de la compañía.

1.3. Definición y descripción del problema

1.3.1. Situación problemática

Actualmente, hay varios marcos de referencia que se pueden utilizar para realizar auditorías o evaluaciones de seguridad previos a la implementación de sistemas y aplicaciones. Sin embargo, en este momento, muchas organizaciones carecen de una metodología clara, precisa y concisa, que permita realizar dicha revisión o auditoría utilizando algún marco de trabajo que se adapte a diversos escenarios y tomando en cuenta las buenas prácticas.

Debido a esta situación, se origina la necesidad de proponer una metodología que tome en cuenta tanto las mejores prácticas de la industria en gestión de tecnologías de información, auditoría de sistemas y seguridad informática, de forma que dicha metodología pueda utilizarse para la evaluación en materia de seguridad de diversas implementaciones. La metodología que se propone busca identificar qué se debe hacer (conjunto de pasos), y cómo debe hacerse (secuencialidad, uso de herramientas, organismos involucrados, entre otros).

1.3.2. Beneficios esperados o aportes del proyecto

El presente proyecto conlleva los siguientes beneficios y aportes:

- Las actividades se realizarán de forma sistemática. Esto favorecerá la eficacia de los colaboradores, porque deberán seguir un proceso claro a la hora de realizar una auditoría de seguridad y se eliminarán posibles retrabajos que podrían surgir sin una metodología definida.
- Se aumentará la eficiencia del proceso de auditoría de seguridad, sin perder tiempo averiguando qué pasos seguir o qué marcos de buenas prácticas utilizar.

1.4. Justificación

La razón principal para el desarrollo de esta investigación es encontrar un método estandarizado, relativamente fácil de entender y repetible, para realizar evaluaciones o auditorías de seguridad informática. A la hora de implementar aplicaciones, sistemas o distintos proyectos de tecnología es infrecuente que se evalúen los riesgos en el campo de la seguridad informática y pueden abrirse vulnerabilidades que comprometan la confidencialidad, integridad o disponibilidad de la información corporativa. El propósito de este proyecto es crear una metodología que permita verificar dicha implementación, antes de aplicarla en los procesos productivos, con una serie de controles y requerimientos de acuerdo con las mejores prácticas de la industria, lo que permitiría asegurar en mayor grado la información y reputación de la organización que utilice la metodología.

1.5. Viabilidad

La viabilidad de este proyecto se puede enfocar en tres facetas que permiten determinar si el proyecto es factible o no.

1.5.1. Punto de vista técnico

La metodología por desarrollar está basada en marcos de referencia o buenas prácticas conocidas, publicadas y de fácil acceso. Las fuentes de información son, en su mayoría, de acceso libre. Desde el punto de vista técnico se profundizará en marcos de buenas prácticas y metodologías de auditoría de sistemas. Es necesario dentro del equipo de investigación, disponer de recursos, con conocimiento básico en auditoría y marcos de gestión de tecnologías de información.

1.5.2. Punto de vista operativo

La parte operacional de la metodología estuvo a cargo del investigador, quien asumió la responsabilidad de desarrollar el marco operativo que se desea lograr. Una vez que dicha metodología sea distribuida, la ejecución y uso recaerán en el personal de los departamentos de auditoría interna, que estará capacitado e instruido para aplicarla.

1.5.3. Punto de vista económico

Al ser un proyecto de investigación y creación de una metodología, realmente solo se requiere una inversión en las horas-persona destinadas a la investigación y creación de esta. Los documentos de los marcos de buenas prácticas por lo general son fácilmente accesibles en Internet, sin un costo adicional y, en caso de tener un costo, dicho monto será cubierto de manera voluntaria por el estudiante investigador, sin que conlleve una inversión económica mayor.

1.6. Objetivos

En este apartado se presentan el objetivo general y los objetivos específicos para el presente proyecto final de graduación, de manera tal que la problemática fundamentada pueda ser traducida en puntos de acción concretos que permitan dar respuesta al planteamiento del problema inicial.

Para la redacción de estos objetivos se utilizó la taxonomía de Bloom de 1956, debido a que su estructura jerárquica facilita la definición de los objetivos desde los niveles más generales a los más específicos, además de que se destaca su utilización como un estándar en el área académica a nivel nacional.

1.6.1. Objetivo general

El objetivo general del proyecto se presenta a continuación:

a. Proponer una metodología para la auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas.

1.6.2. Objetivos específicos

Los objetivos específicos del proyecto son los siguientes:

a. Identificar los principales marcos de buenas prácticas de seguridad informática que puedan utilizarse para la auditoría de sistemas a través de una revisión documental con el fin de seleccionar los que se utilizarán en la investigación.
b. Explicar el proceso de auditoría de sistemas de acuerdo con los marcos de buenas prácticas identificados con el fin de incorporarlos en la metodología desarrollada.
c. Escoger los controles por utilizar en la metodología a partir de los procedimientos detallados en los marcos de buenas prácticas con el fin de evitar la duplicidad.
d. Comparar los procesos descritos en los marcos de buenas prácticas seleccionados con la finalidad de incorporar algunas de sus actividades y controles a la metodología.
e. Diagramar los pasos de la metodología desarrollada con el propósito de facilitar su comprensión y comunicación a las partes interesadas.

1.7. Alcances y Limitaciones

1.7.1. Alcances

Este proyecto contempla la elaboración de una metodología para auditoría de seguridad de sistemas y aplicaciones. A continuación, se describen los alcances del proyecto, en términos de entregables, los cuales están integrados por:

- Documento escrito que identifique los principales marcos de buenas prácticas de seguridad informática que puedan utilizarse para auditoría de sistemas. Asimismo, que describa el proceso de auditoría de sistemas de acuerdo con los marcos de buenas prácticas identificados. Finalmente, que compare los procesos descritos en los marcos de buenas prácticas seleccionados.
- Hoja de cálculo con el listado de los controles por utilizar en la metodología a partir de los detallados en los marcos de buenas prácticas.
- Diagrama de flujo de los pasos de la metodología desarrollada utilizando la notación de BPMN (Modelo y Notación de Procesos de Negocio, por sus siglas en inglés).

Se realizará una prueba de concepto para verificar la validez de la metodología, con un ejemplo real o simulado. Para estas pruebas, se utilizarán proyectos a los que el estudiante pueda acceder, siempre con la debida aprobación de la persona, entidad o empresa propietaria de los datos. Como última opción, podrán utilizarse proyectos ficticios, pero realistas para estas pruebas de concepto, si no se cuenta con la posibilidad de hacerlos con proyectos reales.

1.7.2. Limitaciones

El proyecto no contempla la realización de:

- Metodologías para otro tipo de auditorías de TI fuera del área de seguridad.
- Del ciclo de vida de auditoría no se ejecutarán las fases de: implementación de la metodología más allá de una prueba de concepto, ni la mejora continua del proceso de auditoría.

1.8. Estado de la cuestión

Existen varios marcos de buenas prácticas de seguridad de la información y auditoría de sistemas, así como investigaciones desarrolladas acerca de la creación de metodologías o marcos de trabajo para realizar esta tarea. Se pretende ofrecer un compilado de documentos técnicos, relevantes para el desarrollo de la investigación. Se presenta su identificación, selección y análisis.

1.8.1. Planificación de la revisión

Esta sección tiene como fin realizar una recopilación de investigaciones y publicaciones producidas entre los años 2016 y 2020 a nivel mundial, las cuales basaron su estudio en temáticas que contribuyan a entender la problemática de la auditoría de sistemas y aplicaciones con base en marcos de referencias de buenas prácticas. Para realizarlo, se utilizó Internet como herramienta para la búsqueda de esta información y en especial el buscador de *Google Scholar* (https://scholar.google.com/), el cual permitió extraer diversos tipos de aportes e insumos pertinentes. Durante la búsqueda se utilizó el idioma inglés, además del idioma español, porque generalmente es el idioma más utilizado para la difusión de resultados de investigación científica.

Palabras claves:

Auditoría de seguridad, metodología, controles, ISO, Security audit, methodology, controls, ISO.

1.8.2. Ejecución de la revisión

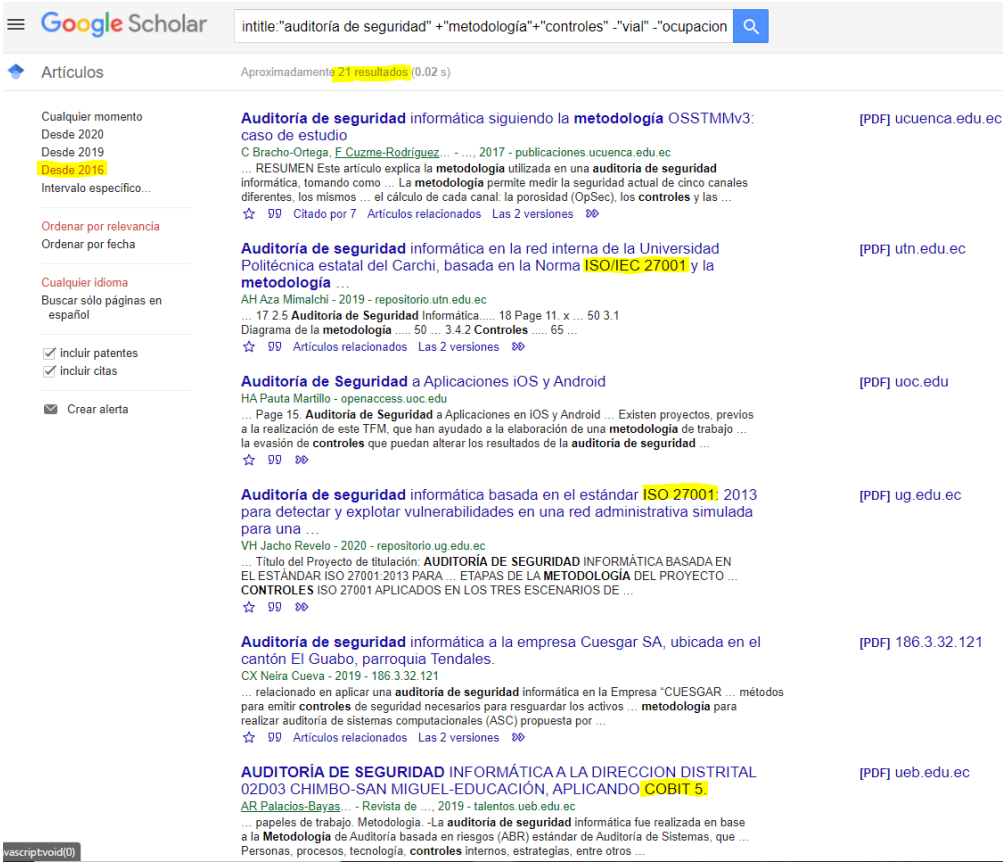
El presente estado de la cuestión es resultado de una investigación de tipo descriptivo que gira en torno al tema de auditoría de seguridad informática basada en marcos de buenas prácticas. Fue necesario centrarse en la recopilación de información referente al tema de estudio, para posteriormente realizar un análisis crítico de esta, de modo que permita finalmente el abordaje más acertado del tema en cuestión.

La realización de la búsqueda en español proporcionó, tras refinar la búsqueda, 21 resultados que a primera vista parecen prometedores. Es particularmente llamativo que aparecen con cierta recurrencia marcos de buenas prácticas, como la familia de ISO 27000 y COBIT 5.

Fue necesario eliminar de los resultados investigaciones referentes a seguridad vial y seguridad ocupacional, por lo que la cadena de búsqueda final fue: *intitle:"auditoría de seguridad" +"metodología"+"controles" -"vial" -"ocupacional".* Los resultados van, por lo general, en implementaciones de marcos de trabajo de auditoría en ambientes específicos (universidades, direcciones distritales, centros de datos, entidades financieras y hospitales) o para usos de tecnologías específicas (aplicaciones móviles, redes inalámbricas, tecnología NFC, aplicaciones web, voz sobre IP, entre otras).

En la Figura 1 puede visualizarse el resultado de esta búsqueda:

Figura 1: Resultados de búsqueda de fuentes en español



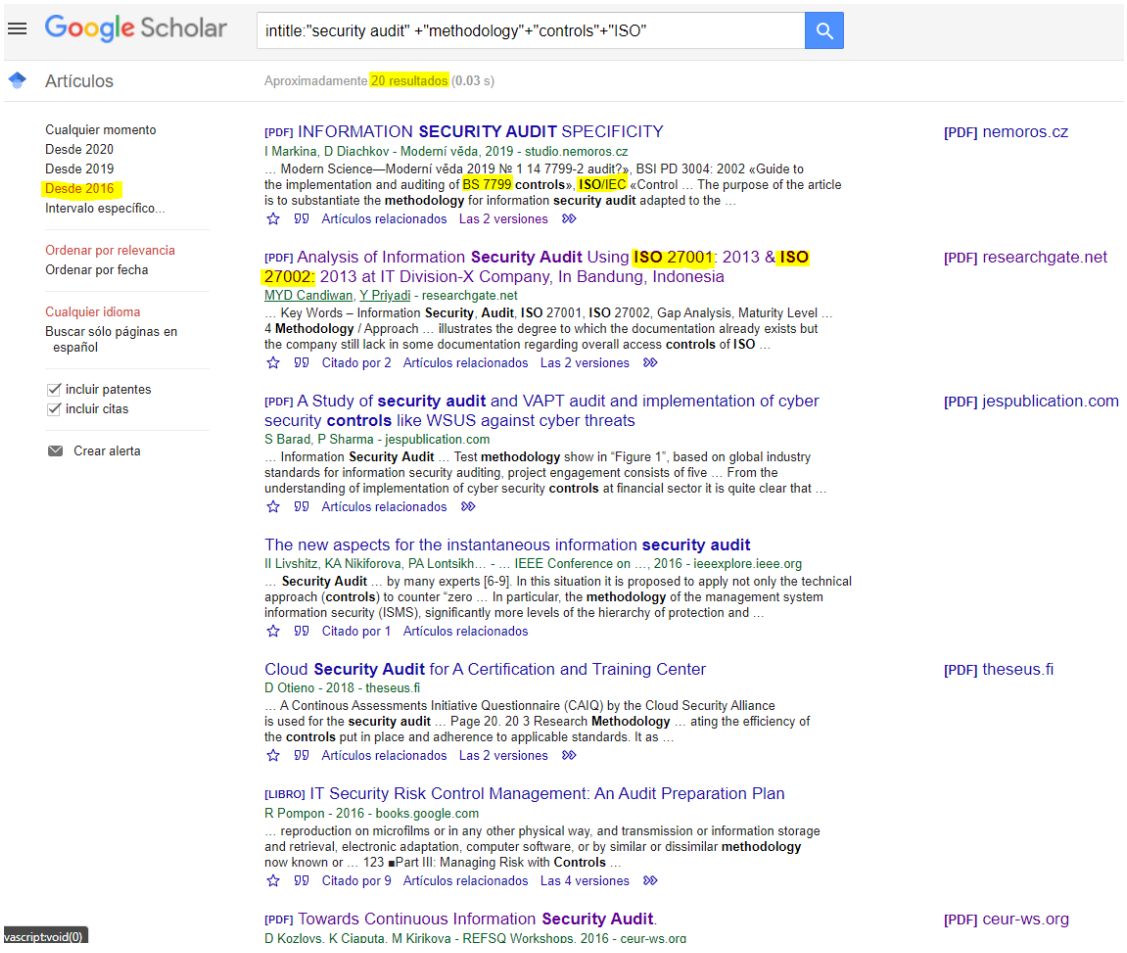
Fuente: Elaboración propia (2021)

De igual modo, la búsqueda en inglés retornó investigaciones sobre la auditoría en ambientes específicos (empresas de telecomunicaciones, función de auditoría interna de una organización, departamento de calidad de software) y la auditoría de tecnologías específicas (computación en la nube y bases de datos), y de nuevo se evidencia la presencia de marcos de buenas prácticas como la ISO 27001 y 27002.

Para delimitar los resultados de la búsqueda se consideró importante incorporar las normas ISO, pues son un estándar ampliamente reconocido por la industria, por lo que la cadena de búsqueda final fue: *intitle:"security audit" +"methodology"+"controls"+"ISO"*

En la Figura 2 puede visualizarse el resultado de esta búsqueda.

Figura 2: Resultados de búsqueda de fuentes en inglés



Fuente: Elaboración propia (2021)

Para descartar los artículos, se realizó una revisión de estos a través de un proceso de *skimming,* que consiste en una lectura de alto nivel del resumen, las conclusiones y el apartado gráfico de los artículos, para identificar rápidamente la relevancia de cada uno.

Para ver un análisis detallado del proceso de *skimming* realizado se pueden referenciar las tablas ubicadas en el Apéndice 1: Detalles de la revisión literaria en inglés y el Apéndice 2: Detalles de la revisión literaria en español, donde se listaron los resultados, el tipo de documento, si resultó ser relevante para esta investigación y finalmente el motivo de su exclusión, en caso de ser así.

Después de revisar se identificaron las siguientes fuentes relevantes detalladas en la Tabla 1:

Tabla 1: Fuentes de información relevante tras el análisis de Literatura

Fuente	Autor(es)	Año	Tipo de documento
[PDF] Information security audit specificity	Markina, I., & Diachkov, D.	2019	Artículo científico
[PDF] Analysis of Information Security Audit Using ISO 27001: 2013 & ISO 27002: 2013 at IT Division-X Company, In Bandung, Indonesia	Candiwan, M. Y. D., & Priyadi, Y.	2016	Artículo científico
Model for efficient development of security audit criteria'	Kelo, T., Eronen, J., & Rousku, K.	2018	Artículo científico
Development of a Security Audit Framework for an Organization	Ujjaman, M.	2018	Tesis
Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio	Bracho-Ortega, C., Cuzme-Rodríguez, F., Pupiales-Yépez, C., Suárez-Zambrano, L., Peluffo-Ordóñez, D., & Moreira-Zambrano, C.	2017	Artículo científico
Auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, basada en la Norma ISO/IEC 27001 y la metodología …	Aza Mimalchi, A. H	2019	Tesis
Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del …	Chifla-Villón, M., Puma-Aucapiña, L., & Villacís-Real, K.	2020	Artículo científico
Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja	Jaramillo, C., Jácome, L., Ordóñez, Á., Gaona, M., Carrión, J., & Palma, M	2017	Artículo científico

Implantación de un proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002 en una entidad financiera de Puno–2016	Puma Arosquipa, M. Y.	2017	Tesis
[PDF] Auditoría de la seguridad de información en una empresa privada costarricense	Chavarría Barquero, R. H.	2018	Tesis
Auditoría a la seguridad informática de los servicios de tecnologías de la información en la ESE Hospital San Francisco de Gachetá.	Novoa, H., & Javier, F.	2017	Monografía

Fuente: Elaboración propia (2021)

1.8.3. Resumen de los resultados

En su investigación (Markina & Diachkov, 2019) destacan los problemas básicos de la seguridad de la información, enfocados en la necesidad de trabajar con métodos efectivos para auditar la seguridad.

El artículo presenta la metodología matricial para realizar una auditoría de seguridad de la información considerando los estándares existentes y el marco teórico de la gestión de la seguridad de la información. Esto permite al auditor generalizar los indicadores de todos los componentes de la seguridad de la información mediante la recopilación de los datos obtenidos, el análisis de los componentes técnicos y de programación del sistema de información, análisis de la seguridad de los recursos de información, análisis de personal y las fuentes de amenazas a la seguridad de la información.

Es de especial atención que el artículo referencia en su contenido marcos de buenas prácticas como ISO 17799:2000, BS 7799-2:2002, BSI PD 3003:2002, ISO 27000 y COBIT 1-5.

(Candiwan & Priyadi, 2016) utilizan los marcos de ISO 27001 e ISO 27002 como base para analizar la auditoría de seguridad en una compañía de telecomunicaciones en Indonesia, tras ser víctimas de varios incidentes de seguridad informática como infecciones de malware, ataques de jáqueres o ausencia de concienciación en seguridad.

Cabe destacar que, además de conducir la auditoría de acuerdo con estos marcos de buenas prácticas, los autores utilizan el modelo de Integración de Modelos de Madurez de Capacidades (CMMI por sus siglas en inglés) para evaluar el nivel de madurez de la organización en cada uno de los dominios auditados, lo que les permite recomendar acciones

concretas para alcanzar un nivel de madurez mínimo y mejorar así la postura de seguridad de la empresa.

También se revisó la investigación de (Kelo, Eronen, & Rousku, 2018), en la que los autores advirtieron que en ocasiones los criterios utilizados para la realización de auditorías de seguridad son ineficientes, por lo que propusieron un modelo que utiliza los criterios de la Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés) y de FICORA, la autoridad regulatoria de comunicaciones de Finlandia. Realizaron una prueba de concepto y obtuvieron resultados prometedores en eficiencia y resultados de la auditoría.

En su tesis de maestría (Ujjaman, 2018) presenta un marco de trabajo para que una organización realice auditorías de seguridad a partir de los estándares ISO/IEC_JCT1. Para evaluar el marco propuesto, el autor preparó cuestionarios y demostró que los resultados de las pruebas de la efectividad del mecanismo de control de gobernanza y seguridad de TI basados en el marco demostraron la eficacia del enfoque. Se buscaba que el marco ayude a una organización a minimizar las vulnerabilidades, garantizar una gobernanza fluida y transparente y proteger los activos de información.

El artículo de (Bracho-Ortega, y otros, 2018) explica la metodología utilizada en una auditoría de seguridad informática, tomando como referencia las recomendaciones de la metodología OSSTMM, versión 3. La metodología permite medir la seguridad actual de cinco canales diferentes: humano, físico, comunicaciones inalámbricas, telecomunicaciones y de redes de datos. Los resultados finales, una vez realizado el análisis pertinente, permiten determinar los valores numéricos de cada uno de estos ítems. Una vez aplicada la metodología, esto ayuda a comprender, en cada ámbito de aplicación, las deficiencias o excesos de los controles operacionales de seguridad que se manejan en una empresa u organización. Esto constituye un criterio importante para controlar las vulnerabilidades que se detecten internamente y poder solucionarlas en su debido momento.

En su tesis de grado (Aza Mimalchi, 2019) realizó una auditoría de seguridad informática en la red interna de la Universidad Politécnica Estatal del Carchi, con base en la norma ISO/IEC 27001 y la metodología OSSTMMv3 para mejorar la seguridad que posee la red interna de la institución. Cabe destacar de este trabajo que, además de utilizar la metodología mencionada, se realizó un alineamiento a las buenas prácticas de ISO 27001.

Los autores del instrumento de auditoría descrito en (Chifla-Villón, Puma-Aucapiña, & Villacís-Real, 2020) realizaron su estudio con el objetivo de proteger la información en

servidores en Instituciones Públicas de Educación Superior del Ecuador. Lo más llamativo de este estudio respecto de la presente investigación es que los autores mencionan el análisis y la selección de estándares que permitieron una alineación en los controles de seguridad y sus técnicas de validación a través de instrumentos fiables y relevantes. Para esto estudiaron la norma ISO 27002:2013 e incorporaron aspectos de la NIST 800-53 R4 con el fin de crear un instrumento con 82 ítems para la realización de la auditoría.

En su artículo (Jaramillo, y otros, 2017) divulgan información sobre normas, estándares y metodologías, utilizados para la gestión de seguridad de un Data Center y Red LAN. Para ese trabajo se utilizó el estándar ANSI/TIA/EIA 942 y la norma ISO/IEC 27002, con metodología MAGERIT. Además, se desarrolló un cuadro comparativo, para exponer las ventajas y características que ofrece cada una, lo cual permite llegar a la conclusión del porqué aplicarlas. De acuerdo con los autores “La aplicación de la Norma ISO/IEC 27002 y el Estándar TIA/EIA 942, son idóneas para el análisis, permiten cubrir la insuficiencia de la gestión de seguridad de la información y la infraestructura para la adecuada implementación, debido a que éstas engloban las mejores prácticas recopiladas de normas y estándares anteriores para el mejoramiento de la seguridad física y lógica.”

En su tesis de grado (Puma Arosquipa, 2017) se examina la importancia de una auditoría de seguridad de información por medio de la implantación de un proceso de auditoría de seguridad de información, que cuenta con 26 actividades y en ellas se toman las buenas prácticas y controles de la norma ISO/IEC 27002. A través del proceso desarrollado se logró disminuir la cantidad de horas necesarias para llevar a cabo la auditoría y reducir los costos de consultoría externa, pues el trabajo recae en la auditoría interna de la organización y además este departamento debe cumplir con la normativa sobre impuestos, establecida por la Superintendencia respectiva.

En su tesis de maestría profesional en auditoría de TI (Chavarría Barquero, 2018) utiliza el documento de “COBIT 5 para la seguridad de la información”, específicamente el proceso DSS05 “Gestionar los Servicios de Seguridad” y además tomó en cuenta aspectos básicos de la norma ISO 27001 y normativa costarricense vinculante en el tema tratado. El capítulo 4 incluye la realización de los papeles de trabajo y plantillas utilizadas a lo largo de la auditoría, que pueden ser utilizadas como referencia a la hora de crear las herramientas de la metodología por desarrollar.

Finalmente, en su monografía (Hilario Novoa, 2017) realiza una auditoría de seguridad informática basada en la norma ISO 27001:2013 y la metodología Magerit V3, integrando pruebas de software, revisión documental, encuestas, listas de chequeo y verificación física, con el fin de generar un informe de auditoría que se puede poner en marcha a través de un plan de mejoramiento y su posterior seguimiento.

2. Capítulo 2: Marco Conceptual

Se generó una nube de conceptos con el objetivo de identificar los conceptos más relevantes mencionados en los artículos y trabajos de investigación seleccionados en el estado de la cuestión. Para generar la

Figura 3, se usó el texto desarrollado en la sección de Resumen de los resultados del estado de la cuestión, eliminando palabras como artículos, preposiciones, pronombres, y otras palabras que no corresponden a conceptos relevantes.

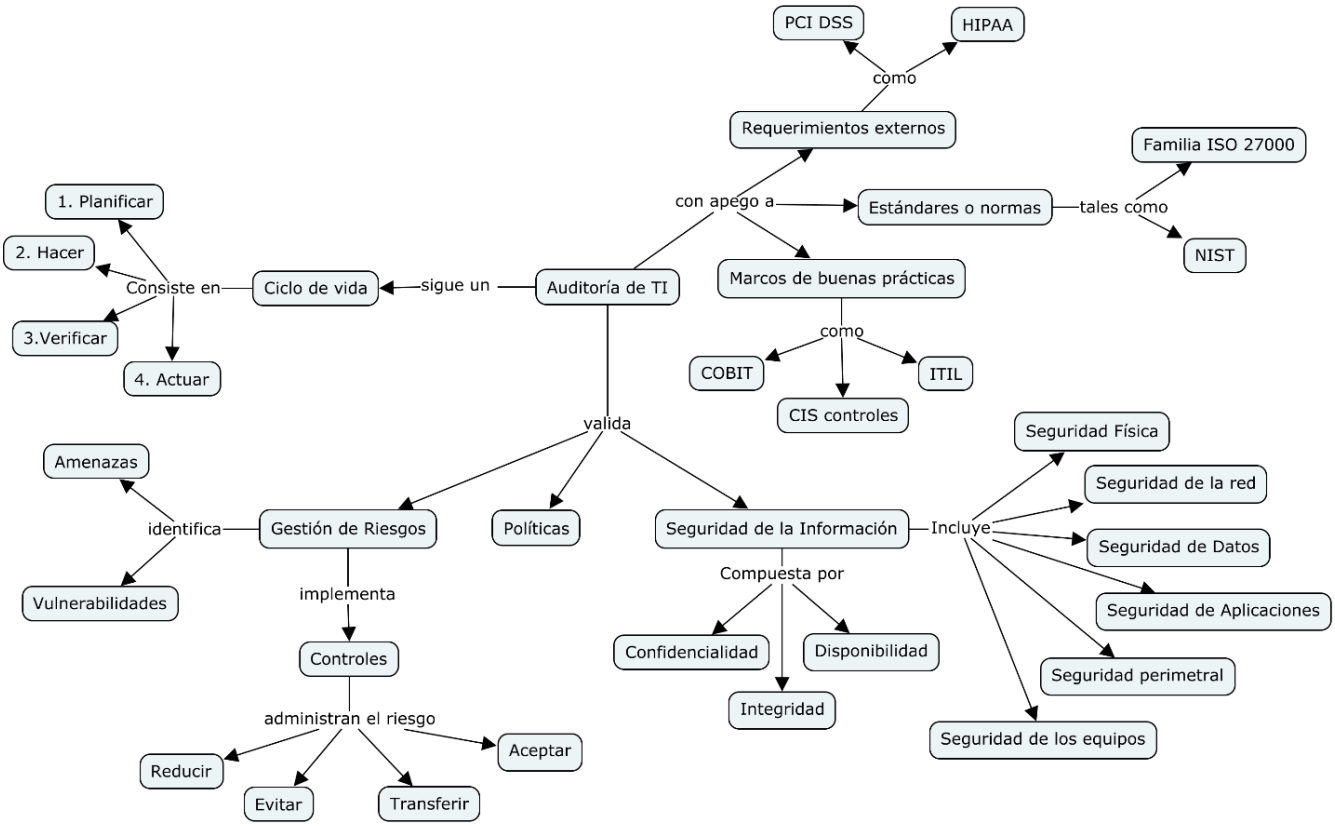
Figura 3: Nube de Conceptos

Fuente: Elaboración propia (2021) usando el sitio: https://www.wordclouds.com/

Con base en la anterior nube de conceptos se realizó un mapa conceptual que presenta de manera gráfica la interrelación de los conceptos más importantes y que se explican con

mayor profundidad dentro del presente marco conceptual. Véase la Figura 4: Mapa conceptual sobre Auditoría de TI.

Figura 4: Mapa conceptual sobre Auditoría de TI



Fuente: Elaboración propia (2021) usando el software CmapTools

Se presenta, a continuación, la definición de los conceptos mencionados con mayor frecuencia y de mayor relevancia para desarrollar este proyecto investigativo. Se debe destacar que, con el fin de brindar un mejor contexto del tema en cuestión, el orden en el que se presentan los conceptos va desde un ámbito general hacia aspectos más específicos necesarios para comprender los diversos elementos asociados al tema de auditoría de seguridad de sistemas y aplicaciones.

Auditoría de tecnología de información

Las funciones principales de una auditoría de tecnología de información (TI) son evaluar los sistemas que existen para proteger la información de una organización. Específicamente, las auditorías de tecnología de la información se utilizan para evaluar la capacidad de la organización para proteger sus activos de información y para distribuir la información de manera adecuada a las partes autorizadas. (Gantz, 2014)

La auditoría de TI tiene como objetivo evaluar lo siguiente:

- ¿Los sistemas informáticos de la organización estarán disponibles para la empresa en todo momento cuando sea necesario? (conocido como **disponibilidad**)
- ¿Se divulgará la información de los sistemas solo a los usuarios autorizados? (conocido como **confidencialidad**)
- ¿La información proporcionada por el sistema será siempre precisa, confiable y oportuna? (mide la **integridad**)

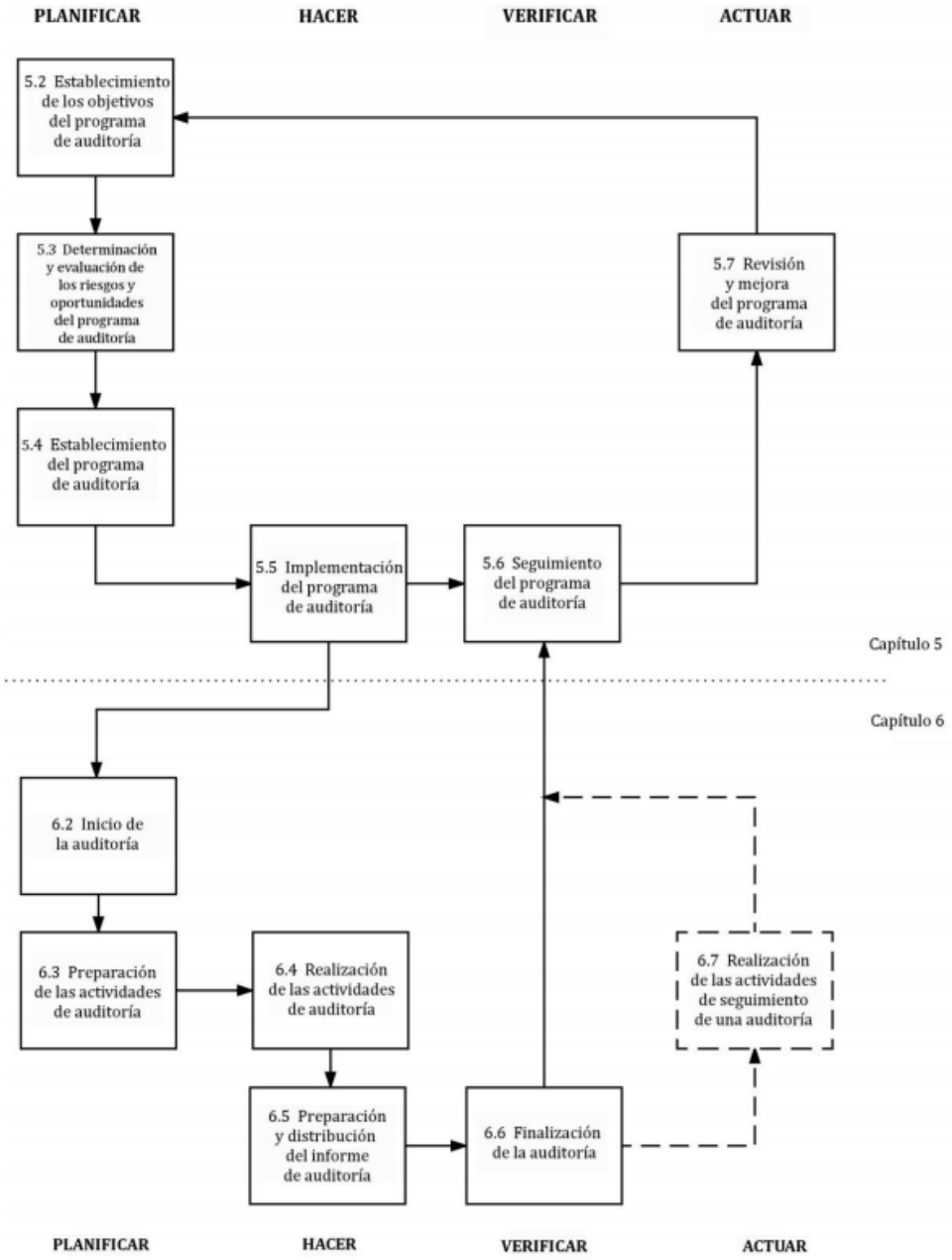
De esta manera, la auditoría espera evaluar el riesgo para el activo más valioso de la empresa (su información) y establecer métodos para minimizar esos riesgos.

Ciclo de vida de la auditoría

La norma ISO 19011 emite directrices para la auditoría de sistemas de gestión y puede utilizarse como buena práctica para la realización de diversos tipos de auditorías, en esta norma, al igual que en otras normas ISO se usa el ciclo de Deming *Planificar-Hacer-Verificar-Actuar* (PDCA).

En la Figura 5: Diagrama de flujo para la gestión de un programa de auditoría, se pueden ver las fases del proceso de auditoría ubicadas en el ciclo PDCA de acuerdo con la norma.

Figura 5: Diagrama de flujo para la gestión de un programa de auditoría



Fuente: (Secretaría Central de ISO, 2018)

Para realizar auditorías de TI, en especial las auditorías de seguridad de sistemas, se siguen una serie de marcos de buenas prácticas y estándares que brindan una guía a la hora de establecer controles y gestionar adecuadamente los servicios y sistemas del departamento de TI.

Estándares y marcos de buenas prácticas para auditar sistemas

COBIT 2019

Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como marco de trabajo, dirigida al control y supervisión de tecnología de la información (TI). Mantenida por ISACA (en inglés: Information Systems Audit and Control Association) (ISACA, 2020). Tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluido un resumen ejecutivo, un marco de trabajo, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión. (ISACA, 2020)

Familia ISO 27000

La serie ISO 27000 de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO). La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). (Lewis, 2018)

Algunas de las normas más importantes de la familia son:

- ISO 27000 - es un vocabulario estándar para el SGSI. Introducción y base para el resto.
- ISO 27001 - Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
- ISO 27002 – Es un código de buenas prácticas para la gestión de seguridad de la información.
- ISO 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO 27001.

- ISO 27004 - son métricas para la gestión de seguridad de la información. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO 27005 - trata la gestión de riesgos en seguridad de la información.
- Otras.

CIS controles v8

Los controles CIS son un número reducido de acciones de seguridad priorizadas, debidamente consensuadas y respaldadas que las organizaciones pueden tomar para evaluar y mejorar su estado de seguridad actual. (Center for Internet Security, 2019). Son un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes. Los 18 controles CIS son desarrollados por una comunidad de expertos en TI que aplican su experiencia de primera mano como defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas globalmente.

Marco de trabajo de *ciberseguridad* de NIST

El marco para la mejora de la seguridad cibernética en infraestructuras críticas del Instituto Nacional de Estándares y Tecnología de los Estados Unidos puede ser utilizado por organizaciones en cualquier sector o comunidad. Este permite que las organizaciones, independientemente de su tamaño, grado de seguridad cibernética o sofisticación de seguridad cibernética, apliquen los principios y mejores prácticas de gestión de riesgos para mejorar la seguridad cibernética y la capacidad de recuperación. (Instituto Nacional de Estándares y Tecnología, 2018)

El marco proporciona una estructura de organización común para múltiples enfoques de seguridad cibernética mediante la conformación de estándares, directrices y prácticas que funcionan de manera efectiva en la actualidad.

A partir de esos estándares, directrices y prácticas, el marco proporciona una taxonomía común y un mecanismo para que las organizaciones realicen lo siguiente:

1. Describir su postura actual de seguridad cibernética
2. Describir su objetivo deseado para seguridad cibernética
3. Identificar y priorizar oportunidades de mejora dentro del contexto de un proceso continuo y repetible
4. Evaluar el progreso hacia el objetivo deseado
5. Comunicarse entre las partes interesadas internas y externas sobre el riesgo de seguridad cibernética

En la Tabla 2 se pueden ver las funciones y categorías del marco de trabajo de *ciberseguridad* de NIST. Cada una de las categorías listadas se subdividen a la vez en subcategorías que son resultados específicos esperados de la implementación de la categoría y por consiguiente de la función.

Tabla 2: Funciones y categorías del marco de trabajo de ciberseguridad NIST

Identificador de la Función	Función	Identificador de Categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BA	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección

RS	Responder	RS.RP	Planificación de respuesta
		RS.CP	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: Elaboración propia basada en (Instituto Nacional de Estándares y Tecnología, 2018)

Notación de BPM (BPMN)

Cabe destacar que para explicar mejor el proceso propuesto, se estableció como objetivo específico de esta investigación diagramar los pasos de la metodología desarrollada con el objetivo de facilitar su comprensión y comunicación a las partes interesadas. Para esto se estableció en los alcances: usar la notación de BPMN.

La notación de modelo de procesos de negocio (BPMN por sus siglas en inglés) según Object Management Group (2011) es una notación estándar, enfocada a ser entendida por toda la organización. Su función es diagramar los flujos de tareas que dan forma a un proceso. Tiene como finalidad entonces, automatizar los procesos a partir de los diseños gráficos y fáciles de entender. Fue desarrollada en el instituto Business Process Management Initiative en el año 2004 ante la necesidad que se tenía de generar una notación estándar para ser entendida por todos los participantes del negocio, desde los altos ejecutivos hasta los técnicos e ingenieros que implementan nuevos procesos.

Con lo anterior, se quería estrechar la brecha entre los que diseñan la automatización del proceso y los que implementan estos diseños, es decir, entre la capa de negocio y la capa de tecnología. En el año 2005, se responsabiliza de la mantención de la notación al Object Management Group (OMG), quien administra además otros estándares y notaciones relacionadas. Desde ese momento en adelante, en el OMG, se han desarrollado versiones actualizadas de la notación, en el año 2010 se oficializó la versión 2.0. En esta nueva versión,

se cambió el nombre a “Business Process Model and Notation”, para abarcar mejor lo que esta herramienta es: una notación para el modelado de procesos de negocio.

Elementos de la notación

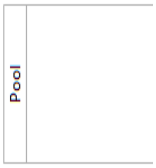
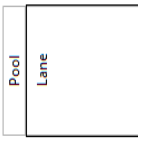
Para lograr el entendimiento de todas las partes involucradas en los procesos de negocio, la notación BPMN describe una serie de elementos que permiten una mayor facilidad en la identificación de las labores relacionadas con las actividades, la conexión entre estas, los artefactos y roles involucrados, relaciones entre procesos, entre otros propósitos.

Se consideran cinco categorías específicas de elementos, las cuales se describen brevemente a continuación:

- Objetos de flujo: contiene los tres elementos principales del modelo. Entre estos se incluyen: las actividades que describen la acción por ejecutar, gateways o elementos de decisión sobre las actividades y los eventos que son acciones que podrían suceder.
- Datos: simbolizan los documentos, las salidas y entradas de datos y las bases de datos.
- Objetos de conexión: existen cuatro formas de conectar los objetos de flujo para representar el ordenamiento lógico de estos. Dentro de esta categoría, se encuentran los flujos de secuencia, flujos de mensajes, las asociaciones y las asociaciones de datos.
- Participantes o *swimlanes*: son elementos que interactúan y realizan tareas específicas. Pueden ser roles internos o externos a la organización. Se incluyen dos elementos dentro de esta categoría: *pool* son las organizaciones o entidades participantes y *lanes* se refiere al rol o área con una sub-participación dentro de un pool dentro de una organización, los cuales se utilizan para organizar y categorizar las actividades.
- Artefactos: son usados para proveer información adicional del proceso y son necesarios para tener diagramas detallados. Permiten añadir texto, imágenes, agrupar tareas, entre otros.

En la Tabla 3, se muestran las categorías de la notación de BPM, una breve descripción de cada una, el tipo de elemento que representa y la notación o símbolo:

Tabla 3: Categorías de BPMN

Categoría	Descripción	Elemento	Notación
Objetos de flujo	Elementos que definen el comportamiento de los procesos	Actividad	
		Evento	
		Compuerta	
Objetos de conexión	Elementos que permiten conectar los objetos de flujo que se dan en el desarrollo de la estructura del proceso	Flujo de secuencia	
		Flujo de mensaje	
		Asociación	
Carriles	Elementos que permiten organizar las actividades separadamente, para apreciar más claridad los procesos y roles.	Pool	
		Lane	
Artefactos	Elementos que permiten ofrecer información adicional de los procesos, dando mayor claridad.	Objetos de datos	
		Grupo	
		Anotación	

Fuente: Elaboración con base en (Santos López & Santos de la Cruz, 2012) Imágenes de Bonitasoft.

En la Tabla 4, basada en OMG (2011), se detallan los elementos básicos de la notación de BPM en su versión 2.0 para la categoría de objetos de flujo. En ella se incluye el nombre del elemento, una breve descripción y la notación que lo representa:

Tabla 4: Elementos de la notación de BPM

Elemento	Descripción	Notación
Eventos de inicio		
Evento de inicio simple	Inicio de un proceso.	
Evento de inicio por mensaje	El proceso comienza al recibirse un mensaje.	
Evento de inicio por tiempo	El proceso inicio a una hora o fecha determinada.	
Evento de inicio condicional	El proceso comienza si se da una condición.	
Evento de inicio por señal	El proceso inicia al recibirse una señal o un aviso.	
Evento de inicio múltiple	El proceso inicia con una combinación de las anteriores.	
Eventos Intermedios		
Evento intermedio simple	El proceso se detiene a la espera de un evento genérico.	
Evento intermedio de mensaje	El proceso continúa después de recibir un mensaje externo.	
Evento intermedio por tiempo	El proceso continúa cuando a una hora o fecha determinada.	
Evento intermedio de señal	El proceso continúa con la recepción de una señal o alerta.	
Evento intermedio condicional	El proceso continúa cuando se cumple una condición determinada.	
Eventos de Terminación		
Evento de terminación simple	Terminación del proceso simple.	

Evento de terminación por mensaje	Terminación del proceso con envío de un mensaje.	
Evento de terminación por error	El proceso termina como resultado de un error.	
Evento de terminación múltiple	El proceso termina con una combinación de los anteriores.	
Actividades		
Tarea simple	Representa una actividad genérica, sin especificar el tipo de tarea que se realiza.	
Tarea manual	Representa una actividad que hace una persona sin ayuda de un sistema o *software* que le facilite la tarea.	
Tarea de usuario	Es una tarea que realiza el usuario utilizando un sistema o interfaz de *software.*	
Tarea de servicio	Es una actividad automatizada que se realiza sin la intervención directa de un usuario.	
Tarea de envío de mensaje	La actividad representa el envío de información, documentos, archivos o similares, a otro usuario.	
Tarea de recepción de mensaje	La actividad representa la recepción de objetos, información, documentos, etc.	
Subproceso	Incluye la ejecución de un subproceso dentro del proceso actual.	
Compuertas		
Compuerta exclusiva	Es una decisión basada en datos que tiene como resultado un camino único entre varios posibles. También se usa para la convergencia de flujos.	
Compuerta inclusiva	Representa una decisión que puede ser verdadera en más de uno de sus caminos, los cuales son ejecutados. También se puede usar en la convergencia de flujos en uno solo.	

Compuesta exclusiva basada en eventos	Igual que la compuesta exclusiva, pero en este caso se decide el camino que se debe seguir al ocurrir un evento determinado.	
Compuerta paralela	Diverge el trabajo en varios caminos que luego convergen usando la misma compuerta.	

Fuente: Información de (Object Management Group, 2011) imágenes de Bonitasoft

3. Capítulo 3: Marco Metodológico

En este capítulo se describe el tipo y diseño de la investigación, caracterizándola para justificar la metodología de trabajo utilizada. Se detallan también las fuentes de información y se hace referencia a las técnicas de recopilación utilizadas. Finalmente, se hace una explicación de la metodología para obtener los resultados del proyecto investigativo.

3.1. Tipo de investigación

Debido a que el objetivo general de este proyecto consiste en proponer una metodología para auditoría de seguridad de sistemas y aplicaciones de acuerdo con marcos de buenas prácticas, se considera que esta investigación corresponde al tipo investigación evaluativa por cuanto no produce conocimiento nuevo ni atiende necesidades de clientes particulares, sino que compara factores y emite criterios a partir de sus hallazgos.

3.2. Alcance investigativo

Debido al contexto de la presente investigación, se considera un estudio de carácter descriptivo, pues busca mostrar los marcos de buenas prácticas identificados, así como especificar las características de estos y de la metodología propuesta.

3.3. Enfoque

Esta investigación utiliza un abordaje cualitativo a la hora de definir el enfoque, debido a que este documento tiene el fin de mostrar una propuesta para realizar auditorías de seguridad de la información usando las buenas prácticas de la industria y las experiencias recolectadas de diferentes experiencias previas recolectadas durante esta investigación.

3.4. Diseño

El presente proyecto es una investigación-acción, que trata de resolver problemas cotidianos e inmediatos y mejorar prácticas concretas. “Su propósito fundamental se centra en

aportar información que guíe la toma de decisiones para programas, procesos y reformas estructurales.” (Hérnandez, Férnandez, & Baptista, 2014, p. 510)

De acuerdo con Hernández et al. (2014) los tres pilares donde se fundamenta la investigación de este tipo son:

- Los participantes que están viviendo un problema son los que están mejor capacitados para abordarlo en un entorno naturalista.
- La conducta de estas personas está influida de manera importante por el entorno en que se encuentran.
- La metodología cualitativa es la mejor para el estudio de los entornos naturalistas.

Hernández et al. (2014) establece que estos estudios construyen el conocimiento por medio de la práctica y caracteriza los estudios de investigación-acción de la siguiente forma:

- La investigación-acción envuelve la transformación y mejora de una realidad. De hecho, se construye sobre esta.
- Parte de problemas prácticos y vinculados con un ambiente o entorno.
- Implica la total colaboración de los participantes en la detección de necesidades (ellos conocen mejor que nadie la problemática por resolver, la estructura por modificar, el proceso por mejorar y las prácticas que requieren transformación) y en la implementación de los resultados del estudio (p. 510).

El análisis de marcos de buenas prácticas de auditoría de seguridad determina que el presente proyecto corresponde a este tipo de estudio, porque cumple con las características mencionadas previamente y los objetos de estudio, así como las fuentes de información serán principalmente los individuos involucrados, es decir auditores de seguridad, porque son estos quienes tienen mayor conocimiento y están más capacitados para abordarlo.

3.5. Población y muestreo

Al ser una investigación con un enfoque cualitativo sobre marcos de buenas prácticas de auditoría de seguridad, la población corresponde a todos los marcos utilizados para este fin y la muestra fue seleccionada de manera discrecional, de acuerdo con el criterio experto y

según los hallazgos del estado de la cuestión donde se pudo identificar cuáles son los más utilizados en la industria.

3.6. Instrumentos de recolección de datos

Se efectuó una revisión documental para recolectar los marcos de referencia, con el fin de identificar los que puedan utilizarse para auditoría de sistemas e incluirlos en el desarrollo de la propuesta. Se aplicó el análisis de contenido de estos, así como los procesos de auditoría descritos y los controles que se detallan en cada uno de los marcos de buenas prácticas, con el objetivo de identificar por criterio experto los que serán utilizados en la propuesta.

3.7. Técnicas de análisis de información

Se analizaron cualitativamente los marcos de buenas prácticas seleccionados para explicar de manera general el proceso de auditoría descrito en cada uno de estos y se seleccionaron los controles que se utilizan en la metodología, tomando como base los detallados en los marcos de buenas prácticas, con el fin de evitar la duplicidad. De igual modo se compararon los procesos descritos en los marcos de referencia y se seleccionaron las actividades y aspectos incluidos en la metodología propuesta.

3.8. Estrategia de desarrollo de la propuesta

En esta etapa del proyecto investigativo se generó la metodología para auditoría de seguridad de sistemas y aplicaciones, de acuerdo con los marcos de buenas prácticas identificados y la elaboración de los papeles de trabajo para auditoría, con los controles seleccionados, la descripción del proceso de auditoría considerando los aspectos identificados en las buenas prácticas. Finalmente, se diseñó el diagrama en notación BPMN que describe los pasos de la metodología desarrollada. Esto con el fin de facilitar la comprensión de la metodología y la comunicación de esta a las distintas partes interesadas.

4. Capítulo 4: Análisis del Diagnóstico

4.1. Identificación de marcos de buenas prácticas, procesos y controles

Tal y como se desarrolló preliminarmente en el marco conceptual, algunos de los marcos de buenas prácticas que se pueden utilizar para auditar sistemas de información son:

- COBIT 2019
- Familia ISO 27000
- CIS controles v8
- Marco de Trabajo de Ciberseguridad de NIST

A continuación, se describen los procesos de auditoría y los controles establecidos por cada uno de estos marcos para posteriormente en el siguiente capítulo desarrollar la propuesta de metodología.

Para cada uno de los marcos seleccionados se utilizó la última versión publicada con el objetivo de mantener la relevancia y nivel de actualización de la investigación.

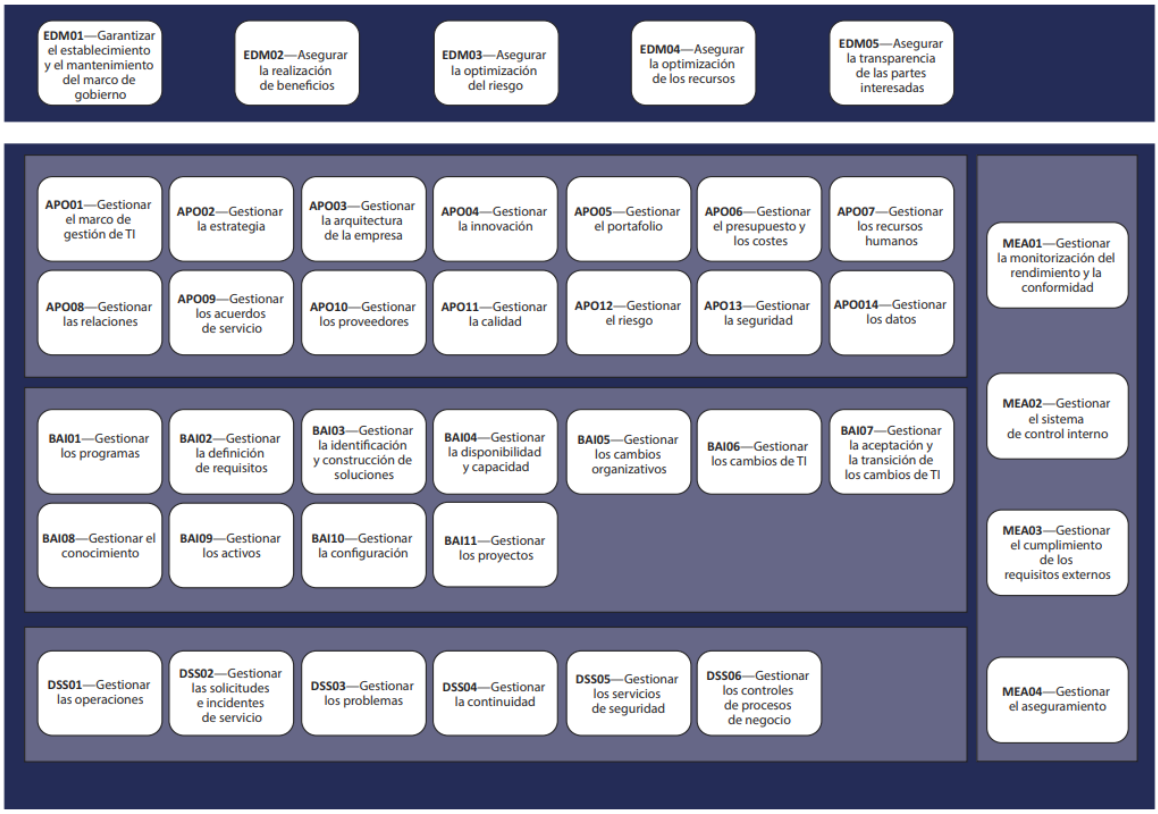
4.1.1. COBIT 2019

Generalidades de COBIT 2019

El marco de trabajo de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés), permite la comprensión del gobierno y la gestión de las tecnologías de información de una organización, así como evaluar el estado en que se encuentran las TI, el cual aprovecha las mejores prácticas de la industria y las herramientas innovadoras de tecnología para fomentar el éxito empresarial (ISACA, 2018).

De acuerdo con ISACA (2018), COBIT utiliza un modelo de procesos que se detalla gráficamente en la Figura 6.

Figura 6: Modelo Core de COBIT



Fuente: (ISACA, 2018)

Estos dominios se encuentran divididos en los procesos organizacionales de gobierno y de gestión. Los cuales se categorizan de la siguiente forma.

- **Gobierno:**
    - Evaluar, dirigir y monitorear (EDM, por sus siglas en el idioma inglés)
- **Gestión:**
    - Alinear, planificar y organizar (APO, por sus siglas en el idioma inglés)
    - Construir, adquirir e implementar (BAI, por sus siglas en el idioma inglés)
    - Entrega, servicio y soporte (DSS, por sus siglas en el idioma inglés)
    - Monitorear, evaluar y valorar (MEA, por sus siglas en el idioma inglés)

COBIT es un marco de gobierno y gestión de tecnologías de información. Sin embargo, puede aportar insumos en la auditoría de seguridad de sistemas y aplicaciones. En la se pueden ver los principales procesos de este marco de gobierno y gestión.

Proceso de auditoría de acuerdo con COBIT 2019

El proceso de evaluación de procesos de COBIT 2019 va alineado al marco de niveles de madurez del CMMI. (Elue, 2020). En COBIT 2019 cada objetivo de gobierno y gestión incluye un componente de proceso, que abarca varias prácticas, cada una de las cuales tiene actividades que ayudan a asegurar el logro de los procesos asociados. Para ayudar a medir el logro del programa de una empresa y su contribución al objetivo general de la empresa, se puede utilizar un esquema de capacidad de proceso, basado en la Integración del modelo de madurez de la capacidad (CMMI) (que varía de 0 a 5). Sin embargo, el uso de COBIT, que puede medir igualmente los mismos logros del programa empresarial, se realiza mediante un concepto llamado "gestión del desempeño de COBIT" (CPM, por sus siglas en inglés).

La gestión del desempeño podría representar el grado de eficiencia del sistema de gobierno y gestión, así como todos los componentes de una empresa y cómo pueden mejorarse para lograr la capacidad y los niveles de madurez requeridos. El modelo CPM se alinea en gran medida con los conceptos de *CMMI Development* V2.02 y los amplía. Los niveles de capacidad y madurez se asignan a todas las actividades del proceso, lo que permite una definición clara de los procesos en diferentes niveles. Esto puede resultar eficaz mediante una evaluación exhaustiva del programa empresarial y las capacidades mediante la gestión del rendimiento.

Existen algunas técnicas que pueden ayudar en la evaluación completa de un programa empresarial. Una técnica notable, que es eficaz y ha resistido la prueba del tiempo en el campo de la gestión de riesgos, es la evaluación de riesgos tecnológicos. La definición de esta evaluación varía de una organización a otra. Sin embargo, mantiene la misma funcionalidad. Esta evaluación examina las áreas clave de personas, procesos y tecnología en relación con un programa empresarial y mide su efectividad.

Por lo tanto, la evaluación puede proporcionar una calificación de puntuación de riesgo basada en la identificación de brechas en su evaluación. La aplicación de CPM puede parecer una tarea desalentadora de aplicar a las evaluaciones o técnicas realizadas por los profesionales del riesgo para su empresa. Sin embargo, dividirlo en varios pasos procesables hace que este esfuerzo sea más alcanzable y manejable. Estos pasos se describen a continuación:

Paso 1: Presentar COBIT 2019 a las partes interesadas y establecer conciencia de evaluación

Durante la ejecución de una evaluación, es importante asegurarse de que las partes interesadas, cuyos procesos y tecnología se están revisando y midiendo, comprendan completamente qué métricas se están evaluando. Por ejemplo, una posible métrica podría evaluar cuántas cuentas privilegiadas no son administradas por una herramienta de administración de acceso privilegiado. Esto también provoca una participación plena durante el proceso de evaluación y ayuda a garantizar la finalización satisfactoria del ejercicio. Este también es el momento de introducir el marco COBIT 2019, que se utilizará para medir de manera efectiva las capacidades y los niveles de madurez del programa empresarial.

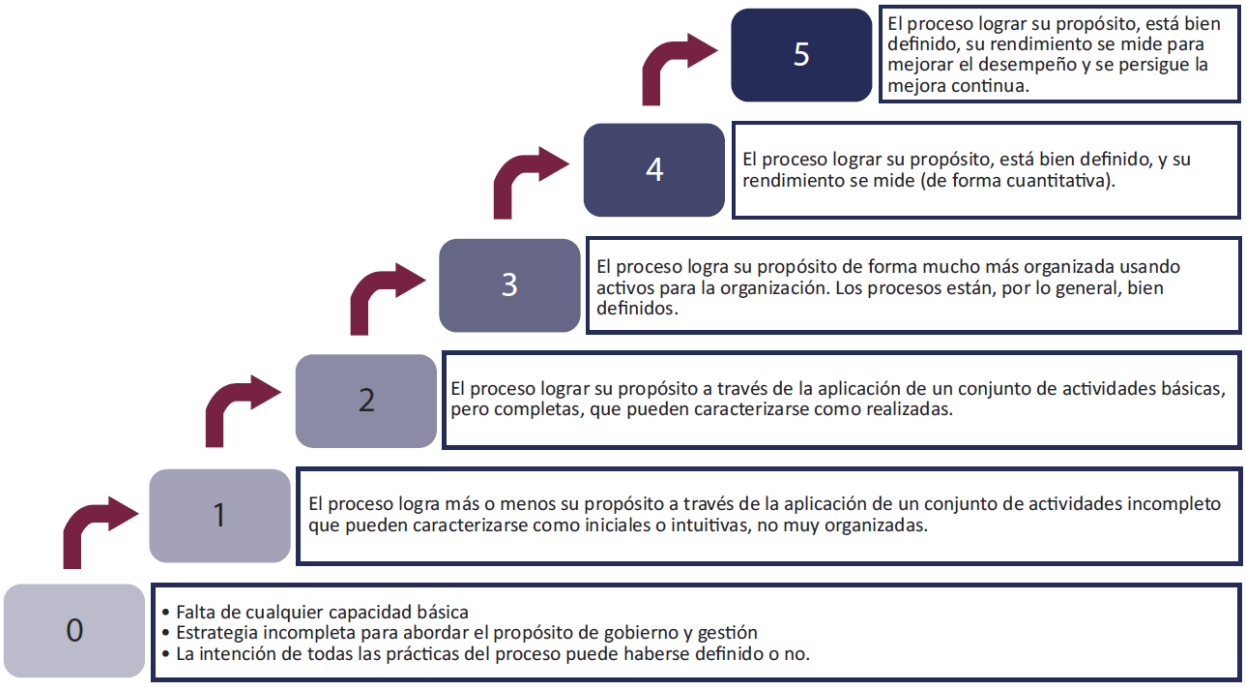
La comprensión de los diversos procesos y tecnologías administrados por estas partes interesadas ayuda a determinar el alcance de la evaluación y orienta el ejercicio de manera más eficaz. Esto, a su vez, ayuda a priorizar áreas clave relevantes para las partes interesadas y la empresa por evaluar.

Paso 2: Adapte el programa y el proceso empresarial al marco COBIT 2019

Adaptar las actividades del proceso a los niveles de madurez y capacidad adecuados es fundamental para el éxito de la evaluación. Esto se incluye en la guía de objetivos de gestión y gobernanza del marco de COBIT® 2019. (ISACA, 2018)

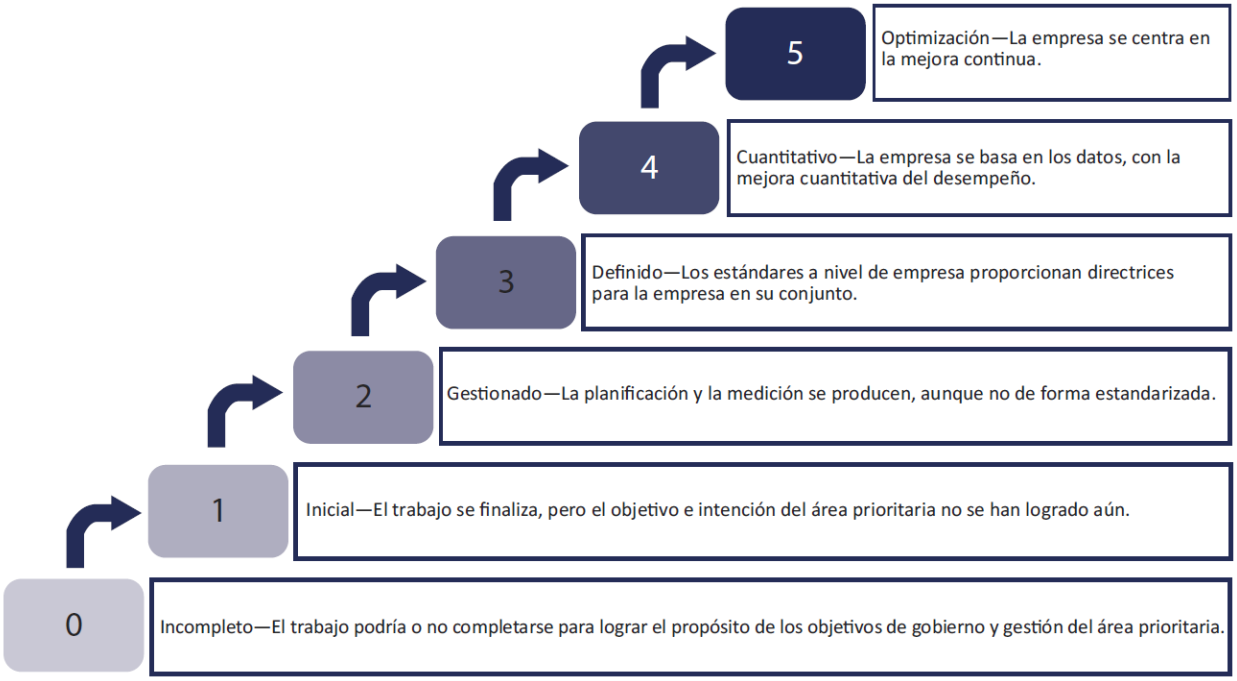
Las actividades del proceso pueden operar en varios niveles de capacidad y madurez, que van de 0 a 5. El nivel de capacidad es una medida del grado de eficiencia de la implementación y del desempeño de un proceso (Figura 7), mientras que el nivel de madurez, que está asociado con áreas de prioridad, es una medida de cómo estos procesos contenidos en el área de prioridad logran ese nivel de capacidad particular, a través de la recopilación de evidencia sustancial subyacente para respaldar los objetivos de la empresa (Figura 8). (ISACA, 2018)

Figura 7: Nivel de madurez para los procesos



Fuente: (ISACA, 2018)

Figura 8: Nivel de madurez para áreas prioritarias



Fuente: (ISACA, 2018)

Paso 3: Evaluar las actividades del proceso

Proporcionar una calificación de puntuación para los niveles de capacidad y madurez se puede lograr utilizando varios métodos. Uno de esos métodos es utilizar las calificaciones disponibles descritas en el marco de COBIT 2019. Las calificaciones utilizan descriptores como: total, en gran parte, parcialmente o no, que tienen porcentajes variables asignados a cada uno. (ISACA, 2018)

Otra calificación de puntuación utilizada podría ser a través de un método formal que conduzca a un conjunto binario de calificaciones de aprobado / reprobado. Sin embargo, un método menos formal (a menudo utilizado en contextos de mejora del desempeño) funciona mejor con un rango de valores de 1 a 5.

Para la evaluación, en función de la madurez del proceso, se asignará un valor de 1 a 5 a los niveles de capacidad y madurez. Esos valores son:

- Inicial: proceso impredecible que está mal controlado y reactivo
- Gestionado: el proceso se planifica, documenta y supervisa en el nivel de proyecto y, a menudo, es reactivo.
- Definido: proceso proactivo destinado a organizaciones
- Gestionado cuantitativamente: proceso medido y controlado
- Optimizado: el enfoque está en el proceso y la mejora continuos

Estos valores se califican subjetivamente, con base en entrevistas con las partes interesadas, revisiones de los documentos de procedimientos ejecutados, programas de supervisión y ejecución de las metas y objetivos de una empresa. (ISACA, 2018)

Paso 4: Obtenga los resultados de la evaluación

Obtener los resultados de la evaluación es un paso crucial para ayudar a la empresa a mejorar en áreas con calificaciones bajas. Las áreas señaladas con calificaciones de puntaje bajo están documentadas con recomendaciones, considerando las fortalezas y las debilidades de la empresa. Los resultados se proporcionan al liderazgo de la empresa y a las partes interesadas para su revisión y priorización. (ISACA, 2018) Las áreas con calificaciones de puntaje bajas también eventualmente se abren camino en un repositorio como un problema o hallazgo. Esto asegura que los problemas o hallazgos sean rastreados hasta su resolución y ayuda a lograr un futuro mejor para los procesos productivos de la compañía.

Controles seleccionados de COBIT 2019

Como se ha explicado anteriormente, COBIT 2019 trasciende los alcances de esta investigación y, desde una perspectiva holística, se puede aplicar a un programa de gobierno y de gestión de tecnologías información. De acuerdo con los alcances de esta investigación se seleccionaron del Modelo Core de COBIT únicamente los procesos y controles (prácticas) relevantes para la implementación de sistemas y aplicaciones. Para realizar esta selección, se utilizó como base el marco de trabajo de *ciberseguridad* de NIST que también es utilizado más adelante. Dicho marco cubre directamente el tema de *ciberseguridad* y brinda un mapeo entre los controles de NIST y las prácticas de gestión de COBIT 5, por lo que seleccionar los controles de COBIT que abarcan temas de *ciberseguridad*, constituye un importante acierto.

Sin embargo, como esta investigación tiene como uno de sus alcances la última versión de las buenas prácticas utilizadas, fue necesario realizar un mapeo manual de las prácticas de COBIT 2019 y COBIT 5, para posteriormente complementar las referencias informativas de NIST CSF con el fin de incluir las prácticas de COBIT 2019 y realizar la selección de controles.

Cabe destacar que ISACA no ha publicado un documento oficial que haga este mapeo de prácticas entre las versiones 5 y 2019, por lo que fue necesario realizarlo como parte de esta investigación y el resultado puede encontrarse en el Apéndice 4: Mapeo de prácticas de COBIT 2019 y COBIT 5. Además, se incluye una versión extendida del NIST CSF core, el cual incluye el mapeo de COBIT 2019 y puede visualizarse en el Apéndice 6: Versión extendida del NIST CSF Core incluyendo COBIT 2019 y controles CIS v8. Después de mapear las prácticas de COBIT 2019 con el marco de *ciberseguridad* de NIST, se seleccionaron un total de 108 controles para considerarlos en la propuesta de solución que se presenta en el capítulo 5. Un extracto de los controles seleccionados puede visualizarse en la Tabla 5. Sin embargo, por el tamaño de esta tabla, la totalidad de esta puede descargarse del siguiente enlace: https://bit.ly/33hfABJ

Tabla 5: Controles seleccionados de COBIT 2019

Proceso COBIT 2019	Práctica de Gobierno o Gestión (Controles)
EDM01 Asegurar el establecimiento y el mantenimiento del marco de gobierno	EDM01.01 Evaluar el sistema de gobierno.
	EDM01.02 Dirigir el sistema de gobierno.
EDM03 Asegurar la optimización del riesgo	EDM03.02 Dirigir la gestión de riesgos.

Fuente: Elaboración propia basada en (ISACA, 2018)

4.1.2. Familia ISO 27000

Generalidades de ISO 27001

Las normas ISO constituyen un conjunto de normas estandarizadas y aceptadas internacionalmente, que tienen como enfoque la mejora de la gestión empresarial por medio de prácticas que permiten la eficiencia y eficacia de procedimientos. La norma ISO/IEC 27001 cuenta con 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 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. El alineamiento estratégico, las necesidades y objetivos de la organización deben ser considerados para influir 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.

Proceso de auditoría de acuerdo con la norma ISO 27001

La norma ISO/IEC 27001 establece el requisito de establecer un plan de auditorías internas, la auditoría Interna se sitúa dentro del proceso de mejora continua y es una herramienta que permite identificar insuficiencias en el sistema y detectar potenciales situaciones de riesgo. De acuerdo con la norma ISO/IEC 27001 la organización debe efectuar auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a. Cumple con:
    1. Los requisitos propios de la organización para su sistema de gestión de la seguridad de la información,
    2. los requisitos de la norma,
b. Una implementación eficaz y un mantenimiento eficiente

La organización debe:

a. Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Los programas de auditoría deben considerar la importancia de los procesos involucrados y los resultados de las auditorías previas
b. Para cada auditoría, definir sus criterios y su alcance
c. Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría
d. Asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías
e. Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de esta.

Los controles por auditar en la norma ISO/IEC 27001 se pueden encontrar en el anexo A de la norma. Dichos controles se clasifican en las siguientes secciones:

1- Política 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

Controles seleccionados de ISO 27001

Los objetivos de control y controles de la norma ISO 27001 se encuentran en el anexo A. Por ser una norma válida para el tema de seguridad de la información, a diferencia de COBIT 2019, todos los 114 controles se consideraron como pertinentes y no es necesario hacer una preselección para la propuesta desarrollada en el capítulo 5. En la Tabla 6 se detalla un extracto de los controles por considerar de la norma ISO 27001 para la metodología propuesta en el Capítulo 5: Propuesta de Solución. Sin embargo, por el tamaño de esta tabla, la totalidad de esta puede descargarse del siguiente enlace: https://bit.ly/335Kxso

Tabla 6: Controles seleccionados de la norma ISO 27001

Sección	Controles de seguridad de la Información
A5	**Políticas de seguridad de la información**
A5.1	**Directrices de gestión de la seguridad de la información**
A5.1.1	Políticas para la seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información

Fuente: Elaboración propia basada en (ISO, 2013)

4.1.3. CIS controles v8

Generalidades de CIS controles v8

El Centro de Seguridad para Internet (Center for Internet Security) es una organización independiente sin fines de lucro que busca desarrollar buenos ejemplos de soluciones de *ciberseguridad* y elaborar prácticas para la seguridad de los sistemas de tecnologías de información ante ataques cibernéticos. Las guías y estándares elaboradas por CIS están en constante actualización y verificación por voluntarios, miembros de una comunidad de profesionales en tecnologías de información, los cuales cuentan con amplia experiencia en este ámbito. (Center for Internet Security, 2019)

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 han estado en constante actualización. Consisten en una guía para las mejores prácticas en seguridad computacional. En el año 2021, esta 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.

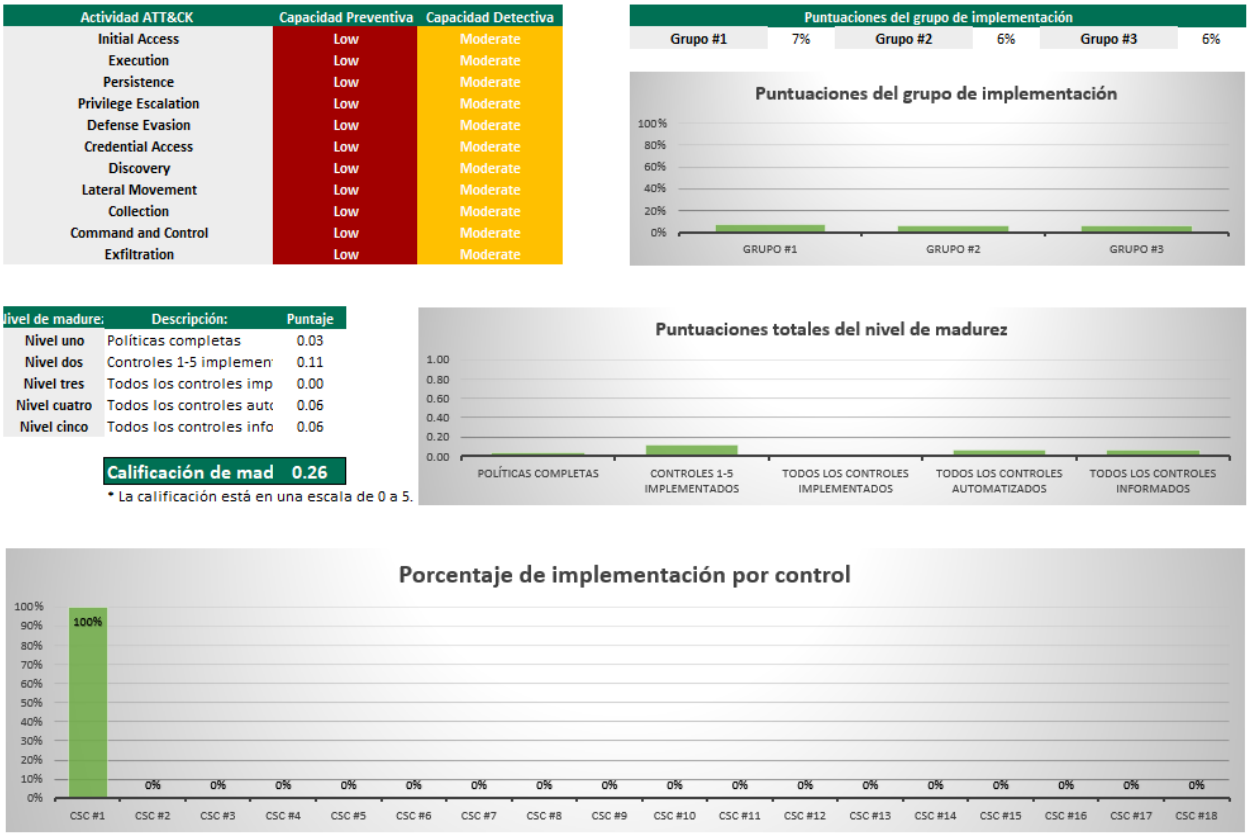
Proceso de auditoría de acuerdo con CIS controles v8

CIS brinda una herramienta gratuita para realizar autoevaluaciones de los controles. El propósito de esta herramienta es proporcionar a las organizaciones una herramienta simple para realizar una evaluación inicial de su nivel de madurez de aseguramiento de la información basada en los controles definidos por los Controles CIS. Para utilizar esta herramienta, el evaluador solo debe completar una serie de preguntas de un menú desplegable en las páginas para cada uno de los 18 controles de CIS.

La herramienta de evaluación genera automáticamente puntajes y nivel de madurez en función de las respuestas a cada pregunta. Estos puntajes se pueden usar para medir el progreso de la organización y qué porcentaje de los controles CIS están en cumplimiento actualmente. Esta herramienta puede descargarse de (Enclave Security , 2021) En la Figura 9

se puede visualizar un ejemplo del *dashboard* generado por esta herramienta, la que puede facilitar la presentación de resultados a las partes interesadas.

Figura 9: Dashboard de cumplimiento de Controles CIS v8



Fuente: Adaptado al español de (Enclave Security , 2021)

Controles seleccionados de controles CIS v8

Para la creación de la versión extendida del NIST CSF Core con COBIT 2019 y controles CIS v8, se tomó como base un mapeo existente de controles CIS versión 8 al marco de NIST CSF, que se puede encontrar en (Center for Internet Security, 2021). En el

Apéndice 5: Resumen del mapeo de controles de CIS con el NIST CSF, se puede ver un extracto del mapeo de controles de CIS v8 con el marco de *ciberseguridad* de NIST. Estos 153 sub-controles, al igual que los de la ISO 27001 son relevantes para una evaluación de *ciberseguridad*, por lo que serán utilizados en el siguiente capítulo para el desarrollo de la propuesta y la selección final de controles.

A continuación, en la Tabla 7: Controles seleccionados de los Controles de CIS se lista un extracto de los controles seleccionados de los CIS CSC versión 8 por utilizar. Sin embargo, por el tamaño de esta tabla la totalidad de esta puede descargarse del siguiente enlace: https://bit.ly/3IAOh5l

Tabla 7: Controles seleccionados de los Controles de CIS

CIS Sub-Control	Tipo de activo	Función de seguridad	Título
Inventario y control de activos de hardware			
1.1	Dispositivos	**Identificar**	Establecer y mantener un inventario de activos detallado
1.2	Dispositivos	**Responder**	Abordar activos no autorizados
1.3	Dispositivos	**Detectar**	Utilice una herramienta de descubrimiento activa

Fuente: Elaboración propia basada en (Center for Internet Security, 2021)

4.1.4. Marco de Trabajo de Ciberseguridad de NIST

Generalidades del NIST CSF

El marco de trabajo y de buenas prácticas NIST CSF (Cybersecurity Framework) provee un enfoque flexible, priorizado, repetible, basado en el desempeño y costo – efectivo, e 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. (Instituto Nacional de Estándares y Tecnología, 2018) El marco es efectivo y respalda la innovación técnica porque es neutral desde el punto de vista tecnológico (no pertenece a un proveedor privativo o promueve una tecnología específica),

pero a la misma vez hace referencia a una variedad de normas, directrices y prácticas existentes que evolucionan con la tecnología.

De acuerdo con el NIST (2018), existe una gran variedad de formas de cómo utilizar el marco. La decisión sobre cómo aplicarlo se deja a la organización implementadora. Por ejemplo, una organización puede decidir utilizar los niveles de implementación del marco para articular las prácticas de gestión de riesgos previstas. Otra organización puede utilizar las cinco funciones del marco para analizar la cartera de gestión de riesgos. Dicho análisis puede o no basarse en una guía complementaria más detallada, aplicado como los catálogos de controles.

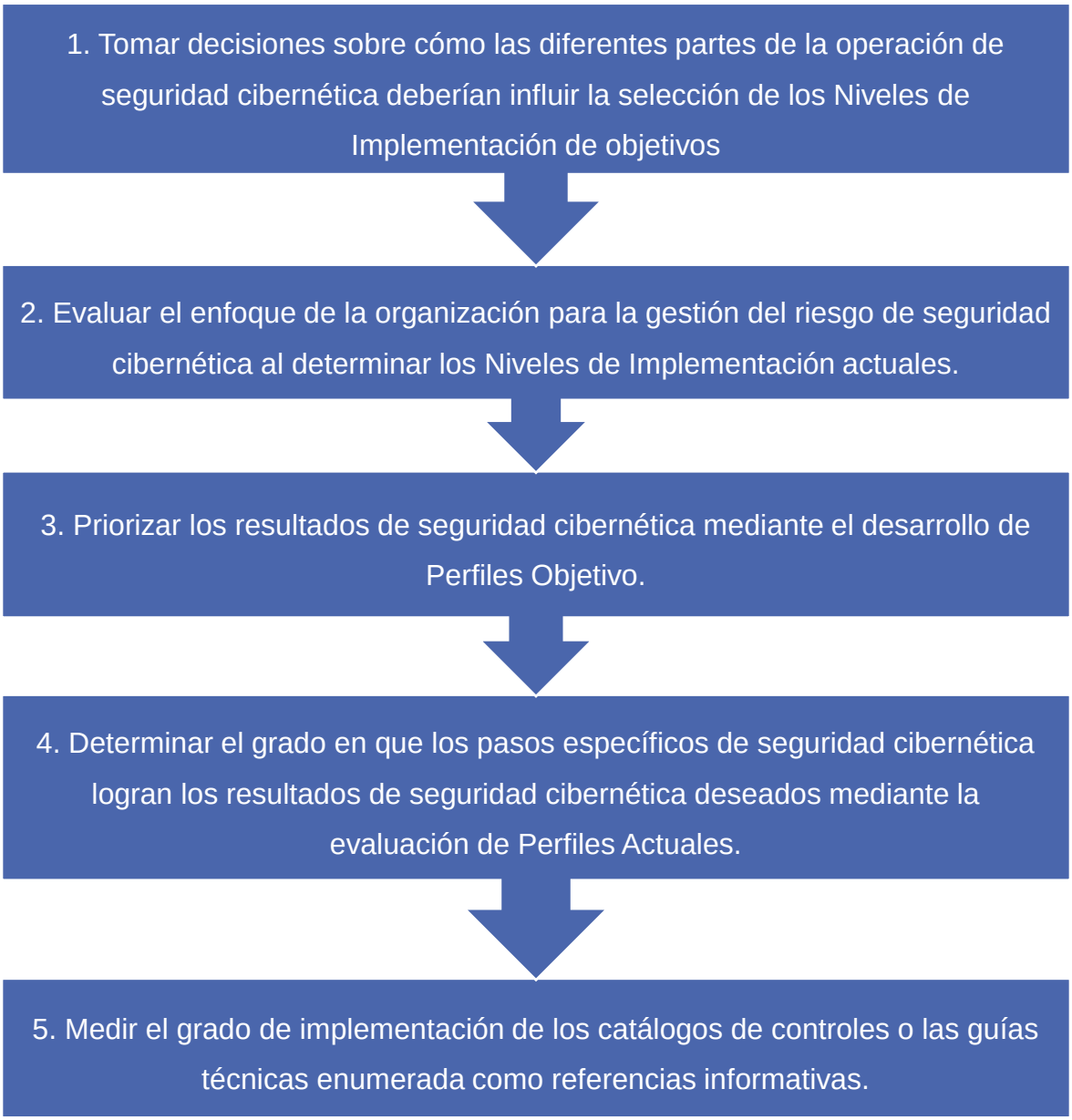
Este último escenario es similar a lo que se busca con la presente investigación, pues lo que se desea es adaptar los marcos estudiados para proponer una metodología de auditoría de aplicaciones y sistemas (un subconjunto de la gestión de riesgos de seguridad).

Proceso de auditoría de acuerdo con NIST CSF

En la sección 4 del documento del NIST CSF se describe cómo utilizar el marco para autoevaluar y demostrar la seguridad cibernética. Las organizaciones que usan el marco pueden medir y asignar valores a su riesgo junto con el costo y los beneficios de los pasos tomados para reducir el riesgo a niveles aceptables. Mientras mejor sea capaz una organización de medir los riesgos, costos y beneficios de sus estrategias y pasos de seguridad cibernética, más racional, eficaz y valioso será su enfoque e inversiones en seguridad cibernética. (Instituto Nacional de Estándares y Tecnología, 2018)

La autoevaluación y la medición deberían mejorar la toma de decisiones sobre las prioridades de inversión y la comunicación con partes interesadas. Los resultados de seguridad cibernética del núcleo del marco apoyan la autoevaluación de la eficacia de la inversión y las actividades de seguridad cibernética de acuerdo con lo descrito en la Figura 10: Proceso de Auditoría de NIST CSF.

Figura 10: Proceso de Auditoría de NIST CSF



Fuente: Elaboración propia basada en (Instituto Nacional de Estándares y Tecnología, 2018)

Controles seleccionados de NIST CSF

Al igual que ISO 27001 y los controles de CIS, el NIST CSF se enfoca directamente en *ciberseguridad* por lo que en esta fase de la investigación no es necesario filtrar controles y se utilizarán la totalidad en el siguiente Capítulo 5: Propuesta de Solución. A continuación, en la Tabla 8: Controles seleccionados de NIST CSF se lista un extracto de los controles del marco

de *ciberseguridad* de NIST a utilizar en la propuesta, sin embargo, por el tamaño de esta tabla la totalidad de esta puede descargarse del siguiente enlace: https://bit.ly/3q097D5

Tabla 8: Controles seleccionados de NIST CSF

Función	Categoría	Subcategoría
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los propósitos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	ID.AM-1: Se inventarían los dispositivos y sistemas físicos dentro de la organización.
		ID.AM-2: Se inventarían las plataformas y aplicaciones de software dentro de la organización.

Fuente: Elaboración propia basada en (Instituto Nacional de Estándares y Tecnología, 2018)

4.2. Comparación de procesos de auditoría

Tal y como se explicó en sus respectivos apartados cada una de las buenas prácticas desarrolladas anteriormente presentan su propio proceso sugerido para la realización de autoevaluaciones o auditorías. De manera general y a modo de resumen se describen a continuación los puntos clave que se consideraron en el capítulo 5, como base para el desarrollo de la propuesta:

COBIT 2019:

- Brinda un proceso de evaluación alineado al marco de niveles de madurez del CMMI (que varía de 0 a 5).
- La evaluación examina las áreas clave de personas, procesos y tecnología y mide su efectividad.

- La evaluación puede proporcionar una calificación de puntuación de riesgo basada en la identificación de brechas.
- Se establece como primer paso informar a las partes interesadas y que estas comprendan el alcance y métricas de la evaluación.
- Se debe proporcionar una calificación de puntuación para los niveles de capacidad. Para esto se pueden utilizar descriptores cualitativos (total, en gran parte, parcialmente o no) o valores cuantitativos (escala de 1 a 5).
- Las áreas señaladas con calificaciones de puntaje bajo, deben ser documentadas con recomendaciones

ISO 27001:

- Se debe establecer una herramienta que permita identificar insuficiencias en el sistema y detectar potenciales situaciones de riesgo.
- La organización debe llevar a cabo auditorías internas a intervalos planificados y proporcionar información.
- Se debe seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría.
- Se debe asegurar de que se informa a la dirección pertinente de los resultados de las auditorías.
- Conservar información documentada como evidencia de la auditoría y de los resultados de esta.

CIS CSC:

- Es destacable el uso de una herramienta simple para realizar una evaluación basada en los controles definidos.
- El evaluador solo debe completar una serie de preguntas de un menú desplegable en las páginas para cada uno de los controles.
- La herramienta de evaluación genera automáticamente puntajes y nivel de madurez en función de las respuestas a cada pregunta.

- Estos puntajes se pueden usar para medir el progreso de la organización y qué porcentaje de los controles están en cumplimiento.

NIST CSF:

- Se pueden medir y asignar valores a su riesgo junto con el costo y los beneficios de los pasos tomados para reducir el riesgo a niveles aceptables.
- La autoevaluación y la medición deberían mejorar la toma de decisiones sobre las prioridades de inversión y la comunicación con partes interesadas.

5. Capítulo 5: Propuesta de Solución

5.1 Proceso de auditoría de sistemas propuesto

Con base en los procesos de auditoría descritos en el Capítulo 4: Análisis del Diagnóstico y a partir de los puntos clave de cada uno, ya mencionados en el apartado de comparación de los procesos de auditoría, se establece el siguiente proceso:

1) Planificación de la auditoría

a) Se establece como primer paso, informar a las partes interesadas, de modo que estas comprendan el alcance y las métricas de la evaluación.
b) En esta etapa se establece el alcance de la auditoría. Si bien el proceso propuesto se enfoca en la implementación de sistemas y aplicaciones, la organización puede seleccionar departamentos, funciones, sistemas o aplicaciones críticas por considerar en el alcance.
c) La evaluación examinará las áreas clave de personas, procesos y tecnología y, además, medirá su efectividad.
d) La herramienta propuesta presenta 5 niveles de madurez. En esta etapa del proceso la organización debe establecer la meta de madurez por alcanzar, es decir, cuál es el nivel de madurez mínimo que se establece como aceptable. Posteriormente, este nivel puede ser elevado en auditorías subsecuentes conforme la organización mejore su nivel de seguridad.
e) La organización también debe establecer cuáles serán las medidas que deben seguir las áreas que no alcancen el nivel mínimo establecido, en materia de seguridad.
f) Se debe seleccionar al personal auditor y asegurarse de la objetividad y la imparcialidad del proceso de auditoría.
g) Si la organización desea modificar de alguna forma la metodología propuesta deberá establecerlo por escrito en esta fase y la alta dirección deberá aprobar el inicio y alcance de la auditoría.

2) **Ejecución de la auditoría**
   a) Es destacable el uso de una herramienta simple para realizar una evaluación basada en los controles definidos.
   b) El evaluador solo debe completar una serie de preguntas de un menú desplegable en las páginas para cada uno de los controles.
   c) La herramienta de evaluación genera automáticamente puntajes y el nivel de madurez, en función de las respuestas a cada pregunta.
   d) Estos puntajes se pueden usar para medir el progreso de la organización y qué porcentaje de los controles están en cumplimiento.
   e) Se utiliza la herramienta propuesta que permite identificar insuficiencias en el sistema y detectar potenciales situaciones de riesgo.

3) **Preparación y distribución del informe**
   a) Se debe conservar información documentada como evidencia de la auditoría y de los resultados de esta.
   b) Se debe asegurar de que se informa a la dirección pertinente de los resultados de las auditorías.
   c) Las áreas señaladas con calificaciones de puntaje bajo, deben ser documentadas con recomendaciones

4) **Seguimiento de la auditoría**
   a) Periódicamente, el equipo de auditoría debe hacer seguimiento de las recomendaciones generadas a partir del informe de auditoría.
   b) Se deben documentar las medidas tomadas para eliminar las brechas identificadas y mitigar los riesgos identificados.

5) **Revisión y mejora del programa de auditoría**
   a) De manera continua, las partes interesadas deben identificar lecciones aprendidas y oportunidades de mejora, tanto para el proceso como para las herramientas utilizadas, los informes de auditoría, entre otros.

Aspectos tomados en cuenta en el desarrollo de la propuesta:

- **Niveles de Madurez:**

Con base en buenas prácticas como COBIT 2019 y CIS controles v8 se estableció, dentro de la propuesta, un marco de madurez de cinco niveles. La herramienta desarrollada calcula automáticamente el resultado de estos niveles, cuya escala está de 0 a 5. Los niveles de madurez propuestos se pueden ver a continuación en la Tabla 9: Niveles de Madurez Propuestos.

Tabla 9: Niveles de Madurez Propuestos

Nivel de madurez:	Descripción:	Puntaje:
Nivel uno	Políticas completas	1.00
Nivel dos	Controles de ID implementados	0.35
Nivel tres	Todos los controles implementados	0.33
Nivel cuatro	Todos los controles automatizados	0.00
Nivel cinco	Todos los controles informados	0.00

Calificación de madurez *:	1.68
* La calificación está en una escala de 0 a 5.	

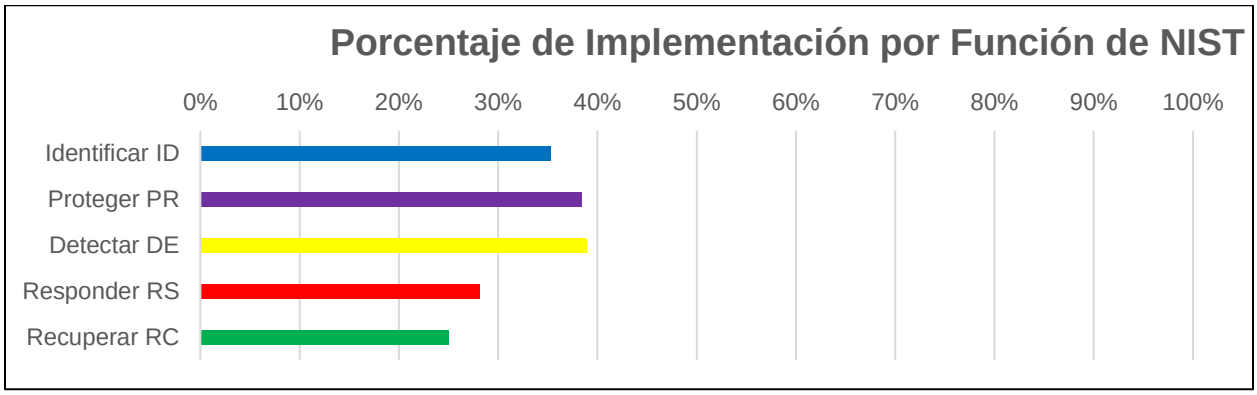
Fuente: Elaboración propia con base en (Enclave Security , 2021)

- **Gráficos de porcentaje de implementación por función y categoría**

Con el objetivo de facilitar la comunicación con las partes interesadas, se desarrolló dentro de la herramienta un apartado de cuadro de mando o *dashboard*, donde se pueden visualizar una serie de gráficos que se generan automáticamente conforme el equipo de auditoría completa todas las preguntas. Como se detalla más adelante en el apartado 5.2 Controles seleccionados para auditoría de sistemas, se seleccionó como base de la propuesta el marco de *ciberseguridad* de NIST, con referencias a los otros marcos de buenas prácticas analizados. Debido a esto los gráficos propuestos se desarrollaron considerando las cinco funciones y las veintidós categorías de NIST CSF, las cuales (funciones y categorías) se explican a continuación.

Para evidenciar el avance de cobertura en la implementación de controles por funciones del marco (identificar, proteger, detectar, responder y recuperar), se presenta el gráfico en la Figura 11:

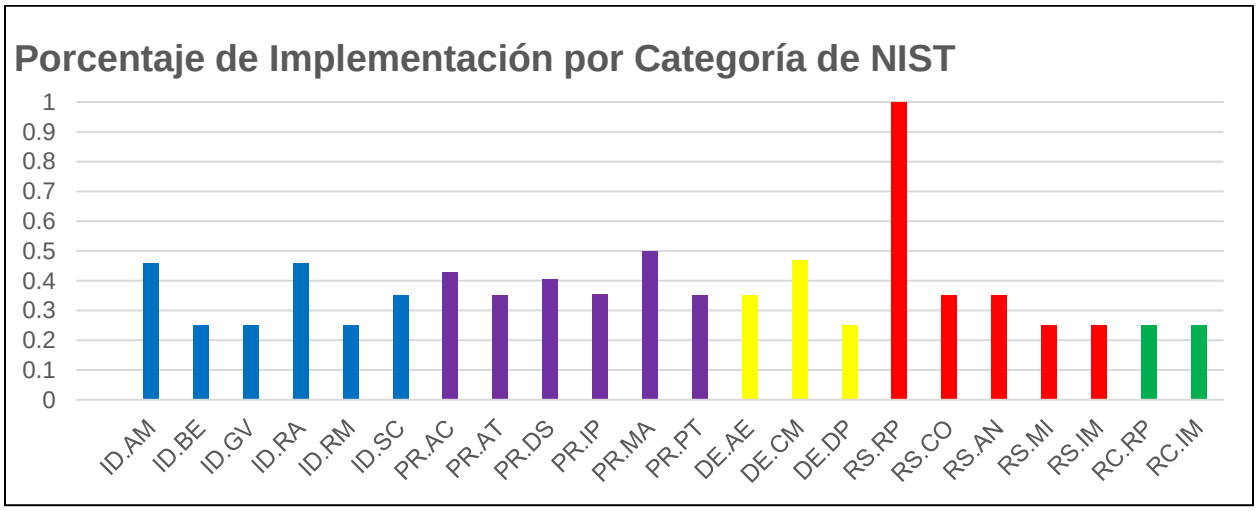
Figura 11: Gráfico ejemplo de porcentaje de Implementación por Función



Fuente: Elaboración propia (2021)

De manera similar, para evidenciar el avance de cobertura en la implementación de controles por categoría del marco se presenta el gráfico en la Figura 12:

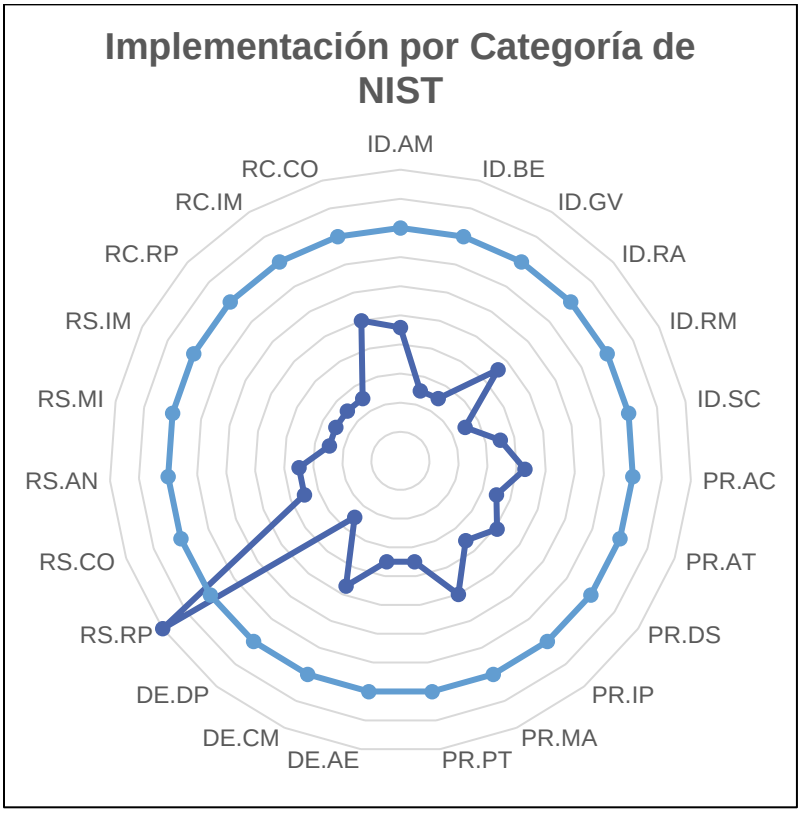
Figura 12: Gráfico ejemplo de porcentaje de Implementación por Categoría



Fuente: Elaboración propia (2021)

Finalmente, tomando como supuesto una meta de ochenta por ciento (80%) en todas las categorías, se presenta a modo de ejemplo, un gráfico de radar donde se pueden personalizar las metas y evidenciar el porcentaje alcanzado después de la auditoría, con el objetivo de identificar brechas y oportunidades de mejora. El ejemplo puede visualizarse en la Figura 13:

Figura 13: Gráfico ejemplo de metas alcanzadas por Categoría



Fuente: Elaboración propia (2021)

5.2 Controles seleccionados para auditoría de sistemas

Para facilitar el desarrollo de la auditoría se creó un papel de trabajo con un total de 108 controles. Cada uno de estos controles se definieron tomando como base el análisis del Capítulo 4: Análisis del Diagnóstico y se catalogaron en las funciones y categorías del marco de *ciberseguridad* de NIST. Además, y según el Apéndice 6: Versión extendida del NIST CSF Core incluyendo COBIT 2019 y controles CIS v8 se incluyeron las referencias informativas de los cuatro marcos de buenas prácticas utilizados, de manera tal que para cada uno de los

controles seleccionados se hace referencia al número de control CIS, la práctica de COBIT 2019, el control o la cláusula de ISO 27001 y la subcategoría de NIST CSF.

El propósito de esta herramienta es proporcionar a las organizaciones un instrumento simple para realizar una evaluación de su nivel de seguridad, basada en los controles definidos por los Controles de NIST CSF, COBIT 2019, CIS CSC v8, e ISO 27001. Para utilizar esta herramienta, el evaluador solo debe completar las respuestas a las listas de preguntas del menú desplegable en la página "Evaluación". Al elegir una opción desplegable para cada control, la herramienta generará automáticamente puntajes y nivel de madurez en función de las respuestas a cada pregunta. Según las respuestas a cada pregunta, la hoja de trabajo del *dashboard* se completará automáticamente con las puntuaciones generales del nivel de madurez. Estos puntajes se pueden usar para medir el progreso de la organización y qué porcentaje de los controles están cumpliendo actualmente.

Para la evaluación apropiada de los niveles de madurez para cada uno de los controles se establecieron cuatro preguntas, cada una con 5 posibles respuestas:

- **Definición de la política**
    - Sin política - Política informal - Política escrita parcial - Política escrita - Política escrita aprobada

- **Implementación del Control**
    - No se ha implementado - Partes de la política implementadas - Implementado en algunos sistemas - Implementado en la mayoría de los sistemas - Implementado en todos los sistemas

- **Automatización del Control**
    - No automatizado - Partes de la política automatizadas - Automatizado en algunos sistemas - Automatizado en la mayoría de los sistemas - Automatizado en todos los sistemas

- **Informe del control a la alta dirección**
    - No reportado - Partes de la política informadas - Informado sobre algunos sistemas - Reportado en la mayoría de los sistemas - Reportado en todos los sistemas

La categorización de los niveles de madurez se estableció de la siguiente manera:

- **Nivel uno:** Hay políticas aprobadas para la totalidad de controles.
- **Nivel dos:** La totalidad de controles de función “identificar” están implementados.
- **Nivel tres:** La totalidad de controles están implementados.
- **Nivel cuatro:** La totalidad de controles están automatizados.
- **Nivel cinco:** La totalidad de controles están informados y reportados.

Finalmente, a modo de ejemplo se presenta en la Tabla 10 un extracto de los primeros 5 controles del papel de trabajo, el acceso a la herramienta completa puede encontrarse en el Apéndice 7: Papel de trabajo propuesto para la metodología.

Tabla 10: Extracto del papel de trabajo propuesto

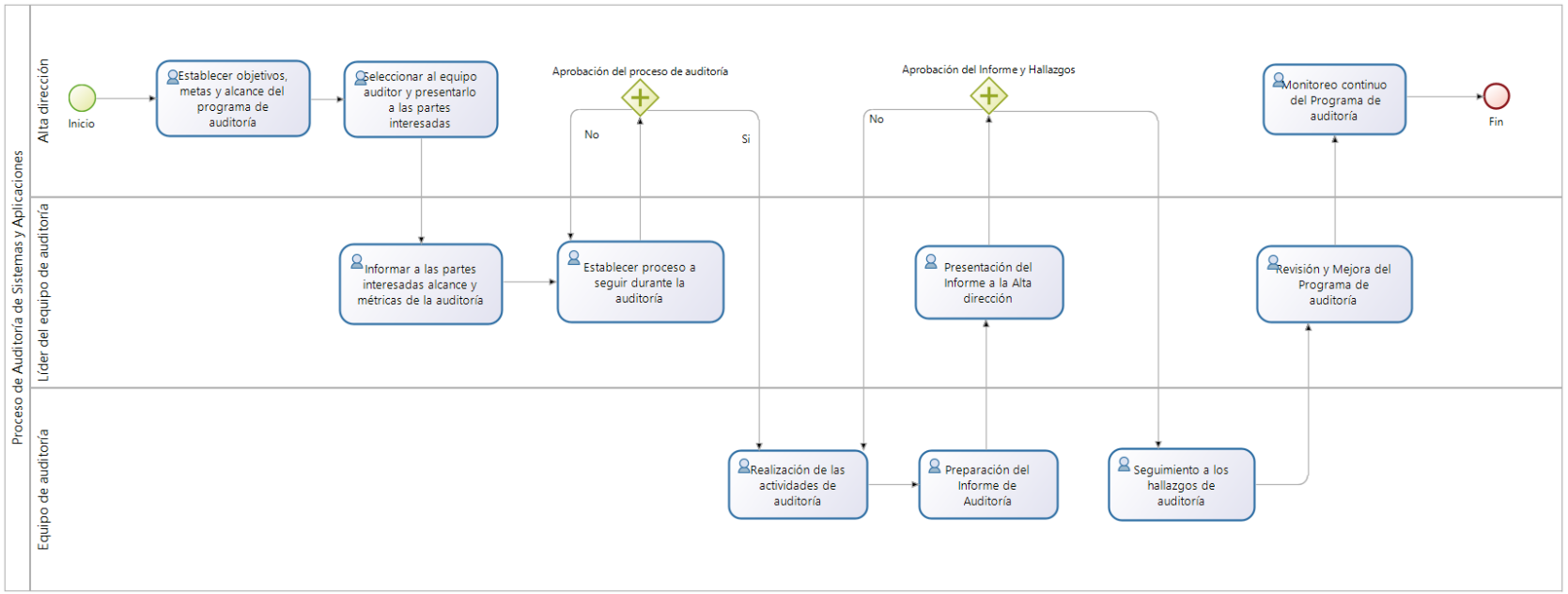
Control ID	Función	Categoría del Control NIST	Código Categoría del Control NIST	Nombre del Control	CIS CSC v8	COBIT 2019	ISO/IEC 27001:2013	NIST CSF	Definición de política	Control implementado	Control automatizado o técnicamente reforzado	Control informado a la empresa	Comentarios
1	Identificar ID	Gestión de	ID.AM	Se inventarían los dispositivos y sistemas físicos dentro de la organización.	1.1	BAI09.01, BAI09.02	A.8.1.1, A.8.1.2	ID.AM-1					
2	Identificar ID	Gestión de	ID.AM	Se inventarían las plataformas y aplicaciones de *software* dentro de la organización.	16.4, 2.1, 2.2	BAI09.01, BAI09.02, BAI09.05	A.8.1.1, A.8.1.2, A.12.5.1	ID.AM-2					

Fuente: Elaboración propia (2021)

5.3 Diagrama del proceso de auditoría propuesto

Finalmente, tal y como se estableció en los alcances y el último objetivo específico el proyecto incluye la elaboración de un diagrama BPMN, con los pasos de la metodología desarrollada. Este diagrama se puede ver en la Figura 14 y se desarrolló tomando como inspiración el ciclo de Deming (planificar, hacer, revisar y actuar) usado en las normas ISO. Se incluyeron las actividades propias de la realización de la auditoría y los pasos propuestos para la planificación, seguimiento y mejora continua del programa de auditoría.

Figura 14: Diagrama de BPMN para el proceso propuesto de auditoría



Fuente: Elaboración propia (2021)

6. Capítulo 6: Conclusiones y Recomendaciones

6.1. Conclusiones

a. La metodología propuesta incluye el proceso y la herramienta, lo que permite realizar una auditoría de sistemas y aplicaciones de acuerdo con los marcos de buenas prácticas seleccionados.
b. La propuesta metodológica se realizó tomando como base las últimas versiones de los cuatro marcos de buenas prácticas encontrados con más frecuencia en el estado de la cuestión: la norma ISO 27001, el marco de COBIT 2019, los controles críticos de CIS versión 8 y el marco de ciberseguridad de NIST.
c. Cada uno de los marcos de buenas prácticas presenta un proceso guía para la realización de auditorías o evaluaciones. Estos fueron debidamente descritos y sus principales características fueron extraídas para completar el desarrollo de la propuesta.
d. Se escogieron un total de 108 controles enfocados en los riesgos críticos de los cuatro marcos de buenas prácticas. Además, para cada uno de los controles seleccionados se incluyeron en la herramienta desarrollada, las referencias relacionadas con el control de cada uno de los marcos. De esta forma, en caso de ser necesario, la persona encargada de la auditoría puede buscar más información en los marcos base.
e. Para la metodología se realizó una comparación de los procesos de auditoría de los marcos de buenas prácticas y se planteó un proceso que toma los puntos clave de los diferentes marcos. La propuesta de proceso de auditoría sigue el ciclo de Deming para el mejoramiento continuo de dicho programa.
f. El uso de BPMN para la realización del diagrama de proceso fue de valor agregado, pues permite entender el proceso y sus roles asociados desde un alto nivel de abstracción y luego extenderlo a toda la compañía para entender los detalles de cada actividad.

6.2. Recomendaciones

a. En un trabajo futuro se deberá ejecutar un plan piloto de implementación de la propuesta, con el fin de identificar oportunidades de mejora, así como verificar la eficacia y eficiencia de la propuesta.
b. A la hora de implementar la propuesta será necesario contar con personal debidamente capacitado de manera general en los marcos de buenas prácticas seleccionados y en el contenido de la propuesta, así como el uso de las herramientas desarrolladas.
c. Es necesario familiarizarse con los procesos de auditoría de los marcos seleccionados, pues estos se tomaron como base para el desarrollo de la propuesta. Además, el personal encargado de las auditorías debe capacitarse en el uso de las herramientas desarrolladas para la realización de la auditoría.
d. Antes de iniciar la implementación del programa de auditoría, la organización debe verificar que los 108 controles seleccionados están considerados en los alcances de la auditoría. En caso de encontrar controles que no apliquen, se debe documentar la decisión, recibir la aprobación de la alta dirección y ajustar las herramientas por utilizar para reflejar esta decisión.
e. La propuesta de metodología y el proceso definido pueden ser adaptados a la realidad de la organización que decida implementar este proceso. Esto con el objetivo de ajustarse a las necesidades específicas de los sistemas o aplicaciones por auditar. Sin embargo, la propuesta está realizada con suficiente nivel de generalidad para que sea fácil de adaptar a diversos escenarios.
f. Para la comunicación y entrenamiento del equipo auditor es muy importante utilizar el diagrama de proceso en notación de BPM, así como las otras referencias gráficas, como las incluidas en el cuadro de mando o *dashboard* incluido en la herramienta desarrollada.

Referencias

Axelos. (2020). *ITIL 4: Connecting Key Concepts*. Obtenido de https://www.axelos.com/itil-4-concepts

Aza Mimalchi, A. H. (2019). *Auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, basada en la Norma ISO/IEC 27001 y la metodología OSSTMMV3.* Obtenido de Repositorio Digital Universidad Técnica del Norte: http://repositorio.utn.edu.ec/bitstream/123456789/9028/1/04%20RED%20218%20TRABAJO%20DE%20GRADO.pdf

Bracho-Ortega, C., Cuzme-Rodríguez, F., Pupiales-Yépez, C., Suárez-Zambrano, L., Peluffo-Ordóñez, D., & Moreira-Zambrano, C. (2018). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio. *Maskana, 8*, 307-319.

Candiwan, M. Y., & Priyadi, Y. (2016). Analysis of Information Security Audit Using ISO 27001: 2013 & ISO 27002: 2013 at IT Division-X Company, In Bandung, Indonesia. *International Journal of Basic and Applied Science*, 77.

Center for Internet Security. (2019). *CIS Controls Spanish Translation*. Obtenido de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Center for Internet Security. (2019). *CIS Controls v7.1 Mapping to NIST CSF.* Obtenido de https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/

Center for Internet Security. (2021). *CIS Controls v8 Mapping to NIST CSF.* Obtenido de https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/

Center for Internet Security. (2021). *CIS Critical Security Controls v8.*

Center for Internet Security. (2021). *CIS CSAT: A Free Tool for Assessing Implementation of CIS Controls*. Obtenido de https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/

Chavarría Barquero, R. H. (2018). *Auditoría de la seguridad de información en una empresa privada costarricense.* Obtenido de Repositorio del Sistema de Bibliotecas, Documentación e Información de la UCR: http://repositorio.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/8845/1/43347.pdf

Chavarría-González, M. C. (2011). La Dicotomía cuantitativo/cualitativo: falsos dilemas en investigación. *Actualidades en Psicología*, 1-35.

Chifla-Villón, M., Puma-Aucapiña, L., & Villacís-Real, K. (2020). Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del Ecuador. *CIENCIA UNEMI, 13(34)*, 127-143.

Cooke, I. (1 de Mayo de 2019). *IS Audit Basics: Developing the IT Audit Plan Using COBIT 2019*. Obtenido de ISACA website: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/developing-the-it-audit-plan-using-cobit-2019

Elue, E. (2020). *Effective Capability and Maturity Assessment Using COBIT 2019.* Obtenido de sitio web de ISACA: https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019

Enclave Security . (2021). *The CIS Critical Security Controls*. Obtenido de https://www.auditscripts.com/download/4588/

Gantz, S. D. (2014). *The basics of IT audit.* Elsevier Inc.

Hérnandez, R., Férnandez, C., & Baptista, M. d. (2014). Metodología de la Investigación. México DF: McGraw-Hill.

Hilario Novoa, F. J. (2017). *Auditoría a la seguridad informática de los servicios de tecnologías de la información en la ESE Hospital San Francisco de Gachetá.* Obtenido de Repositorio de la Universidad Nacional Abierta y a Distancia: https://repository.unad.edu.co/handle/10596/12796

Instituto Nacional de Estándares y Tecnología. (2018). *Marco para la mejora de la seguridad cibernética en infrestructuras críticas*. Obtenido de https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

ISACA. (2018). *COBIT 2019 Marco de Referencia - Introducción y Metodología.* Illinois: ISACA.

ISACA. (2018). *COBIT 2019 Governance and Management Objectives.*

ISACA. (2018). *Diseño de una solución de Gobierno de Información y Tecnología.* Illinois: ISACA.

ISACA. (2020). *COBIT*. Obtenido de https://www.isaca.org/resources/cobit

ISO. (2013). *Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información (ISO/IEC 27001:2013).*

Jaramillo, C., Jácome, L., Ordóñez, Á., Gaona, M., Carrión, J., & Palma, M. (2017). Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja. *Maskana, 8*, 149-162.

Kelo, T., Eronen, J., & Rousku, K. (2018). Model for efficient development of security audit criteria. *In Proceedings of the 17th European Conference on Cyber Warfare and Security: ECCWS*, 244.

Lewis, B. (Marzo de 2018). *ISO/IEC 27000 – KEY INTERNATIONAL STANDARD FOR INFORMATION SECURITY REVISED*. Obtenido de https://www.iso.org/news/ref2266.html

Markina, I., & Diachkov, D. (2019). INFORMATION SECURITY AUDIT SPECIFICITY. *Moderní věda*, 13.

Marrone, M., & Kolbe, L. M. (2011). Impact of IT Service Management Frameworks on the IT Organization. *Business & Information Systems Engineering*, 5-18. Obtenido de https://link.springer.com/article/10.1007/s12599-010-0141-5

Object Management Group. (2011). *Business Process Model and Notation (BPMN) version 2.0.*

Proagilist . (2020). *GESTIONAR SERVICIOS CON ITIL®4*. Obtenido de https://proagilist.es/gestion-servicios-itil-4/

Puma Arosquipa, M. Y. (2017). *Implantación de un proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002 en una entidad financiera de Puno–2016.* Obtenido de Repositorio Institucional de la Universidad Nacional del Altiplano: http://tesis.unap.edu.pe/bitstream/handle/UNAP/6629/Puma_Arosquipa_Max_Yonel.pdf

Santos López, F. M., & Santos de la Cruz, E. G. (2012). Aplicación práctica de BPM para la mejora del subproceso de picking en un centro de distribución logístico. *Revista de la Facultad de Ingeniería Industrial UNMSM*, 120-127.

Secretaría Central de ISO. (2018). *Traducción Oficial ISO 19011.*

Sujana, A., Adinda, N., Lestari, N., Fadriani, H., & Mahardika, A. (2020). *Audit Information System Using Cobit 5.*

Ujjaman, M. (2018). *Development of a Security Audit Framework for an Organization.* Obtenido de UIU Digital Instituitional Repository System: http://dspace.uiu.ac.bd/bitstream/handle/52243/177/Thesis_report_Mahbub_Ujjaman_Final_Feb_2018.pdf

Apéndices

Apéndice 1: Detalles de la revisión literaria en inglés

Número	Fuente	Tipo de documento	Relevante	Justificación de exclusión
1	[PDF] Information security audit specificity	Artículo científico	Sí	-
2	[PDF] Analysis of Information Security Audit Using ISO 27001: 2013 & ISO 27002: 2013 at IT Division-X Company, In Bandung, Indonesia	Artículo científico	Sí	-
3	[PDF] A Study of security audit and VAPT audit and implementation of cyber security controls like WSUS against cyber threats	Artículo científico	No	Uso de una tecnología específica (WSUS) y no trata el tema de auditoría
4	The new aspects for the instantaneous information security audit	Artículo científico	No	Se enfoca en vulnerabilidades de día cero y frecuencia de auditorías
5	Cloud Security Audit for A Certification and Training Center	Tesis	No	Enfocado en seguridad de la nube
6	[LIBRO] IT Security Risk Control Management: An Audit Preparation Plan	Libro	No	Libro general de auditoría de TI, sin ahondar mucho en marcos de buenas prácticas
7	[PDF] Towards Continuous Information Security Audit.	Artículo científico	No	Se enfoca en auditoría automatizada de procesos de negocio
8	Model for efficient development of security audit criteria'	Artículo científico	Sí	-

9	Development of a Security Audit Framework for an Organization	Tesis	Sí	-
10	Enhanced Model for Efficient Development of Security-Audit Criteria	Artículo científico	No	Resultado repetido del #8
11	Factors associated with security/cybersecurity audit by internal audit function	Artículo científico	No	Se enfoca en factores que impactan la función de auditoría, entrenamiento, certificaciones, liderazgo
12	The impact of audit firms' characteristics on audit fees following information security breaches	Artículo científico	No	Se enfoca en tarifas de las firmas
13	[PDF] Implementing Finnish National Security Audit Criteria KATAKRI to Arctech Helsinki Shipyards Inc.	Tesis	No	Cubre una auditoría específica con un estándar seleccionado (KATAKRI), en lugar de comparar varios marcos
14	[PDF] Assessing Information Security Vulnerabilities and Threats to Implementing Security Mechanism and Security Policy Audit	Artículo científico	No	Se enfoca en requerimientos de la política de seguridad y el factor humano
15	A Conceptual Framework of Information Security Database Audit and Assessment	Artículo científico	No	Se enfoca en auditoría de bases de datos
16	Integrating knowledge management into information security: From audit to practice	Artículo científico	No	Se enfoca en administración del conocimiento
17	[LIBRO] Software Quality Assurance: Integrating Testing, Security, and Audit	Libro	No	Se enfoca en aseguramiento de la calidad

18	[PDF] A conceptual framework of information security database audit and assessment in university based organization	Tesis	No	Se enfoca en auditoría de bases de datos
19	Development of Metamodel on Information Security Risk Audit and Assessment for IT Assets in Commercial Bank	Artículo científico	No	Se enfoca en metamodelo sin entrar a considerar la metodología de auditoría o marcos de buenas prácticas
20	[PDF] Cloud cyber-security: Empowering the audit trail	Artículo científico	No	Se enfoca en seguridad de la nube y análisis forense

Fuente: Elaboración propia (2021)

Apéndice 2: Detalles de la revisión literaria en español

Número	Fuente	Tipo de documento	Relevante	Justificación de exclusión
1	Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio	Artículo científico	Sí	-
2	Auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, basada en la Norma ISO/IEC 27001 y la metodología …	Tesis	Sí	-
3	Auditoría de Seguridad a Aplicaciones iOS y Android	Tesis	No	Se centra en la auditoría de aplicaciones móviles
4	Auditoría de seguridad informática basada en el estándar ISO 27001: 2013 para detectar y explotar vulnerabilidades en una red administrativa simulada para una …	Tesis	No	El enfoque de la tesis es más técnico basándose en la ejecución de ataques y usando ISO 27001 como soporte teórico únicamente.
5	Auditoría de seguridad informática a la empresa Cuesgar SA, ubicada en el cantón El Guabo, parroquia Tendales.	Artículo científico	No	Se enfoca en la auditoría de una organización específica sin profundizar en los marcos utilizados
6	Auditoría de seguridad informática a la dirección distrital 02D03 Chimbo-San Miguel-Educación, aplicando COBIT 5.	Artículo científico	No	Se enfoca en la auditoría de una organización específica sin profundizar en los marcos utilizados
7	[PDF] Software para estandarizar el proceso de auditoría de seguridad informática Software to standardize the computer …	Artículo científico	No	Abarca la implementación de un sistema informático de soporte a la auditoría

8	Auditoría de seguridad informática al data center del Hospital La Caleta-Chimbote	Artículo científico	No	Se enfoca en la auditoría de una organización específica sin profundizar en los marcos utilizados
9	Metodología para la auditoría de seguridad en implementaciones de tecnología NFC con dispositivos pasivos	Artículo científico	No	Se enfoca en dispositivos con NFC
10	Marco de referencia para el desarrollo de una auditoría de seguridad informática en aplicaciones Android.	Artículo científico	No	Se centra en la auditoría de aplicaciones móviles
11	Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del …	Artículo científico	Si	-
12	Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja	Artículo científico	Si	-
13	Auditoría de seguridad en el proceso de desarrollo de software acorde a estándar ISO/IEC 15504 en una institución financiera.	Artículo científico	No	Se enfoca en auditar el proceso de desarrollo de *software*
14	Desarrollo de un mecanismo ágil de auditoría a la seguridad informática de la red inalámbrica 802.11 con arquitectura AAA; caso …	Artículo científico	No	Se enfoca en auditoría de redes WLAN

15	Implantación de un proceso de auditoría de seguridad de información bajo la norma ISO/IEC 27002 en una entidad financiera de Puno–2016	Tesis	Si	-
16	Implementación del módulo de auditoría informática para el sistema integrado de actividad docente (SIAD) de la Carrera de Software (CSOFT) de la Universidad …	Artículo científico	No	Abarca la implementación de un sistema informático de soporte a la auditoría
17	[PDF] Auditoría de la seguridad de información en una empresa privada costarricense	Tesis	Si	-
18	[PDF] Esquema Nacional de Seguridad y auditoría	Artículo científico	No	Se trata de un esquema basado en la normativa española y no está basado en marcos de buenas prácticas reconocidos
19	Auditoría Técnica de Seguridad de aplicaciones web	Artículo científico	No	Se enfoca solo en aplicaciones web
20	Auditoría técnica de seguridad de un servicio de Voz sobre IP	Artículo científico	No	Se enfoca solo en voz IP
21	Auditoría a la seguridad informática de los servicios de tecnologías de la información en la ESE Hospital San Francisco de Gachetá.	Monografía	Sí	-

Fuente: Elaboración propia (2021)

Apéndice 3: Procesos de Gobierno y Gestión de COBIT 2019

Por el tamaño de este apéndice se incluye un extracto de la tabla. Sin embargo, la totalidad del apéndice puede descargarse del siguiente enlace: https://bit.ly/3pHcoa1

Procesos de Gobierno y Gestión	Comentario
EDM01 Asegurar el establecimiento y el mantenimiento del marco de gobierno	
EDM02 Asegurar la obtención de beneficios	
EDM03 Asegurar la optimización del riesgo	
EDM04 Asegurar la optimización de los recursos	
EDM05 Asegurar el compromiso de las partes interesadas	

Fuente: Elaboración propia basada en (ISACA, 2018)

Apéndice 4: Mapeo de prácticas de COBIT 2019 y COBIT 5

Por el tamaño de este apéndice se incluye un extracto de la tabla. Sin embargo, la totalidad del apéndice puede descargarse del siguiente enlace: https://bit.ly/3nS6SBJ

Dominio	Objetivos de Gobierno y Gestión	Práctica de Gobierno y Gestión	Práctica de COBIT 5	Comentarios
APO	APO01	APO01.01 Diseñar el sistema de gestión para la I&T de la empresa.	Práctica nueva	
APO	APO01	APO01.02 Gestionar la comunicación de objetivos, dirección y decisiones tomadas.	APO01.04	
APO	APO01	APO01.03 Gestionar la implementación de procesos (para respaldar la consecución de objetivos de gobierno y gestión).	Práctica nueva	
APO	APO01	APO01.04 Definir e implementar las estructuras organizativas.	APO01.01	
APO	APO01	APO01.05 Establecer roles y responsabilidades.	APO01.02	

Fuente: Elaboración propia basada en (ISACA, 2018)

Apéndice 5: Resumen del mapeo de controles de CIS con el NIST CSF

Por el tamaño de este apéndice se incluye un extracto de la tabla. Sin embargo, la totalidad del apéndice puede descargarse del siguiente enlace: https://bit.ly/30XPd2w

CIS Control	CIS Sub-Control	Función de Seguridad	Título	Relación	Subcategoría
1	1		**Inventario y control de activos de hardware**		
1	1.1	**Identificar**	Establecer y mantener un inventario de activos detallado	Equivalente	ID.AM-1
1	1.1	**Identificar**	Establecer y mantener un inventario de activos detallado	Superconjunto	PR.DS-3
1	1.2	**Responder**	Abordar activos no autorizados		DE.5, DE.7
1	1.3	**Detectar**	Utilice una herramienta de descubrimiento activa	Subconjunto	DE.CM-7
1	1.4	**Identificar**	Utilice el registro del protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos empresariales	Subconjunto	DE.CM-7
1	1.5	**Detectar**	Utilice una herramienta de detección de activos pasiva	Subconjunto	DE.CM-7

Fuente: Elaboración propia basada en (Center for Internet Security, 2021)

Apéndice 6: Versión extendida del NIST CSF Core incluyendo COBIT 2019 y controles CIS v8

Por el tamaño de este apéndice se incluye un extracto de la tabla. Sin embargo, la totalidad del apéndice puede descargarse del siguiente enlace: https://bit.ly/3FPlk3G

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los propósitos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	**ID.AM-1:** Se inventarían los dispositivos y sistemas físicos dentro de la organización.	· **CIS CSC** 1 · **CIS CSC v8 1.1** · **COBIT 5** BAI09.01, BAI09.02 · **COBIT 2019** 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-8, PM-5

Fuente: Elaboración propia basada en (Center for Internet Security, 2021), (ISACA, 2018) y (Instituto Nacional de Estándares y Tecnología, 2018)

Apéndice 7: Papel de trabajo propuesto para la metodología

Por el tamaño de este apéndice, se incluye un extracto de la tabla. Sin embargo, la totalidad del apéndice puede descargarse del siguiente enlace: https://bit.ly/3cPlag5

Control ID	Función	Categoría del Control NIST	Código Categoría del Control NIST	Nombre del Control	CIS CSC v8	COBIT 2019	ISO/IEC 27001:2013	NIST CSF	Definición de política	Control implementado	Control automatizado o técnicamente reforzado	Control informado a la empresa	Comentarios
1	Identificar ID	Gestión de	ID.AM	Se inventarían los dispositivos y sistemas físicos dentro de la organización.	1.1	BAI09.01, BAI09.02	A.8.1.1, A.8.1.2	ID.AM-1					
2	Identificar ID	Gestión de	ID.AM	Se inventarían las plataformas y aplicaciones de software dentro de la organización.	16.4, 2.1, 2.2	BAI09.01, BAI09.02, BAI09.05	A.8.1.1, A.8.1.2, A.12.5.1	ID.AM-2					

Fuente: Elaboración propia basada en (Center for Internet Security, 2021), (ISACA, 2018) y (Instituto Nacional de Estándares y Tecnología, 2018)