FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ANÁLISIS DE MADUREZ DEL PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

SUSTENTADO POR:

NEHEMÍAS ASAEL LÓPEZ VARGAS

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

28 DE JULIO, 2025

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

ANÁLISIS DE MADUREZ DEL PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

CARLOS ROBERTO AMADOR
FREDIS DUBAL MEDINA ESCOTO
JESÚS RICARDO RODRÍGUEZ RIVERA

FACULTAD DE POSTGRADO

ANÁLISIS DE MADUREZ DEL PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

Nehemías Asael López Vargas

Resumen

El presente proyecto nace para dar respuesta a la necesidad en la Cooperativa de Ahorro y Crédito Educadores de Honduras (COACEHL) de una mejora en su proceso actual para la gestión de vulnerabilidades. La tecnificación de los procesos organizacionales derivada de la Cuarta Revolución Industrial ha traído el aumento de ciber delitos, pero también a su vez, un crecimiento en cuanto a herramientas de seguridad, estamentos legales y estándares internacionales para administrar las vulnerabilidades en los activos tecnológicos. Tal es el caso de la ISO 27002 o el Marco de Seguridad Cibernética del NIST CSF en su versión 2.0. La investigación cuenta con un enfoque cualitativo, no probabilístico y un alcance descriptivo. La población y muestra han sido seleccionadas por conveniencia y están enmarcadas en el personal se seguridad de la información y en el proceso actual para la gestión de vulnerabilidades de la Cooperativa. Por otro lado, herramientas como el FODA, la entrevista semiestructurada, listas de verificación, la matriz de perfilamiento NIST CSF 2.0, notas de campo entre otras, permitieron identificar necesidades que sustentan la propuesta de este proceso. Tras analizar los resultados obtenidos, se pudo constatar puntos de mejora en el proceso actual como: La falta de un flujo de trabajo consolidado, ausencia de indicadores clave y la necesidad de un mayor aprovechamiento de las soluciones disponibles. Esto ha permitido enlazar las falencias presentes con la respuesta provista mediante la adaptación de algunas funciones del estándar NIST CSF 2.0: Identificar, detectar, responder y añadimos la etapa de evaluar y aprender.

Palabras claves: Seguridad de la Información, Ciberseguridad, Ciber resiliencia, Gestión de vulnerabilidades, NIST.

GRADUATE SCHOOL

MATURITY ANALYSIS OF THE VULNERABILITY MANAGEMENT PROCESS BASED ON THE NIST CSF 2.0 CYBERSECURITY FRAMEWORK FOR THE EDUCADORES DE HONDURAS LIMITADA SAVINGS AND CREDIT COOPERATIVE (COACEHL)

Nehemías Asael López Vargas

Abstract

This project was created to address the need at the Educators of Honduras Savings and Credit Cooperative (COACEHL) to improve its current vulnerability management process. The technological advancement of organizational processes resulting from the Fourth Industrial Revolution has led to an increase in cybercrime, but also to a growth in security tools, legal frameworks, and international standards for managing vulnerabilities in technological assets. This is the case with ISO 27002 and the NIST CSF Cybersecurity Framework (version 2.0). The research uses a qualitative, non-probabilistic approach and a descriptive scope. The population and sample were selected for convenience and are based on the Cooperative's information security staff and current vulnerability management process. Furthermore, tools such as SWOT, semi-structured interviews, checklists, the NIST CSF 2.0 profiling matrix, field notes, and others helped identify needs that support this process proposal. After analyzing the results, we identified areas for improvement in the current process, such as the lack of a consolidated workflow, the absence of key indicators, and the need to better leverage available solutions. This has allowed us to connect the current shortcomings with the response provided by adapting some functions of the NIST CSF 2.0 standard: Identify, Detect, Respond, and we added the Evaluate and Learn stage.

Keywords: Information Security, Cybersecurity, Cyber Resilience, Vulnerability Management, NIST.

DEDICATORIA

A Dios, por permitirme culminar con éxito esta etapa formativa, por proveer lo necesario a lo largo de este camino y darnos la fortaleza y sabiduría para completar este trabajo.

A mi esposa e hijos, ya que son el motor que me mueve cada día salir adelante y con quienes puedo disfrutar, el alcanzar logros como este. Espero sirva de motivación para que mis hijos vean que con esfuerzo y dedicación nada es imposible y que, si se lo proponen, pueden llegar a esto y más.

A mis padres, por su apoyo y amor incondicional aun y a pesar de las fallas y fracasos, por ayudarnos a levantarnos y volverlo a intentar. Agradecerles el sacrifico hecho para poder educarnos y buscar darnos un futuro mejor apropiándonos siempre de la bendición de Dios para nosotros.

AGRADECIMIENTO

. **A Dios**, por permitirme culminar con éxito esta etapa formativa, por proveer lo necesario a lo largo de este camino y darnos la fortaleza y sabiduría para completar este trabajo.

Al Msc. Jorge Raúl Maradiaga Chirinos, mi asesor metodológico, por su apoyo, acompañamiento, paciencia, orientación, instrucción e invaluable guía a lo largo de la realización de este proyecto, por siempre desafiarme y ayudarme a ir más allá en aras de entregar un producto de calidad.

A cada miembro del equipo docente que UNITEC selecciono para impartir los diferentes espacios pedagógicos, pues cada uno con su experiencia y conocimiento contribuyó a una formación sumamente enriquecedora.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

El presente trabajo detalla el análisis y la propuesta de un proceso para gestionar las vulnerabilidades de los sistemas de información en la Cooperativa de Ahorro y Crédito Educadores de Honduras Limitada (COACEHL), lo que resulta necesario por diferentes aspectos de contexto organizacional, legales y regulatorios. A priori, una vulnerabilidad es una debilidad, una brecha (identificada o no), cuya explotación constituye un riesgo de pérdida o exposición de información por parte de la entidad. La característica principal de las vulnerabilidades es que eventualmente, están presentes en todos los activos tecnológicos. Ya sea porque no se conocen (vulnerabilidades de día cero), la inminente obsolescencia (la versión del activo "envejece" y con el tiempo queda sin soporte), malas configuraciones (Por ejemplo: Usuarios y contraseñas débiles o por defecto), suites de cifrados quebrados, etc., las vulnerabilidades están allí. A pesar de ello, no todas las organizaciones disponen de procesos claros y consistentes para afrontar esta situación.

La investigación de esta problemática se realizó en primer lugar, por el interés en conocer cómo ha madurado el concepto de ciberseguridad a nivel internacional y puntualmente, en Honduras. Esto permitió identificar que, en el país, existen todavía enormes desafíos en la materia. Uno de los sectores que muestra mayor avance son las entidades financieras, organizadas bajo la Comisión Nacional de Bancos y Seguros (CNBS) y el Consejo Nacional Superior de Cooperativas (CONSUCOOP), dentro de las cuales se encuentra COACEHL. De allí, que con esta propuesta se pretende ayudar a la Cooperativa a alcanzar sus objetivos estratégicos, a responder a las amenazas del entorno y a su vez, a cumplir con los requerimientos legales y normativos vigentes, dando razón de ser a la iniciativa descrita como producto final.

En segunda instancia, es necesario analizar los aspectos que envuelven esta problemática a

nivel de macroentorno y microentorno. Uno de ellos, es la propia introducción de tecnología en los procesos corporativos motivada en buena parte, por los cambios sociales y económicos experimentados en las últimas décadas. La Tercera y Cuarta Revolución Industrial, han impulsado la integración del componente informático como parte vital del tejido de las organizaciones públicas y privadas. Hoy, no concebimos entidades que no cuenten con redes de dispositivos conectados para su operación, procesos automatizados y digitalizados. Esta realidad, ha dado lugar a la aparición del ciberespacio (que es donde convergen personas, tecnología y datos) y, en consecuencia, a los ciberdelitos. Esta última actividad, ha experimentado un crecimiento exponencial en los últimos años, lo que ha profundizado las preocupaciones y esfuerzos de los gobiernos y diferentes organizaciones. Los mismos, se han visto traducidos en leyes, marcos de referencia, normativas e incluso entes creados específicamente para promover y fortalecer la ciberseguridad a nivel global

En ese sentido, es importante también establecer la relación y diferencia entre conceptos como: Seguridad de la información y ciberseguridad. Esto nos permitirá conocer cómo han evolucionado los mismos, buscando integrarse y robustecer los niveles de seguridad en las entidades, lo que ha abierto un enorme campo de estudio que ha derivado en un compendio de estándares, marcos, metodologías (como la familia de normas ISO, COBIT 2019 o NIST), instrumentos y herramientas temáticas que procuran dar respuesta a los retos y desafíos planteados por un contexto cada vez más sofisticado y complejo en cuanto a gestión de vulnerabilidades se refiere. En este punto cobra relevancia también explorar la situación local, conociendo los esfuerzos orientados a la ciberseguridad en Honduras incluyendo esto, los diferentes aspectos gubernamentales, legales y normativos existentes a la fecha. En este apartado también se requiere identificar la relevancia y el impacto que tiene esta propuesta para COACEHL considerando todos

los elementos descritos previamente.

En cuanto a la dimensión metodológica, al ser un trabajo de investigación con un diseño cualitativo con enfoque descriptivo, se utilizaron técnicas, instrumentos y procedimientos propios de la naturaleza de dicho enfoque tales como: Entrevistas, notas de campo, revisión documental, muestreo no probabilístico, cuya muestra fue seleccionada por conveniencia en base a criterios de inclusión y exclusión establecidos por el investigador.

Para el análisis de los resultados, se utilizaron figuras, cuadros comparativos e instrumentos propios de los estándares internacionales tales como la Matriz de Perfilamiento Organizativo del NIST CSF en su versión 2.0. Esto permitió una mayor comprensión de la situación actual de la Cooperativa, sus procesos y como la propuesta resultante de esta investigación puede ser de beneficio para COACEHL.

Finalmente, el documento describe la propuesta de un proceso para gestionar vulnerabilidades adaptando algunas de las funciones del marco de seguridad cibernética del NIST CSF 2.0, respondiendo de forma clara y concreta a las necesidades identificadas dentro de COACEHL.

1.2 ANTECEDENTES DEL PROBLEMA

Las entidades introducen tecnología para dinamizar sus procesos buscando cumplir con diferentes objetivos estratégicos. Sin embargo, en algunos casos el enfoque es meramente operativo lo que ha dejado de lado la dimensión de seguridad. En Honduras, muchas organizaciones implementan soluciones procurando cerrar sus brechas de seguridad, pero carecen de procesos concretos para gestionar las debilidades o deficiencias presentes en sus activos informáticos, lo que impide alinear la gestión de vulnerabilidades (asociada a la constante evolución y complejidad de los ciberdelitos), con la actividad cotidiana de las entidades. Esto,

eventualmente impacta en las instituciones cuando se enfrentan a incidentes de ataques o explotaciones de dichas vulnerabilidades.

De acuerdo con datos del Índice Nacional de Seguridad Cibernética (NCSI por sus siglas en inglés), Honduras con su indicador de ciberseguridad y de nivel de desarrollo digital en 22.08%, se coloca como uno de los países con menos avances en la materia a nivel de Centroamérica. Esto es aún más preocupante cuando las instituciones estatales son las que evidencian mayor propensión a ser víctimas de ataques informáticos como señala David Zapata en su artículo: "Instituciones del Estado, las más vulnerables a los ciberataques", (2024, agosto 10).

En conjunto, todos estos elementos sin duda están llevando a las organizaciones a tomar mayor consciencia sobre la necesidad de implementar herramientas y procesos para una mejor gestión de vulnerabilidades, tal como lo demuestra el periodista Luis Rodríguez en su artículo: "¿Cuánto aumentó la inversión en ciberseguridad bancaria en Honduras?", (2024, julio 11), donde se detalla un incremento del 2.2% a un 3.7% en gasto tecnológico por parte de las entidades financieras al cierre del año 2023.

Adicionalmente, en el país han ido surgiendo algunas leyes y normativas en un intento por regular diferentes aspectos de ciberseguridad, implícita en ellas, la gestión y explotación de vulnerabilidades. Ejemplos claros son: El Decreto Ejecutivo Número PCM-086-2020, dirigido a reglamentar el Gobierno Electrónico, o el Artículo 398 del Código Penal que tipifican delitos informáticos tales como el acceso sin autorización a los sistemas.

Por otro lado, existen algunas iniciativas, encaminadas a delinear de forma muy general como gestionar el tema de las vulnerabilidades presentes en los sistemas de información. Quizás, la más explícita es la Circular 025 (2022) de la Comisión Nacional de Bancos y Seguros, que, en el Capítulo V, en su Artículo número 19, detalla una propuesta para la Gestión de Ciberseguridad

fuertemente asociada con el Marco NIST CSF 2.0 (con excepción de la función Gobernar que no se encuentra incluida en este artículo de la normativa, sino que se expone en el Capítulo III de esta).

> Como parte del Marco de Gestión de la Seguridad de la Información y Ciberseguridad, las Instituciones Supervisadas deben gestionar la ciberseguridad basado en las mejores prácticas y estándares internacionales que les permita:
> a. Identificar: Tener plenamente identificados los sistemas de información, los activos y los datos expuestos en el ciberespacio, así como su contexto de negocio y los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan su entorno;
>
> b. Proteger: Desarrollar e implementar los controles necesarios para limitar o contener el impacto de eventos potenciales de ciberseguridad;
>
> c. Detectar: Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de eventos de ciberseguridad a través del monitoreo continuo;
>
> d. Responder: Contar con procesos y procedimientos para garantizar respuestas oportunas, durante y después de un incidente de ciberseguridad; y,
>
> e. Recuperar y Aprender: Desarrollar e implementar actividades para la gestión de ciber resiliencia y el retorno a la operación normal después de un incidente. Asimismo, ajustar su Marco de Gobierno de Riesgo en lo relacionado al Marco de Gestión de TI y el Marco de Gestión de la Seguridad de la Información, como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes. (Comisión Nacional de Bancos y Seguros (CNBS), 2022, p. 12)

En esa misma sintonía, el Consejo Nacional Supervisor de Cooperativas en Honduras (CONSUCOOP), publicó en el Diario Oficial la Gaceta, el acuerdo Número 002-15-12-2022; Concerniente en Aprobar la Norma para la Administración de Tecnologías de Información y Comunicaciones (TIC), para las Cooperativas de Ahorro y Crédito (CAC´S). En su Anexo 1, titulado: “Controles a implementar respecto a la Seguridad de la Información”, detalla una serie de medidas mínimas donde se destaca el inciso 6 que explícitamente habla acerca de que se debe: “Controlar las vulnerabilidades técnicas existentes en los sistemas de información” (2023, febrero 1). Esta tendencia sin duda seguirá en aumento ya que las exigencias por parte de organismos regulatorios nacionales e internacionales, moverán a estas organizaciones a la mejora continua en sus entandares y controles de ciberseguridad. Por tal motivo, COACEHL incorpora esto como parte de los objetivos estratégicos de su Plan Operativo Anual, focalizados bajo la dirección del

área de seguridad de la información.

Al considerar todo este contexto, resulta evidente entonces que un proceso para la gestión de vulnerabilidades basado en un marco probado como NIST CSF 2.0, puede contribuir significativamente a suplir ese vacío presente en las organizaciones tanto públicas como privadas. Adicionalmente, el estándar es sumamente adaptable por lo que puede integrarse con otras normas o metodologías como la familia de ISO 27000, COBIT 2019 entre otras, lo que permitiría a COACEHL potenciarse aún más en lo referente a los aspectos de ciberseguridad y gobierno de TI.

1.3 DEFINICIÓN DEL PROBLEMA

Si bien la Cooperativa cuenta con un área de seguridad de la información, con políticas de ciberseguridad y un proceso de gestión de vulnerabilidades, a razón del marcado incremento en las amenazas hacia el sistema financiero hondureño, los requerimientos legales y regulatorios de la CNBS y CONSUCOOP y, ante la necesidad de consolidar los datos provenientes de múltiples fuentes de información, resulta necesaria una alternativa que permita a COACEHL responder de forma estratégica, integral y sistemática a estos desafíos, fortaleciendo permitiéndole asumir una postura más proactiva de cara a posibles incidentes de seguridad.

Adicionalmente, esto viene a apoyar el cumplimiento del Plan Operativo Anual de COACEHL que desde el 2023, ya contemplaba para el área de seguridad de la información el tratar de fortalecer los controles ya existentes (COACEHL, 2023, p. 75). En ese sentido, esta entrega viene a aportar una valiosa contribución en ese particular. A razón de esto, se plantean las siguientes preguntas y objetivos para la investigación.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Qué componentes del Marco de Ciberseguridad NIST CSF 2.0 son útiles para generar un

proceso para la gestión de vulnerabilidades en los sistemas de información de COACEHL?

1.4.2 PREGUNTAS ESPECÍFICAS

1. ¿En COACEHL cómo se gestionan actualmente las vulnerabilidades presentes en sus activos tecnológicos?
2. ¿Qué herramientas utilizan en la Cooperativa para identificar y atender las vulnerabilidades?
3. ¿Dentro del equipo de Seguridad de la Información de COACEHL qué conocimiento y uso hacen de estándares y mejores prácticas para la gestión de vulnerabilidades?
4. ¿Qué beneficios puede recibir COACEHL en el robustecimiento de su postura de ciberseguridad, derivados de la mejora en su proceso de gestión de vulnerabilidades?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Diseñar un proceso adaptando componentes del Marco de Ciberseguridad NIST CSF 2.0, para fortalecer la gestión de las vulnerabilidades presentes en los sistemas de información de COACEHL.

1.5.2 OBJETIVOS ESPECÍFICOS

1. Analizar la gestión de vulnerabilidades vigente para diagnosticar la situación actual del proceso.
2. Determinar que herramientas se usan en COACEHL para la detección y atención de vulnerabilidades de sus activos tecnológicos a fin de modelar como optimizar el aprovechamiento de estos recursos.
3. Identificar el grado de conocimiento y uso de estándares de Seguridad de la Información y Ciberseguridad en COACEHL para validar la utilización de mejores

prácticas en la organización.

4. Establecer cómo la mejora del proceso de gestión de vulnerabilidades basada en el Marco de Ciberseguridad del NIST CSF 2.0 puede ser de beneficio en COACEHL para robustecer su postura de ciberseguridad.

1.6 JUSTIFICACIÓN

La investigación de esta problemática se realizó fundamentalmente como una iniciativa para apoyar a COACEHL con el cumplimiento de los objetivos trazados en su Plan Operativo Anual (POA), dentro de los cuales existen aspectos específicos para el área de seguridad de la información orientados en robustecer sus procesos existentes e indicadores clave de desempeño. Adicionalmente, existe un componente de cumplimiento regulatorio ya que las instituciones financieras se rigen bajo los lineamientos establecidos por organismos como la Comisión Nacional de Bancos y Seguros (CNBS), el Consejo Nacional Supervisor de Cooperativas de Honduras (CONSUCOOP), el Congreso Nacional, entre otros; mismos que exigen la implementación de mejores prácticas para fortalecer los niveles de seguridad en sus ecosistemas informáticos.

Por otra parte, desde una óptica académica, la investigación es importante porque permitió conectar aspectos quizás más técnicos, con marcos teóricos que sustentan estas actividades. Esto contribuyó a establecer relaciones entre una remediación de vulnerabilidades con marcos abordados a lo largo de este programa de Maestría como el NIST CSF 2.0 o COBIT 2019. Asimismo, la investigación permitió comprender los aspectos legales y normativos que impulsan a las organizaciones a buscar implementar estas mejores prácticas en sus procesos.

En el ámbito profesional, el interés se dirigió en aplicar la experiencia personal en el tema y estudiar como variables los elementos que integran una adecuada gestión de vulnerabilidades para poder construir un proceso de remediación de estas, que sea adaptable, repetible y medible, para

que finalmente puede convertirse en una propuesta de valor para COACEHL o cualquier organización interesada en establecer un ciclo similar.

CAPÍTULO II. MARCO TEÓRICO

2.1 MACROENTORNO

2.1.1 UNA APROXIMACIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Ciertamente es imposible garantizar que existe completa seguridad, más aún en los entornos tecnológicos. Pero, es entonces que se necesita identificar formas de mantener estatus de seguridad idóneos en las organizaciones. Costas Santos (2015) nos dice:

> Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad. La seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos (Costas Santos, 2015, p. 27).

Como preámbulo al tema de la ciberseguridad y puntualmente, la gestión de vulnerabilidades, es necesario hablar acerca de un concepto que engloba dichos elementos y este es, la seguridad de la información. Como señala Cano (2017) es necesario: “Entender que la seguridad de la información no es un problema de tecnología, sino de prácticas y de personas, es una lección que muchas organizaciones han tenido que aprender como fruto de las adversidades de la inseguridad” (Cano, 2017, p. 126).

Inicialmente, es requerido hacer una breve distinción sobre qué es Seguridad de la Información. ISO 27001:2022 define esta como la: “Preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad” (Certiprof, 2022, p. 74). Para poder garantizar el cumplimiento de estas propiedades, dentro de su alcance, la Seguridad de la Información aborda dos grandes dimensiones: La seguridad informática y la ciberseguridad.

Figura 1 *Alcance de la Seguridad de la Información*

Fuente: Figura íntegra y completa obtenida del libro: Ciberseguridad: del ciber-crimen a los ataques ciber-físicos (Fuentes Diaz y Macas Carrasco, 2023, p. 26).

Como lo ilustra el diagrama, bajo el Sistema de Gestión de Seguridad de la Información, pueden organizarse y alinearse todos los demás estándares y esfuerzos que se hagan en búsqueda de fortalecer los niveles de protección de la entidad. Fuertes Díaz y Macas Carrasco explican con mucha claridad esta relación:

> La seguridad de la información utiliza diversos estándares internacionales que establecen las mejores prácticas para identificar los riesgos y garantizar la privacidad de los usuarios a través de la inclusión de controles, barreras o herramientas apropiadas para reducir la inseguridad. Además, involucra la búsqueda de mecanismos de protección en donde la información sea el activo primario. Estos mecanismos podrían ser la instauración de políticas, controles de seguridad, dispositivos electrónicos especializados y procedimientos para detectar amenazas y vulnerabilidades que podrán ocasionar graves incidentes de seguridad con un impacto devastador en los ingresos, productividad e imagen de las empresas; he allí su importancia (Fuentes Diaz y Macas Carrasco, 2023, p. 26).

De la ciberseguridad se hará una exposición a lo largo de este documento. Pero aquí es importante dejar definida puntualmente la seguridad informática. Costas Santos (2021) nos indica:

> La seguridad informática comprende el hardware y el sistema operativo, las comunicaciones (por ejemplo, protocolos y medios de transmisión seguros), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad de usuarios, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (Costas Santos,

2021, p. 24).

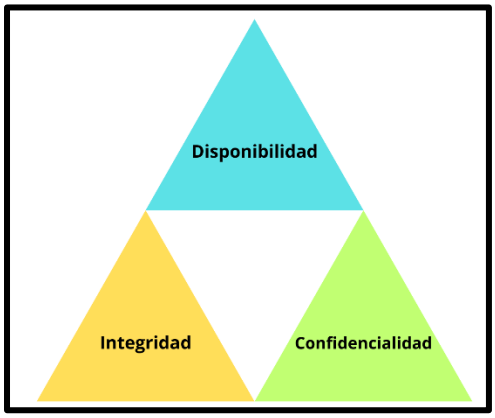
La seguridad informática, la ciberseguridad y otro sinnúmero de estándares de referencia pueden coexistir enmarcados bajo la seguridad de la información e integrados en el Sistema de Gestión de Seguridad de la Información vigente en la organización.

2.1.2 INTRODUCCIÓN A LA CIBERSEGURIDAD

En un contexto cada vez más inmerso en la tecnología y en la búsqueda constante de mayor competitividad, es notorio que los estándares de seguridad han tenido que evolucionar y ampliar sus horizontes. Hoy en día es necesario hablar no solo de seguridad de la información, sino que ir más allá y abordar el tema de ciberseguridad, para abordar de una manera más holística todo el conjunto de brechas existente en los activos tecnológicos. En tal sentido, formalmente la ciberseguridad se define como la: "Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio". (NISTIR 7621, 2016, p. 2). En esa misma dirección, Urcuqui López y Navarro Cadavid (2023) establecen que: “Este concepto se refiere al conjunto de medidas que se implementa para proteger a las personas y a las organizaciones de posibles amenazas a la confidencialidad, la integridad y la disponibilidad de los datos en el ciberespacio” (p. 47). Esta última definición resulta llamativa porque incorpora el componente de todos los esfuerzos que las organizaciones emprenden en busca de fortalecerse frente a las amenazas internas y externas.

A razón de lo anterior, es factible afirmar que, desde su concepción la ciberseguridad busca cumplir objetivos comunes con el estándar ISO 27001:2022 ya que comparten las dimensiones de la seguridad de la información como se ejemplifica en la siguiente figura:

Figura 2 *Dimensiones de la Ciberseguridad.*



Nota: Elaboración propia.

Estas tres dimensiones son directamente afectadas al producirse una explotación de vulnerabilidades ya que la información puede perder su disponibilidad (al experimentar fallas o inestabilidad en los servicios), los datos pueden verse expuestos, faltando con ello a la confidencialidad e incluso, pueden ser adulterados corrompiendo así su integridad.

2.1.3 IMPORTANCIA DE LA CIBERSEGURIDAD

En primer lugar, la ciberseguridad es importante porque la tecnología es parte fundamental de la vida económica de las sociedades modernas. Resulta difícil encontrar alguna actividad que no utilice absolutamente ninguna herramienta que incorpore software o hardware. Entonces, ante la interrogante: ¿Por qué es importante la ciberseguridad?, podemos responder que la razón radica en la dependencia que se ha creado entre tecnología y operatividad. Y como explica Ramírez Pascual:

> Detrás de cualquier organización siempre hay un uso de sistemas digitales y redes con conectividad de alta velocidad que proporcionan un servicio al cliente, siempre buscando un objetivo de eficiencia y rentabilidad en las operaciones empresariales. Igual que las empresas y organizaciones protegen los recursos y los activos físicos, deben proteger también los recursos digitales y los activos frente a los accesos no auto- rizados. La ciberseguridad busca proteger a las organizaciones de los riesgos y amenazas a los que están expuestos los entornos (Ramírez Pascual, 2023, p. 66 – 67).

Esto cobra aún más fuerza cuando se trata de instituciones financieras ya que en ellas

descansa buena medida de los datos de la población de cada país. Como indican Davalos Guillen y Mujica Sánchez (2024, p. 6): “La salvaguarda de los datos personales ha cobrado una importancia crucial en la era digital, especialmente en el ámbito financiero, donde la confidencialidad de la información de los usuarios es esencial”. En esa misma dirección, Echeverria Pérez y Martínez Soria (2024, p. xi) señalan:

> En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una prioridad esencial para las organizaciones. La protección de los datos garantiza la confidencialidad, integridad y disponibilidad de la información, y también fortalece la confianza de los clientes, socios y partes interesadas (Echeverria Pérez y Martínez Soria, 2024, p. xi).

La ciberseguridad, en alguna medida, implica el compromiso de las entidades por salvaguardar no solamente los datos propios, sino que también, de aquellos que han puesto su confianza en la organización sea esta pública o privada.

Una segunda razón que sustenta la importancia de la ciberseguridad, radica en que esta ayuda a las entidades a desarrollar resiliencia digital, que no es otra cosa que la capacidad de adaptarse y responder a los retos que representa un contexto que evoluciona de forma constante y dinámica. Mata (2024, p. 12) propone algunas acciones para construir resiliencia digital en una organización (Como se mostrará más adelante, estas guardan una estrecha relación con el proceso descrito en el marco NIST CSF 2.0 para la gestión de vulnerabilidades).

Figura 3 *Acciones para construir resiliencia digital en una organización.*

Nota: Elaboración propia.

Como tercer punto, pero no menos relevante, es necesario mencionar el aumento de los ciber delitos a nivel global. El especialista en ciberseguridad de la firma Ernst & Young (EY), Jordi José, señala que:

> Según algunas estimaciones, el cibercrimen le costó al mundo alrededor de 7 billones de euros en 2022 (y se espera que llegue a los 10,5 billones de euros en 2025), cifra que incluye el coste directo de recuperarse de un ciberataque, como la eliminación del software malicioso o la restauración de los sistemas, y el lucro cesante o la pérdida de productividad. Representa aproximadamente el 1% del Producto Interior Bruto (PIB) global, muy por encima de la piratería y el tráfico de drogas y casi cuatro veces más que la cantidad que se destina a las donaciones para el desarrollo internacional. Su crecimiento parece imparable y tiene el potencial de convertirse en la tercera mayor economía a nivel mundial en el corto plazo (2023, abril 24).

Las ciber amenazas se vuelven cada vez más sofisticadas y nocivas. Guerra Soto (2023) señala algunos rasgos de aquellas más dañinas: “Las ciber amenazas más destructivas comparten fundamentalmente tres características: su velocidad de ejecución, su intensidad, y el factor sorpresa” (Guerra Soto, 2023, p. 41).

Dicho lo anterior, pueden comprenderse mejor los múltiples esfuerzos que se hacen en ciberseguridad, protección de los datos y en la gestión de vulnerabilidades ya que buscan garantizar la estabilidad y continuidad del negocio frente a la realidad de las amenazas circundantes.

2.1.4 PREÁMBULO A LA PROTECCIÓN DE DATOS

Hasta aquí, se ha hablado de la seguridad de la información, ciberseguridad y de algunos aspectos que sustentan la importancia de la gestión proactiva de vulnerabilidades. Pero en el fondo, es necesario también identificar qué es lo que se está tratando de proteger. En este caso, los datos personales.

En la actualidad, es notorio un aumento en el interés en la protección de los datos. Al respecto, Hernández López (2023) señala:

> Los tratamientos de los datos personales han experimentado un crecimiento espectacular en las últimas décadas. Las nuevas tecnologías facilitan la recogida y el intercambio de datos en una escala sin precedentes en la historia de la humanidad. Las empresas privadas necesitan tratar información personal de los ciudadanos a fin de poder prestarles servicios (por ejemplo, de electricidad, telefonía, agua, gas, etcétera). Por su parte, las administraciones públicas tratan, entre otros, datos referidos a la salud, educativos, fiscales, de servicios sociales o del propio empleo público, lo que nos da muestra de la trascendencia de su actividad, que ha de servir con objetividad los intereses generales. La cuestión clave es que todos estos tratamientos de datos personales realizados por entidades públicas o privadas sean respetuosos con la normativa de protección de datos (Hernández López, 2023, p. 264).

Existe entonces una codependencia entre las entidades prestadoras de algún servicio y los individuos que requieren de estos. En esa relación, se produce un intercambio de datos que conlleva responsabilidad de las partes. Y allí, es donde surge la necesidad de formar políticas que definan las fronteras de lo que es permitido y lo que no en cuanto al uso de datos se refiere.

Ahora bien, es importante detenernos en este apartado para considerar la razón por la que este tipo de dato es de especial interés para los ciber atacantes. Tejerina y Beltrán (2020), indican que se considera dato de carácter personal a: “Toda aquella información que permita dar con la identidad de una persona sin un esfuerzo desproporcionado” (Tejerina y Beltrán, 2020, p. 117).

Burzaco Samper (2020) establece la relación entre el individuo y este tipo de información:

> Toda información sobre una persona física identificada o identificable («el interesado»). Persona física identificable = toda persona cuya identidad pueda determinarse (directa o indirectamente) en particular mediante un identificador (p.ej. un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona) (Burzaco Samper,2020, p. 26).

En otras palabras, un dato personal es todo aquello que nos permite diferenciar a un individuo de entre el resto de la colectividad. Coronado García (2024) define la protección de datos personales de esta forma:

> La protección de datos personales se refiere a las medidas y principios que garantizan que la información sensible se gestione de acuerdo con las leyes y normativas vigentes. Este proceso protege los derechos de privacidad de las personas y establece controles para evitar el acceso no autorizado a datos personales (Coronado García, 2024, p. 61).

Ayjón (2020) expande y ejemplifica de forma particular este concepto incorporando algunos aspectos adicionales:

> Se trata de cualquier información, noticia o dato que permite singularizar a una persona frente al resto, es decir, que le identifica dentro de la colectividad. En el ejemplo que nos sirve de guía para la comprensión de estos conceptos, se trata de los datos personales del denunciante, del denunciado y de los testigos, es decir, toda aquella información que identifique a cada uno de ellos frente al resto de personas, como: nombre, apellidos, edad, sexo, fecha y lugar de nacimiento, domicilio, así como el documento nacional de identidad o pasaporte.
>
> Se trata de un concepto muy amplio, porque no solamente se incluyen los datos básicos que identifican al individuo, sino cualquier otra información sobre el mismo como: la imagen de la persona, el sonido, la dirección de correo electrónico, datos de IP (Internet pratocol), el número de teléfono, las enfermedades que ha padecido, la ideología u opinión política e, incluso, las huellas dactilares y el perfil genético (Ayjón, 2020, p. 94 – 95).

Es decir, este tipo de dato permite establecer un perfilamiento de las personas, basado en patrones de comportamiento o en la huella digital que estas van dejando con su actividad cotidiana, incluso desde los dispositivos que utiliza para conectarse a la red. Buena parte de los esfuerzos de los gobiernos, entidades públicas, privadas y otras organizaciones, va dirigido a fortalecer la seguridad que envuelve los datos personales pues son de los objetivos más codiciados por los ciberdelincuentes.

Otro elemento interesante de estas definiciones, es que la protección de datos no solamente apunta a un documento de identificación o un nombre. Se expande a diferentes formatos en los que se almacena la información e incluso, los medios empleados para su generación. Todo puede volverse un punto de partida para explorar y explotar vulnerabilidades, con la intención de conseguir estos datos.

Una característica adicional sobre estos datos, es que generalmente no son divulgados. Sobre ello, López-Tarruella Martínez (2021) indica:

> Se entiende por datos no divulgados aquellos que una entidad se reserva para su propio uso o el de sus usuarios. Se trata de datos privados en la medida en que son generados por la propia entidad (datos históricos sobre sus clientes); adquiridos por esta (conjuntos de imágenes que una empresa puede adquirir de un centro de salud para entrenar un algoritmo de reconocimiento de imágenes relacionadas con enfermedades cutáneas); o genera- dos por los usuarios de sus servicios (datos que generan los usuarios cuando utilizan el buscador de Google, los mensajes de voz de los usuarios de Alexa, Siri y Cortana) o sus productos (datos que un fabricante de wearables recopila del uso de sus dispositivos). Se trata de información que puede o no estar disponible en Internet y que, en vista de su carácter digital, es presumible que su titular proteja mediante medidas tecnológicas de protección. Esta protección garantiza que el uso que se puede hacer de ella venga determinado por su titular: para actividades de I+D interna o subcontratada; para cederla a terceros a cambio de una remuneración; o para ofrecer servicios basados en esos datos (p. ej., publicidad personalizada).
> Los datos que manejan estas empresas puede ser simples datos electrónicos, o datos que representan información en formato digital tales como tex- tos, imágenes, grabaciones sonoras o audiovisuales. (López-Tarruella Martínez, 2021, p. 67).

En síntesis, estos datos constituyen un insumo clave para la toma de decisiones y la vida operativa de las organizaciones, son sumamente dinámicos y pueden provenir de diversas fuentes. Requieren de un tratamiento especial dada la sensibilidad de su contenido. Hernández López (2023), presenta algunos principios relativos al tratamiento de datos personales que ayudan a entender mucho de lo que los marcos legales vigentes establecen.

Figura 4 *Principios relativos al tratamiento de datos personales*

Fuente: Elaboración propia a partir de Hernández López, 2023, p. 265 – 266.

Todo este preámbulo es importante porque permite una mayor comprensión de las razones que impulsan la creación de los diferentes marcos legales internacionales y nacionales. También ayuda a visualizar con mayor claridad el valor de una adecuada gestión de vulnerabilidades en los activos tecnológicos pues en el fondo, se trata de proteger la privacidad de las naciones, organizaciones y personas.

2.1.5 MARCO LEGAL DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES A NIVEL INTERNACIONAL

Al momento de la elaboración de esta investigación, no existe un marco global estandarizado sobre ciberseguridad por lo que, el contexto se encuentra caracterizado por la ambigüedad y dispersión. A pesar de ello, es un tema en constante evolución ya que la preocupación por parte de los gobiernos y organizaciones crece a medida que lo hacen los requerimientos normativos y las

ciber amenazas. A continuación, se resumen los estamentos legales vigentes más representativos en Asia, Europa y América.

2.1.5.1 ASIA

En 2017, China publico la: “Ley de Ciberseguridad (CSL)”, donde establece que el estado es responsable de "promover un ciberespacio pacífico, seguro, abierto y cooperativo, y establecer un sistema de gobernanza de Internet multilateral, democrático y transparente" (Markovski, Trepykhalin, 2022, p. 8). Dicha ley se encuentra estructurada así:

Tabla 1 *Cuadro resumen de la Ley de Ciberseguridad China*

Capitulo	Sección
Capítulo I: Disposiciones Generales.	Artículo 1 – 14.
Capítulo II: Apoyo y promoción de la ciberseguridad.	Artículo 15 – 20.
Capítulo III: Seguridad de operaciones de redes.	Artículo 21 – 39.
Capítulo IV: Seguridad de la información de redes	Artículo 40 – 50.
Capítulo V: Monitoreo, alerta temprana y respuesta ante emergencias	Artículo 51 – 58.
Capítulo VI: Responsabilidad jurídica	Artículo 59 – 75.
Capítulo VII: Disposiciones complementarias	Artículo 76 – 79.

Nota: Adaptado del Informe de enfoque por países: leyes e iniciativas de políticas relacionadas con Internet en China (Markovski, Trepykhalin, 2022, p. 11 – 24).

Existen otros esfuerzos aislados en Asia como le reciente Ley de Ciberdefensa Activa aprobada en Japón en el mes de febrero de 2025, o el conjunto de leyes de Corea del Sur que incluyen la Ley de Protección de Información Personal (PIPA), la Ley de Redes de TI o la misma Ley de Uso y Protección de la Información Crediticia. En definitiva, todas buscan fortalecer la postura de ciberseguridad de los estados asiáticos.

2.1.5.2 EUROPA

En Europa se cuenta con diferentes iniciativas que han tratado de establecer puntos de referencia no solo para los países miembros de la Unión Europea, sino que también para las demás naciones en el mundo. Este ejemplo resulta sumamente interesante, porque de alguna manera, ofrece indicios de que hay aspectos comunes, transversales a los estamentos legales de todos los países, por lo que quizás en algún momento, se logren acordar marcos globales para la ciberseguridad.

– **Legislaciones a nivel de la Unión Europea**: Del trabajo de Gómez Hervás (2021), se ha elaborado el siguiente cuadro con el resumen de directivas y reglamentos aprobados por la Unión Europea focalizados en la ciberseguridad y protección de los datos.

Tabla 2 *Cuadro de directivas y reglamentos de la Unión Europea enfocados en ciberseguridad y protección de datos*

Legislación	Enfoque de contenido
Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas.
Directiva 2011/93/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011.	Relativa a la lucha contra los abusos y la explotación sexual de los menores y la pornografía infantil.
Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.	Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016.	Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS (Seguridad de Redes e Información por sus siglas en inglés).
Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8 de junio de 2016.	Relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

Reglamento (UE) 2019/796 del Consejo de 17 de mayo de 2019.	Relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros.
Reglamento 2019/881 del Parlamento europeo y del Consejo.	Relativo a ENISA76 (Agencia europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento 526/2013 (Reglamento sobre la Ciberseguridad).
Nueva Estrategia de Ciberseguridad de la UE (Estrategia de la Unión Europea para la Década Digital de 16 de diciembre de 2020).	Con las principales líneas de acción para aumentar la resiliencia de las entidades críticas físicas y digitales.
Directiva actualizada para proteger las redes y sistemas de información (NIS2). Aprobada en 2022 y vigente desde el 2023.	Amplia y actualiza el contenido y enfoque de la NIS1, buscando fortalecer los requisitos de seguridad.

Nota: Elaboración propia a partir de Gómez Hervás (2021, p. 144 – 145).

Otra iniciativa importante es el Convenio de Budapest, publicado en 2001, cuyo enfoque es el ataque frontal a la ciberdelincuencia, bajo el cual diferentes países alrededor se comprometen a luchar en contra de este flagelo. Suarez Campos (2022) lo define así:

> Es un acuerdo internacional inherente al ámbito penal, que determina los procedimientos jurídicos para luchar contra el crimen organizado; específicamente, tienen como propósito combatir los delitos cometidos, bien sea hacia sistemas o medios informáticos o, a través del empleo de los mismos. Este convenio establece en su preámbulo, la necesidad primordial de aplicar una política penal común entre sus miembros, así como de mejorar la cooperación internacional entre ellos con el fin de proteger a la sociedad frente a la ciberdelincuencia. Este tratado es calificado como un acuerdo que califica los esfuerzos de la Comunidad Internacional para fortificar el Estado de Derecho en el ciberespacio (Suarez Campos, 2022, p. 141).

De acuerdo a la Organización Mundial de Propiedad Intelectual (OMPI), al 7 de octubre de 2024, los siguientes Estados se han adherido al Convenio:

> Albania, Alemania, Antigua y Barbuda, Arabia Saudita, Armenia, Australia, Austria, Azerbaiyán, Bahréin, Bielorrusia, Bélgica, Bosnia y Herzegovina, Brunéi Darussalam, Bulgaria, Canadá, Chile, China, Colombia, Costa Rica, Croacia, Cuba, Dinamarca, El Salvador, Emiratos Árabes Unidos, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Federación de Rusia, Filipinas, Finlandia, Francia, Georgia, Grecia, Guatemala, Honduras, Hungría, India, Indonesia, Irlanda, Islandia, Israel, Italia, Japón, Jordania, Kazajstán, Kirguistán, Letonia, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Malasia, Marruecos, México, Mónaco, Montenegro, Nicaragua, Noruega, Nueva Zelandia, Omán, Panamá, Paraguay, Perú, Polonia, Portugal, Qatar,

> Reino de los Países Bajos, Reino Unido, República Checa, República de Corea, República de Moldova, República Dominicana, República Popular Democrática de Corea, Rumania, Ruanda, Serbia, Singapur, Sudáfrica, Suecia, Suiza, Tayikistán, Trinidad y Tobago, Túnez, Turquía, Ucrania, Uruguay (entrada en vigor el 7 de enero de 2025), Uzbekistán y Vietnam (OMPI, 2024, p. 1).

Este último resulta llamativo ya que no se limita únicamente a países miembro de la Unión Europea, y como se observa en el listado, varios países de Latinoamérica forman parte de esta iniciativa, de una u otra manera.

Además de estas disposiciones generales a nivel de Europa, los países de forma independiente también han tenido a bien emprender sus propias iniciativas en estos temas. A continuación, algunos ejemplos de ello.

– **España**: Este país cuenta con abundante normativa dirigida a conformar su estamento jurídico sobre ciberseguridad y protección de datos. Tal es el caso del Reglamento General de Protección de Datos (RGPD) publicado en 2016, cuyo efecto ha trascendido el continente europeo como señala Gascón Marcén (2021):

> El RGPD ha tenido un fuerte impacto en el ámbito de la protección de datos tanto fuera como dentro de las fronteras de la UE. Pero también ha servido como inspiración para el resto de iniciativas regulatorias importantes de la Comisión Europea en el marco del Mercado Único Digital (Gascón Marcén, 2021, p. 231).

Además de este, España cuenta con múltiples instrumentos legales. Algunos de ellos han servido de referencia para otros países. A partir de Gómez Hervás (2021), se resumen en la siguiente tabla:

Tabla 3 *Cuadro de directivas y reglamentos en España enfocados en Ciberseguridad y Protección de datos*

Legislación	Enfoque de contenido
Ley Orgánica 10/1995, de 23 de noviembre.	Código Penal.
Ley 34/2002 de 11 de julio.	Servicios de la sociedad de la información. y de comercio electrónico.
Decreto Real 3/2010 de 8 de enero.	Esquema Nacional de Seguridad (ENS).

Ley 9/2014 de 9 de mayo.	Ley General de Telecomunicaciones.
Ley Orgánica 4/2015.	Protección de la Seguridad Ciudadana.
Decreto Real 381/2015 de 14 de mayo.	Medidas contra el tráfico no permitido o irregular con fines fraudulentos en las comunicaciones electrónicas.
Ley 36/2015 de 28 de septiembre.	Estrategia de Seguridad Nacional.
Reglamento Europeo 2016/679.	Relativo a protección de datos personales.
Directiva de la Unión Europea 2016/943.	Relativa a protección de conocimientos técnicos e información empresarial, y su correlativa española Ley 1/2019 de secretos empresariales.
Decreto Real 1008/2017 de 1 de diciembre.	Aprueba la Estrategia de Seguridad Nacional.
Ley Orgánica 3/2018.	Protección de Datos y garantía de los derechos digitales.
Orden PCI/487/2019, de 26 de abril.	Por la que se publica la Estrategia Nacional de Ciberseguridad 2019 aprobada por el Consejo de Seguridad Nacional y a punto de publicarse la siguiente.
Ley 6/2020, de 11 de noviembre.	Reguladora de determinados aspectos de los servicios electrónicos de confianza (que sustituye a la Ley 59/2003 de firma electrónica).
Ley 7/2020 de 13 de noviembre.	Para la transformación digital del sistema financiero.
Normativa de Infraestructuras Críticas.	Decreto Real 421/2004 de 12 de marzo por el que se regula el Centro Criptológico Nacional.
	Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de Seguridad de las Redes y Sistemas de Información en la Unión.
	Ley 8/2011 de 28 de abril por a que se establecen medias para la Protección de las Infraestructuras Críticas.
	Decreto Real 43/21 de 26 de enero por el que

	se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Nota: Elaboración propia a partir de Gómez Hervás (2021, p. 145 – 147).

Al considerar todo este compendio, es comprensible entonces que España sea un modelo a seguir principalmente para países de habla hispana ya que, al compartir el idioma, se simplifica la comprensión de la documentación existente.

2.1.5.3 ESTADOS UNIDOS

Siendo la cuna de muchas de las empresas líderes en tecnología y de los promotores de diferentes estándares internacionales, Estados Unidos posee un marco legal robusto y complejo orientado a la ciberseguridad. A partir de Aguilar Antonio (2024) se ha elaborado el siguiente cuadro que resume este compendio de leyes focalizadas en la Política Nacional de Ciberseguridad:

Tabla 4 *Tabla de Desarrollo de Política Nacional de Ciberseguridad en Estados Unidos*

Subindicador	Legislación
Unidad de Políticas de Seguridad Cibernética	• Oficina de Ciberespacio y Público Digital del Departamento de Estado de los Estados Unidos. • Agencia de Seguridad Cibernética y de Infraestructura (CSA) que forma parte de la estructura del Departamento de Seguridad Nacional de Estados Unidos.
Coordinación de políticas de ciberseguridad	• Oficina del Coordinador de Asuntos Cibernéticos. • Agencia de Seguridad Cibernética y de Infraestructura (CISA).
Estrategia de seguridad cibernética.	• Ley de mejora de la ciberseguridad (2014). • Ley Nacional de Protección de la Ciberseguridad de (2014). • Estrategia cibernética del Departamento de Defensa (2018). • Estrategia Cibernética Nacional (2018). • Estrategia de Ciberseguridad del Departamento de Seguridad Nacional de EE. UU. (2018). • Estrategia de política internacional sobre ciberespacio del Departamento de Estado (2020). • Estrategia Nacional para la Seguridad 5G de los Estados Unidos de América (2020).

	• Estrategia Nacional de Ciberseguridad (2023). • Estrategia Nacional de Educación y Fuerza Laboral Cibernética (2023). • Plan Estratégico de Ciberseguridad de CISA 2024-2026 (2023).
Plan para implementar la estrategia de ciberseguridad	• Plan de Acción Nacional de Ciberseguridad (2016). • Agencia de Ciberseguridad y Seguridad de Infraestructura: Objetivo estratégico (2019). • Plan de Implementación de la Estrategia Nacional de Ciberseguridad (2023).

Nota: Elaboración propia a partir de Aguilar Antonio (2024, p. 30).

Esta evolución denota un aspecto importante y es el compromiso de los líderes políticos de la nación a pesar de las diferencias ideológicas, ya que se puede observar fluidez en cuanto a la adaptación del contexto legal en función de los retos planteados por la realidad.

2.1.5.4 OTRAS DIRECTRICES INTERNACIONALES

Existen algunas iniciativas impulsadas por entidades como la Organización de las Naciones Unidas (ONU), la Organización de Estados Americanos (OEA), de las cuales Honduras es miembro y que están dirigidas a fortalecer la ciberseguridad y la protección de los datos en sus propios contextos. A continuación, se detallan algunas de ellas:

– **Resolución 45/95 de la ONU**: Aprobada el 14 de diciembre de 1990 por la Asamblea General y titulada como: “Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales”, es un antecedente importante porque establece principios internacionales que regulan aquellos ficheros con información sensible de los individuos e insta a los gobiernos a formular leyes y normativas para cumplir con estos (ONU, 1990, p. 198).

2.1.6 INSPECCIÓN DE MARCOS Y METODOLOGÍAS VIGENTES PARA LA GESTIÓN DE CIBER-RIESGOS

En este apartado, se describe brevemente que marcos y metodologías se encuentran disponibles para la gestión de ciber-riesgos. En definitiva, se debe tener presente que al fin y al cabo estas son herramientas que deben utilizarse según las necesidades del contexto y no buscado demostrar si una es mejor que otra. Es más, en la mayoría de los casos lo que funciona es una tropicalización u adaptación que responda a las necesidades puntuales del contexto.

Sevillano y Beltrán (2020) recopilaron diferentes estándares y marcos de trabajo para la gestión operativa del ciber-riesgo. Estos han sido actualizados a su versión vigente y se muestran en el siguiente cuadro:

Tabla 5 *Estándares y marcos de trabajo para la gestión operativa del ciber-riesgo*

	Estándares y marcos de trabajo para la gestión operativa del ciber-riesgo Definición de procesos y evaluación del nivel de madurez (IT)
ISO.	- ISO/IEC 27001:2022 - Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos. - ISO/IEC 27002:2022 - Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información. - ISO/IEC 27032:2023 - Ciberseguridad: Directrices para la seguridad en Internet. - ISO 27017:2015 - Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube. - ISO/IEC 27018:2019 - Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.
NIST.	- Marco de Seguridad Cibernética (CSF) 2.0 del NIST (2024). - SP 800-53 & 800-53A – Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones.
Europeas	- MageritV3 (España, cumplimiento con la ISO 27001).

(IT)	- CORAS (Noruega). - EBIOS 2010 (Francia, cumplimiento con la ISO 27001). - MEHARI (Francia, cumplimiento con la ISO 27001). - CRAMM (Reino Unido, cumplimiento con la ISO 27001). - BSI Standars (Alemania, cumplimiento con la ISO 27001). - MIGRA (Italia, cumplimiento con la ISO 27001). - Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD (AEPD 2018).
No europeas (IT)	- TARA (Estados Unidos). - OCTAVE Allegro (Estados Unidos). - RISK IT Framework (Estados Unidos). - FAIR (Estados Unidos y Canadá, cumplimiento con la ISO 27001). - AS/NZS 4360 (Canadá). NOTA: Esta metodología se equipara en ocasiones con la ISO 31000 aunque también ayuda a realizar una evaluación operativa del ciber-riesgo. - Canadian TRA (Canadá).

Fuente: Elaborado, actualizado y traducido a partir de Sevillano y Beltrán (2020, p. 54 – 56).

Es importante recordar que esta investigación apunta al análisis y la generación de un proceso para gestionar vulnerabilidades. Como se puede observar, la mayoría de estándares están orientados a la gestión de riesgos en general, listas de control y otros aspectos de gobierno de TI. Sin embargo, partiendo de la ISO 27002 es posible identificar algunos criterios de selección. Dentro de la sección de Controles Tecnológicos, se encuentra el numeral 8.8 titulado: "Gestión de vulnerabilidades técnicas". El siguiente cuadro condensa sus generalidades:

Tabla 6 *Cuadro resumen de Control de Gestión de Vulnerabilidades Técnicas ISO 27002:2022*

Tipo de Control	Dimensiones de Seguridad de la Información	Conceptos de Ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo.	- Confidencialidad.	- Identificar.	Gestión de amenazas y de	- Gobernanza y Ecosistema.

	- Integridad. - Disponibilidad.	- Proteger.	vulnerabilidades.	- Protección. - Defensa.

Fuente: Extraído íntegramente de ISO 27002:2022, numeral 8.8 (s.f.).

Los conceptos de ciberseguridad descritos en el cuadro, hacen referencia a dos funciones del Marco de Ciberseguridad NIST CSF 2.0. Los detalles se ampliarán en la siguiente sección, pero esto confirma que dichos elementos son base para cualquier proceso orientado a gestionar las vulnerabilidades técnicas indistintamente del estándar que se seleccione. A partir de Coronado García (2024) se ha adaptado el siguiente cuadro comparativo entre los marcos que resultan más idóneos para adaptarse en base a los objetivos que persigue esta investigación:

Tabla 7 *Cuadro comparativo de metodologías y marcos para el análisis de riesgos tecnológicos*

Metodología o Marco	Descripción	Etapas o Funciones
OCTAVE.	La metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una de las más conocidas en el mundo de la seguridad informática. Esta metodología se centra en evaluar la criticidad de los activos (es decir, su importancia para la empresa) y las vulnerabilidades que los afectan. Una de las características distintivas de OCTAVE es que involucra tanto a los técnicos de TI como a los directivos de la empresa, lo que permite tener una visión completa de los riesgos.	• **Fase 1**: Identificación de activos. • **Fase 2**: Identificación de amenazas y vulnerabilidades. • **Fase 3**: Evaluación de riesgos y plan de mitigación.
MAGERIT.	En el contexto español, una metodología muy utilizada es MAGERIT, desarrollada por el Centro Criptológico Nacional (CCN). Esta metodología está orientada a la evaluación de riesgos en sistemas de información y es ampliamente utilizada	• **Análisis de los activos**: Se identifican los activos que soportan los procesos de negocio. • **Análisis de los riesgos**: Se estudian las amenazas que podrían afectar esos activos, así

	en la administración pública en España.	como las vulnerabilidades que existen en los sistemas. • **Gestión del riesgo**: Finalmente, se aplican medidas para mitigar los riesgos.
ISO 27002.	La norma ISO 27002 proporciona directrices específicas para la gestión de vulnerabilidades técnicas dentro del marco más amplio de la norma ISO 27001, que es el estándar internacional de referencia para la gestión de la seguridad de la información.	• **Identificar las vulnerabilidades técnicas**: La organización debería disponer de un inventario preciso de activos como requisito previo para una gestión eficaz de la vulnerabilidad técnica. • **Evaluar las vulnerabilidades técnicas**: Implica analizar y verificar los informes para determinar qué tipo de actividad de respuesta y reparación es necesaria. Una vez identificada una posible vulnerabilidad técnica, determinar los riesgos asociados y las medidas que tienen que adoptarse. • **Adoptar las medidas adecuadas para hacer frente a las vulnerabilidades técnicas**: Debería implementarse un proceso de gestión de actualizaciones de software para garantizar que se instalan los parches aprobados y las actualizaciones de aplicaciones más recientes para todo el software autorizado.
NIST CSF 2.0	Este marco desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés), comprende cinco funciones que componen su núcleo.	• Gobernar. • Identificar. • Proteger. • Detectar. • Responder. • Recuperar.

Fuente: Elaborado a partir de Coronado García (2024, p. 42 – 45).

La existencia de todos estos marcos y metodologías de referencia comprueba que existe un creciente interés a nivel global por establecer rutas de respuesta más concretas a las brechas de seguridad que conllevan las vulnerabilidades en los activos tecnológicos.

2.1.7 JUSTIFICACIÓN DE LA ELECCIÓN DE NIST CSF 2.0 COMO MARCO DE REFERENCIA

De la comparativa realizada en el apartado anterior, es posible realizar las siguientes valoraciones:

– Todos los marcos coinciden en la necesidad de identificar los activos tecnológicos y de alguna manera, establecer mecanismos de protección de los mismos frente a riesgos y vulnerabilidades.

– Comparten la necesidad de realizar algún tipo de evaluación de las amenazas para tratar de priorizar la respuesta.

– A pesar de lo anterior, los marcos son bastante genéricos y si bien describen secuencias de acciones que resultan coherentes, no son tan claros en cuanto a la forma de ejecutar las etapas señaladas. En tal sentido, las fases de: Detectar, Responder y Recuperar del NIST CSF 2.0 denotan una perspectiva más transversal de posibles cursos de acción que sea necesario tomar de cara a las ciber amenazas.

– Un factor crítico es que, a diferencia de los demás estándares, NIST CSF incorpora en la versión 2.0 la figura del Gobierno lo que permite una mayor facilidad de conexión con los objetivos estratégicos de la organización.

– Adicionalmente, NIST CSF 2.0 cuenta con su propio modelo de madurez lo que simplifica la evaluación de sus componentes y la identificación de las acciones que debe

tomar la organización para mejorar su postura de ciberseguridad.

– NIST CSF 2.0 es sumamente flexible, puede integrarse con otros marcos de referencia y adaptarse a las necesidades de una organización.

A continuación, se presenta el siguiente cuadro resumen con una comparativa de NIST CSF 2.0 y otros marcos tomando como punto de partida los objetivos y la propuesta de aplicabilidad de la investigación.

Tabla 8 *Criterios de selección del marco de referencia para la investigación*

Criterios	NIST CSF 2.0	OCTAVE	MAGERIT 3	ISO 27002:2022	COBIT 2019
El marco esta fuertemente orientado a la ciberseguridad y gestión de vulnerabilidades.	X	X	-	X	-
Se define una secuencia de etapas para atender las vulnerabilidades en los activos tecnológicos.	X	X	-	X	-
Posee un sistema de evaluación de madurez.	X	-	X	-	X
Puede integrarse con otras metodologías y marcos de referencia.	X	X	X	X	X
Incorpora la figura de Gobierno como parte de la gestión de ciber-amenazas.	X	-	-	-	X

Nota: Elaboración propia.

Por lo anterior, se considera que el Marco de Seguridad Cibernética del NIST CSF en su versión 2.0 se adecua mejor a las necesidades de este trabajo y propuesta. Es importante señalar que, en definitiva, todos los estándares pueden contribuir de una u otra manera en el fortalecimiento de las organizaciones pues cada una cuenta con características y propósitos puntuales.

2.1.8 BREVE INDUCCIÓN AL MARCO DE SEGURIDAD CIBERNÉTICA DEL NIST CSF 2.0

El Instituto Nacional de Estándares y Tecnología (NIST) fue fundado en 1901 y hoy en día forma parte del Departamento de Comercio de los Estados Unidos. En 2024 el Marco de Seguridad Cibernética del NIST fue actualizado a la versión 2.0. Este marco cuenta con tres grandes componentes:

Figura 5 *Componentes del marco de ciberseguridad NIST CSF 2.0*

Nota: Elaboración propia.

– **CSF Core del NIST**: Es una taxonomía de resultados de seguridad cibernética de alto nivel que puede ayudar a cualquier organización a gestionar sus riesgos de seguridad cibernética. Los componentes del CSF Core son una jerarquía de Funciones, Categorías y Subcategorías que detallan cada resultado (NIST, 2024, p. 1).

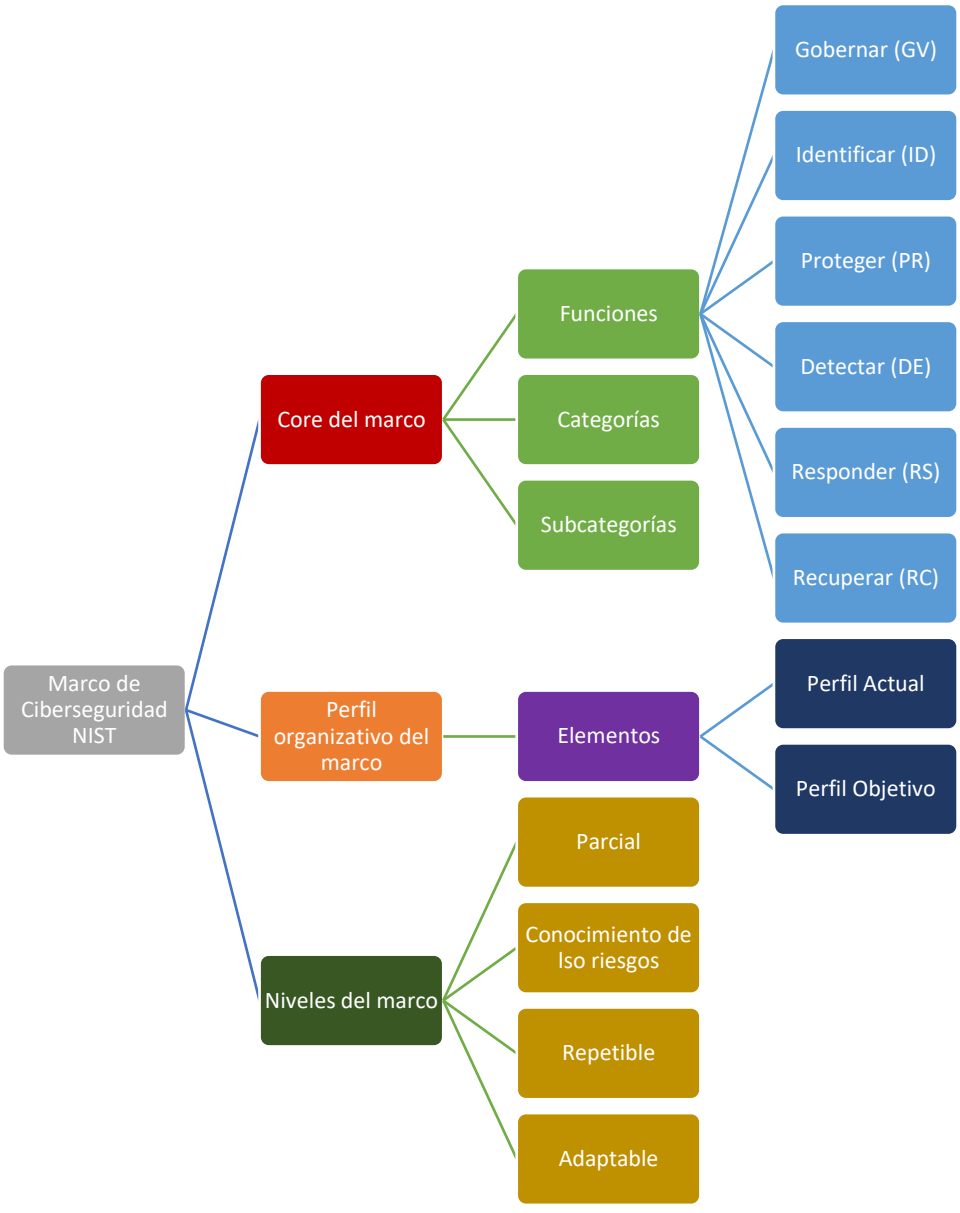
– **Perfil organizativo**: Describe la postura de seguridad cibernética actual u objetivo de una organización en términos de los resultados del núcleo o core del marco (NIST, 2024, p. 6).

– **Niveles del CSF**: Permiten medir el rigor de las prácticas de gobernanza y gestión

de los riesgos de seguridad cibernética de una organización, y proporcionan el contexto de cómo una organización ve los riesgos de seguridad cibernética y los procesos establecidos para gestionar esos riesgos.

De estos tres grandes componentes se desprenden diferentes elementos y artefactos que calzan con el flujo de la gestión de vulnerabilidades y se muestran en el siguiente diagrama:

Figura 6 *Estructura Marco de seguridad cibernética NIST CSF 2.0*



Nota: Elaboración propia.

Previo a exponer como se pueden adaptar algunos aspectos del NIST CSF .2.0 para la gestión de vulnerabilidades, es oportuno comprender en qué consisten originalmente las funciones centrales del marco. A partir de Villa Crespo y Morales Alonso (2017) se describe brevemente en que consiste cada una de ellas:

Tabla 9 *Cuadro resumen de funciones del Framework Core del NIST*

Función	Descripción	Actividades
Gobernar.	Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de la organización.	• Establecer el contexto organizativo. • Definir la estrategia de gestión de riesgos. • Establecer y comunicar las funciones responsabilidades y autoridades. • Supervisar los resultados de las actividades desarrolladas en la gestión de seguridad cibernética en toda la organización para mejorar y ajustar las estrategias.
Identificar.	Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de sistemas, activos, datos y capacidades.	• Identificar los procesos y activos críticos. • Flujos de información de documentos. • Mantener el inventario de software y hardware. • Establecer políticas para la ciberseguridad que incluyan roles y responsabilidades. • Identificar amenazas, vulnerabilidades y riesgos.
Proteger.	Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.	• Gestionar el acceso a activos e información. • Proteger los datos sensibles. • Hacer copias de seguridad de manera periódica. • Proteger los dispositivos. • Gestionar las vulnerabilidades de los dispositivos. • Formación y concienciación en ciberseguridad sobre los usuarios.

Detectar.	Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de seguridad.	• Probar y actualizar los procesos de detección. • Conocer los flujos de datos esperados. • Mantener y monitorizar los archivos de registro. • Comprender el efecto de los eventos de ciberseguridad.
Responder.	Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de seguridad detectado.	• Asegurar que los planes de respuesta sean probados. • Asegurar que los planes de respuesta se encuentren actualizados. • Coordinar a todas las partes interesadas.
Recuperar.	Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para establecer capacidades o servicios que hayan sido afectados durante un evento de seguridad.	• Comunicar con las partes interesadas. • Asegurar que los planes de recuperación se encuentran actualizados. • Gestionar las relaciones públicas y reputación de la compañía.

Nota: Elaboración propia a partir de Villa Crespo y Morales Alonso (2017, p. 268 – 270).

Para los propósitos de esta investigación, se tomarán únicamente algunas de estas funciones pues otras escapan del alcance del proceso que se pretende plantear y competen a otros que la organización debe tener (tal como el proceso de recuperación, la protección de activos, etc.).

2.1.9 EXPLORACIÓN DE LOS ATAQUES INFORMÁTICOS

Previo a realizar un acercamiento a la gestión de vulnerabilidades, es oportuno explorar de

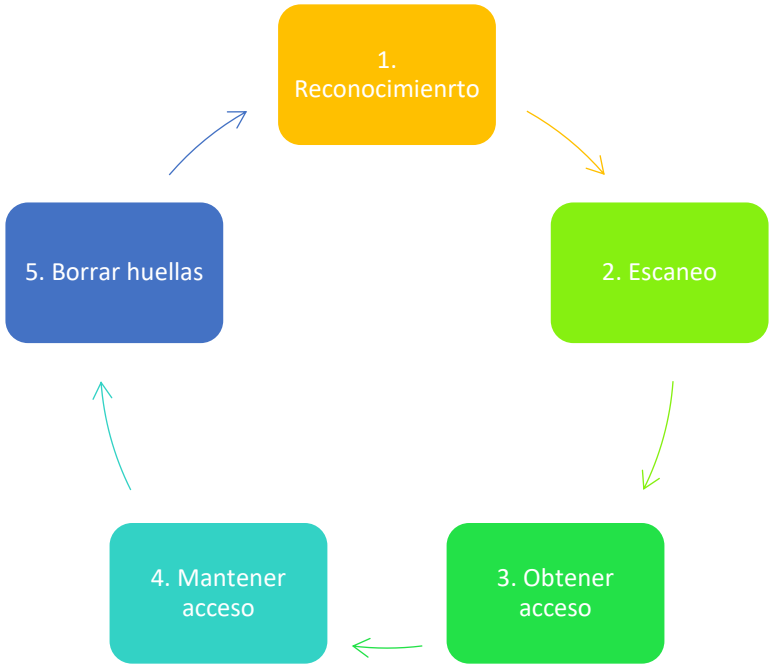
manera general en qué consisten los ataques informáticos y comprender cuál es su relación con estas. La intención no es profundizar en demasía, pues no es el propósito de esta investigación ahondar en el hacking o pruebas de intrusión (que constituye un tema con vasta información en sí mismo), pero si, ofrecer la claridad suficiente como para valorar la importancia de una adecuada gestión de vulnerabilidades justo para prevenir estos ataques.

Los ataques informáticos se sustentan en la explotación de vulnerabilidades. Mata (2020) define dicha actividad de explotación así:

> Estos son ataques cibernéticos que aprovechan las debilidades o agujeros en una red informática para combinar múltiples vulnerabilidades para destruir el objetivo. También se entiende que permite que una computadora atacante o un auditor de seguridad explote una vulnerabilidad conocida en el código, método o ruta para comprometer la seguridad de un sistema informático y obtener acceso a él y controlarlo (Mata, 2020, p. 152).

Una vez hecha esta aclaración, existe un consenso generalizado en las etapas del proceso de hackeo en un ciberataque. El mismo se presenta como un ciclo repetible que se muestra a continuación:

Figura 7 *Diagrama de etapas de un ciberataque*



Fuente: Elaborado a partir de Austidillo (2019, p. 20).

A continuación, se resumen los aspectos relevantes de cada una de las etapas:

Tabla 10 *Actividades por etapa de un ciberataque*

Etapa	Descripción	Actividades clave
1. Reconocimiento.	En esta etapa se intenta recolectar la mayor cantidad de información posible sobre aquello en evaluación, como posibles nombres de usuarios, direcciones IP, servidores de nombre, y cualquier otra información relevante. Durante esta etapa cada elemento de información obtenida es importante y no debe ser subestimada. Adicionalmente tener en consideración; la recolección de una mayor cantidad de información, incrementará la probabilidad de realizar un ataque exitoso.	• Consulta de fuentes públicas. • Recopilación de documentación. • Revisión de registros DNS. • Evaluación de rutas. • Uso de motores de búsqueda.
2. Escaneo (o descubrimiento).	Después de recolectar la mayor cantidad de información sobre la entidad en evaluación desde fuentes externas; como motores de búsqueda; se requiere descubrir ahora las máquinas activas. Es decir, el propósito de este proceso es encontrar cuales son las máquinas que están disponibles o en funcionamiento, pues en el caso de que la máquina no esté disponible no se puede continuar el proceso de pruebas de penetración, y consecuentemente debe continuarse con la siguiente máquina. También se debe intentar obtener indicios sobre el tipo y versión del sistema operativo utilizado en la máquina. Todo lo mencionado ayudará durante el proceso donde se intentará mapear vulnerabilidades.	• Identificar maquinas a evaluar. • Obtener la huella del Sistema Operativo. • Escanear puertos. • Enumerar servicios. • Mapeo de vulnerabilidades.

3. Obtener acceso.	Se enfoca únicamente en establecer acceso hacia un sistema o recurso, evadiendo las restricciones de seguridad desplegadas. Si la anterior etapa correspondiente al análisis de vulnerabilidades fue realizada apropiadamente, esta etapa debe estar bien planificada para ser un golpe de precisión. La meta principal es identificar puntos de entrada hacia la entidad, además de identificar los activos de alto valor. Adicionalmente si la fase correspondiente al análisis de vulnerabilidades fue adecuadamente completada, se debe haber compilado un listado con los activos de alto valor. En última instancia el vector de ataque debe tener en consideración la probabilidad de éxito, y el mayor impacto sobre la entidad.	– Ingeniería social. – Explotación de vulnerabilidades.
4. Mantener acceso. **5. Borrar huellas.**	Las actividades de post-explotación o explotación posterior son aquellas realizadas una vez el sistema ha sido comprometido. Estas actividades se basan en el tipo de sistema operativo. Estas pueden variar desde ejecutar un simple comando "whoami" hasta enumerar cuentas locales.	• Escalada de privilegios. • Obtener usuarios y contraseñas para mantener acceso. • Buscar información clave. • Eliminar rastros de la intrusión.

Nota: Elaboración propia a partir de Caballero Quezada (2022, p. 38 – 155).

Como se puede notar, la explotación de vulnerabilidades es el punto de entrada hacia la infraestructura tecnológica de la entidad. De allí en más, se trata de ganar y consolidar los accesos para continuar escalando y de ser posible, extrayendo información.

Adicionalmente, existen diferentes tipos de ataques que los ciberdelincuentes pueden ejecutar. A partir de Gómez Vieites (2015) se muestran los más comunes:

Tabla 11 *Tipos de ataques informáticos*

Tipo de ataque	Descripción
Actividades de reconocimiento de sistemas.	Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos.
Detección de vulnerabilidades en los sistemas.	Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como exploits).
Robo de información mediante la interceptación de mensajes.	Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.
Modificación del contenido y secuencia de los mensajes transmitidos.	En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como "ataques de repetición" (replay attacks).
Análisis de tráfico.	Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los sniffers. Así, se conoce como eavesdropping a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.
IP Spoofing (Enmascaramiento de la dirección IP).	Sucede un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.
DNS Spoofing (Falsificación de DNS).	Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas web falsas o bien la interceptación de sus mensajes de correo electrónico.
Cambio en el registro	El registro de nombres de dominio utiliza un sistema de autenticación

de nombres de dominio de InterNIC.	de usuarios registrados con un bajo nivel de seguridad. Este proceso de autenticación es necesario para poder solicitar cambios ante InterNIC (base de datos central con los nombres de dominio registrados en Internet) o ante alguna de las empresas registradoras de nombres de dominio. Aprovechando esta debilidad en el proceso de autenticación, un usuario malicioso podría tratar de realizar un cambio en el registro de nombres de dominio para provocar una redirección del tráfico destinado a unos determinados dominios hacia otras máquinas, o bien un ataque de Denegación de Servicio contra una determinada organización.
SMTP Spoofing (Falsificación de remitentes).	El envío de mensajes con remitentes falsos (masquerading) para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Así mismo, este tipo de ataque es muy utilizado por los spammers, que envían gran cantidad de mensajes de "correo basura" bajo una identidad falsa.
Captura de cuentas de usuario y contraseñas.	También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador 6 (keyloggers).
Modificación del tráfico y de las tablas de enrutamiento.	Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos. Así, la utilización del encaminamiento fuente (source routing) en los paquetes IP permite que un atacante pueda especificar una determinada ruta prefijada, que podría ser empleada como ruta de retorno, saltándose todas las reglas de enrutamiento definidas en la red. De este modo, utilizando además el IP Spoofing, un atacante se podría hacer pasar por cualquier máquina en la que el destino pueda confiar, para recibir a continuación los datos correspondientes al equipo que está suplantando.
Conexión no autorizada	Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos

en equipos y servidores.	destacar las siguientes: e Violación de sistemas de control de acceso. – Explotación de "agujeros de seguridad" (exploits). – Utilización de "puertas traseras" (backdoors). – Utilización de rootkits (programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo). – Wardialing (conexión a un sistema informático de forma remota a través de un módem).
Malware (Virus informáticos, troyanos y gusanos).	Entendemos por código malicioso o dañino (malware) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etc.
Ataques de Cross-Site-Scripting.	Son ataques dirigidos, por lo tanto, contra los usuarios y no contra el servidor Web. Así, mediante Cross-Site Scripting, un atacante puede realizar operaciones o acceder a información guardada en un servidor Web en nombre del usuario afectado, suplantando su identidad.
Ataques de inyección de código SQL.	SQL, Structured Query Language (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales. La unidad típica de ejecución de SQL es la consulta (query), conjunto de instrucciones que permiten modificar la estructura de la base de datos (mediante instrucciones del tipo Data Definition Language, DDL) o manipular el contenido de la base de datos (mediante instrucciones del tipo Data Manipulation Language, MDL). En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios. El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada.
Ataques contra los sistemas criptográficos.	Los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para cifrar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado.

Denegación del Servicio (Ataques DoS - Denial of Service).	Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.
Ataques de Denegación de Servicio Distribuidos (DDoS).	Los Ataques de Denegación de Servicio Distribuidos (DDoS) se llevan a cabo mediante equipos zombi. Los equipos zombis son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque. Generalmente los equipos zombis cuentan con una conexión ADSL u otro tipo de conexión de banda ancha, de tal modo que suelen estar disponibles las 24 horas.

Fuente: Elaboración propia a partir de Gómez Vieites (2015, p. 40 – 65).

Este cuadro permite visualizar lo complejo, dinámico y el enorme reto que representa para los expertos en este tema, mantener protegidas a las organizaciones de todas estas amenazas, que cada vez se vuelven más sofisticadas. Con este precedente es momento de dar paso a cómo gestionar las vulnerabilidades presentes en los activos tecnológicos.

2.1.10 ACERCAMIENTO A LA GESTIÓN DE VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN

Antes de continuar, una pregunta clave dentro del campo de la ciberseguridad es: ¿Qué es una vulnerabilidad? Desde la óptica de la ciberseguridad, una vulnerabilidad, es una debilidad existente en los activos tecnológicos. Mata (2024, p. 173) establece que: “Es una debilidad en un sistema informático que puede ser explotada por un atacante”. Urcuqui López, y Navarro Cadavid (2023, p. 51) agregan dos dimensiones importantes a este concepto y son: El “que” (componente a ser explotado) y el “quienes” sufren el daño o afectación (clientes o usuarios de un servicio u aplicación).

Ramírez Pascual ofrece una acotación adicional señalando el peligro que representa una vulnerabilidad:

> Se entiende como un fallo informático que pone en peligro a un servicio o sistema, es decir, se trata de un bug que puede usar un atacante con fines maliciosos, puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. En cierta medida es una puerta de entrada para los ciberdelincuentes. (Ramírez Pascual 2023, p .67).

Una vulnerabilidad implica un riesgo en si misma que puede exponer datos sensibles de la organización, e incluso generar impactos negativos para los individuos y organizaciones. Gómez Vieites (2015) ejemplifica estos efectos con su definición:

> Una vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización. Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos. Pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad...), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad físicas, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etcétera). Se suele emplear una escala cuantitativa o cualitativa para definir el nivel de vulnerabilidad de un determinado equipo o recurso: baja, media y alta (Gómez Vieites, 2015, p. 72).

Es decir, que, desde la óptica de la ciberseguridad, una vulnerabilidad, es una brecha (conocida o no) existente en los activos tecnológicos. Estas constituyen sin duda una amenaza latente en cualquier infraestructura tecnológica.

De hecho, las vulnerabilidades hoy en día conforman un mercado complejo. Una interrogante válida es: ¿De qué forma los ciberdelincuentes consiguen identificar las vulnerabilidades? Baker (2025) entrega una respuesta sumamente reveladora:

> Exist<e un amplio y diverso ecosistema de vulnerabilidades y exploits, un espectro que va desde lo legítimo en un extremo hasta lo ilegal en el otro, con matices grises en el medio. Por el lado legal, los hackers informáticos y los investigadores de seguridad informan reservadamente sobre los bugs a los proveedores o a un tercero legítimo como parte de los procesos responsables de aviso de vulnerabilidades (por ejemplo, en las recompensas por bugs o los avisos a los equipos de respuesta a emergencias informáticas que manejan incidentes de seguridad a nivel nacional). En el otro extremo del ecosistema, los delincuentes compran y venden vulnerabilidades y exploits en la dark web. En un área gris en el medio existen brokers de exploits cuya legalidad se determina en función de con quién comercian. Los atacantes a menudo comparten información entre sí en foros en línea,

> redes sociales y plataformas de mensajería (Baker, 2025, p. 78 – 79).

Cabe señalar que estas vulnerabilidades pueden divulgarse bajo procesos estandarizados como la ISO/IEC 29147:2018 y la ISO/IEC 30111:2019. Sin embargo, como señala Baker, el contexto es complicado y con diversas singularidades, pues hay diferentes fuerzas y actores pujando por esa información. Frente a esta realidad, es donde se vuelve fundamental establecer procesos de atención frecuente y mecanismos de contención.

Esa es la razón por la que la presente investigación en enfoca en el proceso para la gestión de vulnerabilidades, lo que implica una acción intencional y controlada por parte de las organizaciones ya que como menciona Deutsh, es posible que los esfuerzos del pasado no sean suficiente para responder a los desafíos del presente en este ámbito:

> En la época actual de vertiginosos cambios en el software, una auditoría anual no es suficiente para evaluar la seguridad de los sistemas… Sabiendo esto, debemos tener claro que el proceso de análisis y corrección de vulnerabilidades tiene que ser continuo, con independencia de la frecuencia con la que evolucionen las aplicaciones (Deutsch, 2022, p. 150, 152).

Tal como lo establecen Beltrán y Sevillano (2021, p. 284) para que la monitorización de vulnerabilidades sea completa y significativa, debe ser capaz de identificar parámetros clave como: Versiones de sistema, firmware, parches, etc., información relevante para los atacantes (para mapear brechas a explotar) y para los responsables de seguridad (encargados de cerrar esas brechas).

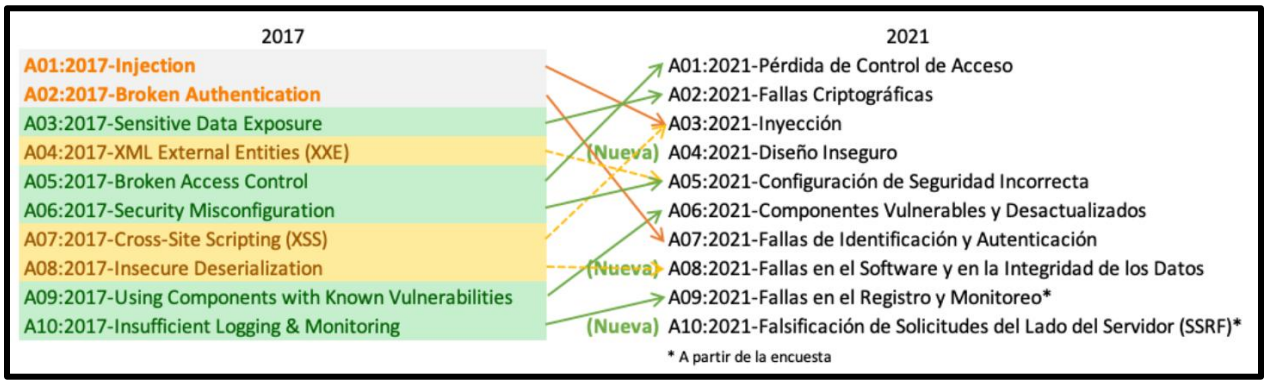
Diego y Fernández Isabel (2020) enlistan algunos de los tipos de vulnerabilidades más conocidos sin ser esta una lista demasiado exhaustiva.

Figura 8 *Tipos de vulnerabilidades más conocidos*

Fuente: Elaboración propia a partir de Diego y Fernández Isabel (2020, p. 67 – 68).

El top 10 de OWASP ofrece un listado de vulnerabilidades más explícito y es una fuente de referencia muy utilizada en el mundo de la ciberseguridad. A continuación, se muestra el detalle en base a los resultados recabados durante el año 2021:

Figura 9 *Top 10 de vulnerabilidades OWASP 2021*



Fuente: https://owasp.org/Top10/es/

Ahora bien, las vulnerabilidades se pueden categorizar. Baker (2025) propone tres grandes

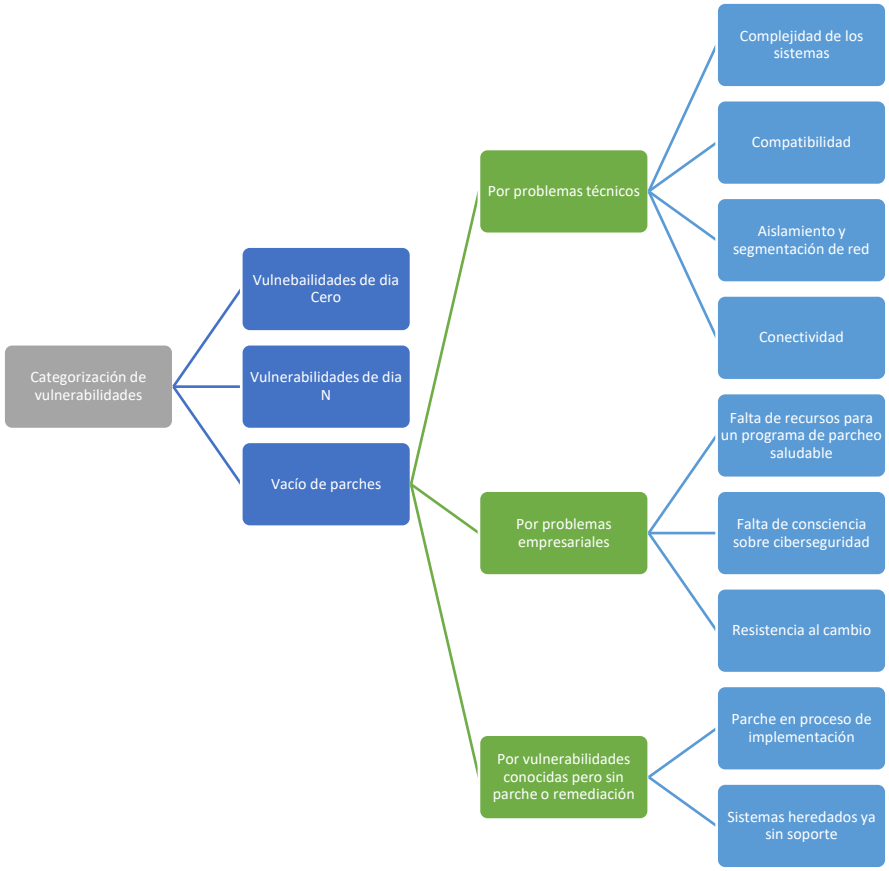
dimensiones:

– **Vulnerabilidades de día Cero**: Sobre ellas, Molina Marín y Orozco (2020) señalan que: “Es una brecha en la seguridad del software o hardware, es un tipo de vulnerabilidad que acaba de ser descubierta y que se presenta de forma desconocida para los sistemas de detección de intrusos” (Molina Marín y Orozco, 2020, p. 4). Nolasco Valenzuela, Gamboa Cruzado y Dextre Alarcón (2023) añaden que esas son: “Una vulnerabilidad en una aplicación o sistema, que ha sido detectada por el atacante antes que, por el dueño, para introducir código malicioso en el intervalo de tiempo previo a su localización y reparación mediante un parche informático” (Nolasco Valenzuela, Gamboa Cruzado y Dextre Alarcón, 2023, p. 336).

– **Vulnerabilidades de día N**: Son aquellas vulnerabilidades ya conocidas o públicas.

– **Vacío de parches**: Hace referencia a la no aplicación de parches correctivos por una razón concreta.

Figura 10 *Categorización de las vulnerabilidades*



Fuente: Elaboración propia a partir de Baker; 2025, p. 70 – 77.

Todas estas vulnerabilidades requieren ser mapeadas y atendidas en un proceso concreto, de modo que se pueden prevenir la mayor cantidad de incidentes provocados por ciber ataques, como esboza Caballero Quezada (2022):

> El proceso de mapear vulnerabilidades implica identificar y analizar las vulnerabilidades de seguridad críticas en el entorno evaluándose. Algunas veces a este proceso también se le denomina como una evaluación de vulnerabilidades. Es una de las áreas clave en un programa para la gestión de vulnerabilidades, a través de lo cual los controles de seguridad de una infraestructura en tecnologías de información, puede ser analizada contra un conjunto conocido o desconocido de vulnerabilidades. Una vez realizados los procedimientos para la captura de información, descubrimiento, y enumeración, es momento de investigar sobre las vulnerabilidades potencialmente existentes sobre la infraestructura en evaluación, las cuales podrían conducir hacia un compromiso; afectando su confidencialidad, integridad y disponibilidad en los sistemas de la entidad (Caballero Quezada, 2022, p. 76).

De forma muy general, Portantier (2013, p. 45) describe la panorámica de un modelo para

la gestión de vulnerabilidades del cual resaltamos, la relevancia que se le da a la implementación de contramedidas a través de un proceso fuerte que permita reducir el impacto negativo de una brecha explotada.

Figura 11 *Modelo General de Gestión de Vulnerabilidades*

Fuente: Elaboración propia a partir de Portantier; 2013, p. 45.

En síntesis, la gestión de vulnerabilidades facilita el establecer una serie de contramedidas que permiten a las entidades mitigar los riesgos que representa la exposición generada por la explotación de estas amenazas.

2.1.11 MÉTODOS Y HERRAMIENTAS PARA EL ANÁLISIS DE AMENAZAS CIBERNÉTICAS

Al momento de encarar una vulnerabilidad existen dos posibilidades. Se puede analizar o se puede tratar de explotar. Esto en sí mismo ya marca una diferencia entre ambas actividades y su alcance. Herrero Pérez (2021) profundiza en el enfoque de una y otra.

> Los análisis de vulnerabilidades tienen el propósito de identificar todas las vulnerabilidades existentes en los sistemas, pero sin llegar a explotarlas. Un análisis de vulnerabilidades también debería comprender aspectos que no se realizan en un test de penetración, como la revisión de las políticas de seguridad de la organización y de la documentación de seguridad. Existen, por tanto, notables diferencias entre un análisis de vulnerabilidades y un test de penetración (Herrero Pérez, 2021, p. 15).

Adicionalmente, es necesario mencionar que hoy en día existen múltiples herramientas a

disposición de los ciber delincuentes y los especialistas en ciberseguridad, dentro de las cuales figuran aquellas orientadas al análisis de vulnerabilidades. A partir de Menéndez Arantes (2022), se han categorizado en el siguiente cuadro.

Tabla 12 *Herramientas para la auditoria de sistemas*

Tipo	Ejemplos
Herramientas del Sistema Operativo.	Ping, tracert, pathping, netstat, nslookup, ipconfig, etc.
Herramientas de análisis de red, puertos y servicios.	Nmap, Zenmap, Angry IP Scanner, etc.
Herramientas de análisis de vulnerabilidades.	Nessus, MBSA, OpenVas, etc.
Analizadores de protocolos.	Wireshark, Caín y Abel, etc.
Analizadores de páginas web.	OWASP Zap, Acunetix, etc.
Herramientas de ataque de fuerza bruta.	John the Ripper, Ophcrack, etc.

Nota: Elaboración propia a partir de Menéndez Arantes (2022, p. 118 – 217).

El análisis de amenazas se realiza para tratar de dimensionar el problema, los activos comprometidos y cuál puede ser el camino más adecuado para su remediación. Dicho esto, es necesario explorar las herramientas a disposición para esta tarea.

2.1.11.1 MÉTODOS PARA EL ANÁLISIS DE AMENAZAS CIBERNÉTICAS

Así como las ciber amenazas, los métodos para su análisis han experimentado cambios de la mano con los avances tecnológicos. El siguiente cuadro nos ofrece una visión panorámica al respecto:

Tabla 13 *Métodos para el análisis de amenazas cibernéticas*

Método	Descripción
Análisis estático.	Técnica que evalúa los comportamientos maliciosos en el código fuente, los datos o los archivos binarios, sin ejecutar directamente la aplicación. Su complejidad ha aumentado debido a la experiencia que han adquirido los cibercriminales en el desarrollo de aplicaciones.
Análisis dinámico.	Métodos automatizados que estudian el comportamiento del malware en ejecución mediante un análisis de la interactividad del atacante y permiten evaluar características que solo pueden ser obtenidas mientras el software está

	en funcionamiento, como, por ejemplo: la inyección de código en ejecución, los procesos en ejecución, la interfaz de usuario, las conexiones de red y la apertura de sockets.
Análisis híbrido.	Método que combina las ventajas de la aplicación de los análisis dinámico y estático.
Inteligencia Artificial.	Área que provee de una serie de técnicas para dar soluciones aproximadas a problemas complejos. Una de ellas, el machine learning tiene como propósito proveer a los sistemas de la capacidad de aprender cómo identificar a un malware sin ser programado de forma explícita.

Nota: Adaptado de Ciberseguridad: un enfoque desde la ciencia de datos (Urcuqui, García 2018, p. 23).

Las diferentes herramientas utilizadas en ciberseguridad emplean algunos de estos métodos en la ejecución de sus escaneos. Hoy en día son frecuentes incluso análisis combinados que buscan realizar evaluaciones más exhaustivas tratando de ofrecer mayor visibilidad de brechas de seguridad potencialmente explotables.

2.1.11.2 DESCRIPCIÓN DEL SISTEMA DE EVALUACIÓN DE CRITICIDAD DE VULNERABILIDADES

Como es de esperar, no todas las vulnerabilidades son iguales. Existen organizaciones dedicadas a reportarlas y documentarlas bajo un mismo formato, que es reconocido por todas las herramientas que analizan vulnerabilidades. Este formato se conoce como: Vulnerabilidades y Exposiciones Comunes (CVE por sus siglas en inglés). Una vez que estas CVE son reportadas y documentadas, se incorporan a las bases de datos de conocimiento de estas herramientas y son notificadas en los sistemas analizados. Algunas de las bases de datos más utilizadas son:

- https://nvd.nist.gov/
- https://www.cve.org/
- https://cve.mitre.org/
- https://www.cvedetails.com/

Para clasificarlas, existe el CVSS (Sistema Común de Puntuación de Vulnerabilidades por sus siglas en inglés) que es una escala del 1 al 10 que determina el nivel de peligrosidad de la vulnerabilidad. También, existen las CWE (Enumeración de Debilidades Comunes por sus siglas en inglés) que no representan una vulnerabilidad en sí misma. Gutiérrez Salazar (2019) nos ayuda a clarificar esta distinción:

> Adicionalmente al CVE, existe algo llamado CWE, que son siglas de Common Weakness Enumeration. Los CWE hacen referencia a debilidades del software, pero no vulnerabilidades, seguramente te preguntaras, ¿cuál es la diferencia? Pues bastante, una vulnerabilidad, te permitirá directamente comprometer la seguridad en una de las tres áreas (confidencialidad, integridad y disponibilidad) si logras explotarla. Por otra parte, una debilidad, de hecho, no necesariamente te permitirá comprometer la seguridad en ninguna forma importante (Gutiérrez Salazar, 2019, p. 127).

A modo de simplificar la comprensión de las puntuaciones de vulnerabilidades, muchas herramientas añaden la dimensión cualitativa mediante el siguiente sistema de categorización por severidad. López (2015), nos ilustra como se realiza la equivalencia hacia valores cualitativos desde la puntuación del CVSS.

Tabla 14 *Correspondencia entre la puntuación CVSS y valor cualitativo (severidad)*

Puntuación de CVSS	Severidad
0	Nula
0.1 – 3.9	Baja
4.0 – 6.9	Media
7.0 – 8.9	Alta
9.0 – 10.0	Crítica

Fuente: Extraído íntegramente desde: Métricas de evaluación de vulnerabilidades: CVSS 3.0 (López, 2015, 21 de julio).

Es así, como típicamente los escáner o analizadores de vulnerabilidades reflejan que un activo puede tener una mezcla de vulnerabilidades con diferentes niveles de severidad. A continuación, se abordan estas soluciones de software.

2.1.11.3 ESCÁNER DE VULNERABILIDADES

Si bien, es posible realizar la investigación manual de las CVE y CWE en las fuentes ya descritas, existen soluciones de software especializadas en esta tarea. A estas, se les conoce como analizadores o escáner de vulnerabilidades. Astudillo (2018) establece de ellas lo siguiente:

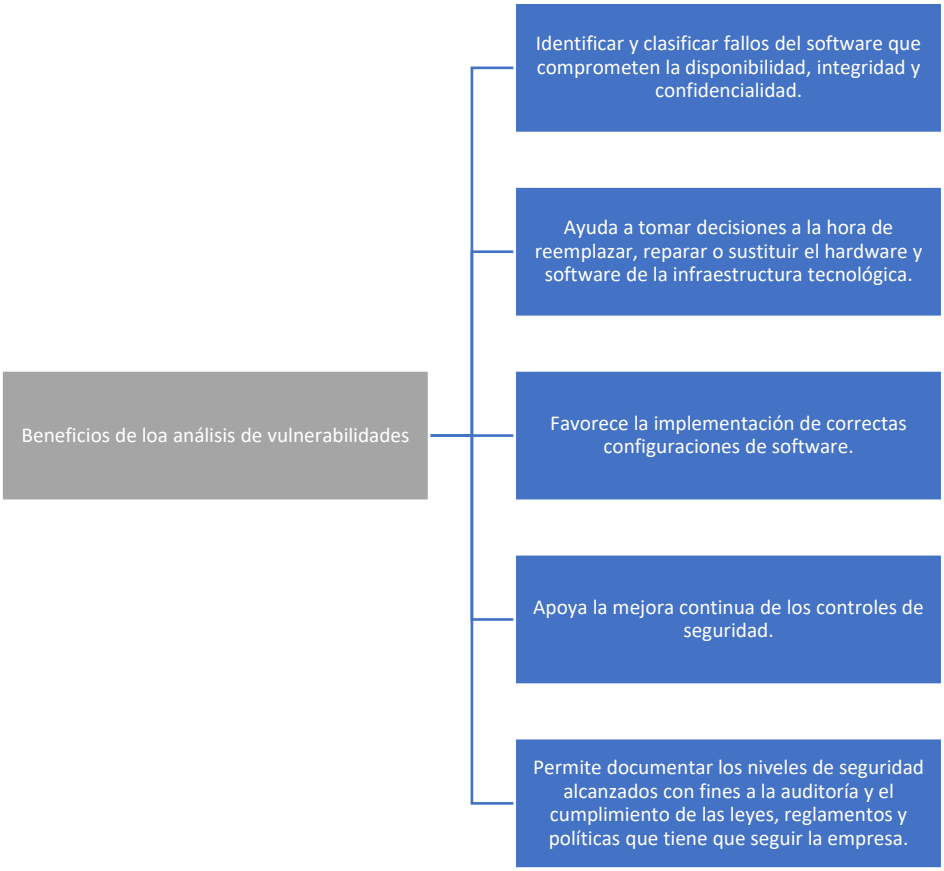
> Los analizadores facilitan la labor del auditor porque permiten ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, a la vez que identifican las vulnerabilidades presentes en dichos sistemas y las clasifican de acuerdo al nivel de riesgo presente. La identificación se realiza de acuerdo a la versión del sistema operativo y de los servicios y aplicaciones detectados comparándolos contra una base de datos de vulnerabilidades que se actualiza frecuentemente conforme nuevos huecos de seguridad son descubiertos (Astudillo, 2018, p. 71).

En una dirección similar Gutiérrez Salazar (2019) nos ofrece la siguiente definición que conecta el apartado anterior con este:

> Un analizador de vulnerabilidades es un software que realiza una serie de verificaciones automatizadas, tal como escaneo de puertos, servicios, y usando dicha información, busca automáticamente vulnerabilidades (CVEs y CWEs) en el sistema que está analizando. Esto es muy útil, ya que en ambientes organizacionales estos softwares permiten hacer auditorías a gran escala mucho más rápido, y como auditor nos facilita encontrar fallas superficiales rápida y fácilmente (Gutiérrez Salazar, 2019, p. 132).

Ambas definiciones están dirigidas a un análisis que puede ser superficial o profundo pero que, contrasta lo existente en el activo tecnológico con la base de vulnerabilidades para proyectar las brechas de seguridad detectadas. Adicionalmente, Menéndez Arantes (2022) señala los beneficios que nos entrega un análisis de vulnerabilidades con estas herramientas:

Figura 12 *Beneficios de los análisis de vulnerabilidades*



Nota: Elaboración propia a partir de Menéndez Arantes (2022, p. 174 – 175).

Por otra parte, el mercado de herramientas en ciberseguridad es sumamente dinámico y se encuentra en constante evolución. Sobre la importancia de las herramientas en la detección de vulnerabilidades, Maíllo Fernández (2020) establece:

> Ahora, nuestro objetivo es analizar todo ello en busca de debilidades en el sistema, a través de las cuales podamos penetrar en él. A estas debilidades es a lo que se conoce con el nombre de vulnerabilidades. Existen muchas herramientas capaces de realizar de modo automático este escáner de vulnerabilidades, aunque hay algunas que por la potencia de las funcionalidades que ofrecen, destacan por encima del resto (Maíllo Fernández, 2020, p. 240).

A continuación, se muestran algunas soluciones que por sus características resultan idóneas por el propósito que persigue esta investigación (el proceso para la gestión de vulnerabilidades) por lo que no se pretende alinear el mismo con un software en específico.

– **Greenbone (OpenVas)**: OpenVas es un escáner de vulnerabilidades con todas las

funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste del rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad. El escáner obtiene las pruebas para detectar vulnerabilidades de una fuente que tiene un largo historial y actualizaciones diarias. OpenVas ha sido desarrollado e impulsado por la empresa Greenbone desde 2006.

– **Nessus- Tenable**: Es una solución que posee una amplia apertura de parametrización de los escaneos de vulnerabilidades, lo que permite ejecutar análisis superficiales y/o a profundidad.

– **Manage Engine Vulnerability Manager Plus:** Esta es una solución sumamente interesante ya que integra la gestión de vulnerabilidades con la remediación de las mismas, yendo un paso más adelante que solo la mera detección de las brechas de seguridad.

A continuación, el siguiente cuadro comparativo que resume las características evaluadas dentro del alcance de esta investigación,

Tabla 15 *Cuadro comparativo de escáner de vulnerabilidades*

Criterio	GreenBone (OpenVas)	Tenbles – Nessus	Manage Engine Vulnerability Manager Plus
Tipo de infraestructura.	Local / Nube	Local / Nube	Local / Nube
Límite de periodo de prueba.	Sin restricción de tiempo, pero con funciones limitadas.	7 días	30 días
Funcionalidades en versión de prueba.	Parciales	Completas	Completas
Equipos administrables en versión de pruebas.	Sin limite	20	20
Método de gestión de	Dirección IP	Dirección IP	Agente

activos.			
Soporte de múltiples versiones de Sistemas Operativos (Windows, Linux, OSX).	Si	Si	Si
Formato de reportes.	CSV, PDF	CSV, PDF	XLSX, CSV, PDF
Base de datos de vulnerabilidades actualizable.	Si	Si	Si
Segmentación de activos por ambiente.	Si	Si	Si
Profundidad de análisis configurable (Superficial o exhaustivo).	Si	Si	Si
Análisis multicapa (Red, sistema operativo, bases de datos, aplicaciones web, configuraciones, etc.).	Si	Si	No (solo en dispositivos con agente)
Automatización de correos y notificaciones.	No	Si	Si
Aplicar remediación automática de vulnerabilidades.	No	No	Si
Proveedor en Honduras	No	DEVEL	AGREGA

Fuente: Elaboración propia.

Como se puede observar, existen bastantes similitudes entre las herramientas evaluadas. Sin embargo, Tenable es la herramienta utilizada actualmente en la Cooperativa y una de las mejores opciones en el mercado por lo que la investigación se enfocara en ella. De este software se resaltan las siguientes bondades:

- **Centralización**: Esta es una solución multifuncional, es decir no solo detecta

vulnerabilidades en sistemas operativos, sino que también, incorpora opciones de detección en dispositivos de red, bases de datos, servidores, estaciones de trabajo, etc. lo que permite que dentro de una misma solución se disponga de herramientas que en otro contexto deberían desplegarse por separado.

– **Automatización de tareas**: Este software permite automatizar varias tareas de entre las cuales destacan:

- Actualización de base de conocimiento de la herramienta.
- Ejecución de escaneos en un horario especificado.
- Envío de reportes (en diferentes formatos) del inventario de activos, vulnerabilidades, etc.

– **Integraciones**: La herramienta puede integrarse con otras soluciones tecnológicas mediante su API.

A pesar de las excelentes características descritas, existe una advertencia que vale la pena considerar, hecha por Gutiérrez Salazar (2019):

> Quiero dejar algo claro, un analizador de vulnerabilidades no es reemplazo para un experto y conocimiento/experiencia en ciberseguridad, y si se trata como tal, podría dar un falso sentido de seguridad, es solo una herramienta más, se deben probar los falsos positivos/negativos, y utilizar experiencia y conocimiento técnico para realizar una auditoría que valga la pena (Gutiérrez Salazar, 2019, p. 133).

Todos estos elementos formaran parte de la propuesta final del proceso que se describirá posteriormente en el Capítulo VI.

2.2 MICROENTORNO

2.2.1 LA CIBERSEGURIDAD EN HONDURAS

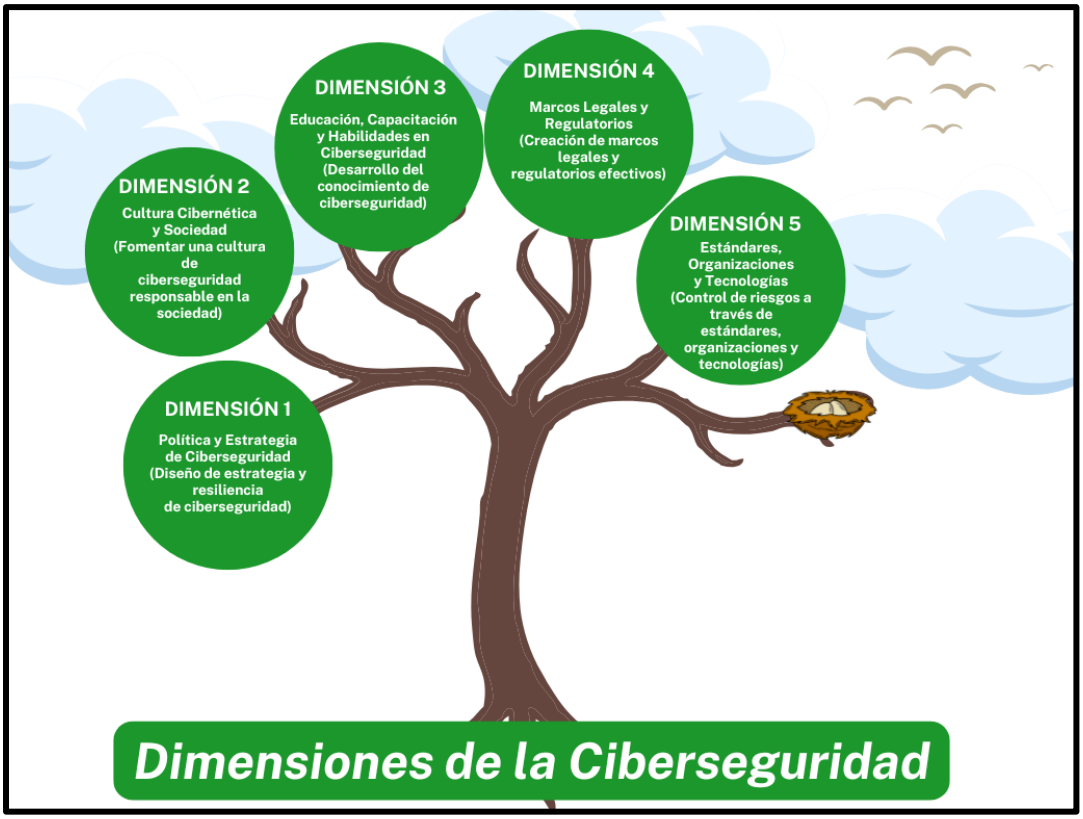
El tema de ciberseguridad en Honduras es ciertamente uno donde queda muchísimo camino por recorrer. Evidencia de ello, es la escaza documentación e indicadores de país evaluando esta

realidad. A continuación, se exponen algunos de los estudios formales y esfuerzos realizados en aras de resaltar los mismos.

2.2.1.1 ESTUDIO OEA – BID SOBRE CIBERSEGURIDAD EN HONDURAS

Lamentablemente es evidente la falta de una visión transversal de país orientada la ciberseguridad, que trascienda los gobiernos o la política en el país. Si bien, en algún momento han existido algunas iniciativas, las mismas han sido aisladas y la falta de continuidad las ha diluido con el tiempo. Esto se ve reflejado en los resultados de estudios como el realizado por el Observatorio de la Ciberseguridad en América Latina y el Caribe en 2020 (BID, OEA, 2020), auspiciado por la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID). El estudio evalúa cinco grandes dimensiones de la ciberseguridad y dentro de cada una de ellas, existen factores o competencias específicas que cada nación debe fortalecer. En el siguiente diagrama se presentan las mismas con su respectiva descripción.

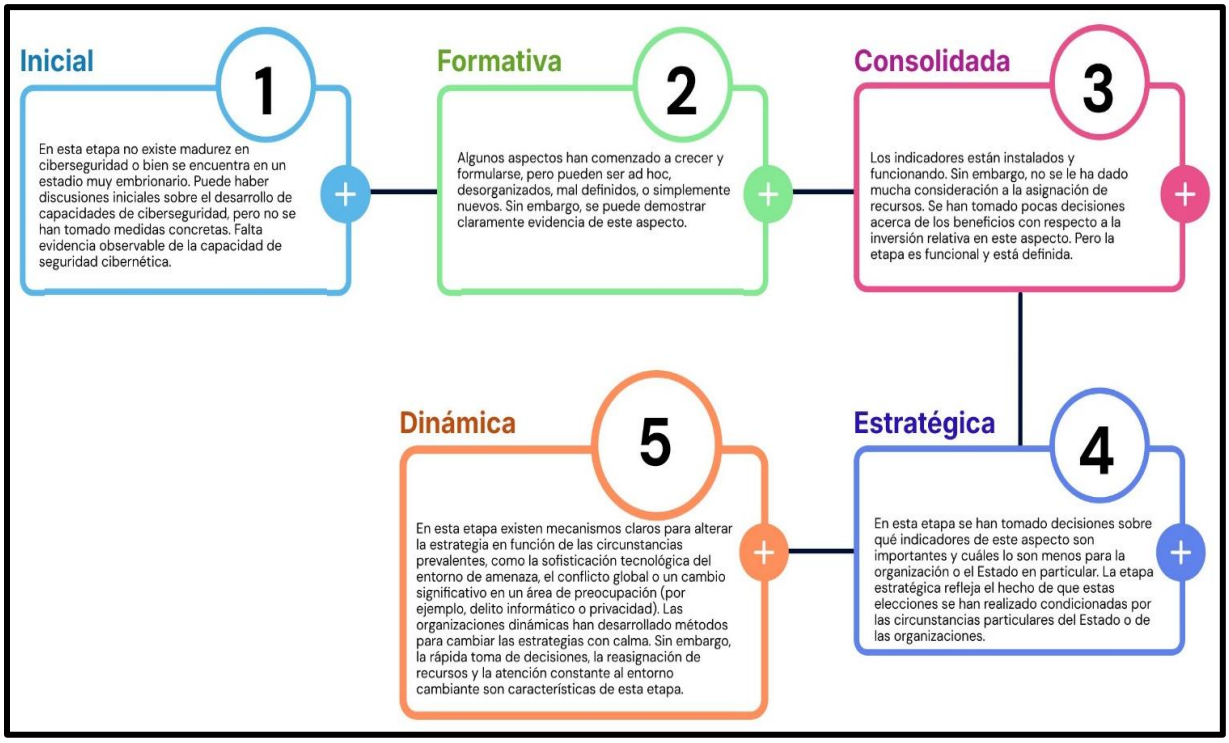
Figura 13 *Dimensiones de la Ciberseguridad evaluadas por BID - OEA en países miembros*



Fuente: Elaboración propia a partir de BID, OEA, 2020, p. 43 – 44).

El modelo de madurez para medir el progreso en cada dimensión consta de cinco posibles niveles. Este es una adaptación del modelo descrito en COBIT 2019 pero enfocado en ciberseguridad desarrollado por la Universidad de Oxford, específicamente por su Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés).

Figura 14 *Modelo de madurez de la capacidad de Ciberseguridad (BID, OEA)*



Fuente: Elaboración propia a partir de BID, OEA, 2020, p. 42.

Con lo expuesto hasta ahora, es momento de analizar los resultados para Honduras en cada una de las dimensiones. Para ello, y a fin de simplificar su comprensión, se han elaborado los siguientes cuadros (BID, OEA, 2020, p. 118 – 119). Es importante mencionar que muchos de los avances descritos en 2020 fueron producto del impacto generado por los resultados del año 2016.

– **Dimensión 1: Política y Estrategia de Seguridad Cibernética**: En esta dimensión fundamentalmente se consideran aspectos macro de iniciativas emanadas desde el Estado orientadas a fortalecer la ciberseguridad. Como se puede observar, la mayoría de indicadores resultaron en un nivel de madurez en etapa: "Inicial". Algunos de los últimos avances se detallan en la sección: "Plan Nacional de Gobierno Digital".

Tabla 16 *Perfil del estado de ciberseguridad en Honduras. Dimensión 1: Política y Estrategia de Seguridad Cibernética*

Dimensión 1: Política y Estrategia de Seguridad Cibernética.

1.1 Estrategia Nacional de Seguridad Cibernética.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Desarrollo de la Estrategia.	1	2	Si	**Formativa**
Organización.	1	1	No	Inicial
Contenido.	1	1	No	Inicial
1.2 Respuesta a Incidentes.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Identificación de Incidentes.	2	2	No	**Formativa**
Organización.	1	2	Si	Inicial
Coordinación.	1	2	Si	Inicial
Modo de Operación.	0	2	Si	Inicial
1.3 Protección de la Infraestructura Crítica (IC).				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Identificación.	1	2	Si	**Formativa**
Organización.	1	2	Si	**Formativa**
Gestión de Riesgos y Respuesta.	1	2	Si	**Formativa**
1.4 Manejo de Crisis.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Manejo de crisis	1	1	No	Inicial
1.5 Defensa Cibernética.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Estrategia.	1	1	No	Inicial
Organización.	1	1	No	Inicial
Coordinación.	1	1	No	Inicial
1.6 Redundancia de Comunicaciones				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Redundancia de Comunicaciones.	1	2	Si	**Formativa**

Fuente: Elaboración propia.

– **Dimensión 2: Cultura Cibernética y Sociedad**: De acuerdo con datos del Instituto Nacional de Estadística (INE, 2024, p. 6) obtenidos a partir de la Encuesta de Hogares 2024 (EPHPM), 9 de cada 10 hogares cuentan con acceso a algún tipo de dispositivo vinculado a las tecnologías de la información y la comunicación (TIC), siendo el teléfono celular el dispositivo más utilizado por los hondureños (88.3%). De la mano con esto y como se detalló en los apartados introductorios de esta investigación, el aumento en ciberataques ha elevado el interés y preocupación por parte de la sociedad hondureña en fortalecer su cultura cibernética. Por estas razones, son comprensibles entonces los resultados arrojados de avances en esta dimensión pues ha existido el involucramiento del gobierno, sector privado

y sociedad en general.

Tabla 17 *Perfil del estado de ciberseguridad en Honduras. Dimensión 2: Cultura Cibernética y Sociedad*

Dimensión 2: Cultura Cibernética y Sociedad.				
2.1 Mentalidad de Seguridad Cibernética.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Gobierno.	1	2	Si	**Formativa**
Sector Privado.	2	2	No	Formativa
Usuarios.	1	1	No	Inicial
2.2 Confianza y Seguridad en Internet.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Confianza y Seguridad en el Internet del Usuario.	1	1	No	Inicial
Confianza del Usuario en los Servicios de Gobierno Electrónico.	1	2	Si	**Formativa**
Confianza del Usuario en los Servicios de Comercio Electrónico.	1	1	No	Inicial
2.3 Comprensión del Usuario de la Protección de la Información en Línea.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2	Si	**Formativa**
2.4 Mecanismos de Denuncia.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Mecanismos de Denuncia.	0	1	Si	**Inicial**
2.5 Medios y Redes Sociales.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Medios y Redes Sociales.	0	2	Si	**Formativa**

Fuente: Elaboración propia.

– **Dimensión 3: Formación, Capacitación y Habilidades de Seguridad Cibernética**: En esta dimensión desde la óptica de la sensibilización, es claro un impulso principalmente desde el sistema financiero con sus diferentes campañas en medios de comunicación y canales digitales, procurando que sus clientes y colaboradores cuenten con fundamentos más fuertes en ciberseguridad. Sin embargo, los resultados de esta dimensión muestran que existe aún una gran brecha por cerrar. Adicionalmente, a nivel del país se cuenta con escazas ofertas de formación y capacitación dedicadas a ciberseguridad, siendo UNITEC la primera Universidad en ofrecer una Maestría con esta especialidad dentro de sus

programas académicos.

Tabla 18 *Perfil del estado de ciberseguridad en Honduras. Dimensión 3: Formación, Capacitación y Habilidades de Seguridad Cibernética*

Dimensión 3: Formación, Capacitación y Habilidades de Seguridad Cibernética.				
3.1 Sensibilización.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Programas de Sensibilización.	1	2	Si	**Formativa**
Sensibilización Ejecutiva.	2	2	No	Formativa
3.2 Marco para la Formación.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Provisión.	1	1	No	Inicial
Administración.	1	1	No	Inicial
3.3 Marco para la Capacitación Profesional.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Provisión.	2	2	No	Formativa
Apropiación.	2	2	No	Formativa

Fuente: Elaboración propia.

– **Dimensión 4: Marcos Legales y Regulatorios:** Como ya se ha descrito previamente en la investigación, Honduras carece de una legislación completa sobre ciberseguridad, pero, es notorio que en la última década se han producido algunos avances en esta dimensión. Ejemplo de ello, son los diferentes decretos publicados en ese periodo (que se detallan en la sección de: Marco Legal de este documento) y las normativas emanadas desde la CNBS o CONSUCOOP.

Tabla 19 *Perfil del estado de ciberseguridad en Honduras. Dimensión 4: Marcos Legales y Regulatorios*

Dimensión 4: Marcos Legales y Regulatorios.				
4.1 Marcos Legales.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Marcos Legislativos para la Seguridad de las TIC.	1	2	Si	**Formativa**
Privacidad, Libertad de Expresión y otros Derechos Humanos en Línea.	1	1	No	Inicial
Legislación Sobre Protección de Datos.	0	1	Si	**Inicial**
Protección Infantil en Línea.	0	1	Si	**Inicial**
Legislación de Protección al Consumidor.	0	1	Si	**Inicial**

Legislación de Propiedad Intelectual.	0	1	Si	**Inicial**
Legislación Sustantiva Contra el Delito Cibernético.	1	2	Si	**Formativa**
Legislación Procesal Contra el Delito Cibernético.	1	1	No	Inicial
4.2 Sistema de Justicia Penal.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Fuerzas del Orden.	1	1	No	Inicial
Enjuiciamiento.	1	1	No	Inicial
Tribunales.	1	1	No	Inicial
4.3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Cooperación Formal.	0	2	Si	**Formativa**
Cooperación Informal.	0	1	Si	**Inicial**

Fuente: Elaboración propia.

– **Dimensión 5: Estándares, Organizaciones y Tecnologías**: Honduras no cuenta con una entidad rectora para dictar la pauta en temas de ciberseguridad. Tampoco existen estándares sumamente detallados. Así que las organizaciones se apegan a marcos internacionales de buenas prácticas para tratar de alinearse y evitar un rezago aún mayor. Una vez más, las entidades financieras son quizás, quienes mayor progreso reflejan en esta dimensión.

Tabla 20 *Perfil del estado de ciberseguridad en Honduras. Dimensión 5: Estándares, Organizaciones y Tecnologías*

Dimensión 5: Estándares, Organizaciones y Tecnologías.				
5.1 Cumplimiento de los Estándares.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Estándares de Seguridad de las TIC.	1	2	Si	**Formativa**
Estándares en Adquisiciones.	1	2	Si	**Formativa**
Estándares en el Desarrollo de Software.	1	1	No	Inicial
5.2 Resiliencia de la Infraestructura de Internet.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Resiliencia de la Infraestructura de Internet.	2	2	No	Formativa
5.3 Calidad del Software.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Calidad del Software.	0	1	Si	**Inicial**
5.4 Controles Técnicos de Seguridad.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**

Controles Técnicos de Seguridad.	0	1	Si	**Inicial**
5.5 Controles Criptográficos.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Controles Criptográficos.	0	2	Si	**Formativa**
5.6 Mercado de Seguridad Cibernética.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Tecnologías de Seguridad Cibernética.	1	2	Si	**Formativa**
Seguro Cibernético.	1	1	No	Inicial
5.7 Divulgación Responsable.				
Componente	**2016**	**2020**	**¿Avance?**	**Etapa**
Divulgación Responsable.	1	1	No	Inicial

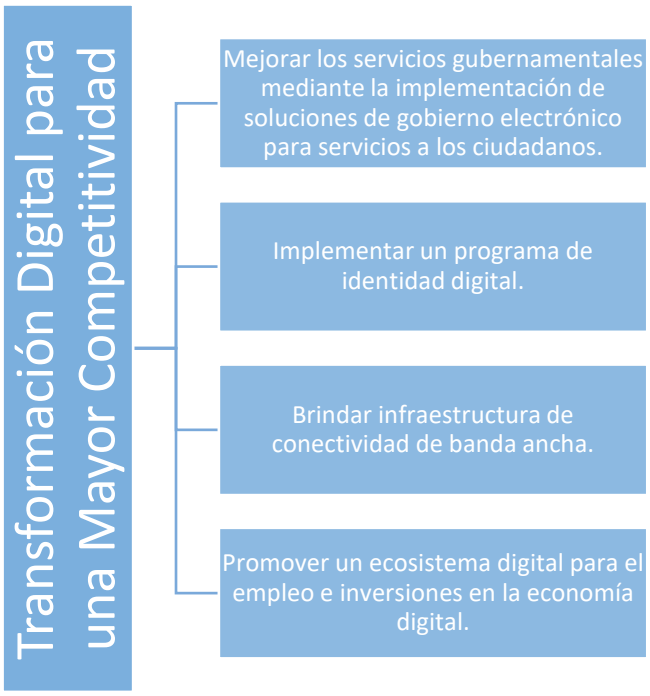
Fuente: Elaboración propia.

Estos datos revelan algunos avances consistentes en materia de ciberseguridad en el periodo comprendido entre el año 2016 y 2020, especialmente en cuanto a: Política y estrategia de seguridad cibernética, cultura cibernética y seguridad, marcos legales y regulatorios y en el apartado de estándares, regulaciones y tecnologías. En el mismo documento (BID; OEA, 2020, p. 117) se detallan algunas de las iniciativas que justifican esa mejora:

– Acuerdo de cooperación con Israel dirigido a fortalecer las capacidades de prevención, defensa y reacción ante eventuales ciberataques a instituciones gubernamentales, administradores de infraestructura y servicios críticos. Los detalles de este se amplían en el apartado: “Marco Legal” de este documento.

– Se logró con el Banco Interamericano de Desarrollo (BID) la aprobación del proyecto HO-L1202: “Transformación Digital para una Mayor Competitividad”, que gira alrededor de 4 ejes temáticos:

Figura 15 *Pilares del Proyecto: "Transformación Digital para una Mayor Competitividad"*



Fuente: Elaboración propia a partir de página web del Proyecto (BID; 2019).

– Firma de acuerdo con México buscando la cooperación entre las Fuerzas Armadas en temas de educación naval y militar, adiestramiento y capacitación, seguridad y defensa nacional, ciberseguridad y ciberdefensa.

– Otras leyes complementarias que se abordaran en el apartado del Marco Legal.

Es evidente que existe una gran brecha por subsanar en todas las categorías evaluadas. Los resultados del estudio sin duda motivaron a las autoridades y en general a la sociedad civil, a buscar estrategias para mejorar. Prueba de ello, es todo el estamento legal y normativo que se ha generado desde el 2022 hasta la fecha. Esto incluye las disposiciones emanadas por la CNBS, CONSUCOOP (que se detallan en el apartado legal), o el Plan Nacional del Gobierno Digital que, dentro de sus pilares, incluye un apartado sobre ciberseguridad que se describe más adelante.

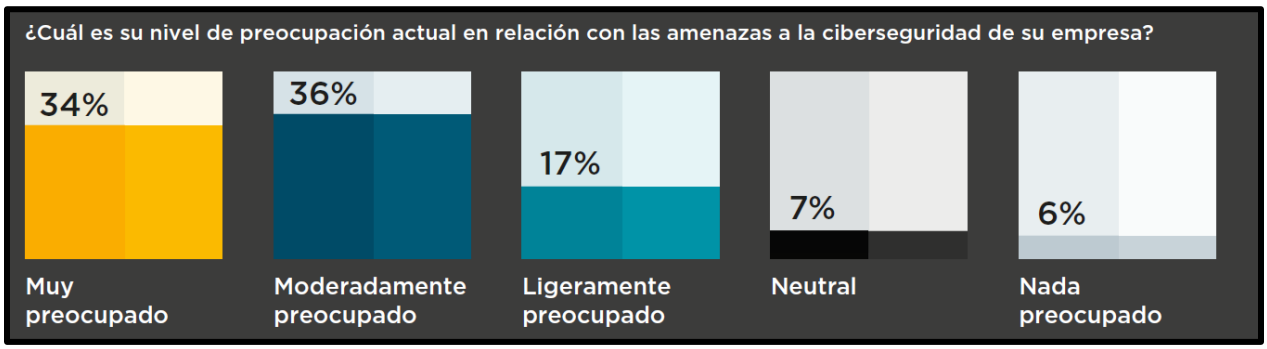
2.2.1.2 HLB: REPORTE DE CIBERSEGURIDAD 2024

La firma consultora HLB con presencia en Honduras, publicó su reporte de ciberseguridad

2024, donde recoge las respuestas de más de 600 líderes de TI de diferentes sectores. De él, rescatamos algunos aspectos.

El primero, está relacionado con los resultados obtenidos en cuanto al nivel de preocupación sobre las amenazas cibernéticas. A continuación, los resultados:

Figura 16 *Resultados de estudio HLB sobre nivel de preocupación de amenazas a la ciberseguridad*



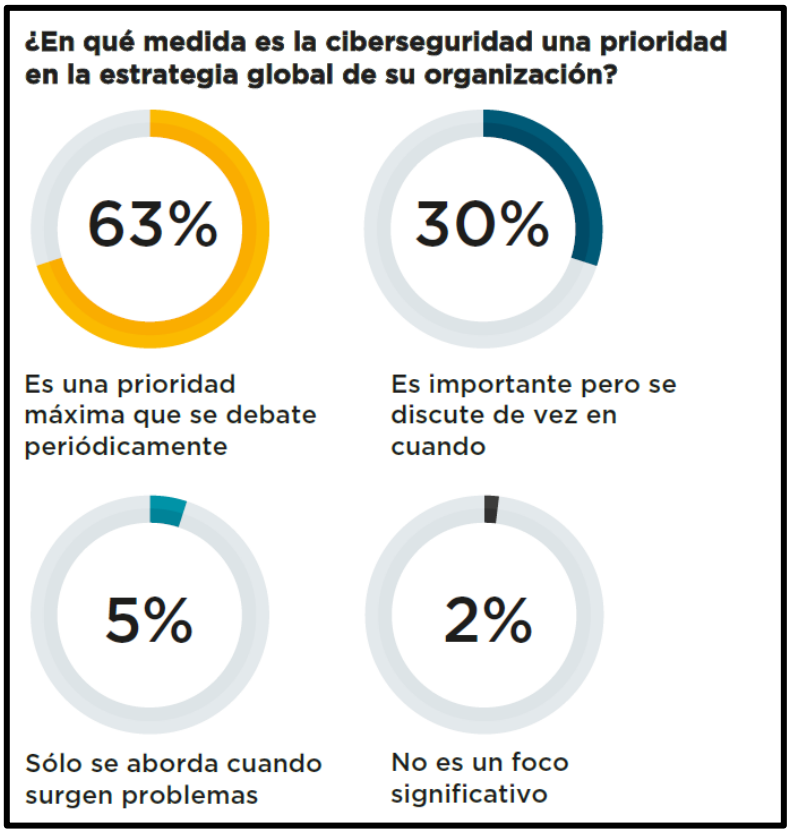
Fuente: Extraído íntegramente desde: Reporte de Ciberseguridad 2024, HLB, p. 5.

De acuerdo con estos resultados, el 70% de los encuestados muestran un nivel de preocupación considerable en cuanto a las amenazas de ciberseguridad, contra un 30% que evidencian una postura opuesta. Esto revela que la mayoría de las organizaciones son conscientes de que existe un riesgo real en las ciber-amenazas y que debe prestárseles la atención debida. Probablemente, ya han experimentado algún tipo de ciberataque, lo que afianza aún más la necesidad de mejorar la postura de ciberseguridad y los controles existentes.

El segundo punto destacable del estudio está relacionado con lo anterior y es en qué medida la ciberseguridad es una prioridad organizativa. Si bien un 63% lo contempla como una prioridad, el resto de los encuestados lo asume como un tema espontaneo lo que evidencia que aún hay camino por recorrer en cuanto a fortalecer el arraigo y apropiación de la ciberseguridad como parte de la cultura organizacional. Es necesario establecer una mayor conexión con los objetivos

estratégicos de la entidad y con las prácticas cotidianas de la misma.

Figura 17 *Resultados de estudio HLB sobre medida de priorización de la ciberseguridad dentro de la estrategia global de la organización*

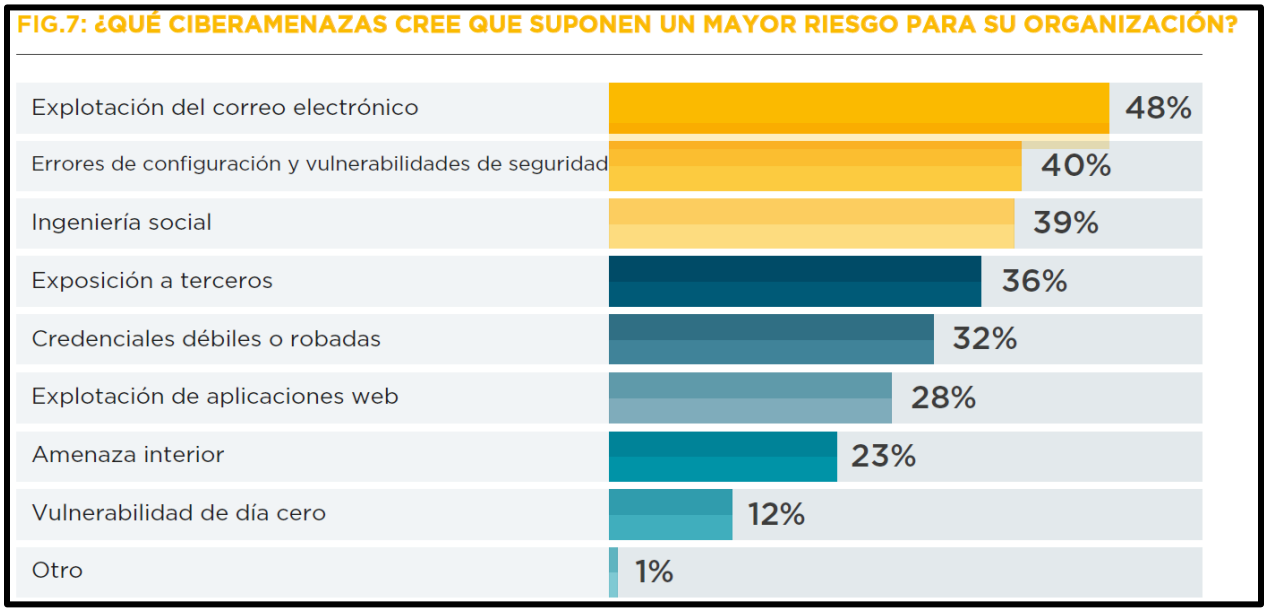


Fuente: Extraído íntegramente desde: Reporte de Ciberseguridad 2024, HLB, p. 15.

En tercer lugar, como parte del estudio se consultó acerca de cuáles son las ciber amenazas que se considera, representan un mayor riesgo para la organización. Estos resultados son llamativos porque se observa cierta dispersión en los mismos, confirmando que los encuestados reconocen que existe la posibilidad de que varias de las opciones se conviertan en puntos potenciales para la explotación de vulnerabilidades. Si bien, el correo electrónico encabeza la lista, se puede observar que la misma está compuesta en buena medida por aspectos directamente relacionados con procesos de configuración, o de gestión de vulnerabilidades.

Figura 18 *Resultados de estudio HLB sobre qué ciber-amenaza suponen un mayor riesgo para*

las organizaciones



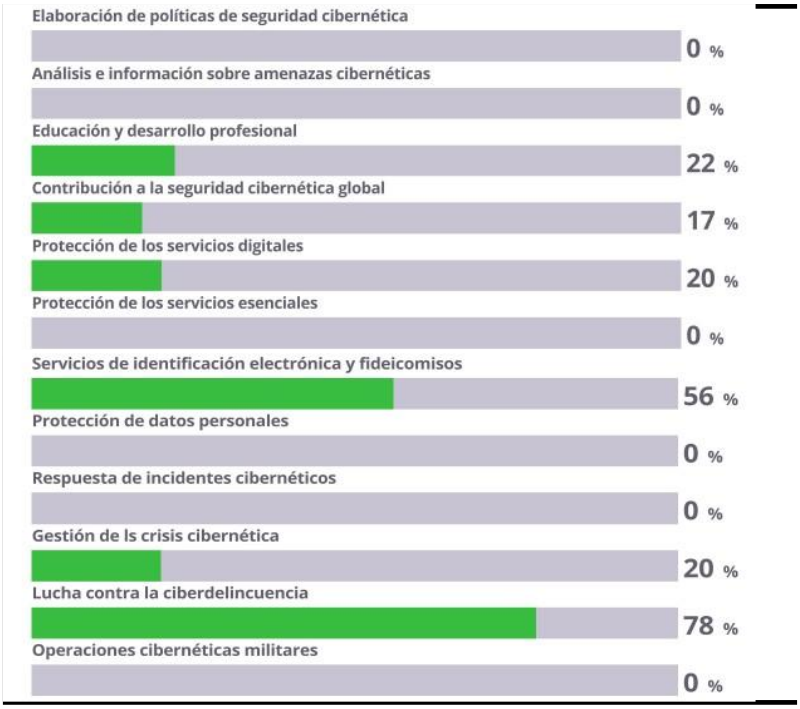
Fuente: Extraído íntegramente desde: Reporte de Ciberseguridad 2024, HLB, p. 13.

Estos últimos resultados resultan valiosos para esta investigación pues la mayoría de esta ciber-amenazas exigen un proceso concreto para su resolución y control. Es aquí donde la propuesta descrita en esta investigación responde a dicha necesidad.

2.2.1.3 ÍNDICE NACIONAL DE CIBERSEGURIDAD (NCSI) EN HONDURAS

Este es un índice que mide cuan preparado esta un país para afrontar amenazas e incidentes de ciberseguridad. El mismo es monitoreado por la Academia de Gobernanza Electrónica (EGA, por sus siglas en inglés), que es una organización consultora enfocada en la transformación digital de las sociedades. Este, evalúa doce capacidades a desarrollar por cada país. Los resultados actuales para Honduras se detallan en la siguiente figura:

Figura 19 *Nivel de cumplimiento de capacidades NCSI por Honduras*



Nota: Elaboración propia a partir de resultados NCSI Honduras, 2022.

Estos resultados no solo evidencian que queda pendiente mucho por hacer en la mayoría de capacidades, sino que también, explican los bajos indicadores generales de Honduras en temas de ciberseguridad, mismos que se condensan en el siguiente cuadro resumen.

Tabla 21 *Indicadores clave NCSI para Honduras*

Indicador	Índice	Posición en el Rankin Global
Índice Nacional de Seguridad Cibernética.	22.08%	122
Índice Global de Ciberseguridad	2%	178
Índice de desarrollo de las TIC	33%	129
Índice de preparación en red	3%	104

Nota: Elaboración propia a partir de resultados NCSI Honduras, 2022.

Los estudios e indicadores presentados muestran resultados de casi 10 años, lo que equivale a 3 periodos de gobierno donde se reflejan muy pocos logros y la clara ausencia de un proyecto de país que permita a Honduras fortalecerse y crecer no de una forma espontánea sino, consistente.

A pesar de ello, se ha tomado a bien recopilar los esfuerzos y resultados de las iniciativas impulsadas hasta la fecha, mismas que comenzamos a detallar a continuación.

2.2.1.4 PLAN NACIONAL DE GOBIERNO DIGITAL 2023-2026

El Gobierno de la Republica de Honduras, reconoce en este documento las falencias existentes en cuanto a avances se refiere en los que constituyen los pilares de la cuarta revolución industrial y, a través de este plan, ha tratado de canalizar sus esfuerzos. Dentro de este existe un apartado enfocado en ciberseguridad que se resume en el siguiente cuadro:

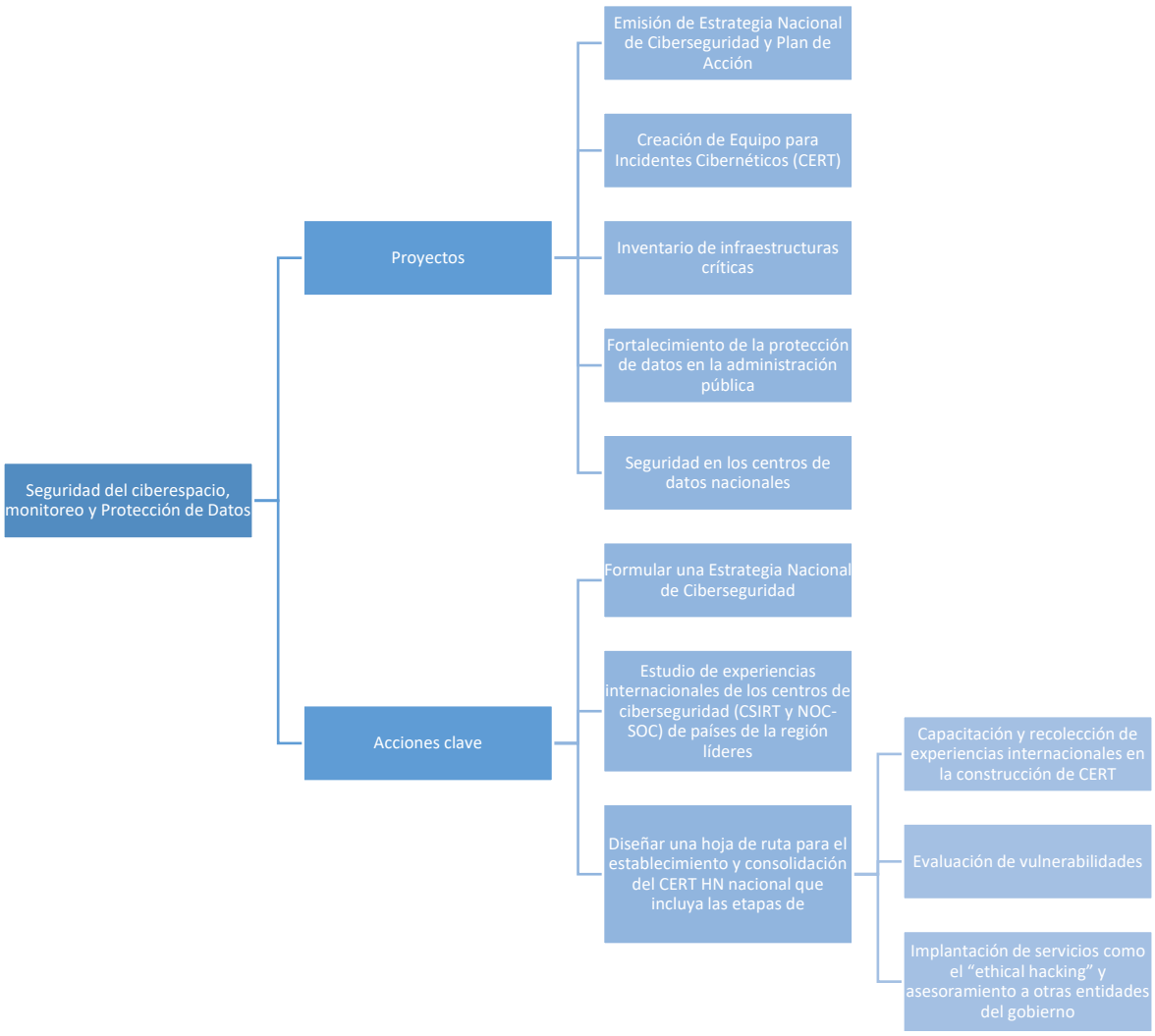
Tabla 22 *Cuadro resumen de Plan Nacional de Gobierno Digital 2023 - 2026 sobre componente ciberseguridad*

Objetivo	Descripción	Metas	Programa
Objetivos en materia de Seguridad en las comunicaciones.	Desarrollar estrategias para mejorar la ciberseguridad nacional y la protección de los activos de la información, así como la coordinación institucional para la prevención y respuesta ante incidentes cibernéticos	➢ Avanzar en el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones -ITU (pasar de una puntuación de 2.20 a 2.75) para finales del cuarto año. ➢ Emisión de la Estrategia Nacional de Ciberseguridad para finales del segundo año. ➢ Formulación y aprobación de la ley de protección de datos y su reglamento para finales del primer año. ➢ Formulación y aprobación de ley de ciberseguridad para finales del segundo año. ➢ Puesta en marcha y plena operatividad de un equipo experto en ciberseguridad para finales del tercer año.	Ciberseguridad: Seguridad del ciberespacio, monitoreo y Protección de Datos

Nota: Adaptado de Plan de Gobierno Digital 2023 – 2026 (Dirección de Gestión por Resultados, 2023, p. 21 – 54).

Del programa de Seguridad del ciberespacio, monitoreo y Protección de Datos, se extraen las iniciativas torales que coinciden con el enfoque de esta investigación.

Figura 20 *Mapa conceptual de Proyectos y Acciones Clave del Programa Seguridad del ciberespacio, monitoreo y Protección de Datos*



Fuente: Elaboración propia a partir de Plan de Gobierno Digital 2023 – 2026 (DIGER, 2023, p. 53).

2.2.1.5 REQUISITO TEMÁTICO DE CIBERSEGURIDAD DEL INSTITUTO DE AUDITORES INTERNOS DE HONDURAS

En febrero de 2025 el Instituto de Auditores Internos (IIA por sus siglas en inglés), emitió un requisito temático enfocado en ciberseguridad que debe ser replicado en todos sus capítulos miembros, incluido el Instituto de Auditores Internos de Honduras. Allí se establece que:

> Este Requisito Temático proporciona un enfoque coherente y exhaustivo para evaluar el diseño y la implementación de la gobernanza, la gestión de riesgos y los procesos de control de la ciberseguridad. Los requisitos representan una base mínima para evaluar la ciberseguridad en una organización (Instituto de Auditores Internos, 2025, p. 2).

En otras palabras, este es un conjunto de requerimientos agrupados en tres grandes categorías: Gobernanza, riesgos y mecanismos de control de ciberseguridad. De ese conjunto de requerimientos y para efectos de este estudio, se resaltan los siguientes aspectos plenamente dirigidos a vulnerabilidades y amenazas:

Tabla 23 *Lista de requerimientos enfocados en la gestión de vulnerabilidades*

Dimensiones	Gobernanza	Gestión de Riesgos	Control
Requerimiento focalizado en gestión de vulnerabilidades-	D. Las partes interesadas se comprometen a debatir y actuar sobre las vulnerabilidades existentes y las amenazas emergentes en el entorno de la ciberseguridad. Entre las partes interesadas se incluyen la Alta Dirección, operaciones, gestión de riesgos, recursos humanos, legal, cumplimiento,	A. Los procesos de evaluación y gestión de riesgos de la organización incluyen la identificación, el análisis, la mitigación y el seguimiento de las amenazas de ciberseguridad y su efecto en la consecución de los objetivos estratégicos.	C. Se establece un proceso para supervisar e informar continuamente sobre las amenazas y vulnerabilidades emergentes en materia de ciberseguridad y para identificar, priorizar y aplicar oportunidades para mejorar las operaciones de ciberseguridad.

	proveedores y otros.		

Nota: Adaptado de Requisito Temático Ciberseguridad (Instituto de Auditores Internos, 2025, p. 2 – 4).

Estos requisitos sin duda añaden una arista interesante ya que no se limitan únicamente a instituciones financieras, sino que su alcance se extiende a cualquier organización en donde exista la figura de un auditor interno. Y en este caso, el Instituto de Auditores Internos de Honduras es quien impulsara la implementación de estas medidas a través de sus miembros.

Hasta aquí se han abordado las generalidades relacionadas con las iniciativas de ciberseguridad en Honduras. Es momento ahora de introducir las regulaciones específicas para el sistema financiero hondureño.

2.2.2 REGULACIONES DEL SISTEMA FINANCIERO HONDUREÑO

Buena parte de los avances obtenidos por Honduras en materia de ciberseguridad, son gracias a las instituciones financieras que operan en el país ya que las mismas, son sometidas al escrutinio constante de sus estándares y procesos, ya sea por entidades supervisoras (como la Comisión Nacional de Bancos y Seguros o el Consejo Supervisor de Cooperativas en Honduras), o por auditorias privadas contratadas para evaluar o certificar a estas organizaciones. Esto se constituye en una fuerza que impulsa al sector financiero a evolucionar y buscar la mejora continua de sus políticas, procesos y prácticas de ciberseguridad. Posteriormente se profundizará en las leyes y normativas existentes en el país, cuando se explore el marco legal, pero, en este apartado se introducirán las normativas que dirigen al sistema financiero, y que están enficadas en la ciberseguridad.

2.2.2.1 NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO (CNBS)

En aras de cumplir con su función como ente rector del sistema financiero hondureño y

conscientes del cambio contante en el dinámico mundo de la tecnología, la Comisión Nacional de Bancos y Seguros actualizo el contenido de la circular No.119/2005 titulada: "Normas para regular la Administración de Tecnologías de la Información y Comunicaciones en las Instituciones del Sistema Financiero" (CNBS, 2005), reemplazándolas con la circular 025/2022 identificada como: "Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio" (CNBS, 2022). A simple vista, parece un cambio superficial de nombres, pero en su contenido se encuentran notables diferencias como lo resume la siguiente tabla.

Tabla 24 *Cuadro comparativo de circulares CNBS sobre componentes de Gobierno de TI, Seguridad de la Información y Ciberseguridad*

Componente	Circular No.119/2005	Circular 025/2022
Objeto de la Norma	ARTÍCULO 1: Regular la administración de las tecnologías de información y comunicaciones utilizadas por las instituciones del sistema financiero; asimismo, regular los servicios financieros y operaciones realizadas por medio de redes electrónicas de uso externo e interno.	ARTÍCULO 1: Regular la gestión de tecnologías de información, continuidad del negocio, seguridad de la información y ciberseguridad en las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros (CNBS), así como a los Grupos Financieros de los cuales éstas formen parte, en función de su tamaño, naturaleza, complejidad de operaciones y perfil de riesgos.
Gobierno de TI	-	ARTÍCULO 5: El Gobierno de TI como parte integral del Gobierno Corporativo, debe establecer la estructura, políticas y procesos garantizando que las TI soportan las estrategias y

		objetivos de la Institución
Seguridad de la Información y Ciberseguridad	SECCIÓN VI: SEGURIDAD DE LA INFORMACIÓN	CAPÍTULO V: DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
Marco de Ciberseguridad		ARTÍCULO 18.- MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar el Marco de Gestión de la Seguridad de la Información y Ciberseguridad, el cual debe incluir al menos los siguientes aspectos: a. La definición de las políticas, procedimientos y controles de seguridad de la información y ciberseguridad; b. La implementación de una metodología de gestión de riesgos de seguridad de la información y ciberseguridad alineada con el Marco de Gobierno de Riesgo de la Institución; c. La designación de una función (área o responsable) encargada de la gestión de seguridad de la información y ciberseguridad; y, d. Un proceso de revisión y actualización para asegurar que la gestión de seguridad de

		la información y ciberseguridad continúa siendo eficaz, de manera que se identifiquen y pongan en práctica modificaciones o mejoras de forma oportuna. Además, debe considerar los activos de información de la Institución Supervisada, así como los vinculados con sus grupos de interés.

Nota: Elaboración propia a partir de circulares No. 119/2005 y 025/2022 de la CNBS.

Sin duda, estas diferencias permiten reconocer los momentos históricos en que fueron emitidas ya que, recogen de alguna manera las necesidades y tendencias vigentes en su época. Por lo tanto, no es de extrañar que mientras una parece más enfocada en el establecimiento de políticas y controles de seguridad de la información, la otra apunta más al gobierno de TI, a la gestión granular de la seguridad de la información y presta especial atención a la ciberseguridad.

Por la temática de esta investigación, es importante profundizar un poco más en el contenido del Capítulo V de las Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio, ya que en este apartado se describen de manera general los requerimientos para las entidades financieras en el país. De especial interés, el articulo 19 donde como ya se detalló en la Definición del Problema, la norma se conecta directamente con el Marco de Ciberseguridad del NIST CSF 2.0.

Figura 21 *Resumen de contenido Capítulo V de la Gestión de Seguridad de la Información y*

Ciberseguridad

Fuente: Elaboración propia a partir de Circular 025 de la Comisión Nacional de Bancos y Seguros (2022, p. 11 – 14).

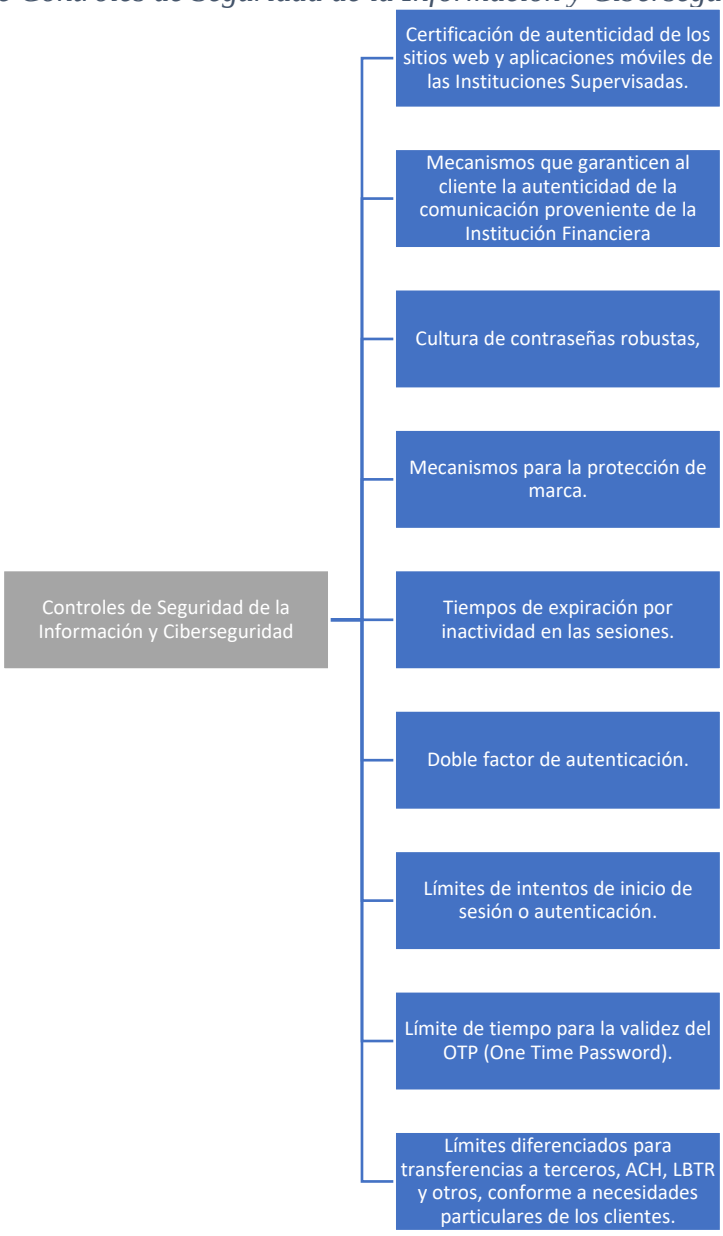
En consecuencia, con esta normativa, se han emitido nuevas resoluciones como, por

ejemplo: Los Lineamientos Mínimos para Prevenir la ocurrencia de Fraudes y Estafas Cibernéticas o la emitida por el Consejo Superior de Cooperativas de Honduras dirigida a las organizaciones bajo su cobertura.

2.2.2.2 LINEAMIENTOS MÍNIMOS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO (CNBS)

En el año 2023 La Comisión Nacional de Bancos y Seguros emitió este conjunto de recomendaciones para las entidades supervisadas titulada: “Lineamientos mínimos para prevenir y mitigar la ocurrencia de fraudes y estafas cibernéticas en contra del usuario financiero” (CNBS, 2023). De entre ellas, merece una mención especial del Articulo 16: Controles de Seguridad de la Información y Ciberseguridad, ya que, si bien no especifica un proceso para gestión de vulnerabilidades, aporta un conjunto de buenas prácticas que contribuyen a resolver algunas de ellas y mejorar la postura de seguridad de las organizaciones. Estas se enlistan a continuación:

Figura 22 *Listado de Controles de Seguridad de la Información y Ciberseguridad*



Fuente: Elaboración propia a partir de Circular 008 de la Comisión Nacional de Bancos y Seguros (2023, p. 8).

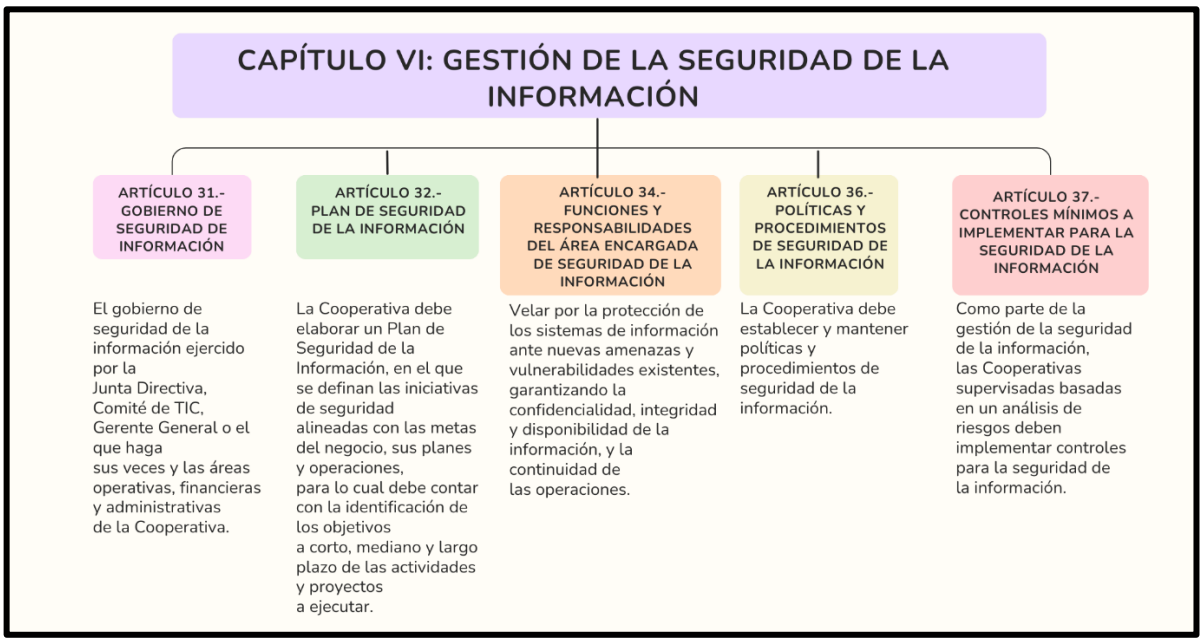
Estas directrices emanadas desde la CNBS, eventualmente son replicadas por todas las demás organizaciones que aglomeran entidades financieras. En esa línea, a continuación, se expone la normativa orientada a las Cooperativas en Honduras.

2.2.2.3 NORMA PARA LA ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Y COMUNICACIONES (TIC) PARA LAS COOPERATIVAS DE AHORRO Y CRÉDITO (CAC´S)

Tal como se describió brevemente en la sección: “Antecedentes del Problema”, en Honduras existe una entidad veedora específica para el sector Cooperativo: El Consejo Superior de Cooperativas (CONSUCOOP). Dicho órgano, tiene la potestad de emitir resoluciones que deben ser cumplidas por las instituciones bajo su cobertura. En tal sentido, la Norma para la Administración de Tecnologías de Información y Comunicaciones (TIC), para las Cooperativas de Ahorro y Crédito (CAC´S), contiene una serie de directrices para las entidades supervisadas. De ella, resumimos el contenido de los artículos del Capítulo VI que competen al alcance de este trabajo de investigación.

Figura 23 *Resumen del Capítulo VI de la Norma para la Administración de Tecnología de Información y Comunicaciones para las Cooperativas de Ahorro y Crédito*



Nota: Elaboración propia a partir de la Norma para la Administración de Tecnología de Información y Comunicaciones para las Cooperativas de Ahorro y Crédito (2023, febrero 1).

El apartado descrito, requiere que las Cooperativas, entre ellas COACEHL, establezcan su

propio Sistema de Gestión de Seguridad de la Información y bajo este, agrupen todas las políticas, procesos y controles. Como se explicó en la sección del macroentorno, la dimensión de ciberseguridad, y la gestión de vulnerabilidades, se encuentran implícitas como parte de este Sistema.

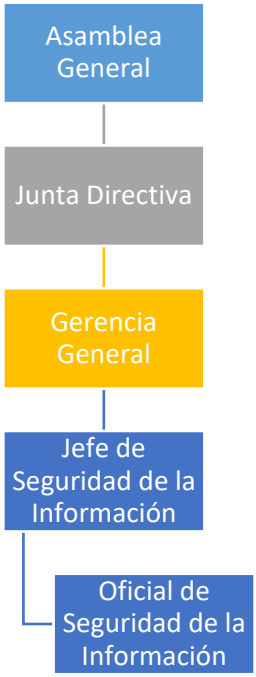
2.2.3 SITUACIÓN ACTUAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

Al ser parte del sector financiero y a su vez, ser reconocida como una de las Cooperativas más sólidas de Honduras, COACEHL es una de las instituciones más prestigiosas en el país. Su segmento objetivo en el mercado son los educadores hondureños, buscando entregarles productos y servicios innovadores que contribuyan a la mejora de su situación económica y calidad de vida.

Dentro del portafolio de los servicios que presta la Cooperativa se encuentran: Cuentas de ahorro, prestamos de usos múltiples, depósitos a plazo fijo, consolidación de deudas y créditos hipotecarios. Adicionalmente, la empresa cuenta con diferentes canales de servicio como ser: Atención en agencias, aplicación web y móvil.

La Cooperativa cuenta con un área dedicada a la seguridad de la información con su respectiva Jefatura. Esta unidad es la encargada del establecimiento de los estándares de ciberseguridad en base a mejores prácticas y lineamientos derivados de leyes o por las directrices del Consejo Nacional Supervisor de Cooperativas (CONSUCOOP). También es el ente interno encargado de velar por el cumplimiento de las estas políticas y procesos dentro de la organización.

Figura 24 *Organigrama del departamento de seguridad de la información*



Nota: Elaboración propia.

El área se encuentra conformada por el jefe y un oficial. Por la naturaleza de sus funciones, este departamento requiere independencia y en tal sentido rinde cuentas directamente a los altos mandos de la organización. En cuanto a los dominios de sus funciones, el equipo se encarga de todo lo relacionado con la seguridad de información, dentro de la cual se encuentra implícita la ciberseguridad.

Por otro lado, si bien la empresa cuenta con su Sistema de Gestión de Seguridad de la Información y con políticas de mantenimiento claramente establecidas, como en la mayoría de instituciones financieras del país, se requiere avanzar en madurez buscando establecer un proceso sólido para la gestión de vulnerabilidades, basado en mejores prácticas. Es por ello que surge la propuesta descrita en esta investigación.

2.2.4 RELEVANCIA DE LA MEJORA DEL PROCESO PARA LA GESTIÓN DE VULNERABILIDADES

En materia de ciberseguridad algunas preguntas clave para cualquier organización son: ¿Cómo se afrontarán las brechas de seguridad en los activos tecnológicos? ¿De qué forma se canalizará toda la documentación e información generada dentro del flujo de actividades o tareas que se ejecutan en la atención de vulnerabilidades?

COACEHL es consciente de los enormes retos que enfrenta como institución financiera en el contexto de la ciberseguridad, no solamente desde una perspectiva normativa y de cumplimiento, sino que también, como entidad responsable de información de la población hondureña sumamente sensible y a su vez, apetecible por los delincuentes. Por ello, busca permanentemente robustecer sus estándares de seguridad y de ahí, la apertura para poder realizar el presente análisis en base al marco NIST CSF 2.0 y así, mejorar su proceso para gestionar vulnerabilidades de una forma sistemática.

2.2.5 IMPACTO Y BENEFICIOS ESPERADOS AL CONTAR CON UN PROCESO PARA GESTIONAR LAS VULNERABILIDADES

Existen muchos beneficios al poseer un proceso para gestionar vulnerabilidades, pero de entre ellos, se enumeran los siguientes:

- **Contribuye a mejorar la postura de ciberseguridad**: Esto debido a que existe claridad sobre las vulnerabilidades existentes en los activos tecnológicos lo que permite planificar de forma estratégica su remediación.

- **Ayuda a cumplir con regulaciones legales y/o normativas**: Muchas instituciones supervisadas deben contar con procesos bien definidos para mantenerse dentro de los parámetros de cumplimiento regulatorio. Adicionalmente, hay países con leyes concretas

cobre ciberseguridad y gestión de vulnerabilidades por lo que tener un proceso claro, sin duda ayudara a cumplir con estos requerimientos.

– **Reduce el riesgo de ciberataques**: Cerrar brechas de vulnerabilidades baja sustancialmente la superficie de ataque y el grado de exposición de una organización. Esto reduce las opciones de los ciber atacantes para explotar debilidades en los activos tecnológicos lo que minimiza el porcentaje de éxito en un intento de escalada.

– **Aumenta los niveles de protección de los datos**: Al atender las vulnerabilidades de forma sistemática, los datos experimentan una mejoría en los niveles de protección y confidencialidad ya que es menos probable que estos sean secuestrados o expuestos sin la debida autorización.

– **Reduce los costos por recuperación**: Remediar oportunamente vulnerabilidades reduce perdidas y costos potenciales por recuperación frente a incidentes. Mucho de este valor se puede invisibilizar hasta que se enfrenta una situación de ataque. Pero cada vez son más los casos que se registran que confirman lo determinante que es una atención de vulnerabilidades preventiva y no correctiva.

– **Facilita la certificación de procesos**: Contar con procesos alineados con estándares como: la familia ISO, COBIT 2019, NIST, entre otros permite a las organizaciones acceder a certificar estos, lo que fortalece la imagen corporativa y confianza de sus clientes.

Para efectos de medición del éxito del proceso se pueden considerar (entre otros), los siguientes indicadores:

– **Total, de activos tecnológicos analizados**: Porcentaje de activos dentro del alcance de los escaneos de las herramientas para la detección de vulnerabilidades.

– **Cantidad de vulnerabilidades identificadas durante el periodo especifico**: Porcentaje de vulnerabilidades existentes en los activos tecnológicos durante el periodo establecido.

– **Número de vulnerabilidades atendidas durante el periodo especifico**: Porcentaje de vulnerabilidades remediadas o mitigadas durante un determinado periodo.

– **Total, de activos atendidos por concepto de remediación de vulnerabilidades**: Porcentaje de activos cuyas vulnerabilidades lograron ser remediadas en un tiempo específico.

2.3 TEORÍAS DE SUSTENTO

2.3.1 LA CUARTA REVOLUCIÓN INDUSTRIAL

Para hablar de una "revolución industrial", sin duda se debe estar frente a una serie de factores que marcan un antes y un después en la historia de la humanidad. El momento clave sin duda como lo describe Joyanes Aguilar (2017, p. 14), sucede en el año 2016 en Davos, Suiza, durante el Foro Económico Mundial donde más de 300 líderes mundiales hicieron acto de presencia. En ese mismo evento, Klaus Schwab, director y fundador de dicho Foro, presentó su libro: "La Cuarta Revolución Industrial", donde expuso formalmente estos rasgos distintivos:

> La Primera Revolución Industrial utilizó agua y la energía a vapor para mecanizar la producción. La segunda utilizó energía eléctrica para producir en masa. La tercera utilizó la electrónica y las tecnologías de la información para automatizar la producción. Ahora se está construyendo una Cuarta Revolución Industrial sobre la tercera, la revolución digital que ha estado ocurriendo desde mediados del siglo pasado. Esta Cuarta Revolución Industrial se caracteriza por una fusión de tecnologías que está difuminando las líneas entre las esferas física, digital y biológica (Schwab, 2020, p. 6).

Al respecto, Useche, Juárez, y Ramírez Restrepo amplían algunos factores por los cuales se considera que actualmente estamos viviendo la cuarta revolución industrial:

> Se denomina revolución dados los cambios abruptos, transcendentales y radicales que impactan en los sistemas económicos, las estructuras sociales e inclusive en el ámbito político, en el cual temas como el gobierno digital, el voto electrónico, las ciudades inteligentes, los ciberataques de

> terroristas inter- nacionales, la masiva participación del electorado en redes sociales y las fake news (noticias falsas) impactan en forma importante el quehacer de los gobernantes (Useche, Juárez y Ramírez Restrepo, 2022, p. 19).

Cada revolución industrial que la humanidad ha experimentado ha sido marcada por una transformación profunda en el tejido político, económico y social. Useche, Juárez, y Ramírez Restrepo (2022) resumen características clave de las revoluciones industriales vividas hasta el momento:

Tabla 25 *Características de las revoluciones industriales*

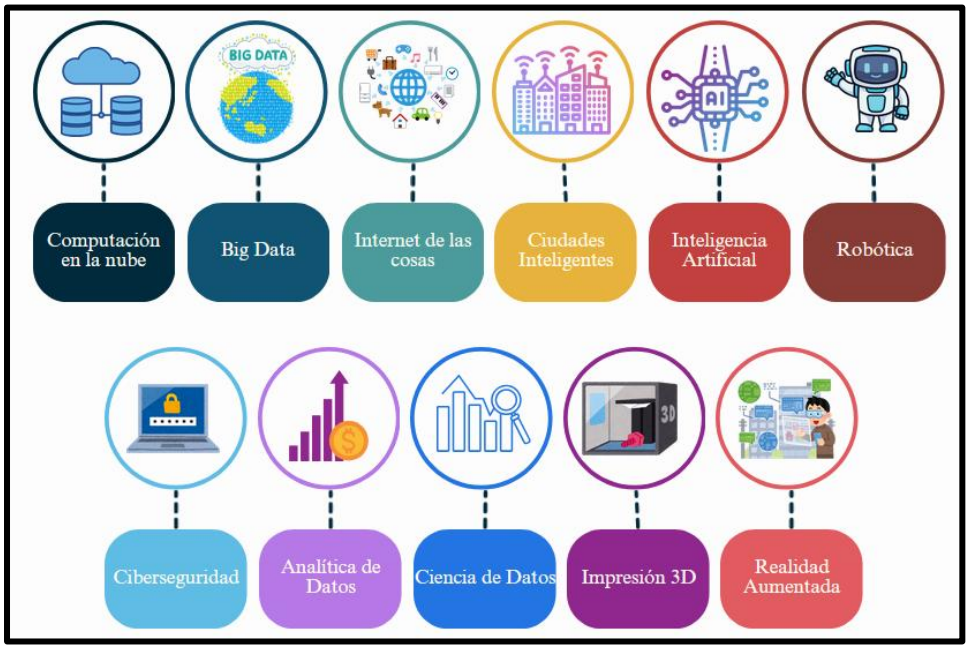
	Primera	**Segunda**	**Tercera**	**Cuarta**
Periodo	1786 – 1840	1870-1914	1945-1970	2000-actual
Fuente energética	Agua-vapor	Petróleo-eléctrica	Electrónica	Limpias-renovables
Tipo de producción	Producción mecanizada	Producción en serie	Producción automatizada	Producción inteligente
Materia prima principal	Hierro	Acero	Datos-información	Conocimientos y nuevos materiales
Invento destacado	El telar mecánico	La cinta transportadora	Microprocesadores	Inteligencia Artificial
Ventaja competitiva	Eficiencia empresarial		Acceso a TIC y capacidad de análisis de datos	Inteligencia emocional
Tipo de economía	Economía industrial		Economía de la información	Economía de la conexión
Transporte y comunicación	Ferrocarriles y telégrafo	Automóviles y radio	Trenes de alta velocidad, Televisión	Movilidad eléctrica, realidad virtual e inteligencia artificial
Hechos destacables	De artesanos y obreros	Desarrollo del transporte. Avances en las telecomunicaciones	Desarrollo del Internet	Se diluyen fronteras entre el mundo físico, digital y

				biológico

Fuente: Useche, Juárez, y Ramírez Restrepo (2022, p. 19 – 20).

Todos estos eventos confirman una cosa: La realidad ha cambiado. Tal como señala Ramírez Barbosa (2024, p. 57), este hito ha traído consigo un fuerte impulso en la tendencia de buscar la eficiencia enfocándose en los pilares fundamentales de la tecnología como lo son: Computación Cuántica, Biotecnología, Big data, Computación en la nube, Robótica, Inteligencia Artificial y por supuesto, la Ciberseguridad. En ese sentido la competitividad juega un rol trascendente pues se constituye en la fuerza que mueve a las entidades a adoptar estas tecnologías (Llanes-Font, Lorenzo-Llanes, 2021, p. 68). Como indica Morera Carballo: "En la actualidad, las empresas son versátiles, se reinventan, enfrentan cambios continuos, son resilientes y manejan enormes volúmenes de datos que no siempre son información" (Morera Carballo, 2022, p. 96). En ese sentido, la siguiente figura refleja lo que hoy constituyen los pilares tecnológicos de la Cuarta Revolución Industrial.

Figura 25 *Los Pilares Tecnológicos de la Cuarta Revolución Industrial*



Nota: Elaboración propia (Joyanes Aguilar, 2017, XVII – XVI).

Toda esta innovación no ha venido sola. Como indica Moya (2023): “El avance de la tecnología, la automatización y la conectividad han creado un mundo interconectado en el que la información es la nueva moneda. Sin embargo, con esta revolución también ha surgido una nueva amenaza: la ciberseguridad” (Moya, 2023, p. 7). A ello se suma lo mencionado por Beltrán y Sevillano (2021): “La transformación digital en la industria para incrementar la eficiencia y la productividad aumentará el número de dispositivos conectados a la red industrial y la superficie de ataques cibernéticos”, (Beltrán y Sevillano, 2021, p. 58).

Al profundizar en este marco conceptual, es evidente entonces que la ciberseguridad es una secuela de la oleada impulsada por la Cuarta Revolución Industrial, que con su inercia ha derivado en nuevas tendencias dentro de los campos del conocimiento y a su vez, ha abierto el camino para la creación y/o actualización de estándares vigentes, tales como la familia ISO 27000 o el mismo NIST.

Adicionalmente, con lo explicado hasta ahora es claro que las entidades comerciales principalmente, son impulsadas a implementar las tendencias de la Cuarta Revolución Industrial por temas de competitividad ya que con la transformación digital buscan mejorar sus procesos y ser más ágiles. Sin embargo, como se ha detallado a lo largo de esta investigación, la introducción de tecnología requiere también de una adecuada gestión de vulnerabilidades.

2.3.2 LAS NORMAS ISO DE LA CALIDAD

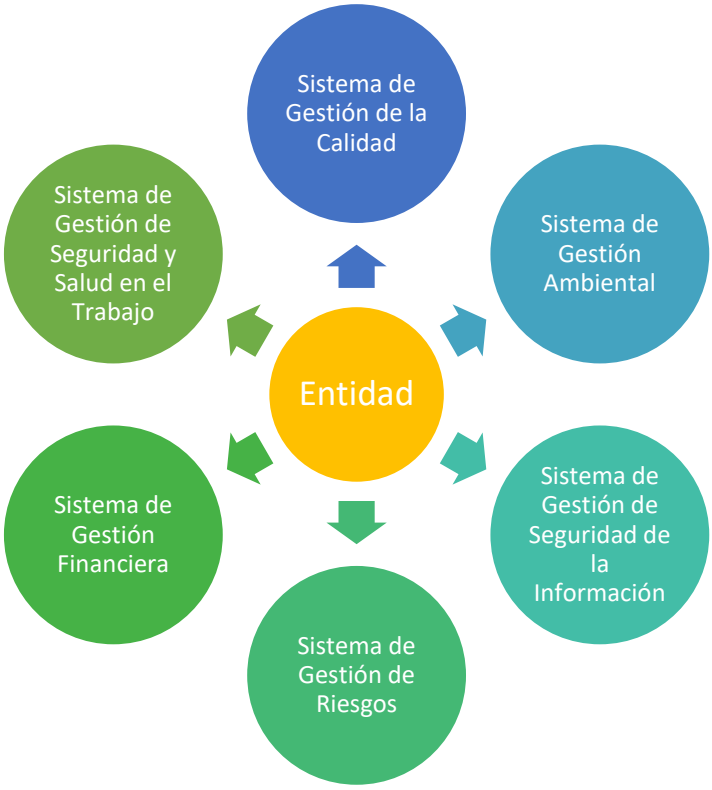
Como se ha descrito previamente, los movimientos de las revoluciones industriales han impulsado cambios en los modelos y paradigmas que adoptan las sociedades y, en la búsqueda de la mejora continua las concepciones de la calidad también han ido evolucionando. Arciniegas y González (2016) explican: “La temática de la calidad ha pasado por toda una serie de concepciones, la mayoría de ellas basadas en momentos coyunturales, y que finalmente fueron

pasando de moda por la falta de soporte científico y de aplicación universal" (Arciniegas y González, 2016, p. 29). Sin embargo, en la actualidad este es un asunto sumamente relevante para las entidades, fruto en parte del trabajo realizado por estas organizaciones (por sus siglas en inglés): Comisión Electrónica Internacional (IEC), Unión Internacional de Telecomunicaciones (ITU) y la Organización Internacional de Normalización (ISO). En particular, sobre esta última, Camisón, González Cruz y Cruz (2006) señalan:

> Sus antecedentes se encuentran en la International Federation of the National Standardizing Associations (ISA), constituida en 1926 y cuya actividad finalizo en 1942. Tras la segunda guerra mundial, la misión de ISA fue asumida por el Comité de Coordinación de Normas de la ONU, embrión de la ISO. El lanzamiento definitivo tuvo lugar en 1946, cuando delegados de 25 naciones decidieron en Londres crear una nueva organización internacional con el propósito de «facilitar la coordinación y unificación internacional de los estándares industriales», en todos los campos excepto el electrotécnico y el electrónico que son competencia del IEC. Su propósito es la promoción mundial del desarrollo de la estandarización y de otras actividades vinculadas, a fin de facilitar el comercio internacional eliminando las barreras técnicas basadas en la certificación (Camisón, González Cruz y Cruz 2006, p. 16).

Esto explica por qué la familia de Normas ISO, es uno de los marcos de referencia más utilizados, ya que permiten establecer sistemas robustos de gestión que se integran entre sí y conectan con la visión, misión, políticas, objetivos y estrategias organizacionales como se ejemplifica en la siguiente figura.

Figura 26 *Ejemplo de Sistemas de Gestión basados en la familia de Normas ISO*



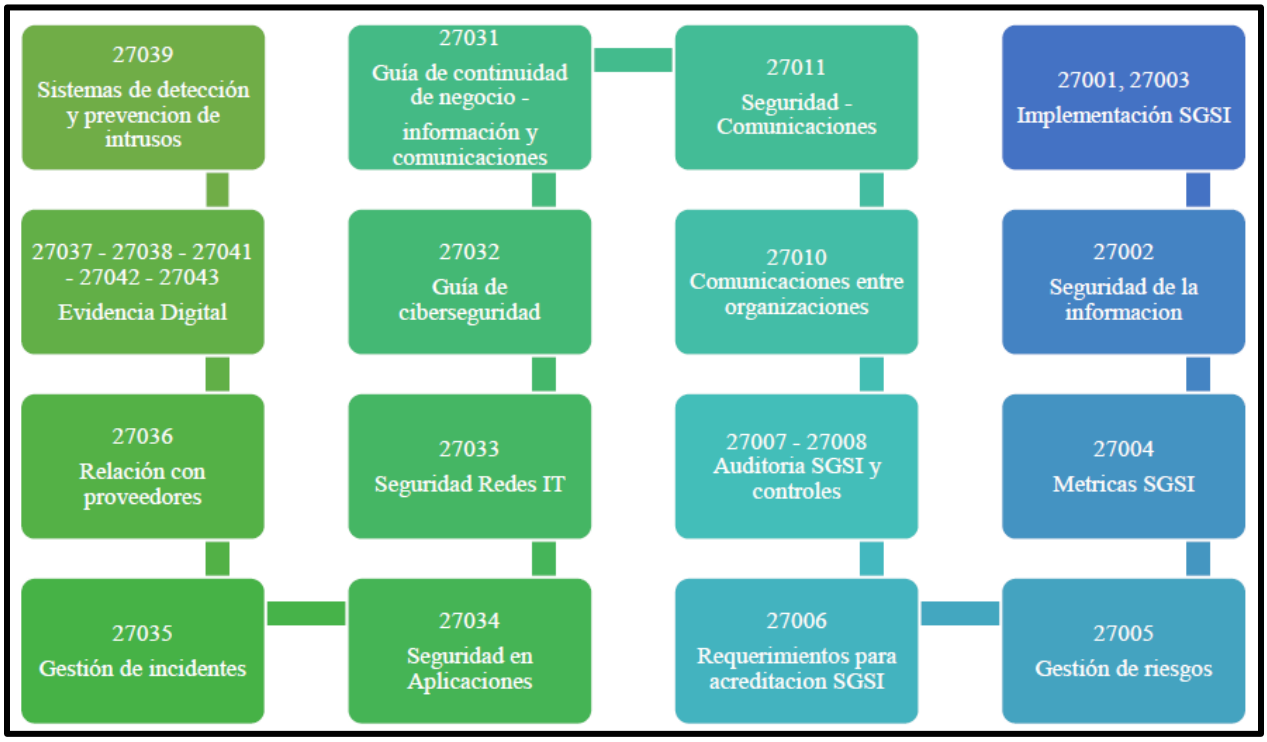
Nota: Elaboración propia.

Un aspecto importante al que contribuyen las normas ISO es a lograr la adopción y estandarización de buenas prácticas. Uribe Macías (2011) establece que:

> Estas normas son un criterio, patrón o modelo a seguir; son reglas que tienen por finalidad definir las características que debe poseer un producto o servicio y la compatibilidad que éstos deben tener para poder ser usados e implementados a nivel internacional, aunque se debe tener en cuenta que las normas desarrolladas por ISO son voluntarias y de libre adopción (Uribe Macías, 2011, p. 45).

Dentro de la familia de normas ISO 27000, existen algunos lineamientos orientados a establecer el Sistema de Gestión de Seguridad de la Información (ISO 27001) o las Directrices de Ciberseguridad para la seguridad en Internet (ISO 27032), entre otros. Dichos estándares pueden integrarse con otros marcos como ser NIST o COBIT 2019 para fortalecer algunas dimensiones de la gestión de vulnerabilidades en los activos tecnológicos.

Figura 27 *Estructura Norma ISO 27000*



Fuente: Presentación íntegra y completa obtenida del Proyecto de Trabajo de Grado titulado: Guía para la implementación de la norma ISO 27032 (Guzmán Solano, 2019, p. 23).

Se introduce esta teoría como parte de esta investigación porque como se ha explicado, hay un vínculo directo y una dependencia entre la seguridad de la información y la ciberseguridad, dentro de la cual se rige la gestión de vulnerabilidades.

Dentro de la ISO 27001:2022 existe el anexo 12.6 titulado: 12.6 Gestión de la vulnerabilidad técnica. Dentro de sus controles de riesgo establece la necesidad de definir un proceso para gestionar las vulnerabilidades: “Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados” (ISO 27001, Anexo 12, *s.f.*). El mismo se amplía en el numeral 8.8 de la ISO 27002:2022. Este control se utiliza más adelante ara evaluar el proceso de gestión de vulnerabilidades vigente en COACEHL.

En resumen, todo este conjunto de guías puede contribuir a robustecer paulatinamente tanto el Sistema de Gestión de Seguridad de la Información como los diferentes procesos existentes en la organización.

2.3.3 GOBIERNO DE TI

En la actualidad, los marcos de referencia reconocen la importancia de conectar los objetivos y planes de tecnología con los objetivos estratégicos de la entidad. Fernández Sánchez (2012) nos dice que:

> El gobierno de TI es el alineamiento estratégico de las TI con la organización de forma tal que se consigue el máximo valor de negocio por medio del desarrollo y mantenimiento de un control y responsabilidades efectivas, gestión del desempeño y gestión de riesgos de TI (Fernández Sánchez, 20212, p. 21).

En otras palabras, el Gobierno de TI busca erradicar el posible vacío existente entre los esfuerzos del equipo de tecnología y la vida productiva de las organizaciones. Sobre ello, Alanis (2021) señala:

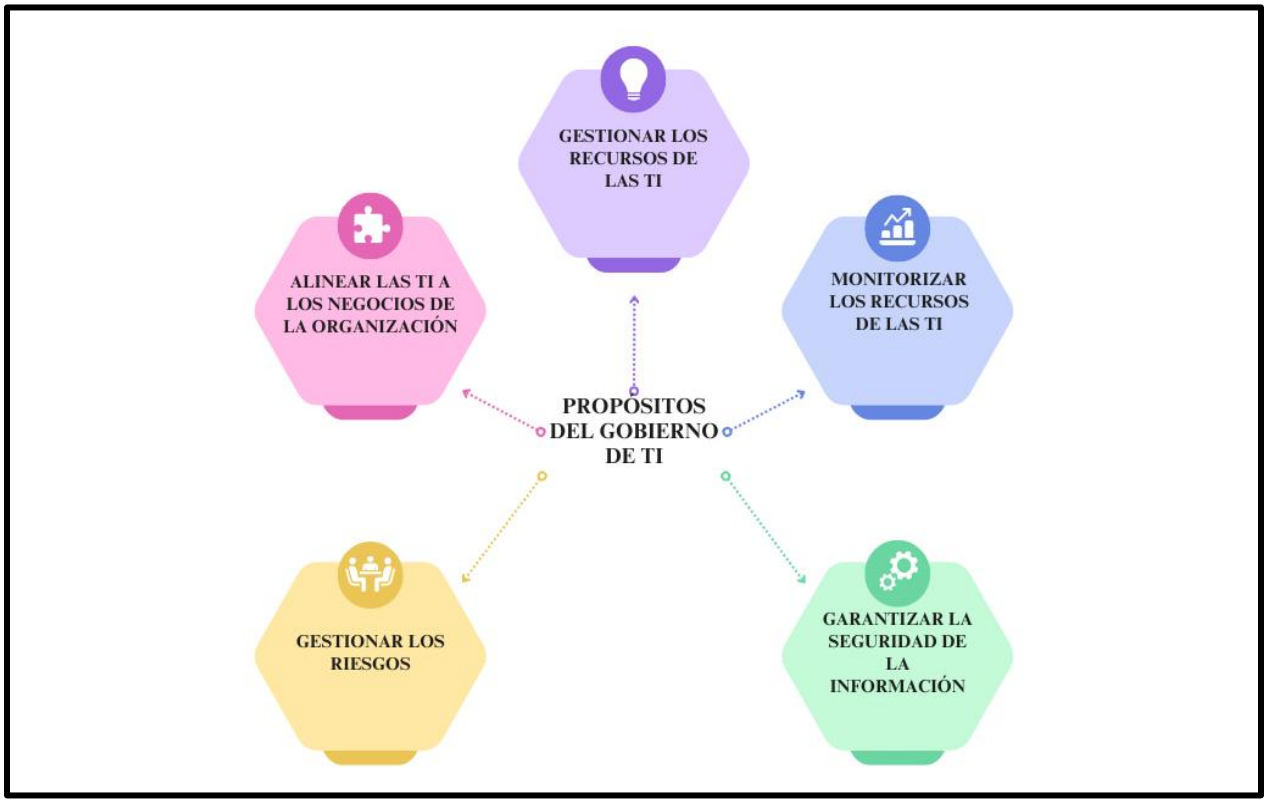
> El Gobierno Corporativo de TI consiste en la definición de las estructuras y procesos organizacionales que aseguran que las funciones de TI en una empresa apoyen y extiendan los objetivos estratégicos de la organización, promoviendo el mejor aprovechamiento de las tecnologías para los fines que la empresa requiera (Alanis, 2021, p. 67).

En ese sentido, el Gobierno de TI no solamente busca encausar de forma estratégica las inversiones en tecnología, sino que también, procura establecer todo el marco necesario para garantizar su buen uso. Esta perspectiva transversal coincide con lo expuesto por Joyanes Aguilar (2015):

> Desde un punto de vista formal, se entiende por gobierno TI (IT Governance), el conjunto de acciones que realiza el departamento de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficaz en respuesta a requisitos regulatorios, operativos o del negocio. Constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que las TI ayuden y faciliten el desarrollo de los objetivos estratégicos definidos (Joyanes Aguilar, 2015, p. 524).

De acuerdo con Gaseta, Motta y Boca Picollini (s.f., p. 19), el Gobierno de TI debe cumplir al menos con los siguientes propósitos:

Figura 28 *Propósitos del Gobierno de TI*



Nota: Elaboración propia.

Como se puede observar, existe un vínculo directo entre el Gobierno de TI y la Gestión de la Seguridad de la Información. Dicha relación se hereda entonces al marco de ciberseguridad y, en consecuencia, a la gestión de vulnerabilidades.

2.4 METODOLOGÍAS

2.4.1 MARCO DE SEGURIDAD CIBERNÉTICA DEL NIST CSF 2.0

Como se ha descrito previamente, NIST CSF 2.0 en una metodología completa para gestionar la ciberseguridad. Para los fines de este trabajo el marco tendrá los siguientes usos:

– Evaluar la situación actual de ciberseguridad de COACEHL en base a las funciones: Gobernar, identificar, detectar y responder.

– Desarrollar el perfil actual y perfil objetivo para identificar las brechas y establecer

puntos de mejora.

– Conformar un proceso para la gestión de vulnerabilidades considerando algunas de las funciones del núcleo.

Los dos primeros aspectos se emplean por medio de dos instrumentos temáticos y el tercero, forma parte de la propuesta descrita en el Capítulo VI.

2.4.2 ISO 27002:2022 CONTROL TECNOLÓGICO 8.8: GESTIÓN DE LA VULNERABILIDAD TÉCNICA

ISO 27002:2022 cuenta con una sección con los controles específicos del estándar por áreas. Para esta investigación es de interés el Control 8.8: Gestión de la vulnerabilidad técnica, cuyo objetivo es evitar la explotación de las mismas.

A partir de Vásquez Vergara (2024) se ha confeccionado el siguiente cuadro resumen con la composición de los 93 controles que evalúa la norma ISO 27002.

Tabla 26 *Tabla de distribución de controles en la ISO 27002*

Categoría	Descripción	Controles
Categoría 1: Mecanismos de control organizacionales.	El fin esencial de estos controles es proporcionar un plan de administración de aseguramiento de la data. Se fija principalmente en: establecer estructuras y prácticas organizativas; definir directrices adecuadas; fomentar una cultura de aseguramiento de la información; asegurar la obediencia de las leyes; gestión activa de riesgos; adaptarse a los cambios; Fomentar la necesidad frecuente de la mejora continua. .	37
Categoría 2: Mecanismos de control de personas.	Se reconoce la participación clave del componente humano en el aseguramiento de la data. Se enfocan en: sensibilización y alineación del personal; Establecer prácticas laborales seguras; definición clara de deberes en el contrato; Evaluación oportuna y aprendizaje sobre incumplimientos. Los protocolos de terminación garantizan una seguridad continua.	8

Categoría 3: Mecanismos de control físicos.	El aseguramiento no es únicamente digital y las autoridades administrativas son responsables de una protección concreta. Esto incluye: Protección de activos y suministros con el cuidado de dispositivos de almacenamiento; Aseguramiento físico; Medidas preventivas contra desastres naturales o imaginarios.	14
Categoría 4: Mecanismos de control tecnológicos.	Estos controles se centran en la infraestructura técnica y cubren: procesos de seguridad desde el diseño del sistema hasta el despliegue mismo; Manutención y configuración de redes; Supervisión continua; Examinación y pruebas frecuentes programadas; Operaciones de revisión y recobro de eventos.	34

Fuente: Elaboración propia a partir de ISO 27002:2022 (s.f.). y Vásquez Vergara (2024, p. 8 – 9).

Esta metodología se utilizará como una segunda validación para identificar las oportunidades de mejora dentro del proceso de gestión de vulnerabilidades en COACEHL.

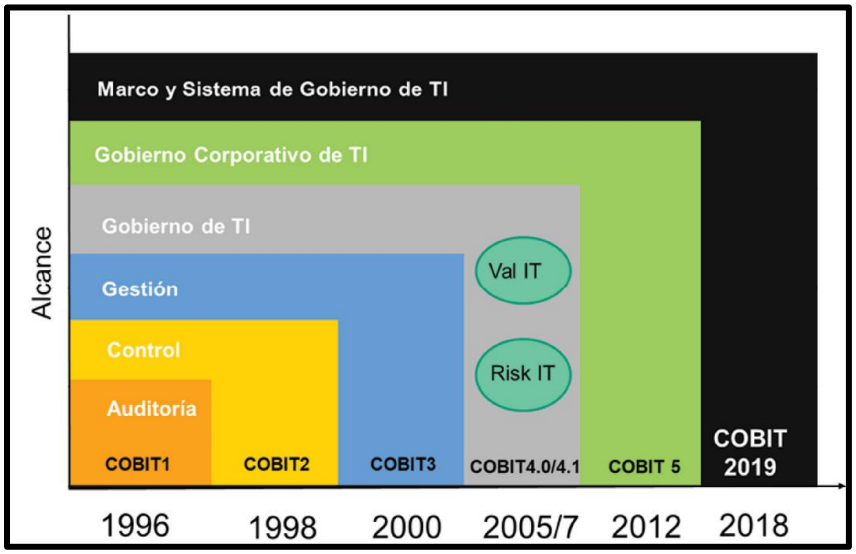
2.4.3 COBIT 2019

Este sin duda es uno de los marcos referentes para Tecnologías de la Información, no solo por lo que aporta por sí mismo, sino que también por la flexibilidad para acoplarse con otros estándares del mercado. Sobre COBIT Joyanes Aguilar (2015) nos dice:

> COBIT nació como una herramienta de auditoría de sistemas de información, pero ha crecido considerablemente, también incluye componentes de seguridad y sobre todo de gobierno TI. Independientemente de la realidad tecnológica de cada caso concreto, COBIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de "mejores prácticas" para la seguridad, la calidad, la eficacia y la efectividad en TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización (Joyanes Aguilar, 2015, p. 531).

Esto es resultado del proceso de madurez que, con el tiempo, el mismo estándar ha ido experimentando lo que le ha permitido ampliar y perfeccionar su alcance tal y como se ejemplifica en la siguiente figura:

Figura 29 *Evolución del marco COBIT*



Fuente: Piattini Velthuis y Ruiz González (2020, p. 103).

El core (núcleo) de COBIT 2019 se compone por objetivos de gobierno y objetivos de gestión. A continuación, la siguiente tabla para resumir su estructura general:

Tabla 27 *Cuadro resumen Modelo Core de COBIT 2019*

Tipo	Dominio	Descripción	Objetivo
Objetivos de Gobierno	Evaluar, Dirigir y Monitorizar (EDM en inglés)	En este dominio, el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia.	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
Objetivos de Gestión	Alinear, Planificar y Organizar (APO)	Aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología	APO01—Gestionar el marco de gestión de I&T
			APO02—Gestionar la estrategia
			APO03—Gestionar la arquitectura empresarial
			APO04—Gestionar la innovación
			APO05—Gestionar el portafolio
			APO06—Gestionar el presupuesto y los costes

			APO07—Gestionar los recursos humanos
			APO08—Gestionar las relaciones
			APO09—Gestionar los acuerdos de servicio
			APO10—Gestionar los proveedores
			APO11—Gestionar la calidad
			APO12—Gestionar el riesgo
			APO13—Gestionar la seguridad
			APO14—Gestionar los datos
	Construir, Adquirir e Implementar (BAI)	Se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.	BAI01—Gestionar los programas
			BAI02—Gestionar la definición de requisitos
			BAI03—Gestionar la identificación y construcción de soluciones
			BAI04—Gestionar la disponibilidad y capacidad
			BAI05—Gestionar el cambio organizativo
			BAI06—Gestionar los cambios de TI
			BAI07—Gestionar la aceptación y la transición de los cambios de T
			BAI08—Gestionar el conocimiento
			BAI09—Gestionar los activos
			BAI10—Gestionar la configuración
			BAI11—Gestionar los proyectos
	Entregar, Dar Servicio y Soporte (DSS)	Aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad.	DSS01—Gestionar las operaciones
			DSS02—Gestionar las peticiones y los incidentes de servicio
			DSS03—Gestionar los problemas
			DSS04—Gestionar la continuidad
			DSS05—Gestionar los servicios de seguridad
			DSS06—Gestionar los controles de procesos de negocio
	Monitorizar, Evaluar y Valorar (MEA)	Aborda la monitorización del rendimiento y la conformidad de I&T con los objetivos de Rendimientos internos, los objetivos de control interno y los requisitos externos	MEA01—Gestionar la monitorización del desempeño y la conformidad
			MEA02—Gestionar el sistema de control interno
			MEA03—Gestionar el cumplimiento de los requisitos externos
			MEA04—Gestionar el aseguramiento

Fuente: Elaboración propia a partir de ISACA (2018, p. 12).

Para esta investigación algunos insumos de COBIT 2019 se conectarán con el Marco de Ciberseguridad del NIST CSF 2.0 para formular una propuesta robusta orientada a la gestión de vulnerabilidades en COACEHL.

2.5 INSTRUMENTOS UTILIZADOS

2.5.1 HERRAMIENTAS DEL MARCO DE SEGURIDAD CIBERNÉTICA DEL NIST CSF 2.0

Como ya se ha mencionado, para los propósitos de este trabajo de investigación, el Marco de Seguridad Cibernética del NIST CSF 2.0 cumplirá con una doble función: La primera será para poder identificar las oportunidades de mejora en el proceso existente de gestión de vulnerabilidades de COACEHL. Y la segunda, refactorizando algunas de sus funciones para la nueva propuesta de dicho proceso. A continuación, describimos un poco más a detalle los instrumentos usados para evaluar la situación actual y el estado objetivo:

– **Componentes del núcleo**: Los componentes del marco tomados en consideración son: Gobernar, identificar, detectar y responder.

– **Matriz de perfilamiento organizativo NIST**: Es un instrumento que permite evaluar componentes del núcleo desde dos visiones: La situación actual y el estatus deseado. El mismo también hace uso del modelo de madurez para identificar el nivel alcanzado por el componente.

– **Niveles del CSF**: Estos niveles permiten medir la madurez de una categoría o subcategoría. A continuación, los parámetros definidos por el marco:

Tabla 28 *Niveles del Marco de Seguridad Cibernética (CSF) del NIST 2.0*

Niveles	Gobernanza de riesgos de seguridad cibernética	Gestión de riesgos de seguridad cibernética

Nivel 1: Parcial.	La aplicación de la estrategia de riesgos de seguridad cibernética de la organización se gestiona de manera ad hoc. La priorización es ad hoc y no se fundamenta formalmente en los objetivos o el entorno de amenazas.	Existe una conciencia limitada sobre los riesgos de seguridad cibernética a nivel organizativo. La organización implementa la gestión de riesgos de seguridad cibernética de forma irregular, caso por caso. Es posible que la organización no disponga de procesos que permitan compartir información en materia de seguridad cibernética dentro de la organización. La organización desconoce generalmente los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y servicios que adquiere y utiliza.
Nivel 2: Conocimiento de los riesgos	Las prácticas de gestión de riesgos son aprobadas por la gerencia, pero pueden no estar establecidas como política para toda la organización. La priorización de las actividades de seguridad cibernética y las necesidades de protección se basan directamente en los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocio/misión.	Existe una conciencia sobre los riesgos de seguridad cibernética a nivel organizacional, pero no se estableció un enfoque de toda la organización para gestionar los riesgos de seguridad cibernética. La consideración de la seguridad cibernética en los objetivos y programas de la organización puede ocurrir en algunos, pero no en todos los niveles de la organización. La evaluación del riesgo cibernético de los activos organizativos y externos se produce, pero no suele ser repetible o recurrente. La información sobre seguridad cibernética se comparte dentro de la organización de manera informal. La organización es consciente de

		los riesgos de seguridad cibernética asociados con sus proveedores y los productos y servicios que adquiere y utiliza, pero no actúa de manera coherente o formal en respuesta a esos riesgos.
Nivel 3: Repetible	Las prácticas de gestión de riesgos de la organización se aprueban y expresan formalmente como política. Las políticas, los procesos y los procedimientos informados sobre los riesgos se definen, se aplican según lo previsto y se revisan. Las prácticas de seguridad cibernética de la organización se actualizan periódicamente sobre la base de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos de negocio/misión, las amenazas y el panorama tecnológico.	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de seguridad cibernética. La información sobre seguridad cibernética se comparte de forma rutinaria en toda la organización. Existen métodos consistentes para responder de manera efectiva a los cambios en los riesgos. El personal dispone de los conocimientos y habilidades necesarios para desempeñar las funciones y responsabilidades que le fueron asignadas. La organización supervisa de forma coherente y precisa los riesgos de seguridad cibernética de los activos. Los altos directivos de seguridad cibernética y no cibernética se comunican regularmente en relación con los riesgos de seguridad cibernética. Los directivos se aseguran de que la seguridad cibernética se considera a través de todas las líneas de operación en la organización. La estrategia de riesgos de la organización recibe información sobre los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y

		servicios que adquiere y utiliza. El personal actúa formalmente sobre esos riesgos a través de mecanismos como acuerdos escritos para comunicar los requisitos básicos, estructuras de gobernanza (por ejemplo, consejos de riesgos), y aplicación y supervisión de políticas. Estas acciones se aplican de forma coherente y conforme a lo previsto, y se supervisan y revisan continuamente.
Nivel 4: Adaptable	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de seguridad cibernética que utiliza políticas, procesos y procedimientos basados en los riesgos para hacer frente a posibles eventos de seguridad cibernética. La relación entre los riesgos de seguridad cibernética y los objetivos de la organización se entiende claramente y se tiene en cuenta a la hora de tomar decisiones. Los directivos supervisan los riesgos de seguridad cibernética en el mismo contexto que los riesgos financieros y otros riesgos organizativos. El presupuesto de la organización se basa en la comprensión del entorno de riesgo actual y previsto y en la tolerancia al riesgo. Las unidades de negocio implementan la visión ejecutiva y analizan los riesgos a nivel de sistema en el contexto de las tolerancias de riesgo de la organización. La gestión de riesgos de seguridad cibernética forma parte de la cultura	La organización adapta sus prácticas de seguridad cibernética basándose en actividades de seguridad cibernética anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos. A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de seguridad cibernética, la organización se adapta activamente a un panorama tecnológico cambiante y responde de manera oportuna y eficaz a las amenazas sofisticadas en evolución. La organización utiliza información en tiempo real o casi real para comprender los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y servicios que adquiere y utiliza, y actuar de forma coherente al respecto. La información sobre seguridad cibernética se comparte

	organizativa. Evoluciona a partir de la concienciación sobre las actividades previas y la concienciación continua sobre las actividades en los sistemas y redes de la organización. La organización puede tener en cuenta de forma rápida y eficaz los cambios en los objetivos de negocio/misión en la forma de abordar y comunicar el riesgo.	constantemente en toda la organización y con terceros autorizados.

Fuente: Niveles del CSF (NIST, 2024, p. 26 – 28).

Para recopilar los datos de las funciones, categorías y subcategorías tomadas en consideración se emplearán instrumentos metodológicos como la entrevista, notas de campo, la observación, revisión documental etc. Luego, se procederá a evaluar los resultados para determinar el nivel de madurez en base a esta tabla.

2.5.2 HERRAMIENTAS DE LA ISO 27002:2022

Muchas de las herramientas son comunes entre el Marco de Ciberseguridad del NIST CSF 2.0, el Anexo 12.6.1 de la ISO 27001:2022 y el apartado del Control Tecnológico 8.8: Gestión de vulnerabilidades técnicas de la ISO 27002. De estos últimos, se incorporan de diferente forma, los siguientes controles a validar dentro de los instrumentos a utilizar:

Tabla 29 *Controles específicos a evaluar sobre la Gestión de vulnerabilidades técnicas ISO 27002*

Control Tecnológico	Control específico	A validar
8.8 Gestión de vulnerabilidades técnicas.	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso.	- Se actualiza con frecuencia el inventario de activos. - Se utilizan herramientas de exploración de vulnerabilidades adecuadas a las tecnologías actuales.

		- Se reciben informes sobre vulnerabilidades de fuentes internas y externas.
	Se deben evaluar las vulnerabilidades técnicas.	- Se analizan y verifican los informes para determinar el tipo de actividad de respuesta necesaria.
	Se deben tomar las medidas apropiadas.	- Se planifican las actividades de remediación de vulnerabilidades. - Se utilizan únicamente fuentes legitimas de actualización (internas o externas). - Se realizan actualizaciones o remediaciones en ambientes de prueba previo a liberarlas en ambientes productivos. - Se mantiene un registro de auditoria para todos los pasos dados en la gestión de vulnerabilidades técnicas.

Nota: Elaboración propia a partir de ISO 27002:2022 (s.f.).

A partir de este cuadro, se elaborará una lista de verificación (Anexo 3) que se utilizará cruzando información desde los instrumentos metodológicos, para validar la existencia o no del requerimiento del control descrito en la ISO 27002.

2.5.3 HERRAMIENTAS DE COBIT 2019

COBIT 2019 contiene múltiples instrumentos que pueden servir de apoyo para cualquier

trabajo de investigación, pero, para la presente propuesta únicamente haremos uso de algunos de los indicadores descritos en las Métricas Modelo del documento: “Objetivos de gobierno y gestión” (ISACA, 2018, p. 19 – 20):

Tabla 30 *Métricas modelo de COBIT 2019 para la gestión de vulnerabilidades.*

Práctica de gestión	Métricas modelo
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Número de pruebas de vulnerabilidad llevadas a cabo en los dispositivos.
	Número de vulnerabilidades descubiertas durante las pruebas.
	Tiempo dedicado a remediar vulnerabilidades.

Fuente: Elaboración propia a partir de ISACA (2018, p. 261).

Los primeros dos indicadores se integran con otros en la propuesta final del proceso para la gestión de vulnerabilidades entregada a COACEHL detallada en el Capítulo VI.

2.6 CONCEPTUALIZACIÓN

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (Certiprof, 2022, p. 86).

Stallings (2004, p. 5) ofrece las siguientes definiciones:

Ataque a la seguridad: Cualquier acción que comprometa la seguridad de la información de una organización.

Mecanismo de seguridad: Un mecanismo diseñado para detectar un ataque a la seguridad, prevenirlo o restablecerse de él.

De Hernández-Sampieri (2014, p. 152 - 162) se extraen los siguientes conceptos:

Investigación con diseño no experimental: Estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para después analizarlos.

Diseños transeccionales (transversales): Investigaciones que recopilan datos en un

momento único.

Diseños transeccionales exploratorios: El propósito de los diseños transeccionales exploratorios es comenzar a conocer una variable o un conjunto de variables, una comunidad, un contexto, un evento, una situación. Se trata de una exploración inicial en un momento específico. Por lo general, se aplican a problemas de investigación nuevos o poco conocidos, además constituyen el preámbulo de otros diseños (no experimentales y experimentales).

Diseños transeccionales descriptivos: Indagan la incidencia de las modalidades, categorías o niveles de una o más variables en una población, son estudios puramente descriptivos.

La Comisión Nacional de Bancos y Seguros establece las siguientes definiciones (CNBS, 2022, p. 3 – 6):

Alta Gerencia: Grupo de personas responsables de la gestión diaria, sólida y prudente de la Institución Supervisada ante la Junta Directiva, Consejo de Administración u órgano equivalente.

Ciber amenaza: Circunstancia que podría explotar una o más vulnerabilidades y afectar la ciberseguridad.

Ciberespacio: Es el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física, sino que es un dominio virtual que engloba todos los sistemas.

Ciber resiliencia: Capacidad de la Institución Supervisada de continuar llevando a cabo su misión, anticipándose, adaptándose a ciber amenazas y otros cambios relevantes en el entorno; y, resistiendo, conteniendo y recuperándose rápidamente de incidentes de ciberseguridad.

Ciberseguridad: Preservación de la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas de información a través del ciberespacio.

CNBS: Comisión Nacional de Bancos y Seguros.

Confidencialidad: Característica que consiste en que la información sea accesible para quienes están autorizados.

Disponibilidad: Característica que consiste en que la información debe estar disponible en el momento que se requiera.

Incidente: Es la ocurrencia de un suceso que afecta adversamente el desarrollo normal de las operaciones de la Institución Supervisada.

Incidente de Seguridad de la Información: Ocurrencia de un suceso que constituye una violación o amenaza de las políticas y los procedimientos de seguridad de la Institución Supervisada, y afecta adversamente la confidencialidad, integridad y/o disponibilidad de la información independientemente de su formato y contenedor.

Infraestructura de TI: Conjunto de hardware, software, redes, instalaciones y otros elementos que se requieren para desarrollar, probar, entregar, monitorear, controlar o dar soporte a los servicios de TI. La infraestructura de TI excluye al recurso humano, los procesos y la documentación.

Integridad: Característica que consiste en que la información esté exacta y completa, y que solo puede ser creada, modificada o eliminada por quien esté autorizado para hacerlo.

Riesgo Tecnológico (RT): Es una subdivisión del Riesgo Operativo y se evalúa en dicha categoría de riesgo. Surge de la potencial pérdida por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal digital de distribución de información.

Tecnologías de Información (TI): Conjunto de recursos tecnológicos que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma

consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

CONSUCOOP: Consejo Superior de Cooperativas.

CSF: Marco de Seguridad Cibernética (Por sus siglas en inglés) del NIST.

Gestión de vulnerabilidades: Proceso sistemático para identificar y abordar brechas de seguridad en los activos tecnológicos.

NIST: Instituto Nacional de Normas y Tecnología (Por sus siglas en inglés).

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas (Certiprof, 2022, p. 87).

El Organismo de Certificación Global (NQA por sus siglas en inglés), define lo siguiente (NQA, s.f., p. 6, 13):

Activo de información: Un conjunto de información, definido y gestionado como una sola unidad, para que pueda ser comprendido, compartido, protegido y explotado. Los activos de información deben identificarse y su valor establecerse asignando su valor a la organización, basándose en los impactos reputacionales y/o financieros que pueden causar si se ven comprometidos.

Información: Es el conjunto o conjuntos de datos que una organización quiere proteger, como registros de empleados, registros de clientes, registros financieros, datos de diseño, datos de pruebas, etc.

Reporte de inventario de activos: Documento con el listado de activos tecnológicos administradores con su respectivo nombre, dirección IP y Sistema Operativo.

Reporte de vulnerabilidades: Reporte con el detalle de las vulnerabilidades identificadas en los equipos con su respectivo nivel de criticidad.

Plantilla de informe de remediaciones: Documento que centraliza y resume las posibles medidas a implementar para remediar las vulnerabilidades detectadas en los equipos.

Matriz de planificación de ventanas de mantenimiento: Documento que contiene la lotificación de los activos planificados para su atención de acuerdo a fechas disponibles.

Reporte de vulnerabilidades mitigadas: Este es un reporte donde puede visualizarse el avance en el proceso de remediación de vulnerabilidades en los activos tecnológicos.

Reporte de excepciones: Eventualmente es posible que algunas remediaciones no puedan aplicarse por un motivo u otro. Estas excepciones deben ser debidamente identificadas, documentadas y sustentadas.

Plantilla de boletín de remediación mensual: Este es un reporte consolidado con las actividades de remediación de vulnerabilidades ejecutadas durante el mes en curso.

2.7 MARCO LEGAL

Como se ha descrito a lo largo de este documento, Honduras no cuenta con un marco legal solido con respecto a la ciberseguridad. Sin embargo, en este apartado se detallan las iniciativas y leyes vigentes en el país orientadas en esa temática.

2.7.1 REGLAMENTO SOBRE GOBIERNO ELECTRÓNICO

Este fue un decreto del Poder Ejecutivo aprobado en Consejo de Ministros y publicado en el Diario Oficial La Gaceta en fecha 26 de septiembre del año 2020. El mismo forma parte de un conjunto de esfuerzos para fortalecer el Gobierno Digital de Honduras y ha sido el cimiento sobre el que se han sustentado otros proyectos orientados a la Transformación Digital y Ciberseguridad. El reglamento consta de cinco grandes títulos, cada uno con sus respectivos capítulos y un total de 137 artículos.

Tabla 31 *Estructura de Reglamento sobre Gobierno Electrónico de Honduras*

Título	Capítulos	Artículos

TÍTULO I: OBJETO, PRINCIPIOS, DEFINICIONES, DERECHOS, DEBERES, RESPONSABILIDADES Y PROHIBICIONES	6	Artículos 1 – 9
TÍTULO II: DE LA GOBERNANZA Y EL MARCO INSTITUCIONAL	5	Artículos 10 – 27
TÍTULO III: DEL USO DE TECNOLOGÍA PARA LA GESTIÓN ADMINISTRATIVA	3	Artículos 28 – 46
TÍTULO IV: INTERRELACIÓN CON LA ADMINISTRACIÓN PÚBLICA	6	Artículos 47 – 75
TÍTULO IV: PROCEDIMIENTO ADMINISTRATIVO EN EL ÁMBITO DE GOBIERNO ELECTRÓNICO	14	Artículos 76 – 131
TÍTULO V: DISPOSICIONES FINALES Y TRANSITORIAS	-	Artículos 132 – 137

Nota: Elaboración propia.

Dentro del reglamento hay aspectos que vale la pena resaltar ya que están conectados con el enfoque de la presente investigación. Al respecto, la ley establece:

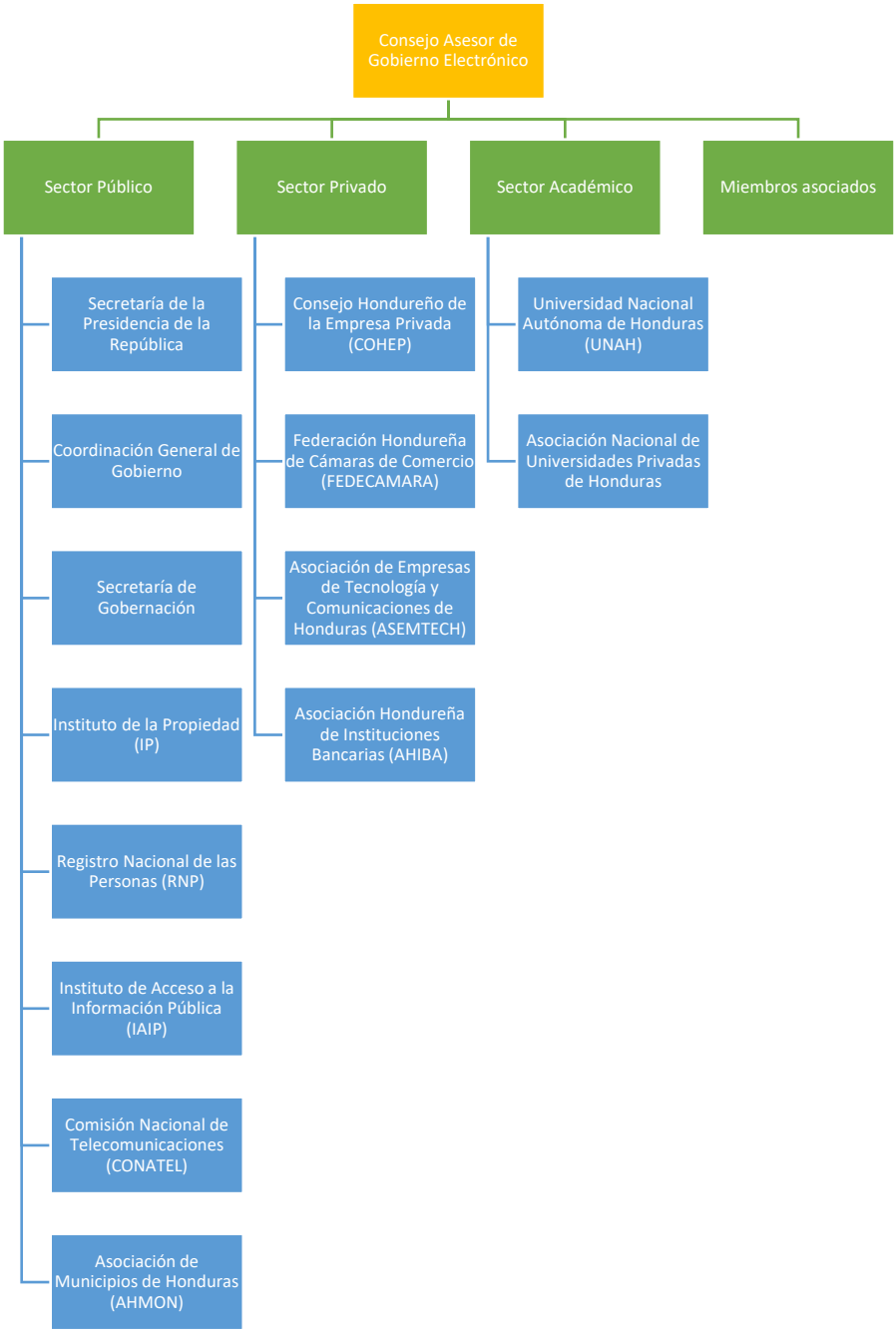
> Artículo 10. – La gobernanza del ecosistema de Gobierno Electrónico estará a cargo del Secretario de Estado en el Despacho de Gestión e Innovación Pública. Además de las que le han sido otorgadas en el Decreto de su creación (Decreto Ejecutivo Número PCM-044-2020 y sus reformas) tendrá las atribuciones, funciones y facultades que se le otorgan en el presente Reglamento.
> Artículo 11. – El Despacho de Gestión e Innovación Pública, es el ente encargado de aprobar los lineamientos, estándares y principios por los cuales habrá de regirse la administración pública en materia de Gobierno Electrónico, lo cual hace en forma exclusiva.
> Artículo 12. - Para efectos de evaluar el grado de madurez de Gobierno Electrónico, el Despacho de Gestión e Innovación Pública, promoverá en coordinación con otras entidades gubernamentales encargadas, las acciones de mejora de la gestión de los procesos de tecnologías de la información y comunicaciones y establecerá un modelo y metodología de evaluación.
> Artículo 13. – El Despacho de Gestión e Innovación Pública se auxiliará de un Consejo Asesor conforme a lo dispuesto en el Capítulo V del presente título de este Reglamento.
> Artículo 14. – Son facultades del Despacho de Gestión e Innovación Pública:
> 13. Aprobar y velar por el cumplimiento de los estándares de ciberseguridad, calidad, diseño a que deban sujetarse las entidades de la Administración Pública.
> 20. Definir los estándares de seguridad, calidad y experiencia del usuario que deban seguir las soluciones desarrolladas por el Gobierno (Reglamento sobre Gobierno Electrónico, 2020, p. 13 – 14).

De este extracto, podemos profundizar algunos aspectos. El primero de ellos, es que se define que la gobernanza del ecosistema de Gobierno Electrónico estará bajo la figura del Secretario de Estado en el Despacho de Gestión e Innovación Pública. Es decir, que las directrices de esta

Secretaría serán aplicables para todas las dependencias del Estado. Este es un avance importante porque hasta entonces no existía algo similar.

Un segundo elemento significativo, yace en la creación de un Consejo Asesor de Gobierno Electrónico multisectorial integrado por representantes de las diferentes entidades de la siguiente forma:

Figura 30 *Organigrama del Consejo Asesor de Gobierno Electrónico*



Nota: Elaboración propia a partir de Reglamento sobre Gobierno Electrónico, 2020, p. 17.

Finalmente, es importante señalar que el Artículo 14 en el numeral 13, establece que es competencia de esta secretaria, establecer y velar por los estándares de ciberseguridad a implementarse dentro de las dependencias del Estado. Actualmente, esta institución se conoce

como: Secretaría Nacional de Ciencia, Tecnología e Innovación (SENACIT).

2.7.2 CÓDIGO PENAL DE HONDURAS

Dentro del Código Penal de Honduras, publicado el 10 de mayo de 2017, bajo decreto legislativo No. 130-2017, se incluyen ciertos artículos con alguna relación con la ciberseguridad. En los apartados: “Seguridad de las redes y de los Sistemas Informáticos” y “Ciberterrorismo o Terrorismo Electrónico” tipifica algunos ciberdelitos.

Tabla 32 *Código Penal: Artículos relacionados con la ciberseguridad*

Articulo	Delito	Definición	Pena
398	Acceso no autorizado a los Sistemas Informáticos.	Quien, vulnerando las medidas de seguridad establecidas para impedirlo, accede sin autorización a todo o en parte de un sistema informático.	De seis a dieciocho meses o multa de cien a doscientos días.
399	Daños a datos y Sistemas Informáticos.	Quien por cualquier medio y sin autorización introduce, borra, deteriora, altera, suprime o hace inaccesible de forma grave datos informáticos.	Prisión de uno a dos años o multa de cien a trescientos días.
400	Abuso de dispositivos.	La fabricación, importación, venta, facilitación o la obtención para su utilización de dispositivos, programas informáticos, contraseñas o códigos de acceso, destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informáticos	Prisión de seis meses a un año o multa de cien a doscientos días.
592	Ciberterrorismo o Terrorismo Electrónico	Quien por cualquier medio o procedimiento y sin autorización, accede a un	Prisión de cuatro a seis años y multa de trescientos a mil días.

		sistema informático de la Administración Pública del Estado o que preste servicios de carácter estatal, impide el acceso al mismo o altera, cambia, o daña datos en el contenido, con la intensión de impedir el correcto funcionamiento de un servicio o para causar terror o miedo en la población	

Nota: Elaboración propia a partir del Código Penal (2017, p. 93, 94, 131).

Estos delitos se cometen en su mayoría cuando un atacante consigue explotar vulnerabilidades y escalar privilegios, por lo que de alguna manera se conectan con el proceso de gestión que busca proponer esta investigación.

2.7.3 ACUERDO MARCO DE COOPERACIÓN ENTRE EL GOBIERNO DE LA REPÚBLICA DE HONDURAS Y EL GOBIERNO DEL ESTADO DE ISRAEL

Dentro de este acuerdo suscrito entre ambos gobiernos y publicado en el Diario Oficial La Gaceta, del 6 de diciembre de 2016, se establece el apoyo en cuatro áreas fundamentales.

Figura 31 *Proyectos de apoyo dentro del Acuerdo de Cooperación entre Israel y Honduras*

Nota: Elaboración propia a partir del Acuerdo Marco de Cooperación entre el Gobierno de la Republica de Honduras y el Gobierno del Estado de Israel (2016, p. 9).

Es de interés para este estudio el apartado: “Fortalecimiento de las capacidades de la

Dirección Nacional de Investigación e Inteligencia (DNII)", pues en él se detallan algunas iniciativas orientadas a fortalecer la ciberseguridad y son: La creación del Centro de Respuesta a Emergencias Informáticas (CERT) y del Centro de Operaciones de Seguridad Gubernamental (G-SOC), el cual tendría capacidad de monitoreo en tiempo real e investigativas dentro del aparato estatal. De acuerdo con Diario El Heraldo, diferentes instituciones estaban dentro del alcance de este proyecto:

> Aunque el decreto 139-2016 indica que el equipo es parte del fortalecimiento de la Dirección Nacional de Investigación e Inteligencia (DNII), EL HERALDO conoció que son 16 instituciones las que serán parte de proyecto.
> Entre ellas están las que forman parte de la ciberdefensa, como la Secretaría Nacional de Defensa (SEDENA), las Fuerzas Armadas (FFAA), la Secretaría de Seguridad, CONATEL, Corte Suprema de Justicia (CSJ), el Ministerio Público (MP) en general, incluyendo la Agencia Técnica de Investigación Criminal (ATIC). De igual forma abarcará la infraestructura crítica, que son todas aquellas instituciones que al ser atacadas por un hacker de forma maliciosa impida que el gobierno pueda desarrollar su trabajo con normalidad. Estas son: la Empresa Nacional de Energía Eléctrica (ENEE), ya que un criminal del ciberespacio puede provocar que el sistema interconectado nacional no funcione y dejar a oscuras el país. Asimismo, la Secretaría de Finanzas (SEFIN), la Comisión Nacional de Bancos y Seguros (CNBS), el Instituto Nacional de Migración (INM) y el Registro Nacional de las Personas (RNP), entre otras que al ser alteradas podrían paralizar el funcionamiento del Estado… Para el Estado de Honduras, el funcionamiento del CERT es de carácter confidencial y de momento solo se conoce que funcionará en las instalaciones de CONATEL, con técnicos en informática que serán capacitados por expertos israelitas. Lo fundamental dentro del proyecto es la elaboración de una Estrategia Nacional de Ciberseguridad para la protección de instituciones gubernamentales (2017, octubre 10).

Como se detalla en la nota, la iniciativa se manejó bajo algunos criterios de confidencialidad, lo que dificulta la obtención de mayor información sobre el estatus de avance de la misma a esta fecha.

2.7.4 OTRAS LEGISLACIONES NACIONALES ORIENTADAS A LA CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

Actualmente, Honduras no cuenta formalmente con una Ley de Protección de Datos Personales. Sin embargo, existen algunas leyes y anteproyectos, mismos que reconocen ese derecho y se detallan a continuación:

- **Ley Nacional del Sistema de Bases de Datos de ADN**: Publicada en el Diario

Oficial La Gaceta en 2023, esta ley tiene como propósito habilitar la creación de Bases de Datos de ADN en Honduras, principalmente para que sirvan como instrumento de apoyo para el Ministerio Público y la Dirección General de Medicina Forense. Dentro del Artículo 4 numerales 12 y 13 se establecen dos defunciones importantes para esta investigación y es lo que rescatamos de ella:

> 12) Ciberseguridad: También conocida como seguridad digital, es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales.
> 13) Privacidad: Es la protección de los datos personales frente a quienes no deberían tener acceso a los mismos, y la capacidad de los usuarios de determinar quién puede acceder a su información personal (Ley del Sistema Nacional de Bases de Datos de ADN, 2023, p. 6).

Si bien la ley no profundiza demasiado en esta materia, ejemplifica como dentro de las nuevas legislaciones se contempla ya el tema de ciberseguridad de forma específica, evidenciando la consonancia con los cambios de paradigmas marcados por la Cuarta Revolución Industrial, de la que Honduras no puede quedar fuera.

- **Constitución de la Republica de Honduras**: Dentro de la Constitución de 1982, existen algunos Artículos dirigidos a la protección de la información de la ciudadanía.

> Artículo 76. Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.
> Artículo 100. Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial. Los libros y comprobantes de los comerciantes y los documentos personales únicamente estarán sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la Ley. Las comunicaciones, los libros, comprobantes y documentos a que se refiere el presente artículo, que fueren violados o sustraídos, no harán fe en juicio. En todo caso, se guardará siempre el secreto respecto de los asuntos estrictamente privados que no tengan relación con el asunto objeto de la acción de la autoridad (Constitución de la República, 1982, p. 5 – 6).

En el año 2013 el Congreso Nacional público en el Diario Oficial La Gaceta diferentes reformas constitucionales, entre ellas, modificaciones al Artículo 182 de la Constitución para adicionar al Hábeas Corpus, la figura del Hábeas Data, lo que representa un antecedente para el fortalecimiento de la protección de datos personales, quedando de la siguiente manera:

> ARTÍCULO 182.-El Estado reconoce la garantía de Hábeas Corpus o Exhibición Personal, y de Hábeas Data. En consecuencia, en el Hábeas Corpus o Exhibición Personal toda persona agraviada

> o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el de Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la siguiente manera:
> 1) EL HABEAS CORPUS O EXHIBICIÓN PERSONAL:
> a) Cuando se encuentre ilegalmente presa, detenida cohibida de cualquier modo en el goce de su libertad: y,
> b) Cuando en su detención o prisión legal, se apliquen al detenido o preso tormentos, torturas, vejámenes. exacción ilegal y toda coacción, restricción molestia innecesaria para su seguridad individual o para el orden de la prisión.
> 2) EL HABEAS DATA
> Toda persona tiene el derecho de acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa ya esté contenida en bases de datos, registros Públicos o Privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística.
> Las acciones de Hábeas Corpus y Hábeas Data se deben ejercer sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Únicamente deben conocer de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tiene la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y a la propia imagen (2013, enero 24, p. 17 – 18).

Como se puede observar, esta reforma empodera a la ciudadanía sobre la información que entrega para ser almacenada en todas las bases de datos tanto públicas como privadas. De alguna manera reconoce también el enorme valor de los datos personales y protección que desde el Estado se les debe procurar.

- **Ley de Transparencia y Acceso a la Información Pública**: Ley publicada en el Diario Oficial La Gaceta el 30 de diciembre de 2006 y que, en su Capítulo V, reconoce como garantía el Hábeas Data y regula el acceso a los datos personales:

> ARTÍCULO 23.-HÁBEAS DATA. Se reconoce la garantía de Hábeas Data.
> ARTÍCULO 24.- SISTEMATIZACIÓN DE ARCHIVOS PERSONALES Y SU ACCESO. Los datos personales serán protegidos siempre. El interesado o en su caso el Comisionado Nacional de los Derechos Humanos por si o en representación de la parte afectada y el Ministerio Público podrán incoar las acciones legales necesarias para su protección. El acceso a los datos personales únicamente procederá por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores.
> ARTÍCULO 25.- PROHIBICIÓN DE ENTREGA DE INFORMACIÓN. Ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas (Ley de Transparencia y Acceso a la Información Pública, 2006, p. 57 – 58).

Esto dio pie al Anteproyecto de Ley de Protección de Datos Personales que se describe a

continuación.

– **Anteproyecto de Ley de Protección de Datos Personales**: Esta es una propuesta que data desde el año 2013. Lastimosamente, no ha sido prioritaria para la clase política hondureña pues a la fecha esta no ha sido aprobada en su totalidad. A continuación, un breve resumen de su contenido.

Tabla 33 *Cuadro resumen de contenido en Anteproyecto de Ley de Protección de Datos Personales*

Sección	Descripción
Título I: Disposiciones Generales.	Establece el objeto de la Ley, el cual consiste en la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. También detalla el ámbito de aplicación de la Ley, haciendo la salvedad que no será aplicable a las bases de datos de personas naturales destinadas a actividades personales o domésticas; las que tienen por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito. Finalmente, el Título I, define una serie de términos jurídicos y técnicos en materia de protección de datos.
El Título II: Principios y Derechos Básicos para la Protección de Datos Personales.	Presenta la base de la interpretación y aplicación de la normativa de protección de datos. Ha de ser la brújula que guía el actuar de los titulares y responsables, garantiza la efectiva aplicación del derecho a los titulares y orientan las decisiones del órgano de control como las instancias judiciales. La recopilación de los principios parte de la Resolución 45/95 de la ONU, los establecidos en las legislaciones española, mexicana, uruguaya y costarricense, contextualizado a terminología legal hondureña.
El Título III: Derechos de Protección de Datos.	Dividido en dos capítulos, en el primer capítulo se establecen las disposiciones generales e incluyendo en el mismo el tratamiento de datos de carácter personal de menores de edad. En el segundo capítulo se desarrollan los derechos ARCO, definiendo los conceptos de: Acceso, rectificación, cancelación y oposición.
Título IV: Procedimientos para hacer efectivos los Derechos de Acceso,	Describe los procedimientos para ejercer los derechos de acceso, rectificación, cancelación y oposición ante el responsable del tratamiento. Para la recolección de datos, la persona titular o su representante, debe manifestar su consentimiento por escrito; ya sea en

Rectificación, Cancelación y Oposición.	un documento físico o electrónico, o en cualquier otra forma legalmente prevista, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. Se incluye el formato y la información que debe contener la solicitud que presenta el titular de los datos personales, los plazos que ha de resolver el responsable del tratamiento y atiende posibles casos especiales que se pueden dar en la práctica o situaciones imprevistas.
Título V: Los Tratamientos y Obligaciones de los responsables.	Enumera la responsabilidad y los principales deberes que tiene el responsable del tratamiento y el encargado del tratamiento. Es importante aclarar que ambos sujetos son considerados obligados, pero no solidarios. El responsable del tratamiento por ser el que obtiene el consentimiento del titular, es a quien recae el grueso de las obligaciones y sanciones por incumplimiento. Por otro lado, el responsable del tratamiento debe asegurar que los datos que brinde al encargado son correctos y cerciorarse del manejo adecuado de estos por parte de éste.
Título VI: Seguridad de datos.	Establece los lineamientos para el responsable del tratamiento y el Instituto de Acceso a la Información Pública (IAIP) en materia de seguridad. El responsable de la base de datos tiene la obligación de adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de la información, evitando su alteración, destrucción o acceso no autorizado. Consecuentemente, quienes intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional o funcional, aún después de finalizada su relación con la base de datos. El IAIP, como órgano regulador establecerá los requisitos y las condiciones que deban reunir las bases de datos, y de las personas que intervengan en la recolección, almacenamiento y uso de los datos.
Título VII: Categoría Especiales de Datos.	Regula el tratamiento de los datos sensibles qué utilizados de manera discrecional o abusiva pueden infringir la privacidad e imagen de la persona, causando daños patrimoniales, y/o discriminación. Asimismo, se regulan los datos que manejan los operadores de telecomunicaciones, y aquellos que se utilizan para fines publicitarios y la actividad financiera, crediticia y comercial; en este caso, a pesar que la CNBS tiene su propia normativa, se recalca que los derechos de acceso, rectificación, cancelación y oposición se aplican también a normas especiales. Estableciendo también en esta categoría las bases de datos de las Fuerzas y Cuerpos de Seguridad, y desarrollando lo relativo a la video vigilancia.
Título VIII: Cesión de Datos y Prestación de Servicios.	Aclara que el responsable del tratamiento de la base de datos, pública o privada, solo podrá comunicar los datos contenidos en ellas cuando el titular haya dado su consentimiento expreso e inequívoco, y se haga sin

	vulnerar los principios y derechos reconocidos en esta Ley y su Reglamento. Asimismo, presenta una serie de supuestos considerados como excepciones al consentimiento requerido para ceder datos personales.
Título IX: Transferencia Internacional de Datos.	Se establece en un capítulo único en cual se establece la transferencia de datos personales, la cual se realiza con países u organismos internacionales que proporcionan niveles de tratamiento y protección adecuados. Siendo el IAIP, el órgano que evalúa el tratamiento y la protección es dichas transferencias.
Título X: Disposiciones sectoriales.	Este Título se divide en dos capítulos y establece cuales son los requisitos para la creación de bases de datos del Sector Público y del Sector Privado, además de otras cuestiones relativas a las aplicaciones de Ley en algunas bases de datos concretas, como las de la agencia tributaria.
Título XI: De los Mecanismos de Vigilancia y Sanción.	Detalla los roles que tiene el IAIP en materia de protección de datos personales, ahora considerado no solo como el Instituto de Acceso a la Información Pública, sino también de Protección de Datos Personales – siguiendo la línea de su referente normativo mexicano, el IFAI. También se detalla el procedimiento que el titular del dato personal debe evacuar ante el IAIP, una vez el responsable del tratamiento no haya respetado sus derechos o vulnerado lo dispuesto en esta Ley o en las normas que la desarrollen. También se hace una tipificación de las faltas, desde las leves a las muy graves, brindando una descripción sobre lo que consiste cada una.
Título XII: Cánones.	Propone que para la inscripción de base de datos en el IAIP y para cuantos otros actos así se dispongan legal o reglamentariamente llevará consigo el pago de cánones en la búsqueda de sostenibilidad financiera e inversión continua en tecnología.

Nota: Elaboración propia a partir de Anteproyecto de Ley de Protección de Datos Personales (2021, IAIP, p. 3 – 6).

Evaluando el contenido descrito, es notorio que el anteproyecto posee elementos sumamente enriquecedores y una perspectiva amplia del tema de protección de datos, contemplando tanto al sector público como privado. Si bien no está completamente enfocada a la ciberseguridad de forma explícita, si busca fortalecer principalmente el marco de confidencialidad e integridad de los datos administrados por las entidades en el país, e incluso fuera de sus fronteras.

– **Anteproyecto de ley que establece medidas para prevenir los actos de odio y discriminación en redes sociales e internet**: Esta iniciativa que paso su primer debate en 2018, entremezcla elementos de ciberseguridad con lineamientos que fueron considerados lesivos del derecho de libertad de expresión, (conocida popularmente como: "Ley mordaza"), por lo que no contó con el suficiente apoyo para su completa aprobación y publicación. Entre los elementos destacables de esta propuesta, es que contempla la creación de un Comité Interinstitucional de Ciberseguridad, que sería la entidad encargada de implementar una Estrategia Nacional de Ciberseguridad. Esto funcionaria bajo la jurisdicción de CONATEL. Un segundo aspecto importante, es que se recomienda al Poder Ejecutivo realizar las acciones pertinentes para la adhesión de Honduras al Convenio sobre la Ciberdelincuencia, de Budapest.

A modo de cierre para esta sección, es oportuno comentar que es notorio y evidente que hace falta ejercer un rol más protagónico por parte del Estado para impulsar un sólido marco general de ciberseguridad en Honduras, pues si bien el sector privado (principalmente el financiero) parece ir un tanto más adelante, la nación requiere que todos los actores de la vida productiva se apropien, empoderen y comprometan con el tema. Solo entonces los indicadores del país experimentaran una mejora sustancial. En segundo lugar, se requiere que se les dé mayor continuidad a las diferentes iniciativas orientadas al fortalecimiento de la ciberseguridad, evitando el sesgo partidista que no hace más que entorpecer el progreso de las instituciones y del país. En último lugar, es claro que hay mucha dispersión de información del marco legal, por lo que es necesario establecer leyes que organicen y orquesten de forma más congruente el estamento hondureño en ciberseguridad.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

Así como lo establece Trejo Sánchez (2021): “En el apartado de la metodología se delimitará el enfoque, el o los métodos, las técnicas y las herramientas que se emplearán en la investigación” (Trejo Sánchez, 2021, p. 76). Es decir, que en esta sección es donde se expone todo el marco metodológico que apoyara esta investigación.

3.1 LIMITACIONES DEL ESTUDIO

Se establece que la presente investigación es un estudio de caso intrínseco pues no se pretende generalizar los hallazgos. Sin embargo, el interés inherente yace en que como se constató en los apartados del macroentorno y microentorno, claramente en COACEHL existe una marcada necesidad de una propuesta que responda a: ¿Cómo se pueden afrontar los retos y desafíos que representa la ciberseguridad y en particular, la gestión de vulnerabilidades? Por otro lado, este es un campo en constante evolución por lo que pueden surgir nuevas líneas de investigación enfocadas en esta temática como, por ejemplo: Incorporación de la Inteligencia Artificial en la ciberseguridad corporativa, automatización de procesos y tareas en la gestión de vulnerabilidades con RPA, diseño de sistemas de alertas tempranas, etc. En ese sentido, este tipo de investigaciones aún están abriéndose especio dentro del contexto local y, por lo tanto, es posible tratar de desarrollar estas y otras propuestas.

En lo referente a la población y muestra seleccionados, se consideran valiosos pues ofrecen una excelente aproximación de cómo funcionan aspectos como la seguridad de la información y ciberseguridad en organizaciones con un cierto grado de madurez, característica que Honduras resulta difícil de encontrar ya que, por diferentes motivos descritos ampliamente en el marco teórico, no existen muchas entidades que abran sus puertas a este tipo de trabajos de investigación (principalmente por aspectos de confidencialidad dada la temática), que especialicen unidades

organizativas o que dispongan de personal experto en estas ramas del saber. De hecho, en el país sigue representando un reto para los gerentes justificar las inversiones realizadas en personal y herramientas de seguridad pues generalmente son percibidas como gasto y no como un garante de reducción de pérdidas. Los criterios y rigurosidad definidos para la selección de la población y muestra se encuentran descritos más adelante en este capítulo.

Finalmente, con lo descrito hasta ahora y en el primer capítulo, estas unidades y procesos existen como parte del cumplimiento normativo establecido bajo las directrices emitidas por la CNBS y CONSUCOOP, por lo qué, las condiciones dentro de las cuales se describen los resultados, el análisis y la propuesta de aplicabilidad están enmarcados por ciertas condiciones que pueden dificultar su generalización.

Puesto este preámbulo, a continuación, se detallan los aspectos metodológicos de la investigación.

3.2 ENFOQUE Y MÉTODOS

Para comenzar, es necesario establecer qué es el enfoque desde la óptica de la metodología de la investigación. Niño Rojas indica que: "Se hace referencia a la investigación cuantitativa y cualitativa" (Niño Rojas, 2019, p. 27). Es decir, por la naturaleza del enfoque, la investigación puede tomar uno de tres posibles caminos: Cualitativo, cuantitativo o mixto.

A razón de la distinción en el enfoque, es importante entonces identificar el mismo para esta investigación. Inicialmente, para validarlo se realiza el siguiente análisis preliminar de los objetivos propuestos:

Tabla 34 *Matriz de análisis del enfoque de los objetivos específicos*

Objetivo específico	Enfoque
Analizar la gestión de vulnerabilidades vigente para diagnosticar la situación actual del proceso.	Cualitativo
Determinar que herramientas se usan en COACEHL para la detección y atención de vulnerabilidades de sus activos	Cualitativo

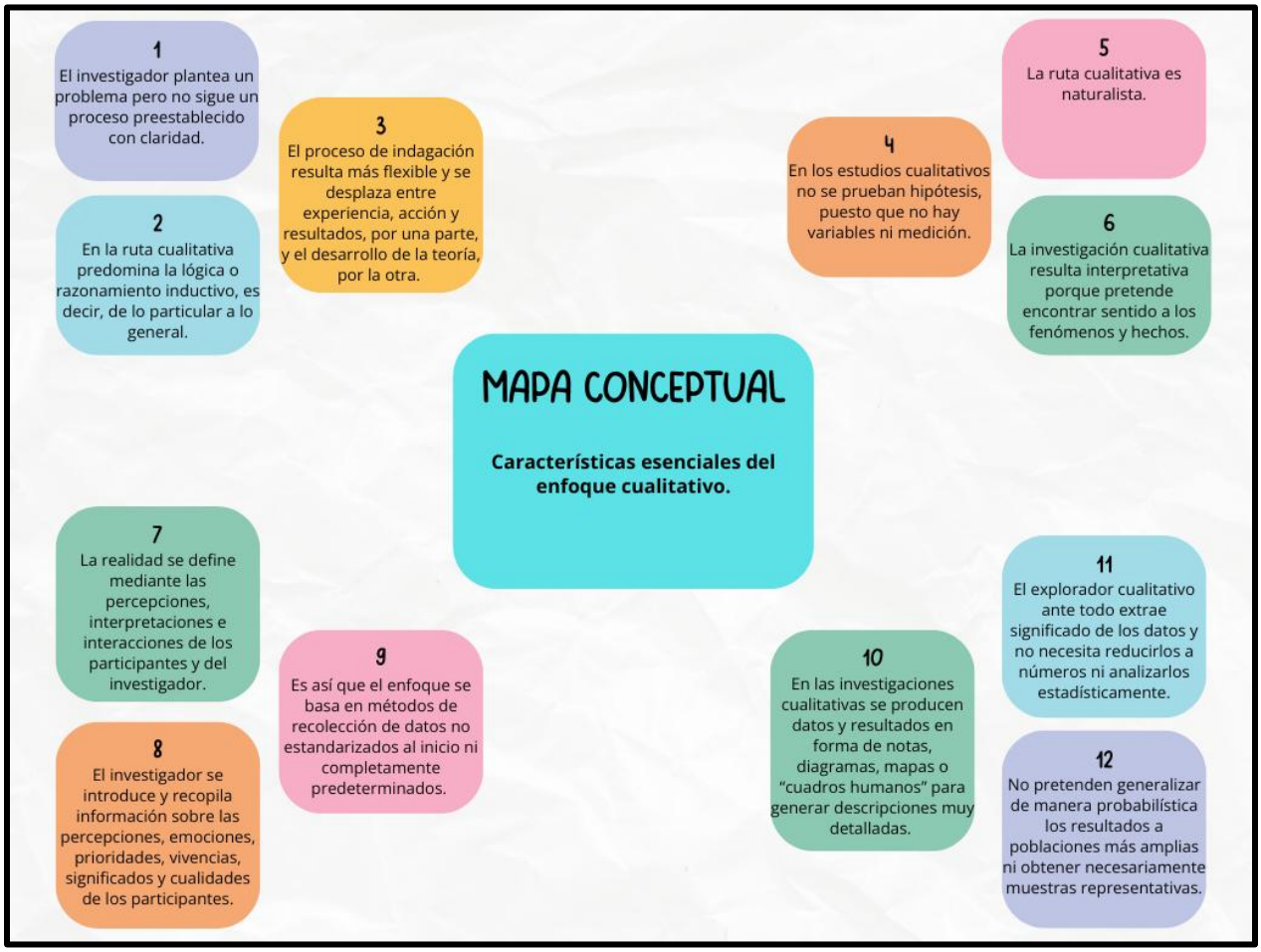
tecnológicos a fin de modelar como optimizar el aprovechamiento de estos recursos.	
Identificar el grado de conocimiento y uso de estándares de Seguridad de la Información y Ciberseguridad en COACEHL para validar la utilización de mejores prácticas en la organización.	Cualitativo
Establecer cómo la mejora del proceso de gestión de vulnerabilidades basada en el Marco de Ciberseguridad del NIST CSF 2.0 puede ser de beneficio en COACEHL para robustecer su postura de ciberseguridad.	Cualitativo

Nota: Elaboración propia.

Como se puede observar, el presente estudio cuenta con un enfoque cualitativo. Sobre este Bernal Torres (2022) nos explica: “Su preocupación no es prioritariamente medir, sino cualificar, describir e interpretar el fenómeno (situación o sujeto) social a partir de rasgos determinantes según sean percibidos por los elementos, mismos que están dentro de la situación estudiada” (Bernal Torres, 2022, p. 58). Estas características calzan con los resultados de la matriz de análisis.

Para reforzar esta aseveración, es necesario ahondar en las características propias del enfoque. Hernández Sampieri y Mendoza Torres (2023) detallan algunas características representativas del enfoque cualitativo que se resumen en la figura que se muestra a continuación:

Figura 32 *Características esenciales del enfoque cualitativo*



Nota: Elaboración propia a partir de Metodología de la Investigación (Hernández Sampieri, Mendoza Torres, 2023, p. 9).

Al evaluar los objetivos de esta investigación contrastándolos con estas características podemos afirmar entonces que la misma tiene un enfoque cualitativo, ya que resulta interpretativa (porque pretende encontrar sentido a los hechos), se producen datos y resultados en forma de notas, ejemplos y diagramas, para generar descripciones detalladas sobre el tema.

3.3 ALCANCE

¿Qué es el alcance? Pérez, Pérez y Seca indican que: "El alcance es la profundidad que pretendemos darle a nuestra investigación" (Pérez, Pérez y Seca, 2020, p. 213). Es decir, que el

alcance permite determinar que tanto nos sumergiremos en un determinado tema. El alcance de una investigación está delimitado por su enfoque y tipo. Por el objetivo y contenido de la presente investigación, se considera la misma de tipo descriptivo. Para sustentarlo, se plantea lo descrito por Carhuancho Mendoza y Nolazco Labajos (2019), sobre las investigaciones descriptivas:

> En este proceso se evidencia que el investigador sustenta de manera concreta la situación preocupante, precisa un contexto e identifica necesidades, lo que le permite desarrollar la intención de la investigación y que lleve a la delimitación de la misma dependiendo en gran medida de los que se pretende en el estudio (Carhuancho Mendoza, Nolazco Labajos, 2019, p. 22).

Bernal Torres (2022), amplia sobre los rasgos diferenciadores de las investigaciones descriptivas:

> En tales estudios se muestran, narran, reseñan o identifican hechos, situaciones, rasgos, características de un objeto de estudio, se realizan diagnósticos, perfiles, o se diseñan productos, modelos, prototipos, guías, etcétera, pero no sedan explicaciones o razones de las situaciones, los hechos, los fenómenos, etcétera (Bernal Torres, 2022, p. 141).

Al evaluar los objetivos, el contenido y enfoque de esta investigación se considera que la misma es descriptiva ya que se exploran generalidades de la seguridad de la información, ciberseguridad y sobre las vulnerabilidades en los sistemas de información. También, se procura generar una propuesta que responda a un problema o una necesidad en un contexto especifico.

3.4 DISEÑO

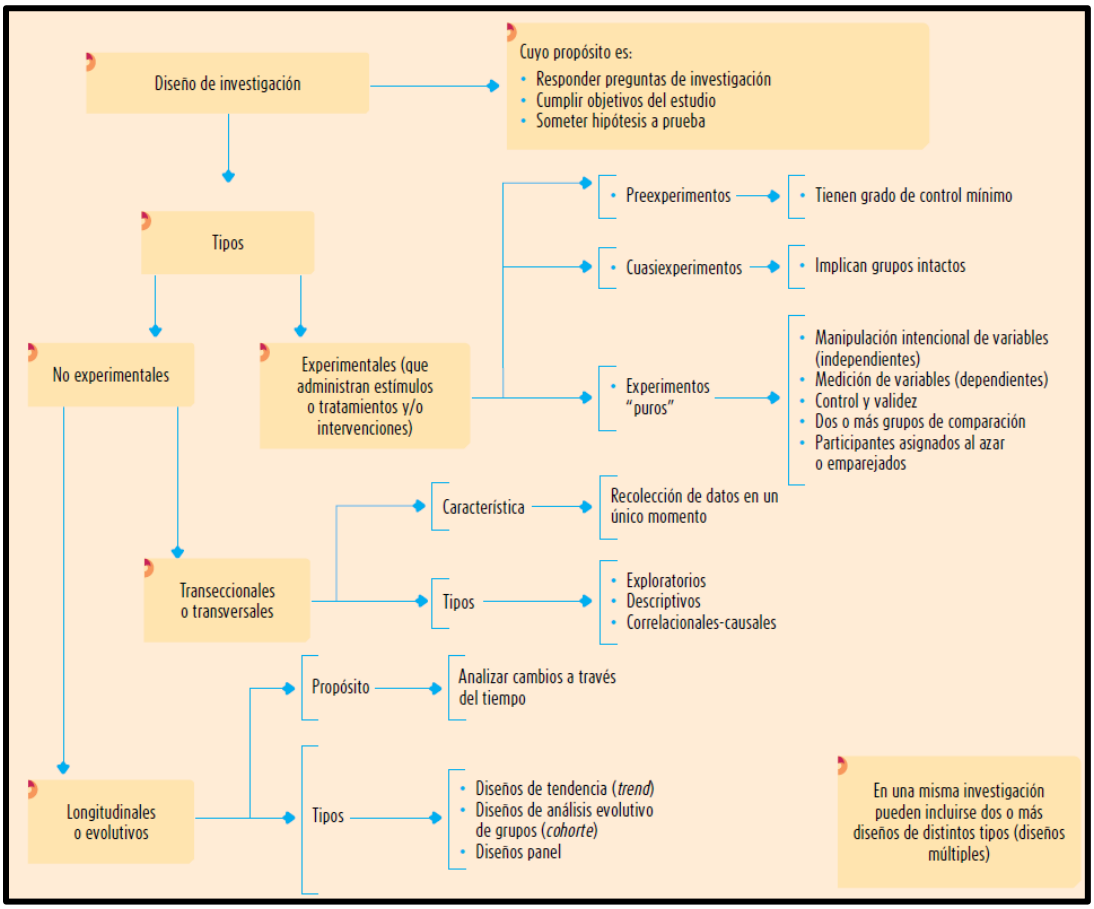
Arispe Alburqueque, Yangali Vicente y Guerrero Bejarano (2020, p. 64) indican que: “Los diseños son la guía o el plan para que el investigador pueda desarrollar el proceso de investigación en lo referente a la obtención de la información”. Niño Rojas (2019) profundiza aún más al respecto:

> En su sentido específico, el diseño metodológico cubre una franja básica del plan general que se orienta a describir de manera concreta, según cada investigación, las estrategias y procedimientos para abordar el estudio del objeto, a la luz de las teorías del marco correspondiente (Niño Rojas, 2019, p. 53).

Este apartado es relevante porque en base al enfoque de la investigación, se encaminan el resto de elementos a desarrollar para la recolección de datos y análisis de los datos, así como

también para su informe final. El diseño permite al investigador mantenerse dentro de los parámetros de lo permitido de acuerdo con la naturaleza de la investigación. De ahí en más, que, al contar con un enfoque cualitativo, dirigiremos el diseño de este trabajo bajo esas condiciones.

Figura 33 *Esquema de posibles diseños para investigaciones con enfoque cualitativo*



Fuente: Presentación íntegra y completa obtenida de: Metodología de la Investigación. 6ta. Edición (Hernández-Sampieri, Fernández Collado y Baptista Lucio, 2014, p.127).

A modo de resumen (los conceptos irán expandiéndose a lo largo de este capítulo y en el apartado de conceptualización) y de acuerdo con esta figura, la presente investigación será de tipo: No experimental, transeccional y descriptiva.

Las investigaciones se realizan sobre un grupo focal. Esto requiere entonces que hablemos sobre tres términos clave: Población, muestra y muestreo.

3.4.1 POBLACIÓN

Acerca de las poblaciones, Gregorio Rojas explica:

> Las unidades de análisis son los objetos o personas con ciertas características especia- les que proveen la información para comprender el problema. Estás unidades, deben reunir ciertos requisitos para estar incluidos en el marco de elegibilidad requerido en el estudio, a fin de que puedan ser útiles en el proceso de investigación (Gregorio Rojas, 2023, p. 148).

Lo descrito por el autor permite visualizar que existe un gran conjunto que engloba los elementos de un todo (población). El siguiente diagrama ejemplifica esta relación:

Figura 34 *Representación de relación entre población y muestra*

Nota: Elaboración propia.

En el caso particular de COACEHL, el área de seguridad de la información cuenta con su respectiva Jefatura y el Oficial de Seguridad de la Información. La entidad cuenta con su Sistema de Gestión de Seguridad de la Información y sus respectivos procesos y controles. Sin embargo, la investigación se centrará específicamente en el proceso para gestionar las vulnerabilidades en los activos tecnológicos, pues forma parte del alcance de esta. Adicionalmente, se deben tener en

cuenta los detalles previamente expuestos en el apartado: “Limitaciones del estudio”.

3.4.2 MUESTRA

Una muestra no es otra cosa que un segmento de un todo. Gómez, M. (2009, p. 102) la define como: “Una parte de la población a estudiar”. Puntualizando desde una perspectiva más cualitativa Hernández Sampieri establece que: “En la ruta cualitativa, es el grupo o conjunto de personas, eventos, sucesos, comunidades, etc., sobre el cual se habrán de recolectar los datos, sin que necesariamente sea estadísticamente representativo del universo o población que se estudia” (Hernández Sampieri, Mendoza Torres, 2023, p. 447).

Como se ha detallado hasta aquí, en la dimensión de personas la muestra la conforman el jefe y el oficial del área de seguridad de la información, en el apartado de procesos, la practicas vigentes en COACEHL para gestionar vulnerabilidades y para la dimensión de documentación examinada para esta investigación, la misma se sustentará con al menos 60 fuentes bibliográficas de un total de 1450 resultados de artículos indexados en Google Académico enfocados en el marco de Ciberseguridad del NIST CSF 2.0 y otros recursos de apoyo como libros disponibles en el CRAI (Centro de Recursos para el Aprendizaje y la Investigación) de UNITEC, estándares internacionales, leyes, normativas vigentes, estudios de organismos internacionales, memorias anuales, etc., procurando que las mismas no tengan más de cinco años de antigüedad.

A modo de resumen se presenta el siguiente cuadro con los valores a considerar:

Tabla 35 *Cuadro resumen de población y muestra de la investigación*

Dimensión	Población	Muestra
Personal	2	2
Procesos	1	1
Documentación	1450	60

Nota. Elaboración propia.

3.4.3 MUESTREO

Considerando las definiciones descritas hasta aquí, es presumible entonces que, al hablar del muestreo, es la actividad de extracción de información de una población. Se dice que la misma debe ser representativa para poder contar con el peso y la validez necesaria.

Por la naturaleza y dirección de este trabajo investigativo, este será del tipo: No Probabilístico o dirigido, pues las unidades muestrales no son aleatorias o al azar, sino que, serán seleccionadas intencionalmente, bajo el cumplimiento de ciertas condiciones. Y, al ser de tipo cualitativo Gregorio Rojas señala que en ellas: "No se calculan muestras, sino que se identifican eventos, sujetos o informantes que van a proporcionar o a generar la información necesaria para comprender la situación de estudio" (Gregorio Rojas, 2023, p. 150). Sobre el muestreo, se deja por sentado que el mismo será por conveniencia ya que la misma será seleccionada en base a los criterios delineados por el investigador. Estos criterios se exponen en el apartado a continuación.

3.5 CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

3.5.1 PERSONAL

COACEHL cuenta con personal preparado y con experiencia en diferentes campos del conocimiento. Sin embargo, por los propósitos que persigue esta investigación se tomaran en cuenta los siguientes criterios de inclusión y exclusión:

Tabla 36 *Tabla de Criterios de inclusión y exclusión del personal*

Criterios de inclusión	Criterios de exclusión
Experiencia en el sector financiero o cooperativo.	Falta de experiencia en el sector financiero o cooperativo.
Con formación profesional en el campo de tecnología.	Sin formación profesional en el campo de tecnología.
Labora en el departamento de seguridad de la información de COACEHL.	Labora en otros Departamentos dentro de la Cooperativa.
Conocimiento de estándares y marcos de seguridad de la información (Familia ISO	Desconocimiento de estándares y marcos de seguridad de la información (Familia ISO

27000, COBIT 2019, etc.).	27000, COBIT 2019, etc.).
Experiencia en el área de seguridad de la información.	Sin experiencia en el área de seguridad de la información
Dominio del Sistema de Gestión de Seguridad de la Información y de políticas y procesos para la gestión de vulnerabilidades vigentes en la Cooperativa COACEHL.	Desconocimiento del Sistema de Gestión de Seguridad de la Información y de políticas y procesos para la gestión de vulnerabilidades vigentes en la Cooperativa COACEHL.

Nota. Elaboración propia.

Por la naturaleza de la investigación, es requerido que los participantes cumplan con estas características a fin de garantizar la comprensión de los objetivos, los conceptos abordados y la propuesta de aplicabilidad descrita en el Capítulo VI.

3.5.2 PROCESOS

Como institución financiera, COACEHL cuenta con múltiples procesos por departamento, pero, para efectos de esta investigación se considerarán específicamente aquellos dentro del Sistema de Gestión de Seguridad de la Información dirigidos a la gestión de vulnerabilidades.

Tabla 37 *Tabla de Criterios de inclusión y exclusión de procesos*

Criterios de inclusión	Criterios de exclusión
Es definido por el departamento de seguridad de la información.	No es definido por el departamento de seguridad de la información.
Está enmarcado dentro de la política de seguridad de la información.	No forma parte del compendio de políticas de seguridad de la información.
Describe el proceso de remediación de vulnerabilidades.	Enfocados en otros ámbitos de la Seguridad de la Información y/o Ciberseguridad.

Nota. Elaboración propia.

3.5.3 DOCUMENTACIÓN

La línea temática abordada en este trabajo de investigación es sumamente amplia y variada. De hecho, admite una amplia gama de recursos. Por tal motivo, se ha tratado de recopilar documentación apegada a la literatura académica, rigor científico, estándares internacionales y marco legal.

Tabla 38 *Tabla de Criterios de Inclusión y Exclusión de Documentos*

Criterios de inclusión	Criterios de exclusión
Documentos con respaldo legal, académico, científico enfocados en la temática de esta investigación, publicada principalmente durante los últimos 5 años.	Documentación con fecha de publicación anterior al año 2021.
Documentación pública ligada a instituciones financieras en Honduras y principalmente a COACEHL y que este enmarcada en el enfoque de esta investigación.	Documentación sensible que pueda exponer a COACEHL o a sus clientes.

Nota. Elaboración propia.

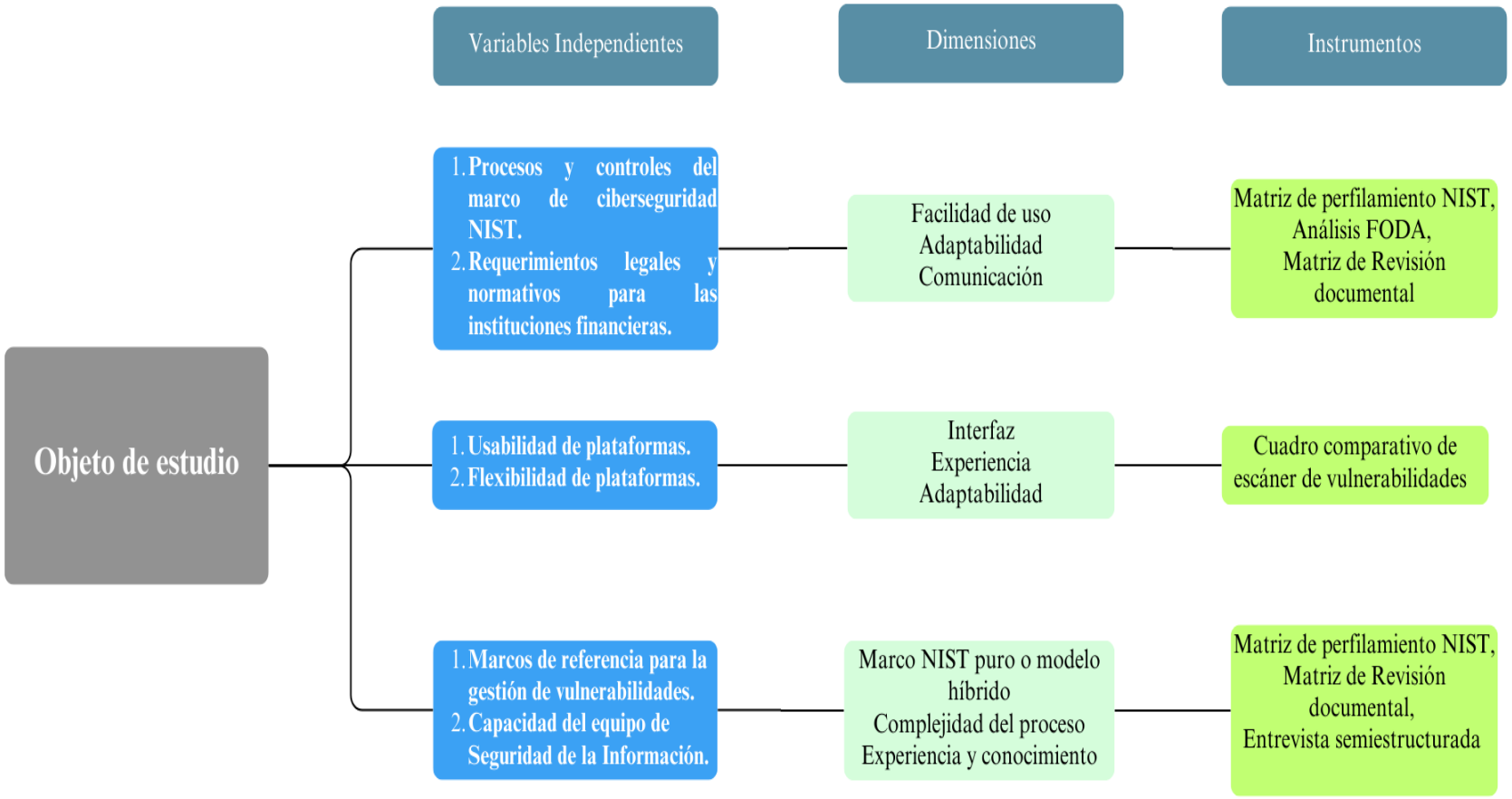
3.6 OPERACIONALIZACIÓN DE LAS VARIABLES

Esta actividad permite tratar el tema de estudio desde una óptica más científica y menos sensible a sesgos. Santiesteban Naranjo (2014) la define así:

> Operacionalizar significa otorgar valores a los constructos principales que aparecen en ella. La operacionalización de variables se realiza por cuanto existen cualidades del objeto, que no son directamente observables; estos requieren de la atomización en dimensiones e indicadores que son directamente cuantificables (Santiesteban Naranjo. 2014, p. 114).

Para un mayor orden y claridad, la operacionalización de variables se presenta de dos formas: Visual y tabular. Ambas se muestran a continuación:

3.6.1 ESQUEMA DE LAS VARIABLES DE ESTUDIO



3.6.2 OPERACIONALIZACIÓN DE LAS VARIABLES

Variable	Def. Teórica	Def. Operativa	Dimensiones	Indicador	Tipo estadístico	Escala	Instrumento
Procesos y controles del marco de ciberseguridad NIST.	El Marco de Seguridad Cibernética (CSF) 2.0 está diseñado para ayudar a las organizaciones de todos los tamaños y sectores – lo que incluye a la industria, el gobierno, la academia y las organizaciones sin fines de lucro - para gestionar y reducir sus riesgos de seguridad cibernética (NIST, 2024, p. iv).	Adaptación de marco de ciberseguridad para la gestión de vulnerabilidades.	Nivel de madurez del componente.	Número de procesos alineados con NIST, o ISO 27002.	Cualitativo.	Alta. Media. Baja.	Matriz de perfilamiento NIST, Análisis FODA.
Requerimientos legales y	Requisitos: Condiciones	Evaluación de cómo el proceso	Adaptabilidad Comunicación	Nivel de cumplimiento.	Cualitativo.	Alto. Medio.	Matriz de perfilamiento

normativos para las instituciones financieras.	imprescindibles para algo (Greco, 2009, p, 370).	contribuye al cumplimiento de los requisitos legales y normativos sobre ciberseguridad y gestión de vulnerabilidades.				Bajo.	NIST, Matriz de Revisión documental, Cuadro comparativo de escáner de vulnerabilidades Entrevista semiestructurada.
Usabilidad de plataformas.	Usabilidad: Grado en que un sistema, un producto o servicio puede ser utilizado por determinados usuarios para conseguir objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso (ISO 9241-11:2019, *s.f.*).	Evaluación de facilidad de uso de plataformas orientadas a la gestión de vulnerabilidades.	Interfaz Experiencia.	Nivel de facilidad de uso	Cualitativo.	Alta. Media. Baja.	
Flexibilidad de plataformas	Capacidad de un producto para adaptarse a cambios en sus	Evaluación de flexibilidad de las herramientas para adaptarlas a	Adaptabilidad.	Nivel de adaptabilidad.	Cualitativo.	Alta. Media. Baja.	

	requisitos, contextos de uso o entorno del sistema (ISO 25010:2023, *s.f.*).	las necesidades del negocio y del proceso de gestión de vulnerabilidades.					
Metodologías para la gestión de vulnerabilidades.	Vulnerabilidad: debilidad de un sistema que puede ser aprovechada por un atacante, para generar riesgos a la organización o al propio sistema (Mata García, 2023, p. 239).	Evaluación de marcos de referencias para la gestión de vulnerabilidades.	Marco NIST CSF 2.0 puro o modelo hibrido. Complejidad del proceso.	Nivel de adecuación del marco NIST CSF 2.0 para generar un proceso que simplifique la gestión de vulnerabilidades.	Cualitativo.	Alta. Media. Baja.	Matriz de Revisión documental.
Competencia del equipo de Seguridad de la Información.	Competencia: Capacidad para aplicar conocimientos y habilidades con el fin de alcanzar los resultados previstos (ISO 45001:2018, *s.f.*).	Medición de las competencias del equipo de Seguridad de la Información.	Experiencia y conocimiento.	Nivel de competencia del equipo en aspectos clave de seguridad de la información, ciberseguridad y gestión de vulnerabilidades.	Cualitativo.	Alta. Media. Baja.	Entrevista Semiestructurada.

3.7 TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS, ANÁLISIS DE DATOS

3.7.1 TÉCNICAS

Sobre las técnicas, Baena Paz (2017) indica que: “Las técnicas se vuelven respuestas al “cómo hacer” y permiten la aplicación del método en el ámbito donde se aplica” (Baena Paz, 2017, p. 83). Por otro lado, Bautista Cárdenas (2021) establece que: “La investigación cualitativa. Metodológicamente se caracteriza por el énfasis que hace en la aplicación de las técnicas de descripción, clasificación y significación” (Bautista Cárdenas, 2021, p. 29). Este último utiliza una palabra clave: Significación. En estudios cualitativos este es un factor determinante ya que se busca profundizar la relevancia e importancia del tema abordado.

Entre las técnicas a emplear para la recolección de información se incluyen:

– **La entrevista**: Esta es una de las técnicas más utilizadas en los procesos de investigación cualitativos ya que permite cubrir gran cantidad de aspectos de una forma fluida. Pulido Varón, Quintero Arango y Gutiérrez Avendaño (2024) establecen lo siguiente:

> En investigación se utiliza para conocer las percepciones y experiencias de participantes que poseen información clave debido a que están inmersos en el problema que se busca solucionar, así como de expertos conocedores cuyo conocimiento es valioso en el estudio (Pulido Varón, Quintero Arango y Gutiérrez Avendaño, 2024, p. 49).

Dentro de esta definición se pueden visualizar algunos aspectos ya descritos en los criterios de selección como ser: La necesidad de que entre los entrevistados se cuente con personas que dominen la temática y segundo, que posean información clave.

– **La observación**: Pulido Varón, Quintero Arango y Gutiérrez Avendaño (2024) señalan: “La observación, como técnica de recolección de información, contempla la captación directa de datos de personas, situaciones y contextos en su entorno natural” (Pulido Varón, Quintero Arango y Gutiérrez Avendaño, 2024, p. 53).

– **Diarios y bitácoras**: Estos son formatos que permitan capturar información en

momentos puntuales. Particularmente se emplearán mediante notas de campo sobre las que Gibbs establece que: “Son las notas que el investigador toma sobre sus pensamientos y observaciones cuando está en el “entorno” de campo que investiga” (Gibbs, 2014, p. 194). Es decir, son escritos que el investigador realiza durante el proceso de captura de información. Su importancia radica en que captan detalles clave para el trabajo de investigación.

– **Cronograma de actividades con base a las etapas del proceso de gestión de vulnerabilidades**: Esto no es más que la temporización de las actividades tomando como punto de referencia las etapas del proceso y los objetivos específicos planificados, desglosándolos en acciones para cumplir con estos (Gregorio Rojas, 2023, p.157).

3.7.2 INSTRUMENTOS ELABORADOS

Un instrumento no es más que el medio utilizado para obtener información o, dicho de otra forma: “La materialización de un método o una técnica. Es el material impreso para la recopilación de la información” (Santiesteban Naranjo, 2014, p. 122). Resultan necesarios ya que no solo mantienen enfocada la recolección de datos, sino que también permiten mantener la confianza de las organizaciones sobre cuál es la información considerada dentro del alcance del proyecto.

3.6.2.1 INSTRUMENTOS TEMÁTICOS

Para una mejor organización de los instrumentos, estos se han categorizado por su naturaleza en: Temáticos y metodológicos. Esta estructura se verá reflejada en la sección de Anexos.

– **Cuadro comparativo de escáner de vulnerabilidades**: Documento de apoyo para realizar la evaluación de características de herramientas para la identificación y remediación de vulnerabilidades en activos tecnológicos **Ver Anexo 1**.

– **Matriz de perfilamiento NIST**: Cuadro para evaluación del estado de una

organización de cara a los componentes del núcleo NIST. Permite establecer un perfil actual y un perfil objetivo de ciberseguridad para la organización. **Ver Anexo 2**.

3.6.2.2 INSTRUMENTOS METODOLÓGICOS

– **Matriz de revisión documental**: Documento que sintetiza los datos relevantes de las fuentes consultadas para sustentar la investigación. **Ver Anexo 3**.

– **Matriz FODA**: "Herramienta clave para hacer una evaluación pormenorizada de la situación actual de una organización o persona sobre la base de sus debilidades y fortalezas, y en las oportunidades y amenazas que ofrece su entorno" (Sánchez Huerta, 2020, p. 16). Esta es una herramienta ampliamente utilizada por su flexibilidad y adaptabilidad. **Ver Anexo 4**.

– **Formato para notas de campo:** Para este instrumento se adaptará un ejemplo detallado por Hernández-Sampieri, Fernández Collado y Baptista Lucio (2014, p. 402). **Ver Anexo 5**.

– **Matriz de análisis de datos**: Matriz en la que se enumeran los objetivos y las preguntas de investigación y se identifica la forma en que cada uno de los componentes de los métodos ayudará a responderlas (Maxwell, 2019, p. 211). **Ver Anexo 6**.

– **Cuestionario semiestructurado**: El instrumento correspondiente a la técnica de la entrevista es el guion o cuestionario semiestructurado, conformado por preguntas abiertas (Pulido Varón, Quintero Arango y Gutiérrez Avendaño, 2024, p. 49). **Ver Anexo 7**.

3.6.2.3 INSTRUMENTOS DE MONITOREO Y CONTROL

– **Diagrama de Gantt**: El cronograma de actividades se representará a través de un diagrama de Gantt. **Ver Anexo 8**.

3.7.3 PROCEDIMIENTOS

Para el desarrollo de este trabajo de investigación se hará uso de herramientas en línea (mediante Google Workspace) y en papel. Esto como opciones de contingencia en caso de que se imposibilite el uso de alguno de los instrumentos en digital o físico. A continuación, se expone brevemente el procedimiento a seguir según cada instrumento descrito en la investigación.

Tabla 39 *Cuadro resumen de procedimientos por instrumento*

Instrumento	Procedimiento
Cuadro comparativo de escáner de vulnerabilidades.	– Preparar ambientes de pruebas con cada una de las herramientas seleccionadas. – Completar el cuadro comparativo basándose en las características fundamentales necesarias para el proceso de gestión de vulnerabilidades.
Matriz de perfilamiento organizativo NIST.	– Recopilar insumos por medio de la entrevista, notas de campo y revisión documental para elaborar un perfil actual y un perfil objetivo de las funciones NIST CSF 2.0 enfocadas en la gestión de vulnerabilidades. – Completar la matriz de perfilamiento organizativo del NIST CSF 2.0 para mapear el nivel de madurez de las funciones evaluadas.
Matriz de revisión documental.	– Realizar búsquedas dirigidas entre los recursos del CRAI y Google Académico para identificar documentación relacionada con el enfoque de esta investigación. – Completar la matriz de revisión documental con datos relevantes de las obras consultadas.
Matriz de Análisis FODA.	– Recopilar insumos por medio de la entrevista, notas de campo y revisión documental para identificar las Fortalezas, Debilidades, Oportunidades y Amenazas del proceso de gestión de vulnerabilidades de la Cooperativa.

Notas de campo.	– Tomar notas de actividades, observaciones, ideas y otros detalles que se consideren pertinentes con la investigación, durante las visitas a la Cooperativa. Esto con el objetivo de captar información adicional que no haya sido recopilada por otros instrumentos.
Matrices de análisis de datos.	– Completar esta matriz, procesando en ella los datos recopilados de las diferentes fuentes, siguiendo el flujo descrito en el apartado del Plan de Análisis.
Entrevista al personal de Seguridad de la Información.	– Desarrollo del formato de entrevista con el personal de Seguridad de la Información de la Cooperativa.
Diagrama de Gantt.	– Ejemplificación del proceso de gestión de vulnerabilidades en un mes calendario.

Nota: Elaboración propia.

De manera general, los instrumentos a utilizar fueron elaborados dentro de la asignatura: "Metodología de la Investigación", para posteriormente ser validados y aplicados en COACEHL. Los resultados fueron procesados, analizados y preparados para completar el documento de investigación como parte del espacio pedagógico: "Trabajo Final".

3.7.4 PLAN DE ANÁLISIS

A diferencia del enfoque cuantitativo donde se requiere completar todo el trabajo de campo y luego hacer la interpretación y análisis de resultados, en la contraparte cualitativa esto sucede de forma paralela como se evidencia en la figura siguiente:

Figura 35 *Flujo de datos en el análisis cualitativo*

<table>
<tr><th>Actividad</th><th>Antes</th><th>Durante</th><th>Después</th></tr>
<tr><td>Trabajo de campo</td><td></td><td colspan="2">Periodo de recopilación de datos</td></tr>
<tr><td rowspan="3">Análisis</td><td colspan="3">Condensación de datos</td></tr>
<tr><td></td><td colspan="2">Elaboración y verificación de datos</td></tr>
<tr><td></td><td colspan="2">Presentación de datos</td></tr>
</table>

Nota: Elaborado a partir de Métodos de investigación cualitativa: fundamentos y

aplicaciones: (Páramo Morales, Campo Sierra y Maestre Matos, 2020, p. 35).

Lo anterior no quiere decir que el análisis de datos cualitativo no puede seguir un proceso. Es más bien, una forma para comprender que la recolección y condensación de los mismos es recursiva.

Ahora bien, el siguiente esquema permite visualizar como se puede plantear el análisis de datos cualitativos de una forma coherente y progresiva.

Figura 36 *Análisis de la información cualitativa*

Fuente: Figura íntegra y completa obtenida de: Investigación cualitativa: claves para estudiantes universitarios (Pulido Varón, Quintero Arango y Gutiérrez Avendaño, 2024, p. 76).

En concordancia y de manera general, se estará llevando el siguiente plan de análisis de los datos obtenidos a través de los diferentes instrumentos:

Figura 37 *Plan de análisis de los datos*

Nota: Elaboración propia.

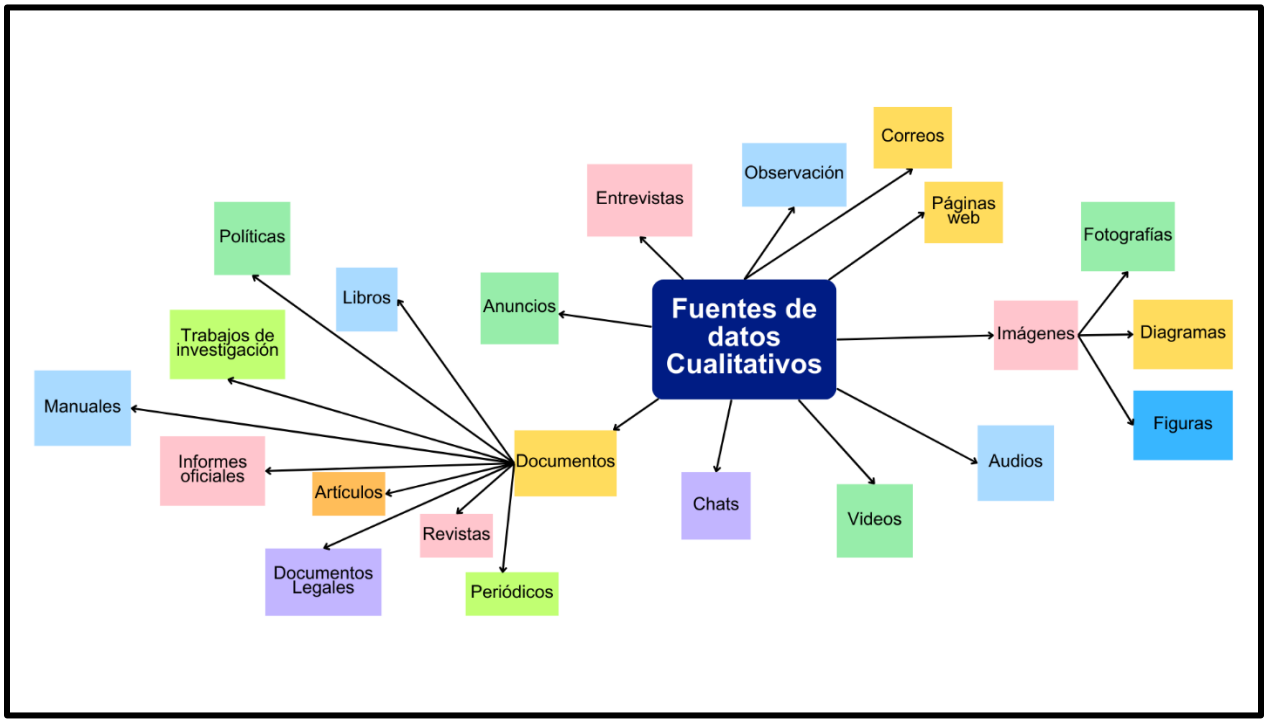
Finalmente, para completar esta tarea se estarán utilizan matrices para el análisis de datos que se describen en el apartado de instrumentos de este trabajo de investigación.

3.8 FUENTES DE INFORMACIÓN

Una de las características del enfoque cualitativo es la amplia variedad de recursos de información que puede incorporar. Trejo Sánchez establece que: "Las fuentes de consulta son los recursos bibliohemerográficos que suministraron información para la construcción del proyecto de investigación; incluyen los que sirvieron de apoyo para la delimitación del marco teórico-conceptual. Se presentan en forma de un listado" (Trejo Sánchez, 2021, p. 76).

Como se puede observar en la siguiente figura, los datos cualitativos pueden presentar diferentes formas y provenir de múltiples fuentes. Esto puede proporcionar una riqueza de contenido y abrir espacio a la creatividad del investigador.

Figura 38 *Fuentes de datos cualitativos*



Nota: Elaboración propia a partir de: El análisis de datos cualitativos en investigación cualitativa (Gibbs, 2014, p. 22).

Ante tal diversidad de datos, es necesario identificar qué cosas constituyen fuentes primarias o secundarias. Monroy Mejía y Nava Sanchezllanes (2018) nos ofrecen estas definiciones:

> a) Fuentes primarias. Son testimonios de testigos oculares de los hechos pasados y objetos reales que se usaron en el pasado y que se pueden examinar en el presente.
> b) Fuentes secundarias. Es la información que proporcionan las personas que no participaron directamente en un hecho. Estos datos se encuentran en enciclopedias, diarios, publicaciones periódicas y otros materiales (Monroy Mejía y Nava Sanchezllanes, 2018, p. 103).

Considerando esto, en el siguiente cuadro se presenta una categorización de recursos en base a la distribución propuesta por Cruz del Castillo y Olivares Orozco (2014).

Tabla 40 *Clasificación de recursos por tipo de fuente*

Tipo	Recurso
Fuentes primarias	• Libros. • Artículos científicos. • Reportes de investigación.

	• Antologías. • Ponencias en congresos. • Tesis. • Testimonios de expertos. • Monografías. • Disertaciones.
Fuentes secundarias	• Compilaciones • Listados de referencias. • Enciclopedias. • Diccionarios. • Resúmenes.

Nota: Elaboración propia a partir de Cruz del Castillo y Olivares Orozco (2014, p. 133).

Por otro lado, está el reto de no perder de vista el objetivo de la investigación y por ello es importante definir criterios de selección que canalicen y filtren estos insumos para tomar en consideración únicamente aquellos que cumplen con el enfoque del trabajo que se desarrolla.

3.8.1 FUENTES PRIMARIAS

Para esta investigación se consideran fuentes primarias los múltiples insumos disponibles en el Centro de Recursos para el Aprendizaje y la Investigación (CRAI), mismo que se convirtió en un apoyo importante a través de los diferentes recursos bibliográficos disponibles (Libros, revistas, artículos científicos, etc.) que han alimentado el proyecto. También las diferentes publicaciones obtenidas a través de la herramienta Google Académico enfocadas en Seguridad de la Información, Ciberseguridad y el Marco NIST CSF en su versión 2.0. Finalmente, se consideran fuentes primarias los datos obtenidos de los diferentes instrumentos aplicados al personal de seguridad de la información de COACEHL

3.8.2 FUENTES SECUNDARIAS

Se constituyen como fuentes secundarias las consultas realizadas a listas de referencias, diccionarios, enciclopedias, resúmenes de materiales encontrados mediante Google Académico, periódicos, etc.

3.9 CONGRUENCIA METODOLÓGICA

3.9.1 MATRIZ DE CONGRUENCIA

N°	Preguntas de investigación	Objetivo	Metodología	Variables	Dimensiones	Indicadores	Instrumentos
1	¿En COACEHL cómo se gestionan actualmente las vulnerabilidades presentes en sus activos tecnológicos?	Analizar la gestión de vulnerabilidades vigente para diagnosticar la situación actual del proceso.	Cualitativa	Procesos, políticas.	Nivel de madurez del proceso.	Número de procesos y políticas identificados para la gestión de vulnerabilidades, análisis de contenido de documentos del marco NIST.	Matriz de análisis FODA, lista de verificación basada en ISO 27002, notas de campo, matriz de perfilamiento organizativo NIST, entrevista semiestructurada.
2	¿Qué herramientas utilizan en la Cooperativa para identificar y atender las vulnerabilidades?	Determinar que herramientas se usan en COACEHL para la detección y atención de vulnerabilidades de sus activos tecnológicos a fin de modelar como optimizar el aprovechamiento de estos recursos.		Metodologías y herramientas.	Nivel de uso de herramientas y metodologías en la gestión de vulnerabilidades.	Frecuencia de menciones de metodologías, satisfacción con herramientas utilizadas.	Matriz de análisis FODA, lista de verificación basada en ISO 27002, entrevista semiestructurada.
3	¿Dentro del equipo de Seguridad de la	Identificar el grado de conocimiento y uso de estándares		Estándares y marcos de referencia	Nivel de conocimiento de marcos de	Conocimiento y uso de estándares y marcos de referencia.	Matriz de análisis FODA, entrevista semiestructurada.

	Información de COACEHL qué conocimiento y uso hacen de estándares y mejores prácticas para la gestión de vulnerabilidades?	de Seguridad de la Información y Ciberseguridad en COACEHL para validar la utilización de mejores prácticas en la organización.		(NIST, ISO 27002, COBIT 2019, etc.).	referencia de ciberseguridad.		
4	¿Qué beneficios puede recibir COACEHL en el robustecimiento de su postura de ciberseguridad, derivados de la mejora en su proceso de gestión de vulnerabilidades?	Establecer cómo la mejora del proceso de gestión de vulnerabilidades basada en el Marco de Ciberseguridad del NIST CSF 2.0 puede ser de beneficio en COACEHL para robustecer su postura de ciberseguridad.		Eficacia en la gestión de vulnerabilidades.	Nivel de competencia del equipo en aspectos clave de seguridad de la información, ciberseguridad y gestión de vulnerabilidades.	Número de procesos optimizados. Mejoras perceptibles en el proceso de gestión de vulnerabilidades.	Entrevista semiestructurada.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se presentan y analizan los datos obtenidos mediante los instrumentos (tanto temáticos como metodológicos) aplicados durante el desarrollo del trabajo de investigación, en COACEHL. Los mismos fueron validados por el juicio de expertos, en este caso, por el maestro guia. M. Sc. Jorge Raúl Maradiaga Chirinos garantizando que fueran comprensibles por los participantes y que, permitieran generar la información necesaria para enriquecer la investigación. Para reducir el uso de papel, se utilizó la herramienta Google Forms. Esto permitió que las respuestas se almacenaran automáticamente en una hoja de cálculo para su posterior procesamiento y análisis.

Los resultados, constituyen el fundamento para responder a la pregunta general planteada al inicio de este documento: ¿Qué componentes del Marco de Ciberseguridad NIST CSF 2.0 son útiles para generar un proceso para la gestión de vulnerabilidades en los sistemas de información de COACEHL?

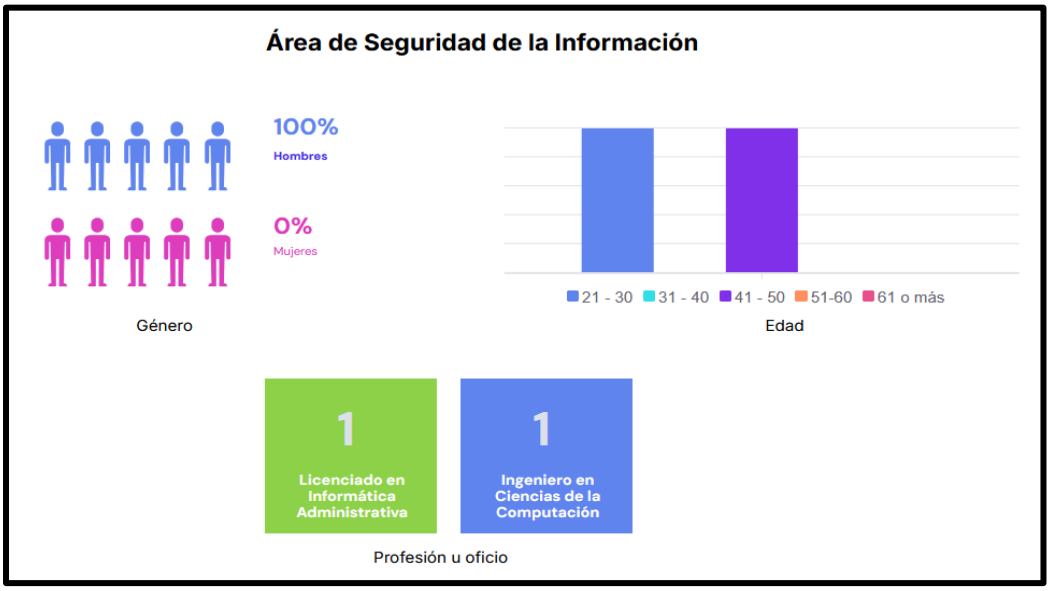
4.1 INFORME DE APLICACIÓN DE INSTRUMENTOS, RECOLECCIÓN DE DATOS E INTERPRETACIÓN DE RESULTADOS

Los resultados detallados en este capítulo se basan en las respuestas de los colaboradores del departamento de seguridad de la información de COACEHL, observaciones hechas por el investigador durante las visitas a la Cooperativa y en los datos obtenidos por medio de la aplicación de los diferentes instrumentos.

La población está integrada por dos personas: El jefe y un oficial. Para la recolección de datos, ambos participaron en el proceso por lo que los resultados reflejan una tasa de respuesta del 100%. De los datos demográficos obtenidos se puede destacar en primer lugar, que COACEHL es una institución abierta a personas de diferentes edades lo que permite la combinación de

experiencia con juventud. Actualmente ambos colaboradores son del género masculino. A continuación, una gráfica con el resumen de esta información.

Figura 39 *Datos demográficos*



Nota: Elaboración propia.

Otro elemento importante es el nivel académico de los colaboradores pues ambos cuentan con su título a nivel de Pregrado (Uno en Ingeniería en Ciencias de la Computación y otro con una Licenciatura en Informática Administrativa) y uno ellos, posee estudios de Posgrado, lo que denota que la organización se preocupa por seleccionar a individuos que cuenten con conocimientos especializados en la materia para estas posiciones. Para los objetivos de la investigación esto es importante ya que garantiza la plena comprensión de los conceptos, estándares descritos y objetivos que persigue la propuesta del proceso y también, asegura que la misma será de valor y aceptable para COACEHL.

4.2 SÍNTESIS Y TRIANGULACIÓN DE HALLAZGOS

De acuerdo con los datos recabados mediante los diferentes instrumentos se encontraron los hallazgos descritos a continuación:

4.2.1 GENERALIDADES DE LA ORGANIZACIÓN Y DEL PROCESO DE GESTIÓN DE VULNERABILIDADES

En primera instancia era necesario conocer algunos aspectos generales de la organización para tener mayor claridad sobre la situación actual del proceso de gestión de vulnerabilidades. Para ello, se aprovecharon algunas de las preguntas de la entrevista semiestructurada:

Tabla 41 *Distribución de preguntas de entrevista enfocadas en el análisis de la situación actual*

Sección del instrumento de la entrevista	Preguntas
Datos demográficos.	1, 2, 3, 4
Exploración de estructura e identidad organizacional.	5, 6.
Gobierno de TI y alineamiento estratégico.	11, 12, 15.
Identificación y Gestión de Activos.	18
Detección y Gestión de vulnerabilidades técnicas.	19, 20, 21, 22, 23, 24.

Nota: Elaboración propia.

El detalle de los resultados y su análisis correspondiente se muestran a continuación. Cabe señalar que en los apartados donde los participantes coinciden en sus respuestas, las columnas se han unificado para evitar repeticiones innecesarias.

Tabla 42 *Matriz de preguntas orientadas al análisis de la situación actual del proceso de gestión de vulnerabilidades*

Sección del instrumento	Pregunta	Oficial	Jefe
Exploración de estructura e identidad organizacional.	6. ¿Qué es lo que más le agrada de trabajar en COACEHL y en el área de seguridad de la información?	Las oportunidades desarrollo profesional en el campo de conocimiento.	Siempre busca la mejora continua, y son disciplinados.
Gobierno de TI y alineamiento estratégico.	11. ¿Cuál de las siguientes políticas se aplican en la empresa? (Puede marcar varias opciones).	- Política de Seguridad de la Información. - Política de gestión de activos tecnológicos (o equivalente). - Política para la gestión de vulnerabilidades. - Política de respaldo y recuperación frente a desastres.	
	12. ¿Cuál de los siguientes procesos se aplican en la empresa? (Puede marcar varias opciones).	- Proceso de aplicación de parches. - Proceso de remediación de vulnerabilidades. - Proceso de respaldo y recuperación frente a desastres.	
	15. Como parte de las actividades de seguimiento y cumplimiento de políticas y procesos. ¿Se genera alguno de los siguientes reportes o indicadores de desempeño (KPI) para los Altos Mandos? (Puede seleccionar varias opciones).	- Indicadores de aplicación de parches. - Indicadores de cobertura de agentes de seguridad en activos tecnológicos.	
Identificación y Gestión de Activos.	18. ¿La organización comprende el riesgo de seguridad cibernética para la misma, los activos y los individuos por medio de algunas de estas prácticas? (Puede marcar varias opciones).	- Se identifican, validan y registran las vulnerabilidades de los activos.	
Detección y Gestión de vulnerabilidades técnicas.	19. Describa como se gestionan las vulnerabilidades en los activos tecnológicos actualmente.	Mediante herramientas y el proceso definido.	Se utilizan varias herramientas de detección de vulnerabilidades y hay

			un proceso de vulnerabilidades.
	20. Describa como se mantiene un registro de auditoria o documentan todos los pasos dados en la gestión de vulnerabilidades técnicas.	Mediante reportes y en el proceso de vulnerabilidades.	Mediante informes/reportes y los pasos se encuentran en el documento de proceso de vulnerabilidades.
	21. ¿De dónde se reciben informes sobre vulnerabilidades en los activos tecnológicos (Puede marcar una o ambas)?	- Fuentes internas. - Fuentes externas.	
	22. Al considerar como se monitorean los activos para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos. ¿Cuáles de las siguientes opciones describen a la organización? (Puede seleccionar varias opciones).	- Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos. - Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.	
	23. Sobre el análisis de eventos adversos (Seleccione aquellas que se practican en la organización).	- Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas. - Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos.	
	24. ¿Se dispone de los siguientes ambientes (Puede marcar varias opciones)?	- Pruebas (o Desarrollo). - Pre-Producción. - Producción.	

Nota: Elaboración propia

A continuación, profundizamos en los resultados y análisis correspondientes por cada sección.

a) Exploración de estructura e identidad organizacional: En este apartado se trata de conocer algunas generalidades de la unidad de seguridad de la información en COACEHL. Una de las cuestiones evaluadas es que los colaboradores identifiquen que es lo que más les agrada acerca de su trabajo en la Cooperativa.

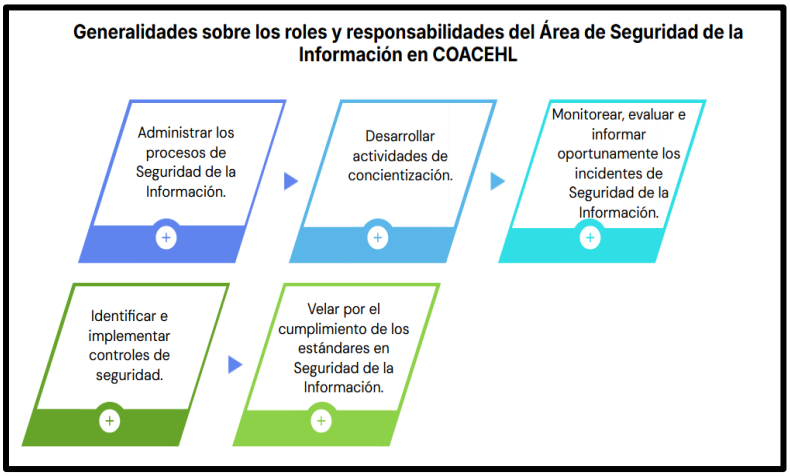
Figura 40 *Cultura y clima organizacional en COACEHL*

Nota: Elaboración propia.

De acuerdo con las respuestas podemos deducir que COACEHL ha generado condiciones que le permiten a sus colaboradores, percibir que es un lugar donde pueden crecer personal y profesionalmente.

Por otro lado, en este apartado también se solicitó a los participantes una descripción sobre los roles y responsabilidades asociadas al área de seguridad de la información y, a sus puestos.

Figura 41 *Generalidades sobre la unidad de seguridad de la información*

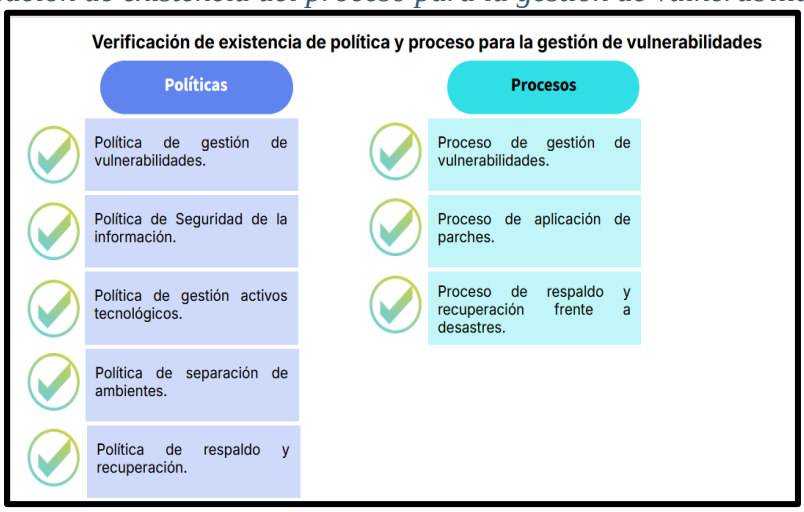


Nota: Elaboración propia.

Los resultados demuestran que el equipo de seguridad de la información es el responsable de cuidar todo lo relacionado con los elementos descritos en el apartado del marco teórico (Seguridad de la Información, Ciberseguridad y Seguridad Informática).

b) Gobierno de TI y alineamiento estratégico: En este apartado se pretende validar aspectos relacionados con el Gobierno de TI y el alineamiento estratégico, por ejemplo, la existencia de procesos y políticas relacionadas con la gestión de vulnerabilidades. Los resultados se muestran en la siguiente figura.

Figura 42 *Verificación de existencia del proceso para la gestión de vulnerabilidades*



Nota: Elaboración propia.

Como se puede observar, COACEHL cuenta con un conjunto de políticas y procesos bien definidos, incluido el tema de la gestión de vulnerabilidades.

c) Detalles sobre el proceso de gestión de vulnerabilidades: Estos resultados denotan que existe algún nivel de trazabilidad en la gestión de vulnerabilidades pues se detalla por parte de los participantes que existe un proceso definido y con ciertos niveles de medición.

Todos los aspectos descritos hasta aquí y recogidos mediante la entrevista, evidencian que para COACEHL, la seguridad en sus activos tecnológicos es una prioridad. De allí, que se busca mejorar la gestión de vulnerabilidades.

4.2.2 DEFICIENCIAS EN LA CONSOLIDACIÓN DE LA GESTIÓN DE VULNERABILIDADES

Si bien la Cooperativa cuenta con su proceso y política para la gestión de vulnerabilidades, la misma se encuentra fuertemente orientada a la aplicación de parches (o actualizaciones). Esto se pudo constatar a través de los diferentes instrumentos, pero fue mediante las notas de campo que se logró captar con mayor detalle esta falencia.

Tabla 43 *Nota de campo de análisis de situación actual*

Fecha:	02/05/2025
Lugar:	COACEHL, Oficina principal.
Hora Inicio:	07:45 a.m.
Hora Final:	08:30 a.m.
Tipo:	☐ Evento ☐ Idea ☒ Actividad

Descripción:

Se realizó una sesión exploratoria con el jefe de Seguridad de la Información para conversar sobre algunas generalidades orientadas en las siguientes aristas.

1. Acerca de la estructura organizacional.

En este apartado se expuso que COACEHL cuenta con su propia unidad de Seguridad de la Información integrada por su Jefatura y un Oficial.

2. Herramientas.

Se nos indicó que actualmente la Cooperativa cuenta con la solución para la aplicación de parches y se está en proceso de implementación del escáner de vulnerabilidades. Adicionalmente, se realizan escaneos por parte de proveedores externos en ejercicios de identificación de vulnerabilidades (se exige al menos 1 vez al año la ejecución de estos).

3. Gestión de activos.

Esta se realiza por parte de la Gerencia de TI y se entrega a Seguridad de la Información en caso de ser requerida.

4. Proceso de Gestión de Vulnerabilidades.

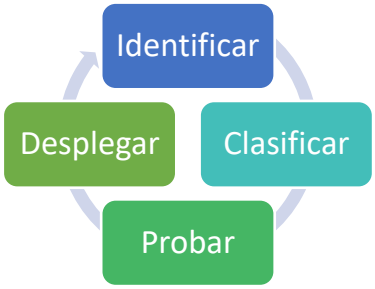
Este se encuentra definido a nivel de política y como proceso (flujograma). De manera general se establecen las siguientes etapas:

1. Identificar.
2. Clasificar.
3. Probar.
4. Desplegar.

Nota: Elaboración propia.

Actualmente el proceso para la gestión de vulnerabilidades consta de cuatro etapas como se muestra en la figura siguiente:

Figura 43 *Proceso actual de gestión de vulnerabilidades en COACEHL*



Nota: Elaboración propia.

De forma resumida estas son algunas de las actividades desarrolladas en cada etapa:

Tabla 44 *Detalle de actividades del proceso actual para gestión de vulnerabilidades*

Etapa	Descripción de actividades
Identificar.	– Actualización del inventario de activos. – Despliegue de agentes de herramientas de seguridad. – Detección de nuevos parches pendientes de instalar.
Clasificar.	– Aprobación y/o rechazo de actualizaciones. – Clasificación de vulnerabilidades y actualizaciones en base a criticidad.
Probar.	– Se aplican las remediaciones en ambientes controlados de prueba.
Desplegar.	– Las remediaciones se aplican en ambientes productivos.

Nota: Elaboración propia.

Adicionalmente, la sección: "Desafíos y oportunidades de mejora", dentro del instrumento de la entrevista se incluyeron preguntas orientadas a identificar puntos de dolor del proceso actual, así como para conocer el grado de receptividad del equipo de esta propuesta.

Tabla 45 *Distribución de preguntas de entrevista enfocadas en los desafíos y oportunidades de mejora del proceso actual.*

Sección del instrumento de la entrevista	Preguntas
Desafíos y oportunidades de mejora.	29, 30, 32.

Nota: Elaboración propia.

En esta misma línea se muestran las respuestas exteriorizadas por el equipo de

seguridad de la información:

Tabla 46 *Matriz de preguntas sobre beneficios esperados*

Sección del instrumento	Pregunta	Oficial	Jefe
Desafíos y oportunidades de mejora.	29. ¿Cómo se identifican mejoras en los procesos, procedimientos y actividades de gestión de Seguridad de la Información y Ciberseguridad? (Puede marcar varias opciones).	- Las mejoras se identifican a partir de evaluaciones. - Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativas.	
	30. Desde su experiencia: ¿Cuáles son los principales desafíos que enfrenta la empresa en temas de Seguridad de la Información y Ciberseguridad?	- La obsolescencia de los activos tecnológicos. - Desarrollar mayor agilidad en el cierre de brechas de seguridad. - Automatización de procesos. - Mayor complejidad de los ciberataques.	
	32. ¿Qué tanto interés tiene en esta propuesta de proceso para la gestión de vulnerabilidades basado en el Marco de Ciberseguridad del NIST?	- Mucho.	

Nota: Elaboración propia.

En cuanto a la forma en cómo se identifican mejoras, los participantes indican que estas se reconocen por medio de ejercicios de evaluación y durante la ejecución de los procesos, procedimientos y actividades. Esto permite mapear debilidades y tratar de incorporar acciones correctivas de forma flexible.

Figura 44 *Resultados de cómo se identifican mejoras en los procesos, procedimientos y*

actividades dentro del departamento de seguridad de la información

Nota: Elaboración propia.

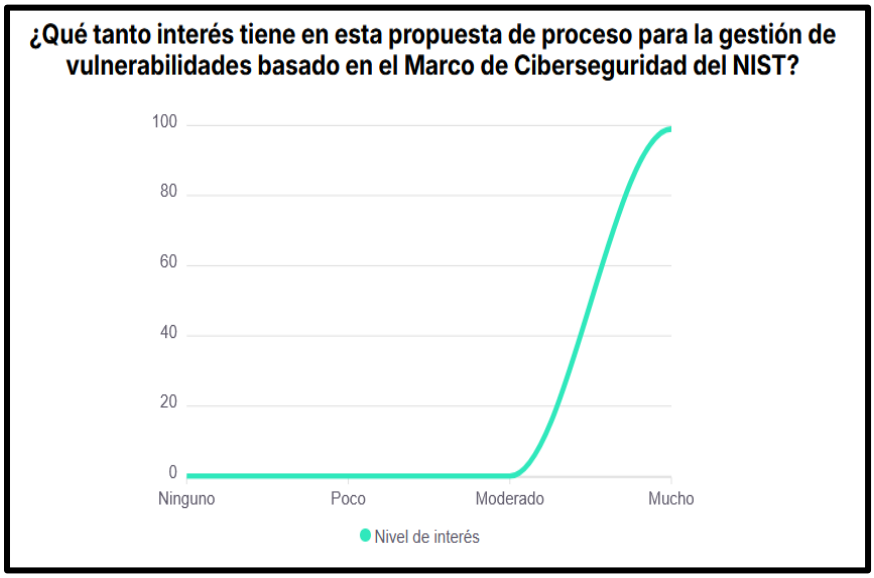
Adicionalmente y como se evidencio en el marco teórico, algunas de las fuerzas impulsoras de cambio en las organizaciones han sido derivadas de la Cuarta Revolución Industrial, entre ellas, la ciberseguridad y la automatización de tareas. Esto concuerda con las respuestas de los participantes quienes reconocen la influencia de esas tendencias como parte de los retos y desafíos que el contexto le plantea a la organización.

Figura 45 *Resultados sobre los principales desafíos que enfrenta la empresa en Seguridad de la Información y Ciberseguridad*

Nota: Elaboración propia.

Por otro lado, las respuestas de los participantes indican que el 100% de ellos tiene alto interés en recibir una propuesta que les ayude a fortalecer su proceso de gestión de vulnerabilidades actual.

Figura 46 *Resultados de la medición de interés en la propuesta para la gestión de vulnerabilidades basada en el Marco de Ciberseguridad del NIST CSF 2.0*



Nota: Elaboración propia.

Este proceso evidencia el esfuerzo que la organización realiza en temas de fortalecerse en materia de ciberseguridad. Sin embargo, es notorio que el mismo está fuertemente focalizado hacia un tipo de remediación y no responde a la amplia variedad de vulnerabilidades existentes en los activos tecnológicos pues no todas se remedian aplicando actualizaciones o parches de seguridad.

4.2.3 NIVEL DE MADUREZ DEL PROCESO DE GESTIÓN DE VULNERABILIDADES

Aplicando la matriz de perfilamiento NIST CSF 2.0 y sus niveles de madurez se buscaba establecer en cuál de ellos se ubicaba el proceso de gestión de vulnerabilidades vigente. Los datos fueron captados de las respuestas 13, 14, 16, 18, 21, 22, 23, 29 del instrumento de la entrevista y complementados con insumos obtenidos desde las notas de campo.

Los criterios considerados para establecer el nivel de madurez de cada aspecto evaluado, están descritos dentro del apartado: 2.5.1 Herramientas del Marco de Seguridad Cibernética del NIST CSF 2.0. Los resultados de alguna manera coinciden con lo descrito en el microentorno, pues el contar con marcos legales y regulatorios, entidades supervisoras y un mayor grado de concientización en las entidades financieras, ha permitido avanzar en la implementación de mejores prácticas, políticas y procesos que respalden la operación de las instituciones, permitiéndoles alcanzar considerables niveles de madurez.

En resumen, los hallazgos de la Matriz de Perfilamiento NIST CSF 2.0 permiten identificar con claridad la necesidad de COACEHL de alinear su proceso de gestión de vulnerabilidades con marcos de referencia probados. También se ha identificado que se deben fortalecer las estrategias para reflejar los resultados y avances en las actividades ya que actualmente esto es ambiguo.

Tabla 47 *Matriz de cruce de respuestas de entrevista con Niveles del CSF del NIST 2.0*

Función	Categoría	Subcategoría	Pregunta en entrevista	Nivel actual
Gobernar (GV).	Política (GV.PO).	GV.PO-01: La política de gestión de riesgos de seguridad cibernética se establece en base al contexto organizativo, la estrategia de seguridad cibernética y las prioridades, y es comunicada y aplicada.	13. ¿Cuál de los siguientes aspectos se cumplen en cuanto a las políticas de Seguridad de la Información y Ciberseguridad?	Repetible.
		GV.PO-02: La política de gestión de riesgos de seguridad cibernética se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización.		
	Supervisión (GV.OV).	GV.OV-01: Los resultados de la estrategia de gestión de riesgos de seguridad cibernética se revisan para informar y ajustar la estrategia y la dirección.	14. Al considerar el tema de la supervisión o seguimiento. ¿Qué descripciones coinciden con las prácticas de la institución? (Puede marcar varias opciones).	
		GV.OV-02: La estrategia de gestión de riesgos de seguridad cibernética se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización.		
		GV.OV-03: El rendimiento de la gestión de riesgos de seguridad cibernética de la organización se evalúa y revisa para realizar los ajustes necesarios.		
Identificar (ID).	Gestión de activos (ID.AM).	ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización.	16. Sobre los activos (Por ejemplo: Datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos (Puede marcar varias opciones).	
		ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización.		
		ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores.		
		ID.AM-07: Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.		
		ID.AM-08: Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida.		
	Evaluación de riesgos (ID.RA)	ID.RA-01: Se identifican, validan y registran las vulnerabilidades de los activos.	18. ¿La organización comprende el riesgo de seguridad cibernética para la misma, los activos y los individuos por medio de algunas	

			de estas prácticas? (Puede marcar varias opciones).	
		ID.RA-02: Se recibe información sobre amenazas cibernéticas de foros y fuentes de intercambio de información.	21. ¿De dónde se reciben informes sobre vulnerabilidades en los activos tecnológicos (Puede marcar una o ambas)?	
		ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización.		
		ID.RA-04: Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades	18. ¿La organización comprende el riesgo de seguridad cibernética para la misma, los activos y los individuos por medio de algunas de estas prácticas? (Puede marcar varias opciones).	
		ID.RA-07: Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento		
		ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades		Conocimiento de los riesgos.
	Mejora (ID.IM).	ID.IM-01: Las mejoras se identifican a partir de evaluaciones.	29. ¿Cómo se identifican mejoras en los procesos, procedimientos y actividades de gestión de Seguridad de la Información y Ciberseguridad? (Puede marcar varias opciones).	Repetible.
		ID.IM-02: Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.		
		ID.IM-03: Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos.		
		ID.IM-04: Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de seguridad cibernética que afectan a las operaciones.		
Detectar (DE).	Monitoreo continuo (DE.CM).	DE.CM-01: Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos.	22. Al considerar como se monitorean los activos para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos. ¿Cuáles de las siguientes opciones describen a la organización? (Puede seleccionar varias opciones).	
		DE.CM-02: Se monitorea el entorno físico para detectar posibles acontecimientos adversos.		
		DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.		
		DE.CM-06: Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar acontecimientos potencialmente adversos.		

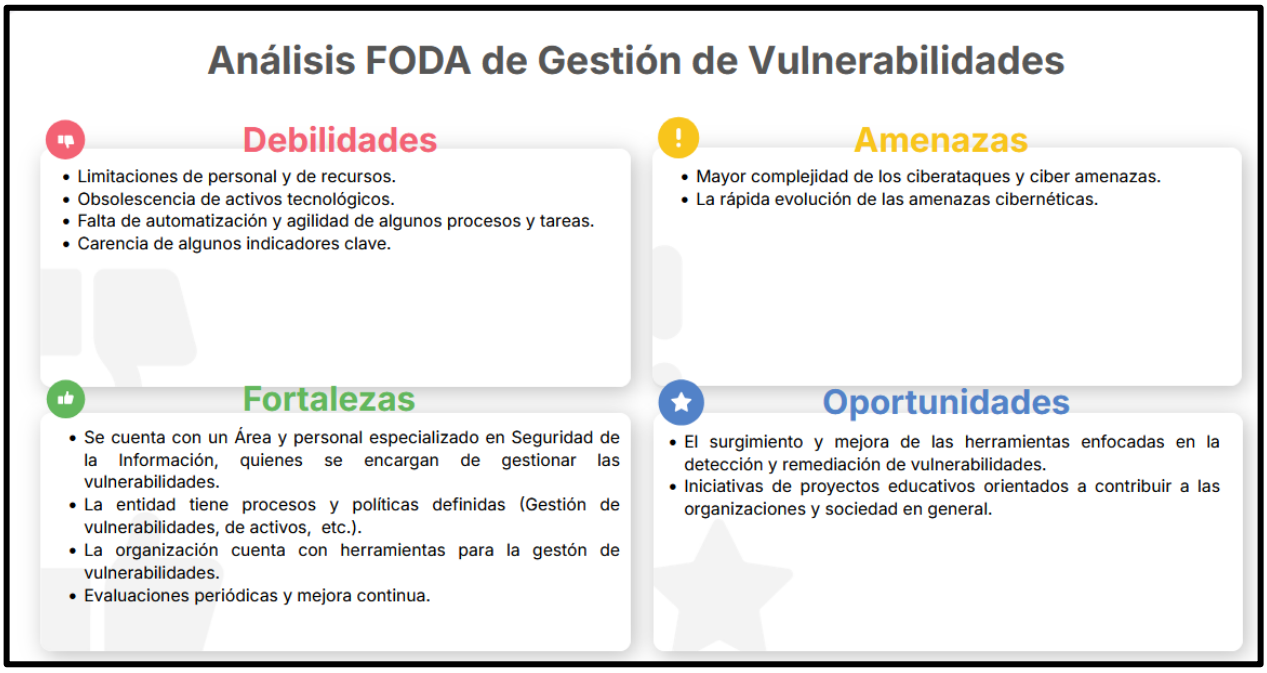
		DE.CM-09: Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles acontecimientos adversos.		
	Análisis de eventos adversos (DE.AE).	DE.AE-02: Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas.	23. Sobre el análisis de eventos adversos (Seleccione aquellas que se practican en la organización):	
		DE.AE-03: Se correlaciona la información procedente de diversas fuentes.	21. ¿De dónde se reciben informes sobre vulnerabilidades en los activos tecnológicos (Puede marcar una o ambas)?	Conocimiento de los riesgos.
		DE.AE-04: Se comprende el impacto estimado y el alcance de los acontecimientos adversos.	23. Sobre el análisis de eventos adversos (Seleccione aquellas que se practican en la organización):	Repetible.
		DE.AE-06: La información sobre acontecimientos adversos se proporciona al personal y a las herramientas autorizadas.		
		DE.AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis.		
		DE.AE-08: Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos.		

Nota: Elaboración propia.

4.2.4 APROVECHAMIENTO PARCIAL DE LAS HERRAMIENTAS DISPONIBLES

A través de los diferentes instrumentos se pudo comprobar que la Cooperativa cuenta con software especializado en la detección de vulnerabilidades. A continuación, detallamos los datos captados:

– **Dimensión de fortalezas del FODA referente al uso de herramientas en la gestión de vulnerabilidades**: La Cooperativa posee una solución para el despliegue de parches y otra para la identificación de vulnerabilidades. Estas cuentan con su respectiva licencia y soporte vigente por parte de proveedores.



– **Lista de verificación basada en ISO 27002:** Esta lista de verificación inicial no ahonda en detalles. Sin embargo, permite corroborar el uso de este tipo de herramientas por parte del equipo de seguridad de la información como parte del proceso de identificación de vulnerabilidades dentro de la infraestructura tecnológica.

Tabla 48 *Lista de verificación sobre la gestión de vulnerabilidades técnicas*

Controles	Aplicado		Observaciones
	SI	NO	
I. Identificación de vulnerabilidades técnicas.			
1. Se tiene definidas las funciones y responsabilidades asociadas a la gestión técnica de vulnerabilidad, incluida supervisión de vulnerabilidad, evaluación de riesgo de esta, actualización, monitoreo de activos y cualquier responsabilidad de coordinación necesaria.	X		El departamento de seguridad de la información es el responsable de velar por todo aquello relacionado con la gestión de vulnerabilidades.
2. Se tiene identificados los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento de las mismas, en el caso de programas informáticos y otras tecnologías.	X		La Cooperativa cuenta con licenciamiento de soluciones de software, para detectar vulnerabilidades en sus activos tecnológicos, personal especializado, procesos y políticas para este fin.
3. Se usan herramientas de exploración de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si la aplicación de parches a las vulnerabilidades fue exitosa.	X		Efectivamente, las herramientas existentes pueden ejecutar escaneos superficiales o en profundidad y también, validar el estado en aplicación de parches.
4. Se realizan pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades.	X		Se ejecutan diferentes ciclos de pruebas tanto por parte del equipo de seguridad de la información como por terceros contratados.
5. La organización cuenta con procedimientos y capacidades para detectar existencia de vulnerabilidades en sus productos y servicios.	X		Si ya que se cuenta con diferentes escaneos focalizados que evalúan la existencia de vulnerabilidades en los productos y servicios de COACEHL.
II. Evaluación de vulnerabilidades técnicas.			
6. Se analizan y verifican los informes para determinar qué actividad de respuesta y reparación es necesaria.	X		Se reciben y analizan los resultados de los informes tanto internos como externos para identificar los activos afectados y las remediaciones pertinentes.
7. Se identifican los riesgos asociados y las acciones a realizar, una vez identificada una posible vulnerabilidad técnica. Estas acciones pueden consistir en la actualización de los sistemas vulnerables o en la aplicación de otros controles.	X		
I**II. Medidas apropiadas para hacer frente a las vulnerabilidades técnicas.**			
8. Se cuenta con un proceso de gestión de actualizaciones de "software" para garantizar que se instalan los parches y actualizaciones de aplicaciones más recientes para todo el "software" autorizado.	X		Se cuenta con una política y un proceso específico para este control.
9. Se define un calendario para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes.	X		El equipo de seguridad de la información planifica y ejecuta las acciones frente a las notificaciones de vulnerabilidades.
10. Se prueban y evalúan actualizaciones antes de instalarlas para garantizar que son eficaces y no provocan efectos secundarios que no se puedan tolerar.	X		La Cooperativa cuenta con ambientes de prueba donde se certifica si hay afectación antes de desplegar en ambientes productivos las actualizaciones.
IV. Otras consideraciones.			
11. Se mantiene un registro de auditoría para todos los pasos realizados en gestión de vulnerabilidades técnicas.	X		Existe un registro de las acciones realizadas en la gestión de vulnerabilidades que se revisa mediante auditorías internas y externas.
12. El proceso de gestión de vulnerabilidad técnica se debería supervisar, evaluar periódicamente para garantizar su eficacia y eficiencia.	X		El proceso se revisa al menos una vez al año para identificar puntos de mejora y garantizar su eficiencia.

Nota: Elaboración propia

– **Entrevista al equipo de seguridad de la información**: Para cumplir con el segundo objetivo orientado a identificar el uso y percepción de las herramientas de identificación de vulnerabilidades en COACEHL, se incluyó una sección dentro del instrumento de la entrevista focalizado en capturar datos relevantes sobre este particular, puntualmente las respuestas a las interrogantes 25 – 28 están diseñadas para tal propósito.:

Tabla 49 *Distribución de preguntas de entrevista enfocadas en la exploración de herramientas*

Sección del instrumento de la entrevista	Preguntas
Exploración de Herramientas.	25, 26, 27, 28.

Nota: Elaboración propia.

El detalle con los datos captados se muestra a continuación:

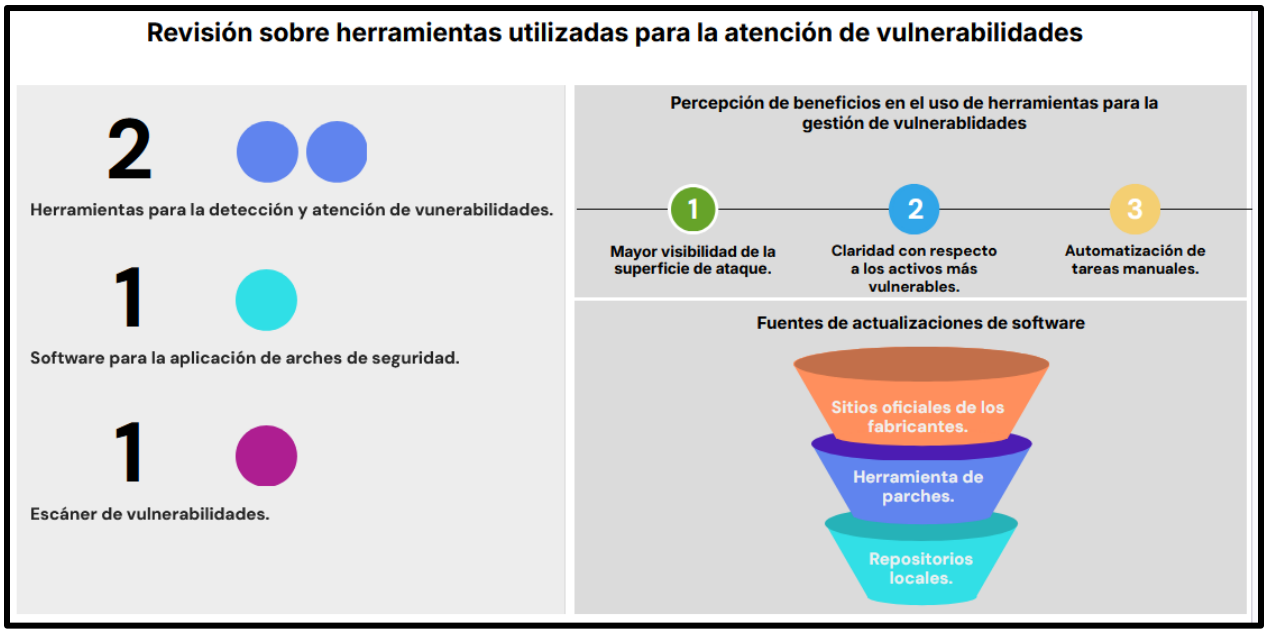
Tabla 50 *Matriz de preguntas para la evaluación del uso de herramientas en la detección de vulnerabilidades*

Sección del instrumento	Pregunta	Oficial	Jefe
Exploración de Herramientas	25. ¿Actualmente se cuenta con algunas de estas herramientas? (Puede marcar varias opciones).	- Herramienta de parcheo. - Escáner de vulnerabilidades.	
	26. ¿Se emplea alguno de estos productos? (Puede marcar varias opciones).	- Nessus (o Tenable). - Manage Engine Endpoint Central.	
	27. ¿Qué beneficios encuentra usted en estas herramientas? (Puede seleccionar varias opciones).	- Mayor visibilidad de la superficie de ataque. - Claridad con respecto a activos más vulnerables. - Automatización de tareas manuales.	
	28. Las actualizaciones de software se obtienen y despliegan desde (Puede marcar varias opciones).	- Sitios oficiales de los fabricantes. - Herramienta de gestión de parches. - Repositorios locales.	

Nota: Elaboración propia.

Inicialmente, es importante comentar sobre las herramientas, que el equipo de seguridad de la información señala que, como parte de las mejoras del departamento, se han venido gestionando los recursos para la implementación de estas herramientas. Adicionalmente, el equipo coincide en los beneficios percibidos em el uso de estas soluciones, mismas que vienen a ampliar las capacidades y los servicio que seguridad del información entrega a COACEHL.

Figura 47 *Resultados de revisión de herramientas utilizadas para la gestión de vulnerabilidades*



Nota: Elaboración propia.

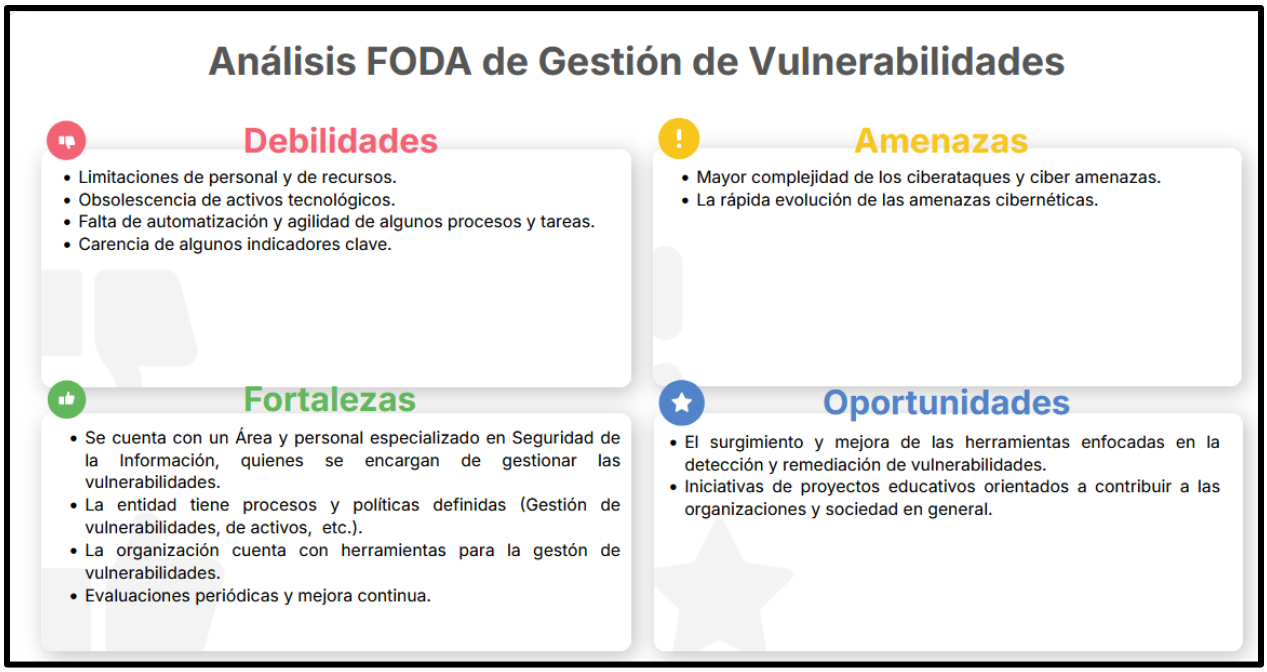
Estas soluciones han permitido algunos avances en cuanto a centralizar y consolidar las actualizaciones y como tal, la gestión de vulnerabilidades. Sin embargo, se requiere una mayor conexión entre las herramientas y el proceso de gestión de vulnerabilidades. Adicionalmente, no existe un flujo que canalice de forma estandarizada todos los reportes generados, dándole un mayor orden y sentido a esta información. Esto genera un cumulo de datos sin mayor sentido. De acuerdo con NIST CSF 2.0 esta automatización de tareas debe conectarse de forma más granular con los demás componentes del proceso y con los

objetivos estratégicos del negocio.

4.2.5 FALTA DE INDICADORES CLAVE DE DESEMPEÑO

Por medio de la matriz FODA se logró identificar la ausencia de algunos indicadores clave. Actualmente la organización mide la aplicación de parches de seguridad, pero no las vulnerabilidades atendidas ni tampoco excepciones. Esto es importante porque es necesario establecer la trazabilidad de la atención de las vulnerabilidades en el tiempo.

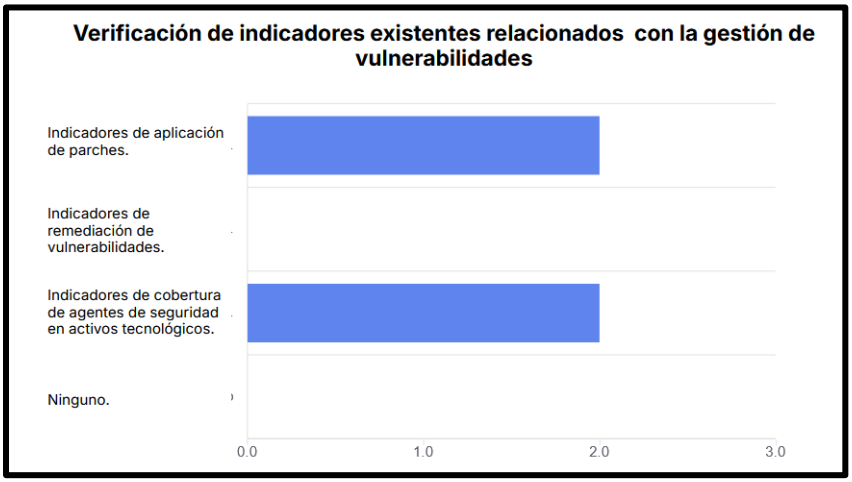
Figura 48 *Análisis FODA de la de gestión de vulnerabilidades*



Nota: Elaboración propia.

También en base a las respuestas obtenidas en la entrevista podemos establecer que se cuenta con los siguientes indicadores.

Figura 49 *Verificación de indicadores existentes relacionados con la gestión de vulnerabilidades*



Nota: Elaboración propia.

Si bien COACEHL cuenta con la mayoría de los indicadores descritos encontramos que existen oportunidades de mejora especialmente en el seguimiento de remediación de vulnerabilidades distintas a actualizaciones de seguridad. Esto genera una visión parcial y fragmentada de las vulnerabilidades existentes dentro de la infraestructura tecnológica.

4.2.6 CONOCIMIENTO Y USO DE MEJORES PRÁCTICAS Y MARCOS DE REFERENCIA

Como parte de la investigación era necesario indagar si el equipo de seguridad de la información de COACEHL cuenta con conocimientos de los estándares internacionales (como la familia ISO 27000, COBIT 2019, o el mismo NIST) y si estos se han implementado de alguna manera dentro de la Cooperativa. Esto es relevante no solo para comprender la forma en que se usan estos estándares como parámetro de medición sino también, para respaldar la importancia de la propuesta para la organización.

Para este objetivo se emplearon principalmente la Matriz FODA y entrevista semiestructurada:

- **Dimensión de fortalezas del FODA en cuanto al conocimiento y uso de**

estándares de seguridad de la información y ciberseguridad: Una de las fortalezas de COACEHL es que para el área de seguridad de la información procura contratar a personal con conocimiento y experiencia en el uso de estándares internacionales. También (y como ya se ha mencionado en otros apartados), la organización cuenta con su Sistema de Gestión de Seguridad de la Información (basado en ISO 27001) y algunas de las prácticas de ITIL y COBIT 2019.

– **Entrevista al equipo de seguridad de la información**: Dentro de la sección: "Gobierno de TI y alineamiento estratégico", se agruparon las preguntas dirigidas a esta exploración sobre el conocimiento y uso de estándares internacionales en el proceso de gestión de vulnerabilidades.

Tabla 51 *Distribución de preguntas de entrevista enfocadas en la exploración del conocimiento y uso de mejores prácticas*

Sección del instrumento de la entrevista	Preguntas
Gobierno de TI y alineamiento estratégico.	8. 9, 10.

Nota: Elaboración propia.

Los resultados y su análisis correspondiente se muestran a continuación.

Tabla 52 *Matriz de preguntas sobre exploración del conocimiento y uso de estándares de Ciberseguridad*

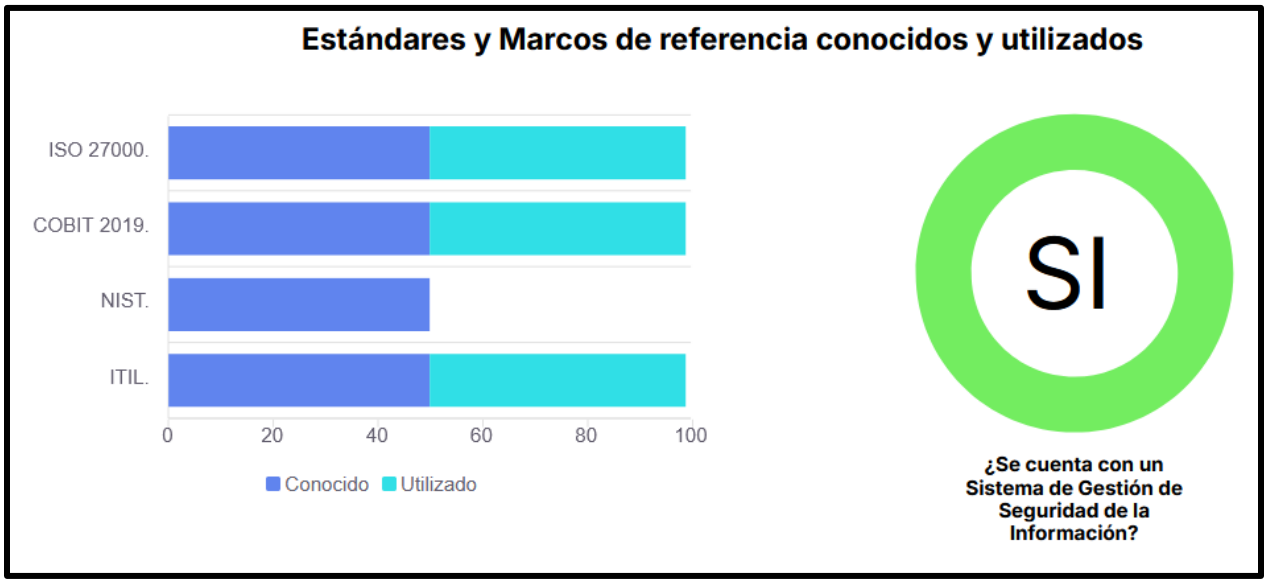
Sección del instrumento	Pregunta	Oficial	Jefe
Gobierno de TI y alineamiento estratégico.	8. ¿Qué marcos conoce relacionados con Gobierno de TI, Seguridad de la Información y Ciberseguridad? (Márquelos).	- Familia ISO 27000 (27001, 27002, 27005, etc.). - COBIT 2019. - NIST. - ITIL.	
	9. ¿Cuál de los siguientes marcos se aplica en la empresa? (Márquelos).	- Familia ISO 27000 (27001, 27002, 27005, etc.).	

		- COBIT 2019. - ITIL.
	10. ¿La empresa cuenta con un Sistema de Gestión de Seguridad de la Información?	- Si.

Nota: Elaboración propia.

De acuerdo con las respuestas de los participantes, se puede constatar que cuentan con conocimiento en los estándares y marcos referentes en Seguridad de la Información y Ciberseguridad. La mayoría de ellos también forman parte del conjunto de buenas prácticas aplicadas en COACEHL. Únicamente, en el caso de NIST aún no se utiliza en la organización.

Figura 50 *Resultados de evaluación de estándares y marcos de referencia conocidos y utilizados*



Nota: Elaboración propia.

Un segundo aspecto evaluado fue la existencia del Sistema de Gestión de Seguridad de la Información, que se encuentra dentro de lo descrito por la ISO 27001. Esto solamente para efectos de mantener la coherencia teórica, ya que como se mencionó en la sección del

macroentorno, este envuelve todo el conglomerado de procesos y políticas orientadas a la seguridad de la información y ciberseguridad.

Con todo lo detallado hasta ahora como resultado de la aplicación de los instrumentos, es momento de dar paso a las conclusiones y recomendaciones.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Considerando los resultados obtenidos mediante los diferentes instrumentos aplicados a los colaboradores del departamento de seguridad de la información de COACEHL, se establece que que hay una oportunidad para mejorar el proceso de gestión de vulnerabilidades ya existente.

1. En base a los resultados del perfilamiento NIST CSF 2.0 se concluye que el proceso actual se encuentra mayormente en un nivel: Repetible. Sin embargo, el control ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades se encuentra en una etapa de conocimiento lo que denota que la forma en que se recibe, procesa y canaliza la información sobre vulnerabilidades debe ajustarse para consolidar y estandarizar el tratamiento y respuesta de la organización para las brechas de seguridad identificadas. Esto coincide de alguna manera con el contexto de país pues como se describió en el microentorno y marco legal existen pocas iniciativas y un bajo avance en la adopción de mejores prácticas de ciberseguridad en las organizaciones.
2. Considerando los hallazgos encontrados mediante la Lista de verificación de ISO 27002:2022 y la Matriz de Análisis FODA, se ha podido constatar que la entidad cuenta con un cierto grado de automatización del proceso, utilizando algunas soluciones de software ya implementadas para la aplicación de parches de seguridad y

escaneo de vulnerabilidades. Sin embargo, es evidente la desconexión entre las herramientas y el proceso de gestión de vulnerabilidades lo que representa una posible mejora en el proceso. La mayoría de los marcos de referencia (incluido el NIST CSF 2.0) están recomendando a las organizaciones a conectar: Personas, procesos y herramientas de modo que todo contribuya al cumplimiento de los objetivos estratégicos del negocio.

3. A través de la entrevista semiestructurada se logró establecer que el personal de seguridad de la información cuenta con un alto nivel de conocimiento sobre marcos de referencia como: COBIT 2019, la familia ISO 27000 o el Marco de Seguridad Cibernética del NIST CSF 2.0 lo que permite garantizar la comprensión del propósito de la investigación, así como reconocer el valor y la relevancia de la propuesta con las mejoras identificadas. Al contar con el criterio de un equipo de expertos en esta unidad, se ha comprobado que es necesaria una mayor utilización de este tipo de estándares para dar más consistencia y vigencia a los procesos de la institución. Definir los procesos en base a mejores prácticas contribuye a que las organizaciones puedan realizar estudios más precisos para reconocer mejoras, medir sus avances en madurez de manera más concreta e incluso prepararse para certificaciones organizacionales.
4. Finalmente, el proceso de gestión de vulnerabilidades se encuentra en su estado de madurez actual por la influencia que han ejercido las normativas emitidas por entidades como: El Congreso Nacional, la Comisión Nacional de Bancos y Seguros, el Consejo Superior de Cooperativas, etc., por los esfuerzos de mejora continua planteados en el Plan Operativo Anual de COACEHL y por la iniciativa del equipo de seguridad de la información quienes de una forma empírica definieron las etapas del

proceso vigente.

5.2 RECOMENDACIONES

1. Se recomienda rediseñar el proceso buscando que este logre rescatar las fortalezas de lo que ya se hace, pero también, que incorpore las mejoras necesarias para robustecer la gestión de vulnerabilidades dentro de COACEHL. Esto incluye la programación de las remediaciones, la implementación de algunos indicadores y la documentación de las diferentes actividades realizadas por etapa.
2. En cuanto a las herramientas y recursos, es necesario encontrar formas de lograr sacar mayor beneficio de los recursos disponibles procurando centralizar y automatizar la gestión de vulnerabilidades, aumentar la productividad y hacer un uso óptimo de los mismos.
3. Usar estándares probados dentro de los procesos organizacionales, no solamente contribuye al cumplimiento de aspectos legales y normativos. Esto fortalece a las organizaciones pues les permite operar bajo esquemas de trabajo eventualmente certificables y menos subjetivos. Lo anterior, permite una mayor trazabilidad, seguimiento y medición de cumplimiento de forma más precisa. Por ello, es necesario lograr formular una propuesta sustentada en dichos estándares como el Marco de Seguridad Cibernética del NIST 2.0 para que COACEHL pueda usarlo en la gestión de vulnerabilidades.
4. Se debe mejorar la generación de reportes o informes con indicadores clave de desempeño (KPI) de actividades en la remediación de vulnerabilidades. Esto es importante para qué, tanto las áreas como la gerencia, puedan tener visibilidad suficiente para ver avances y tomar decisiones que fortalezcan la ciberseguridad a nivel

de toda la organización.

5. Generar recursos explicativos (como videos, presentaciones y documentos guias explicativos) para que el equipo de seguridad de la información se apropie de la propuesta y pueda encaminar su adopción en COACEHL.

CAPÍTULO VI. APLICABILIDAD

6.1 PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST CSF 2.0 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

El presente capitulo detalla la propuesta de un proceso para la gestión de vulnerabilidades considerando las capacidades actuales de COACEHL, pero a su vez, deja sentadas las bases para potenciales mejoras futuras que se puedan incorporar en la organización y específicamente, en la unidad de seguridad de la información.

6.2 JUSTIFICACIÓN

Considerando los hallazgos identificados mediante la aplicación de los diferentes instrumentos, se ha podido comprobar que, si bien COACEHL cuenta con un proceso y seguimiento de las vulnerabilidades en sus activos tecnológicos, existen oportunidades de mejora de cara a alcanzar mayor madurez, especialmente en cuanto a la consolidación del flujo a seguir, la documentación generada, uso de herramientas e indicadores de desempeño.

Se ha establecido que el proceso actual debe ampliarse para cubrir no solamente lo relacionado con la dimensión de parches o actualizaciones sino cualquier vulnerabilidad en los activos tecnológicos. Además, este no deja claro el tratamiento que se le dará a hallazgos de pruebas de penetración o auditorías externas, así como tampoco permite determinar cómo organizar la información generada durante la ejecución de las tareas. En última instancia, falta

establecer indicadores de desempeño específicos y congruentes con la actividad de remediación de vulnerabilidades.

Es así, como esta propuesta busca fortalecer el alineamiento de las actividades de seguridad de la información, en cuanto a gestión de vulnerabilidades se refiere, para generar una mayor conexión con los objetivos estratégicos de COACEHL, permitiéndole a la organización garantizar la prestación de servicios de forma continua y con los niveles de calidad que sus clientes merecen.

6.3 OBJETIVOS DE LA PROPUESTA

6.3.1 OBJETIVO GENERAL

Exponer un proceso estructurado para la gestión de vulnerabilidades adaptando algunas de las etapas del Marco de Seguridad Cibernética del NIST CSF 2.0, mejorando con ello la capacidad de la organización para identificar y mitigar riesgos de seguridad de manera más eficiente y alineada con un estándar reconocido globalmente.

6.3.2 OBJETIVOS ESPECÍFICOS

1. Demostrar y caracterizar el flujo de gestión que se puede aplicar a las vulnerabilidades de los sistemas de COACEHL, desde su reporte inicial a través de diversas fuentes hasta su resolución final, con el fin de comprender y describir el proceso completo.
2. Exponer cómo documentar de manera más eficiente y estructurada las actividades de gestión de vulnerabilidades, facilitando el seguimiento, la auditoría y la comunicación dentro del equipo y con otras partes interesadas.
3. Ejemplificar cómo se pueden usar Indicadores Clave de Desempeño (KPI) para medir de forma efectiva el rendimiento del proceso de gestión de vulnerabilidades, permitiendo una toma de decisiones informada y la mejora continua.

6.4 RELACIÓN DE HALLAZGOS Y ESTRATEGIA DE RESPUESTA

En este apartado se establece la conexión entre los hallazgos descritos en el Capítulo V y las estrategias de respuesta que hacen parte de la propuesta del proceso para la gestión de vulnerabilidades.

– **Estrategias de mitigación de la matriz FODA**: La matriz FODA es un excelente instrumento para enriquecer el autoconocimiento organizacional e identificar potenciales puntos de mejora. Para este proyecto, dichas mejoras están enfocadas en el proceso de gestión de vulnerabilidades. Por otro lado, este análisis permite darle un mayor sentido a esta propuesta, puntualizando la respuesta a las necesidades identificadas en el proceso de recolección y análisis de datos. Estas estrategias se agrupan en cuatro grandes categorías:

- Estrategias FO (Fortalezas + Oportunidades): Describen como explotar las fortalezas internas para aprovechar las oportunidades externas.
- Estrategias DO (Debilidades + Oportunidades): Detallan como afrontar las debilidades internas canalizando las oportunidades externas.
- Estrategias FA (Fortalezas + Amenazas): Indican la forma en que se pueden utilizar las fortalezas internas para superar las amenazas externas.
- Estrategias DA (Debilidades + Amenazas): Señalan como mitigar las debilidades internas de cara a las amenazas externas.

Tabla 53 *Análisis y estrategias de mitigación de la Matriz FODA*

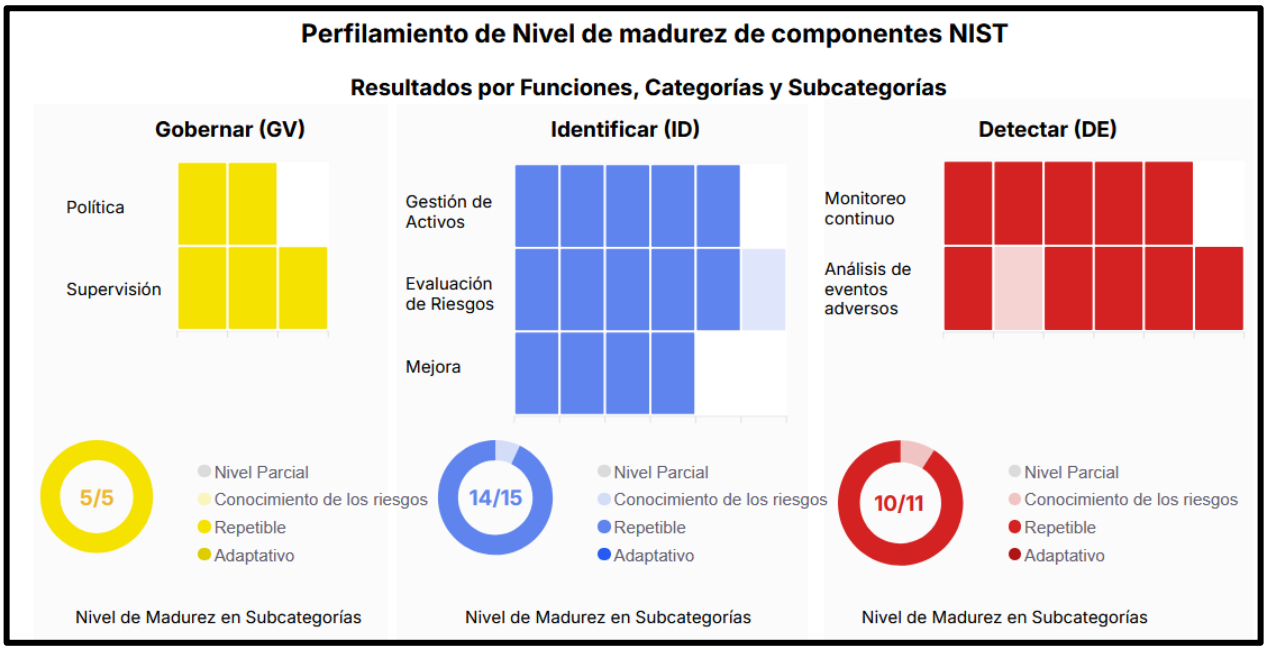
		Análisis interno	
		Fortalezas	**Debilidades**
		• Se cuenta con un Área y personal especializado en Seguridad de la Información, quienes se encargan de gestionar las vulnerabilidades. • La entidad tiene procesos y políticas definidas (Gestión de vulnerabilidades, de activos, etc.). • La organización cuenta con herramientas para la gestión de vulnerabilidades. • Evaluaciones periódicas y mejora continua.	• Limitaciones de personal y de recursos. • Obsolescencia de activos tecnológicos. • Falta de automatización y agilidad de algunos procesos y tareas. • Carencia de algunos indicadores clave.
Estrategias	**Oportunidades**	**Estrategias FO (Fortalezas + Oportunidades).**	**Estrategias DO (Debilidades + Oportunidades).**
	• El surgimiento y mejora de las herramientas enfocadas en la detección y remediación de vulnerabilidades. • Iniciativas de proyectos educativos orientados a contribuir a las	• **Nuevas estrategias para gestionar las vulnerabilidades**: Explotar las mayores y mejore capacidades que incorporan las soluciones de software modernas, principalmente las que integran diferentes características como la detección y remediación automática de vulnerabilidades. • **Alianzas estratégicas con instituciones educativas**: COACEHL puede apostarle a profundizar con alianzas estratégicas con instituciones educativas para	• **Adoptar la automatización de tareas y planear el crecimiento progresivo del área**: Automatizar algunas tareas puede ayudar a liberar tiempo del recurso humano ya disponible y aplacar un poco la necesidad de personal. Esto entretanto la organización planifica el crecimiento progresivo del área en función de su capacidad. • **Mejorar la gestión del ciclo de vida de tecnologías**: La obsolescencia es parte de la vida de los activos tecnológicos y

	organizaciones y sociedad en general.	aprovechar aún más su apertura a proyectos de investigación lo que le puede aportar una fuente de iniciativas que potencian la innovación y el cambio.	es importante planificar la periodicidad de las migraciones en congruencia con las fechas de fin de soporte socializadas por los fabricantes. • **Diseñar indicadores de desempeño orientados a la gestión de vulnerabilidades:** Establecer indicadores clave para la gestión de vulnerabilidades permitirá no solo mayor visibilidad sobre la superficie de ataque, sino que un mejor control y seguimiento de las remediaciones aplicadas en el tiempo.
	Amenazas	**Estrategias FA (Fortalezas + Amenazas).**	**Estrategias DA (Debilidades + Amenazas).**
	• Mayor complejidad de los ciberataques y ciber amenazas. • La rápida evolución de las amenazas cibernéticas.	• **Fortalecer la cultura de ciberseguridad**: Para poder afrontar los retos y amenazas del contexto se requiere fortalecer la cultura de ciberseguridad en toda la organización, por medio de diferentes estrategias (capacitación, boletines, campañas de concientización, ejercicios de prueba, etc.), impulsadas por el equipo de seguridad de la información. También es importante lograr el involucramiento de los dueños de los aplicativos o activos tecnológicos en el proceso de gestión de vulnerabilidades.	• **Mejora continua**: Promover la mejora continua de los procesos para adaptarse a los nuevos desafíos en ciberseguridad. Esto debe hacerse contemplando también los resultados históricos de los indicadores de desempeño para tomar decisiones en base a los datos.

Nota: Elaboración propia.

– **Perfilamiento NIST**: Al interiorizar en los elementos evaluados se pueden reconocer algunas áreas que requieren mejoría. La siguiente figura permite visualizar estos aspectos de forma general.

Figura 51 *Análisis del nivel de madurez en funciones del Marco NIST CSF 2.0*



Nota: Elaboración propia.

Otro detalle importante es que todavía no se alcanza el nivel más alto, lo que denota que se necesitan hacer o implementar algunos ajustes adicionales para fortalecer el proceso existente. Algunos aspectos puntuales se pueden establecer al cotejar los resultados actuales con los requerimientos del siguiente nivel del CSF de NIST 2.0 (en este caso el nivel 3 y 4) dentro del apartado: Gestión de riesgos de seguridad cibernética.

Para una mayor comprensión, a continuación, se presentan dos cuadros: El primero, es la Matriz de Perfilamiento NIST y el segundo es una tabla donde se puede ver la conexión entre los principales hallazgos encontrados y los objetivos de esta propuesta, que sirve como antesala a la exposición de las etapas del nuevo proceso para la gestión de vulnerabilidades.

Tabla 54 *Matriz de Perfilamiento Organizativo NIST CSF 2.0*

COMPONENTES DEL NÚCLEO			Perfil Actual	Perfil Objetivo	Acciones requeridas
Función	**Categoría**	**Subcategoría**			
Gobernar (GV).	Política (GV.PO).	GV.PO-01: La política de gestión de riesgos de seguridad cibernética se establece en base al contexto organizativo, la estrategia de seguridad cibernética y las prioridades, y es comunicada y aplicada.	Repetible	Adaptable	- Aplicar estas acciones de forma coherente y conforme a lo previsto. Supervisar y revisarlas continuamente. - Se requiere adaptar las actividades de seguridad cibernética en base a mejores prácticas, lecciones aprendidas e indicadores. - Utilizar la información en tiempo real (o casi real) para comprender los riesgos de seguridad cibernética asociados a sus proveedores, productos y servicios que adquiere y utiliza, y actuar de forma coherente al respecto. - La información sobre seguridad cibernética se comparte constantemente en toda la organización y
		GV.PO-02: La política de gestión de riesgos de seguridad cibernética se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización.			
	Supervisión (GV.OV).	GV.OV-01: Los resultados de la estrategia de gestión de riesgos de seguridad cibernética se revisan para informar y ajustar la estrategia y la dirección.			
		GV.OV-02: La estrategia de gestión de riesgos de seguridad cibernética se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización.			
		GV.OV-03: El rendimiento de la gestión de riesgos de seguridad cibernética de la organización se evalúa y revisa para realizar los ajustes necesarios.			
Identificar (ID).	Gestión de activos (ID.AM).	ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización.			
		ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización.			
		ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores.			
		ID.AM-07: Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.			
		ID.AM-08: Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de			

		vida.			con terceros autorizados.
	Evaluación de riesgos (ID.RA)	ID.RA-01: Se identifican, validan y registran las vulnerabilidades de los activos.			
		ID.RA-02: Se recibe información sobre amenazas cibernéticas de foros y fuentes de intercambio de información.			
		ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización.			
		ID.RA-04: Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades			
		ID.RA-07: Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento			
		ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades	Conocimiento de los riesgos.	Repetible	
	Mejora (ID.IM).	ID.IM-01: Las mejoras se identifican a partir de evaluaciones.	Repetible	Adaptable	
		ID.IM-02: Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.			
		ID.IM-03: Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos.			
		ID.IM-04: Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de seguridad cibernética que afectan a las operaciones.			
Detectar (DE).	Monitoreo continuo	DE.CM-01: Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos.			

	(DE.CM).	DE.CM-02: Se monitorea el entorno físico para detectar posibles acontecimientos adversos.			
		DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.			
		DE.CM-06: Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar acontecimientos potencialmente adversos.			
		DE.CM-09: Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles acontecimientos adversos.			
	Análisis de eventos adversos (DE.AE).	DE.AE-02: Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas.			
		DE.AE-03: Se correlaciona la información procedente de diversas fuentes.	Conocimiento de los riesgos.	Repetible	
		DE.AE-04: Se comprende el impacto estimado y el alcance de los acontecimientos adversos.	Repetible.	Adaptable	
		DE.AE-06: La información sobre acontecimientos adversos se proporciona al personal y a las herramientas autorizadas.			
		DE.AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis.			
		DE.AE-08: Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos.			

Nota: Elaboración propia.

Tabla 55 *Relación entre objetivos de la propuesta y estrategias de respuesta*

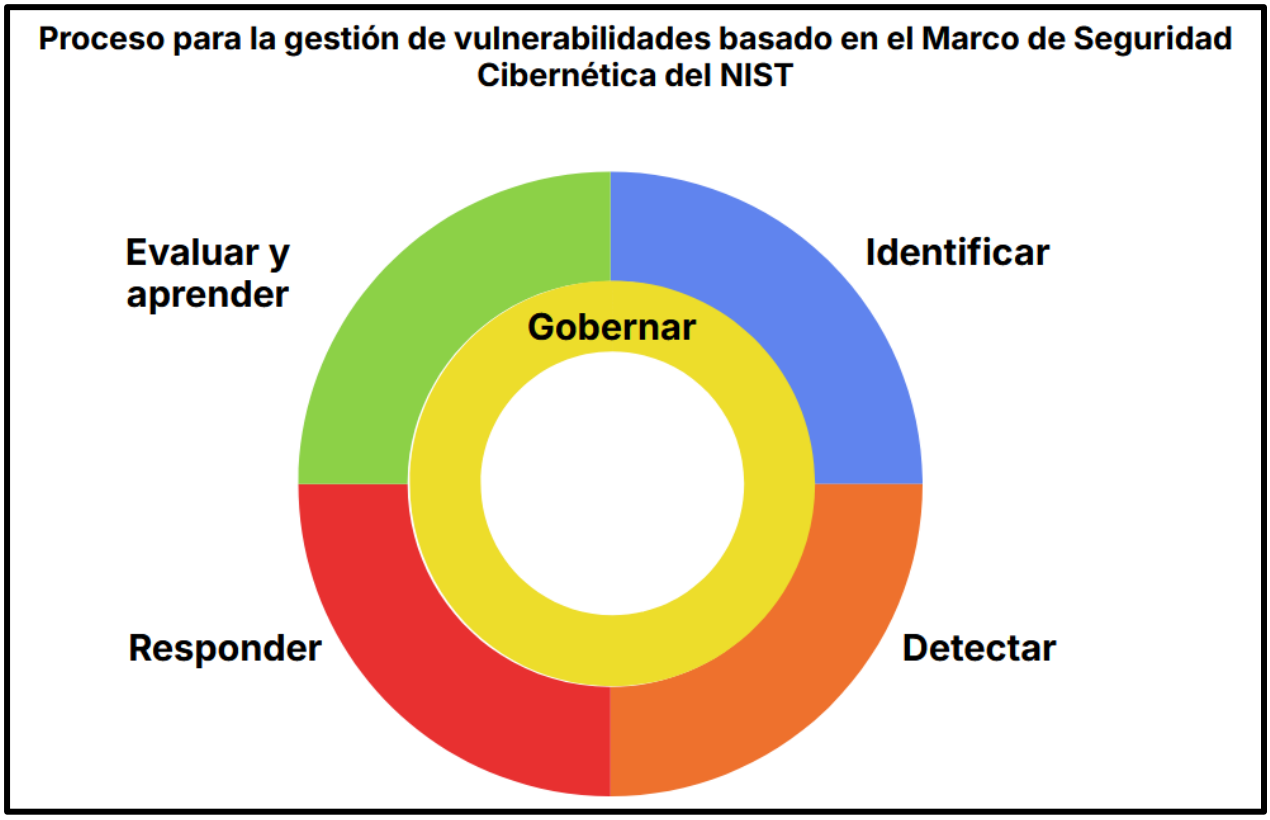
N°	Objetivo de propuesta	Estrategias de mitigación de la Matriz de análisis FODA	Acciones requeridas en base a la Matriz de Perfilamiento Organizativo de NIST
1	Demostrar el flujo que pueden seguir las vulnerabilidades reportadas desde diversas fuentes de información.	Nuevas estrategias para gestionar las vulnerabilidades.	Aplicar estas acciones de forma coherente y conforme a lo previsto. Supervisar y revisarlas continuamente.
2	Modelar mediante el uso de herramientas de software, como se pueden documentar las actividades del proceso de gestión de vulnerabilidades.	Fortalecer la cultura de ciberseguridad.	Utilizar la información en tiempo real (o casi real) para comprender los riesgos de seguridad cibernética asociados a sus proveedores, productos y servicios que adquiere y utiliza, y actuar de forma coherente al respecto.
3	Ejemplificar Indicadores Clave de Desempeño (KPI) que pueden utilizarse para medir el rendimiento en la gestión de vulnerabilidades.	Diseñar indicadores de desempeño orientados a la gestión de vulnerabilidades.	Se requiere adaptar las actividades de seguridad cibernética en base a mejores prácticas, lecciones aprendidas e indicadores.
			La información sobre seguridad cibernética se comparte constantemente en toda la organización y con terceros autorizados.

Nota: Elaboración propia.

6.5 ETAPAS DEL PROCESO DE GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO NIST CSF 2.0

Algunos de los componentes del Marco de Seguridad Cibernética del NIST CSF 2.0 pueden adaptarse para formar un ciclo coherente en el proceso de remediación de vulnerabilidades como se detalla en la siguiente figura:

Figura 52 *Proceso para la Gestión de Vulnerabilidades basado en el Marco de Seguridad Cibernética del NIST*



Nota: Elaboración propia.

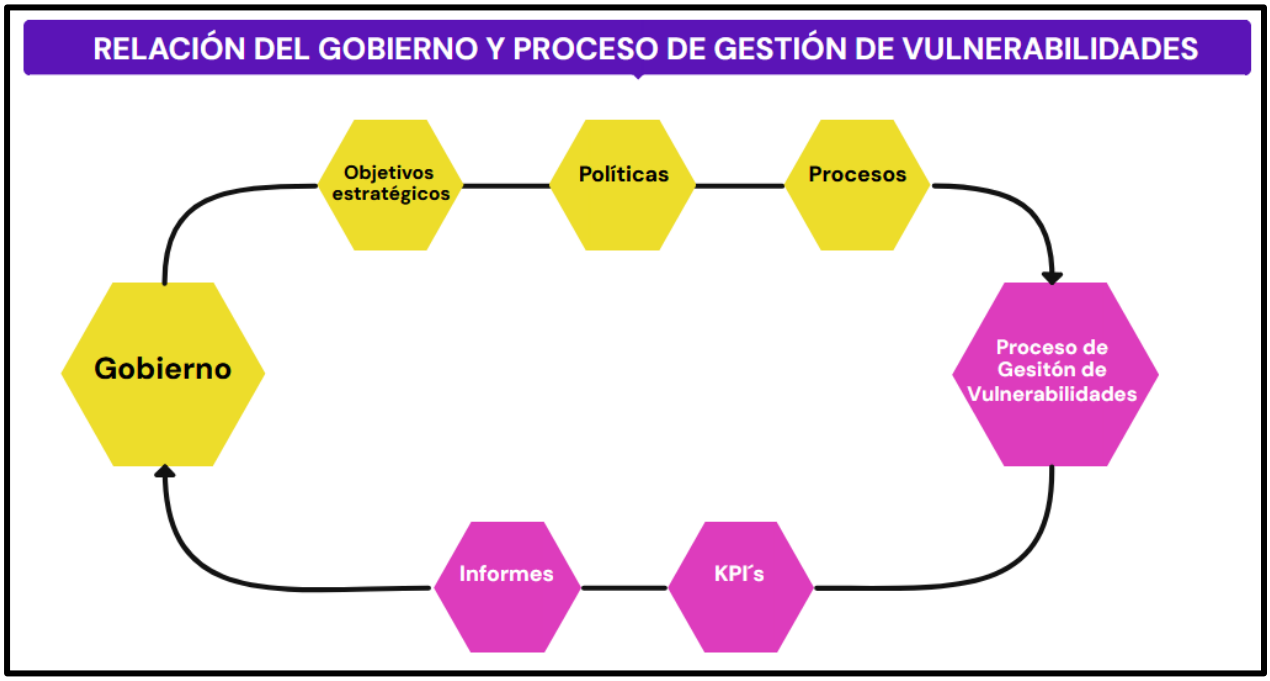
A continuación, se detallan las etapas de este proceso y los insumos generados en cada instancia:

6.5.1 GOBERNAR

En esta instancia se pretende ofrecer un espacio para conectar las políticas, otros procesos y

objetivos estratégicos del negocio con la gestión de vulnerabilidades. También, esta función se establece para que exista el seguimiento y la rendición de cuentas producto de la ejecución del proceso, generando indicadores de desempeño (KPI) e informes que permitan a los altos mandos dimensionar la postura de seguridad de la entidad y tomar decisiones informadas en base a los resultados.

Figura 53 *Relación del proceso de gestión de vulnerabilidades y la función Gobierno*



Nota: Elaboración propia.

En COACEHL, las políticas y procesos se revisan al menos una vez al año por lo que existe la apertura para implementar mejoras en sus prácticas en el corto plazo. En ese sentido el proceso de gestión de vulnerabilidades puede contribuir a identificar:

- Servicios y procesos del negocio expuestos a indisponibilidad por vulnerabilidades no atendidas u obsolescencia.
- Eficiencia y eficacia en la gestión de vulnerabilidades.
- Postura del negocio en cuanto a ciberseguridad se refiere.

El detalle sobre informes e indicadores entregados como parte del proceso de gestión de vulnerabilidades se exponen en el apartado: Evaluar y aprender.

6.5.2 IDENTIFICAR

En esta etapa es donde se mapean los activos tecnológicos de la organización. Para que la identificación sea efectiva es importante mantener el inventario de equipos actualizado registrando las altas y bajas que forman parte del ciclo de vida de la tecnología.

Tabla 56 *Entradas, procesos y salidas de etapa Identificar*

Entradas	Procesos	Salidas	Indicadores
- Inventario de activos a la fecha.	- Identificación de nuevos equipos (Servidores, estaciones de trabajo, etc.). - Instalación de agentes de herramientas de seguridad. - Ingreso de nuevos activos a grupos y escaneos. - Depuración de objetos dados de baja.	- Inventario de activos actualizado.	- Métrica de servidores. - Métrica de estaciones de trabajo. - Métrica de dispositivos de red.

Nota: Elaboración propia.

La vigencia de este inventario es fundamental para tener una visión completa de la superficie de ataque existente en la organización.

A continuación, ampliamos un poco más las actividades:

– **Identificación de nuevos equipos** (Servidores, estaciones de trabajo, dispositivos de red, etc.): Implica el registro de estos activos en el medio destinado para llevar el control (CMDB, Base de datos, hoja de cálculo, etc.).

– **Instalación de agentes de herramientas de seguridad**: Hace referencia al despliegue de todos los agentes y herramientas de seguridad en los equipos (Antivirus, SIEM, herramienta de parcheo, etc.).

– **Ingreso de nuevos equipos a escaneos o grupos de atención** (Servidores, estaciones de trabajo, etc.): Aquí es donde los activos deben ser ingresados a los grupos o contenedores creados previamente para organizarlos según su tipo (Servidores, estaciones de trabajo, dispositivos de red, etc.).

– **Depuración de objetos dados de baja**: Los activos dados de baja deben ser depurados de las herramientas para economizar licencias, optimizar el consumo de recursos empleado para analizar elementos inexistentes y limpiar las vistas de los datos en los reportes. Esto también evidencia un buen manejo de ciclo de vida de los activos tecnológicos.

El inventario de activos debería evidenciar al menos los siguientes detalles:

- Nombre identificador del dispositivo.
- Dirección IP.
- Ambiente (Si aplica).
- Servicio (Si aplica).
- Área dueña del activo o servicio.
- Criticidad del activo (Si aplica).

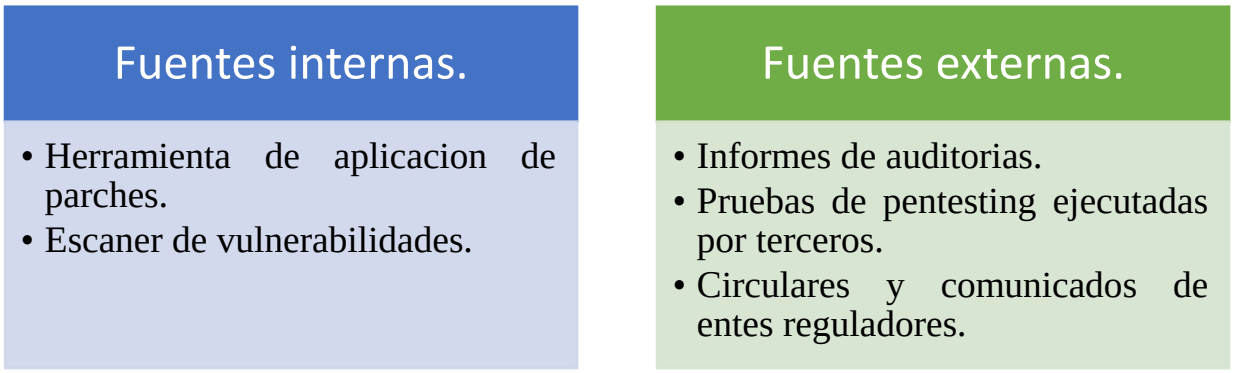
Estos detalles juagan un rol fundamental para poder conectar posteriormente las vulnerabilidades con los activos y principalmente, con los servicios que estas tecnologías prestan a clientes internos y externos de la Cooperativa. Por ello, se incluye a las áreas dueñas de los activos o aplicaciones para no solo abordar detalles técnicos, sino que también, conectar estos con la vida

productiva de COACEHL.

6.5.3 DETECTAR

En este apartado es importante mencionar que la institución cuenta con diferentes fuentes de datos acerca de las vulnerabilidades presentes en sus equipos informáticos. Las mismas se pueden categorizar de la siguiente manera:

Figura 54 *Origen de datos sobre vulnerabilidades em COACEHL*



Nota: Elaboración propia.

La intención del proceso es poder canalizar la información obtenida por todos estos afluentes tratando de homologar información clave que pueda simplificar la respuesta a las vulnerabilidades detectadas de una forma estandarizada.

En esta etapa se identifican y analizan las vulnerabilidades en los activos tecnológicos. Considerando estos resultados se planifican las actividades de respuesta.

Tabla 57 *Entradas, procesos y salidas de etapa Detectar*

Entradas	Actividades	Salidas	Indicadores
- Inventario de activos a la actualizado. - Resultados de escaneos de herramientas especializadas	- Identificación de vulnerabilidades. - Investigación de acciones de remediación. - Planificación de ventanas de	- Reporte de vulnerabilidades. - Reporte de parches. pendientes de aplicar.	- Métrica inicial de vulnerabilidades. - Métrica inicial de parches. - Métrica inicial de equipos.

propias o por parte de terceros.	remediación considerando el inventario actualizado.	- Informes de investigación para la remediación de vulnerabilidades. - Informe de parches aplicables. - Planificación de ventanas de mantenimiento.	

Nota: Elaboración propia.

La función Detectar descansa sobre las herramientas disponibles en la organización para tales fines, pues son ellas quienes ofrecen visibilidad acerca de las vulnerabilidades existentes en la infraestructura tecnológica. A continuación, ampliamos en mayor detalle las actividades:

– **Identificación de vulnerabilidades**: En este punto el escáner muestra las vulnerabilidades identificadas en los activos. Esto está directamente relacionado con la forma en que se actualizan las bases de conocimiento de estas herramientas (si de forma automática o con cierta periodicidad). Las mismas se pueden categorizar de diferentes maneras:

Tabla 58 *Formas de categorización de las vulnerabilidades*

Categorización de vulnerabilidades	Detalle
Por criticidad.	- Criticas. - Altas. - Medias. - Bajas. - Informativas.
Por tipo.	- Vulnerabilidades de sistemas. - Vulnerabilidades de software. - Vulnerabilidades de bases de datos. - Vulnerabilidades de día cero. - Vulnerabilidades en dispositivos de red. - Errores de configuración.

Nota: Elaboración propia.

– **Investigación de acciones de remediación**: Las acciones de remediación pueden

ser varias en función de la complejidad del caso. Pueden ir desde la aplicación de una actualización hasta la necesidad de establecer parámetros en archivos de configuración de forma manual. En tal sentido, si bien las herramientas sugieren alguna acción, se recomienda siempre hacer las evaluaciones específicas de los casos que así lo ameriten. Aquí se sugiere establecer plantillas para documentar las vulnerabilidades y correspondientes acciones de remediación. Esto permitirá gestionar mejor el conocimiento sobre cómo se remedian vulnerabilidades en ciertos productos específicos. Como parte de la propuesta se entregarán algunas plantillas de modelo que se pueden adecuar para usarse en esta etapa.

– **Planificación de ventanas de remediación considerando el inventario actualizado**: La atención de las vulnerabilidades debe calendarizarse para tener clara la traza de las acciones emprendidas y simplificar el seguimiento de impactos potenciales en caso de afectación. Estos ciclos pueden hacerse de forma quincenal o semanal en función de las necesidades de la organización. Esto contribuirá también a la notificación de las actividades y dejar caramente establecidos los tiempos de pruebas, despliegues en producción y para la validación de los servicios.

Una vez que se han completado las tareas de la etapa de detección, es momento de proceder a responder en base a las planificaciones y a los reportes de las métricas obtenidas a lo interno o como resultado de pruebas llevabas a cabo por terceros.

6.5.4 RESPONDER

Se toman medidas en relación con las vulnerabilidades detectadas. Lo ideal es hacerlo de forma progresiva aplicando inicialmente las soluciones en ambientes de prueba y posteriormente en producción.

Tabla 59 *Entradas, procesos y salidas de etapa Responder*

Entradas	Actividades	Salidas	Indicadores

- Reporte de vulnerabilidades. - Reporte de parches. pendientes de aplicar. - Informes de investigación para la remediación de vulnerabilidades. - Informe de parches aplicables. - Planificación de ventanas de mantenimiento.	- Ingreso de tickets y controles de cambio en la plataforma de Service Desk. - Ejecución de mantenimientos planificados. - Generación de documentación para evidencias.	- Correos de notificación. - Reporte de vulnerabilidades remediadas. - Reporte de parches instalados. - Reporte de equipos atendidos. - Reporte de excepciones. - Reporte de incidentes y fallas generadas por actividades de remediación.	- Métrica de vulnerabilidades remediadas. - Métrica de parches instalados. - Métrica de dispositivos atendidos. - Métrica de excepciones.

Nota: Elaboración propia.

A continuación, explicamos en detalle estas actividades:

– **Ingreso de tickets y controles de cambio**: Para efectos de generar trazabilidad y un registro histórico de las actividades, es importante asociarlas a un numero de Ticket (Para ambientes de pruebas) o un Control de Cambios (en ambientes de Producción) dentro de la plataforma ya existente en COACEHL.

– **Ejecución de mantenimientos planificados**: Se ejecutan las remediaciones de vulnerabilidades en los ambientes y activos planificados. En esta etapa es importante generar las evidencias documentales de las acciones ejecutadas tanto las que resultaron satisfactorias como los posibles errores o fallos.

– **Generación de documentación para evidencias**: Esto incluye los diferentes insumos que pueden producirse para dejar constancia de las actividades realizadas durante la remediación de vulnerabilidades. Esto puede incluir: Correos electrónicos, tickets,

controles de cambio, reportes, capturas de pantalla, etc. Dicha documentación, puede ser útil para dar constancia y respaldo de los acontecimientos suscitados en el tiempo. A continuación, resumimos como entrelazar estas actividades con sus respectivas salidas:

Tabla 60 *Evidencia documental generable durante la remediación de vulnerabilidades*

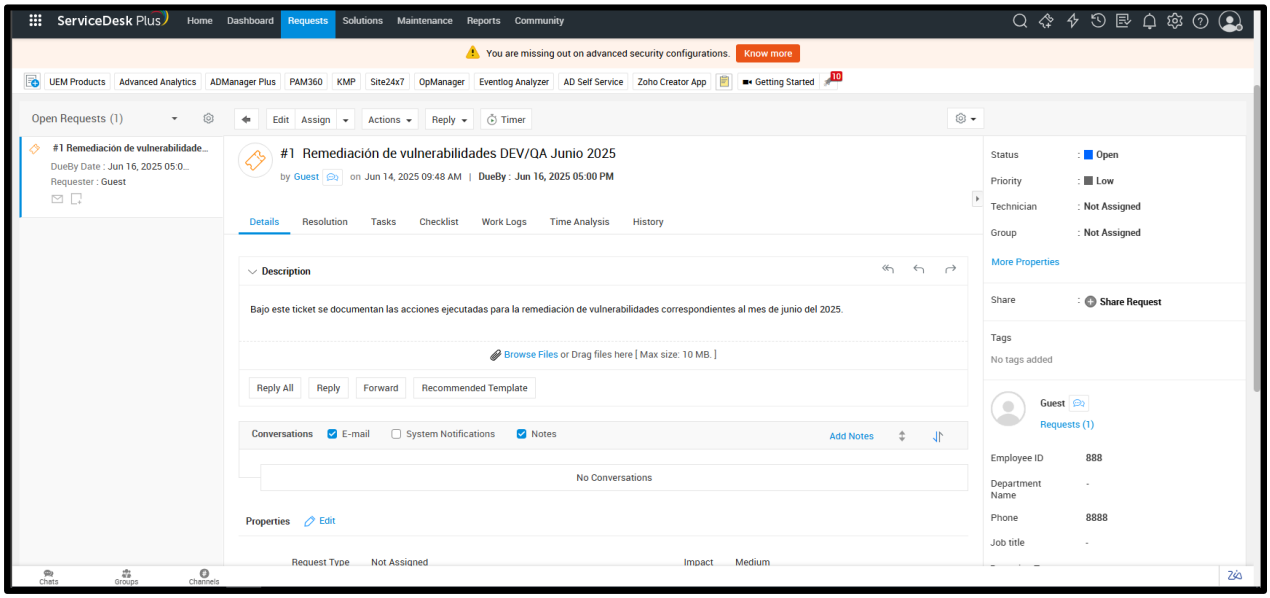
Actividad	Descripción	Documentación
Remediación de vulnerabilidades en ambiente de pruebas. Remediación de vulnerabilidades en ambiente de producción.	Se aplican las remediaciones en ambientes de prueba. Se recomienda dejar estas acciones bajo ticket (en los ambientes no productivos) y control de cambios (en los ambientes productivos) para adjuntar allí las evidencias documentales correspondientes.	- Tickets. - Controles de cambio. - Correos de notificación. - Reporte de vulnerabilidades atendidas. - Reporte de parches aplicados. - Reporte de equipos atendidos. - Evidencias de remediación. - Excepciones (si las hay y sus causas).

Nota: Elaboración propia.

COACEHL cuenta con una herramienta para gestionar tanto los tickets como los controles de cambio. En este escenario lo que se propone es utilizar los correlativos generados automáticamente por esta plataforma para asociarlo con el resto de la documentación del proceso. Vale mencionar que los datos mostrados en esta y subsecuentes figuras son meramente ejemplos parte de un laboratorio personal independiente y no representan activos ni información propiedad de COACEHL. Esto para no exponer información sensible de la Cooperativa.

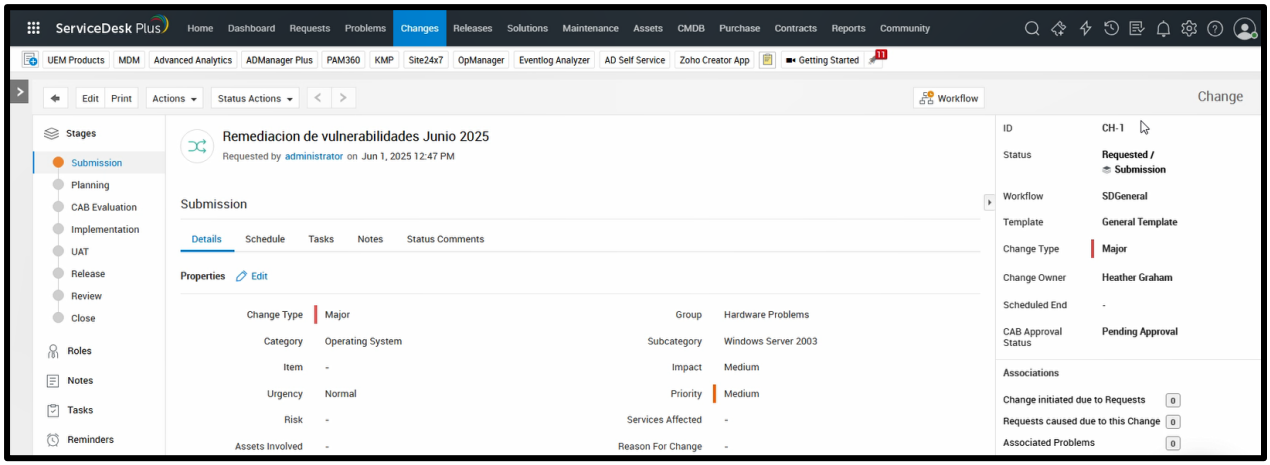
Figura 55 *Ejemplo de un ticket para documentar la remediación de vulnerabilidades en ambientes*

no productivos



Nota: Elaboración propia.

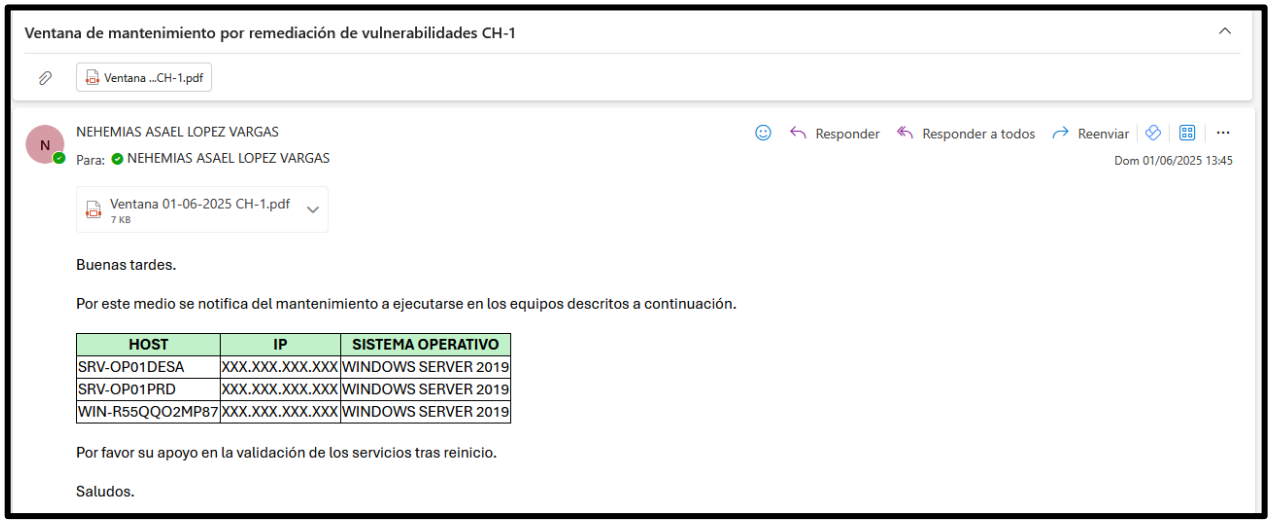
Figura 56 *Ejemplo de un control de cambio para documentar la remediación de vulnerabilidades en ambientes productivos*



Nota: Elaboración propia.

Estos correlativos pueden insertarse en los nombres de carpetas, las cabeceras de los correos electrónicos y en los títulos de los reportes lo que permite identificar con suma facilidad que archivos pertenecen un ambiente u otro.

Figura 57 *Ejemplo de correo electrónico para una ventana de remediación de vulnerabilidades*



Nota: Elaboración propia.

Como se puede observar, el título del correo está directamente relacionado con el número de control de cambio generado en la herramienta de Service Desk. Un detalle importante aquí, es que bajo una misma cadena de correos se pueden marcar tres momentos clave en el proceso de remediación.

– **Antes**: A modo de notificación como en el ejemplo de la figura anterior.

– **Durante**: Indicando la finalización de los mantenimientos y la realización de pruebas funcionales. A su vez, se puede iniciar algún compás de espera de 24 a 48 horas para corroborar que no existe afectación en los servicios en la actividad cotidiana.

– **Después**: Transcurrido el tiempo establecido para la certificación del buen funcionamiento en las aplicaciones o servicios se puede generar un correo cerrando completamente la actividad de remediación de vulnerabilidades.

Por otro lado, una buena práctica es adjuntar en el correo algún reporte con el detalle de las vulnerabilidades que se atenderán. Esto ayuda a que todos los involucrados tengan conocimiento acerca de los componentes que pueden verse afectados durante la actividad. Nuevamente, en este

apartado es importante asociar el número de ticket o control de cambios a estos archivos, sean estos generados por las herramientas con que cuenta COACEHL, o entregados por terceros.

Figura 58 *Ejemplo de un reporte adjunto en correo con el detalle de las vulnerabilidades a remediar*

COACEHL

Resumen detallado de parches

Generado el - jun. 1, 2025 01:36 p. m. (America/Costa_Rica)

Ver los detalles de los parches y de los equipos relacionados en la red.

Detalles del filtro

Operador lógico	Columna	Criterios	Valor
	Grupo personalizado	equal	WIN-R55QQO2MP87
AND	Estado del parche	equal	Que faltan

Dirección IP	Nombre del equipo	ID del parche	ID de boletín	Sistema operativo	Descripción del parche	Estado del parche	Dominio	Paquete de servicio	Fecha de implementación	Comentarios	Desinstalación del parche
*****	*****	400009	AV-FCS03	Windows Server 2019 Datacenter Edition (x64)	The latest update for Microsoft Defender (1.429.283.0)	Que faltan	*****	Windows Server 2019 (x64)	--	--	Sin soporte
*****	*****	347601	TU-072	Windows Server 2019 Datacenter Edition (x64)	Adobe Acrobat Reader DC (x64) (25.001.20474)	Que faltan	*****	Windows Server 2019 (x64)	--	--	Sin soporte
*****	*****	347962	TU-888	Windows Server 2019 Datacenter Edition (x64)	VMware Tools (x64) (12.5.2)	Que faltan	*****	Windows Server 2019 (x64)	--	--	Sin soporte
*****	*****	41354	MSRT-001	Windows Server 2019 Datacenter Edition (x64)	Windows Malicious Software Removal Tool x64 - May 2025 (KB890830)	Que faltan	*****	Windows Server 2019 (x64)	--	--	Sin soporte
*****	*****	41063	MS25-APR14	Windows Server 2019 Datacenter Edition (x64)	KB5055681, 2025-04 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB5054695)	Que faltan	*****	Windows Server 2019 (x64)	--	--	Con asistencia
*****	*****	500106	SP-019	Windows Server 2019 Datacenter Edition (x64)	Microsoft .NET Framework 4.8 Runtime	Que faltan	*****	Windows Server 2019 (x64)	--	--	Sin soporte

Nota: Elaboración propia.

Finalmente, durante esta etapa es importante recopilar las evidencias de remediación o de excepción. Esto puede ser vía reportes, capturas de pantalla u otros archivos que puedan dar fe de los hechos. En el caso de las remediaciones estas pueden ser muestras de los escaneos ejecutados posteriores a la remediación, capturas de pantalla o reportes de parches aplicados, etc. Para el caso de las excepciones, es importante sustentar las causas por las cuales la vulnerabilidad no pudo ser remediada. Y, en caso de ser producto de afectación en los servicios, es importante dejar constancia de ello sea vía correo electrónico u otro medio.

Todas estas evidencias pueden organizarse en carpetas o directorios, comprimirse y

adjuntarse en el Service Desk bajo el ticket o control de cambio ingresado para estas actividades.

En el siguiente diagrama se muestra cómo puede organizarse dicha información:

Figura 59 *Diagrama de organización de documentación generada durante la remediación de vulnerabilidades*

Nota: Elaboración propia.

6.5.5 EVALUAR Y APRENDER

En esta etapa se contrastan las métricas iniciales con lo atendido para poder medir el

desempeño. También, es importante captar las lecciones aprendidas que puedan contribuir a la mejora del proceso.

Tabla 61 *Entradas, procesos y salidas de etapa Evaluar y Aprender*

Entradas	Actividades	Salidas	Indicadores
- Reporte de vulnerabilidades remediadas. - Reporte de parches instalados. - Reporte de equipos atendidos. - Reporte de excepciones. - Reporte de incidentes y fallas generadas por actividades de remediación.	- Consolidación de documentación de evidencias del mes. - Identificación y documentación de lecciones aprendidas. - Preparación de informe de actividades en base a indicadores.	Informe de actividades y cumplimiento.	Indicadores consolidados.

Nota: Elaboración propia.

Seguidamente, ampliamos cada una de las actividades de esta etapa:

– **Consolidación de documentación de evidencias del mes**: Implica la revisión de las evidencias documentales generadas durante la ejecución de las actividades planificadas para la remediación de vulnerabilidades, buscando asegurar que la información este completa.

– **Identificación y documentación de lecciones aprendidas**: El camino de la remediación de vulnerabilidades no es lineal y en ocasiones, a pesar de las muchas pruebas y preparativos preliminares, algo puede fallar. Por eso es importante generar memoria acerca de las lecciones aprendidas en el proceso.

– **Preparación indicadores de desempeño e informe de actividades**: En esta etapa es donde se pueden preparar los indicadores de desempeño en base a los resultados del mes.

También se elabora el informe correspondiente para los altos mandos. Para ello, es necesario contar con las métricas generadas durante el periodo contemplado.

Figura 60 *Ejemplo de métricas por etapa y posibles indicadores a generar*

ETAPA/ MÉTRICAS		RESPONDER	INDICADORES
IDENTIFICAR	Métrica inicial de dispositivos.	Métrica de dispositivos atendidos. Métrica de excepciones.	$\% = \frac{Métrica\ atendido}{Métrica\ inicial}$
DETECTAR	Métrica inicial de vulnerabilidades.	Métrica de vulnerabilidades remediadas.	$\% = \frac{Métrica\ remeediado}{Métrica\ inicial}$
	Métrica inicial de parches.	Métrica de parches instalados.	$\% = \frac{Métrica\ instalado}{Métrica\ inicial}$

Nota: Elaboración propia.

Es aquí donde se evidencia la importancia de la generación de métricas pues permiten establecer líneas base de trabajo claras y eventualmente, poder medir el desempeño. Con estos insumos es posible construir un reporte consolidado de remediación de vulnerabilidades. Estos se detallan en el apartado de Medidas de control.

Otro aspecto importante para tratar de rescatar en esta etapa son las lecciones aprendidas. Esto está muy ligado a la gestión del conocimiento que pueda existir en la organización. Una estrategia simple puede ser implementar una bitácora de incidentes que permita registrar eventos adversos producto de una actividad de remediación. Estos casos deben evaluarse y determinar la ruta de acción más adecuada para evitar afectación en los servicios.

Esto nos lleva a un punto relevante y es la necesidad de replantear la remediación y evaluación de algunas vulnerabilidades. Esto puede ser producto de la complejidad del caso o las implicaciones de estas: Por ejemplo:

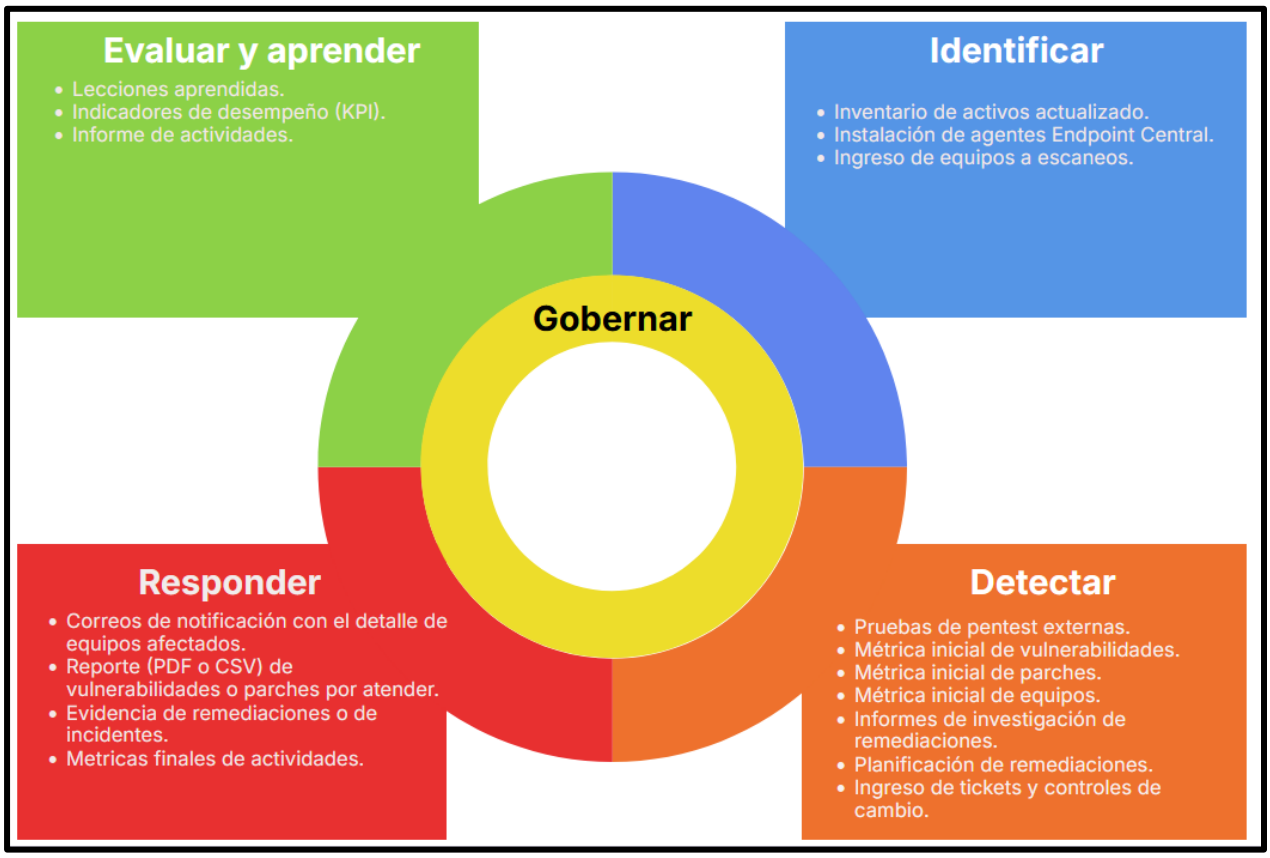
- Sistemas operativos obsoletos.

- Aplicativos sin soporte por parte del fabricante.
- Participación de terceros en la remediación.
- Proyectos de migración a mediano o largo plazo.

Para todo aquello que no se resolverá en 30 días o menos se recomienda crear escaneos e indicadores separados para no invisibilizar las actividades recurrentes por casos excepcionales sin perder de vista que estas vulnerabilidades se encuentran presentes dentro de la infraestructura tecnológica.

Finalmente, se presenta la siguiente figura para demostrar como el proceso permite organizar toda la información generada en cada etapa del mismo.

Figura 61 *Resumen de artefactos generados por etapa del proceso de gestión de vulnerabilidades*



Nota: Elaboración propia.

6.6 ASIGNACIÓN DE RESPONSABILIDADES DEL PROCESO

En el apartado anterior se describen las etapas y artefactos que pueden generarse o empleare durante la ejecución de las diferentes tareas que conlleva cada instancia. Sin embargo, una dimensión importante es la asignación y distribución de responsabilidades entre los diferentes equipos involucrados tanto en la planificación, ejecución y evaluación de los resultados de las actividades de atención de vulnerabilidades. Por ello, a continuación, se presenta una matriz RACI que resume la interacción y el rol de estos:

	Jefe de Seguridad de la Información	Oficial de Seguridad de la Información	Áreas del Negocio	Gerencia de Tecnologías de la Información	Gerencia de Riesgos	Comité de Riesgos
Elaboración/actualización y aprobación del proceso de gestión de vulnerabilidades.	R	I	-	C	C	A
Actualización de inventario de activos.	C	R	I	A	I	-
Ejecución de escaneos de vulnerabilidades.	A	R	-	C	I	-
Planificación de ventanas de mantenimiento.	A	R	I	C	I	-
Notificación de ventanas de mantenimiento.	R	A	I	C	I	-
Ejecución de remediación de vulnerabilidades.	R	A	I	C	I	-
Consolidación de evidencias y excepciones.	R	A	-	C	I	-
Llenado de Matriz de Atención de Vulnerabilidades.	A	R	-	C	I	-
Elaboración de indicadores e informe de actividades.	A	R	-	C	I	I
Seguimiento de resultados en Matriz de Atención de Vulnerabilidades	C	I	-	C	A	R

Nota: Elaboración propia.

En síntesis, la función de Gobierno es ejercida por la Gerencia de Riesgos y la Gerencia General representado en el Comité de Riesgos y las funciones restantes (Identificar, Detectar, Responder, Evaluar y Aprender) son compartidas entre el equipo de tecnología y se seguridad de

la información.

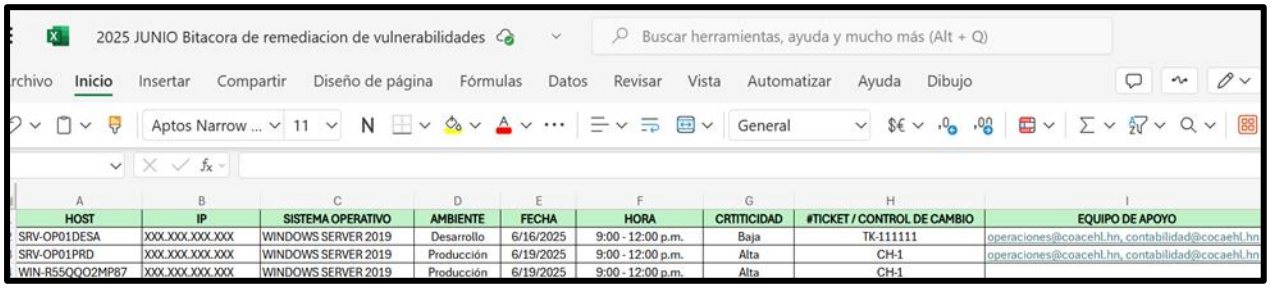
En cuanto a las mejoras del proceso, estas pueden ser motivadas por: El cumplimiento de objetivos del Plan Operativo Anual, hallazgos de auditorías o resultados de estudios de investigación como este. Las mismas deben ser discutidas en el Comité de Riesgos y aprobadas por la Gerencia General.

6.7 MEDIDAS DE CONTROL

Para asegurar el cumplimiento y trazabilidad del proceso, se recomienda establecer algunos mecanismos de control y evaluación que permitan a COACEHL medir la eficiencia y eficacia en la atención de las vulnerabilidades. A continuación, detallamos ciertas propuestas:

– **Bitácora de remediación de vulnerabilidades**: Matriz donde se puede calendarizar el detalle de los equipos por atender en base al inventario existente. Esto se puede asociar con los números de tickets y/o controles de cambio ingresados previamente en la mesa de ayuda.

Figura 62 *Ejemplo de bitácora de remediación de vulnerabilidades*

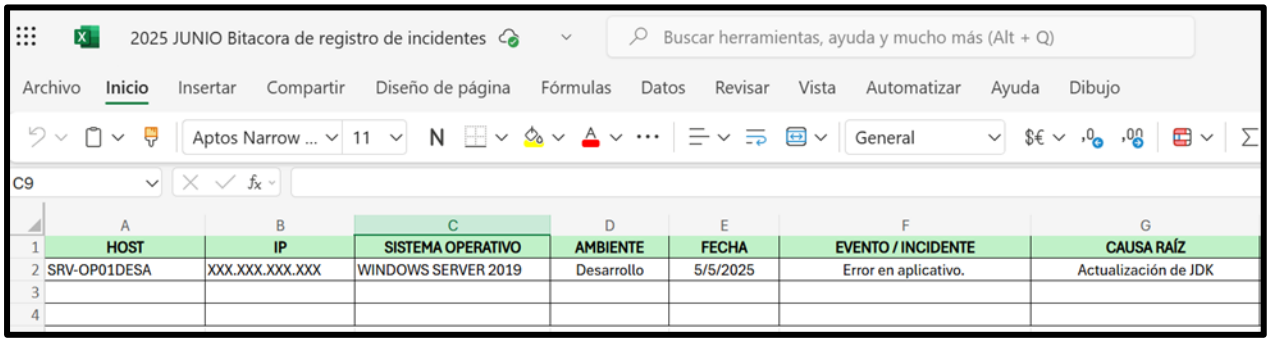


HOST	IP	SISTEMA OPERATIVO	AMBIENTE	FECHA	HORA	CRTITICIDAD	#TICKET / CONTROL DE CAMBIO	EQUIPO DE APOYO
SRV-OP01DESA	XXX.XXX.XXX.XXX	WINDOWS SERVER 2019	Desarrollo	6/16/2025	9:00 - 12:00 p.m.	Baja	TK-111111	operaciones@coacehl.hn, contabilidad@cocaehl.hn
SRV-OP01PRD	XXX.XXX.XXX.XXX	WINDOWS SERVER 2019	Producción	6/19/2025	9:00 - 12:00 p.m.	Alta	CH-1	operaciones@coacehl.hn, contabilidad@cocaehl.hn
WIN-R55QOO2MP87	XXX.XXX.XXX.XXX	WINDOWS SERVER 2019	Producción	6/19/2025	9:00 - 12:00 p.m.	Alta	CH-1	

Nota: Elaboración propia.

– **Bitácora de registro de incidentes**: En esta tabla se busca registrar aquellos eventos adversos generados como resultado de una remediación de vulnerabilidades. La intención es lograr identificar la causa raíz del incidente y poder buscar otras estrategias de solución que no afecten los servicios.

Figura 63 *Ejemplo de bitácora de registro de incidentes*

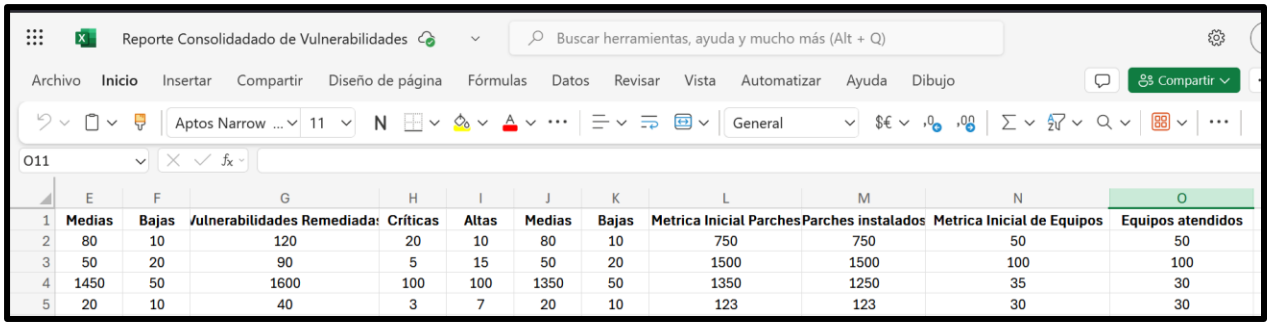


HOST	IP	SISTEMA OPERATIVO	AMBIENTE	FECHA	EVENTO / INCIDENTE	CAUSA RAÍZ
SRV-OP01DESA	XXX.XXX.XXX.XXX	WINDOWS SERVER 2019	Desarrollo	5/5/2025	Error en aplicativo.	Actualización de JDK

Nota: Elaboración propia.

– **Reporte consolidado de vulnerabilidades**: Cuadro que sintetiza y conecta las métricas iniciales (de equipos, vulnerabilidades y parches), lo atendido y las excepciones, preparando el terreno para la construcción de los indicadores de desempeño.

Figura 64 *Ejemplo de un reporte consolidado de vulnerabilidades*

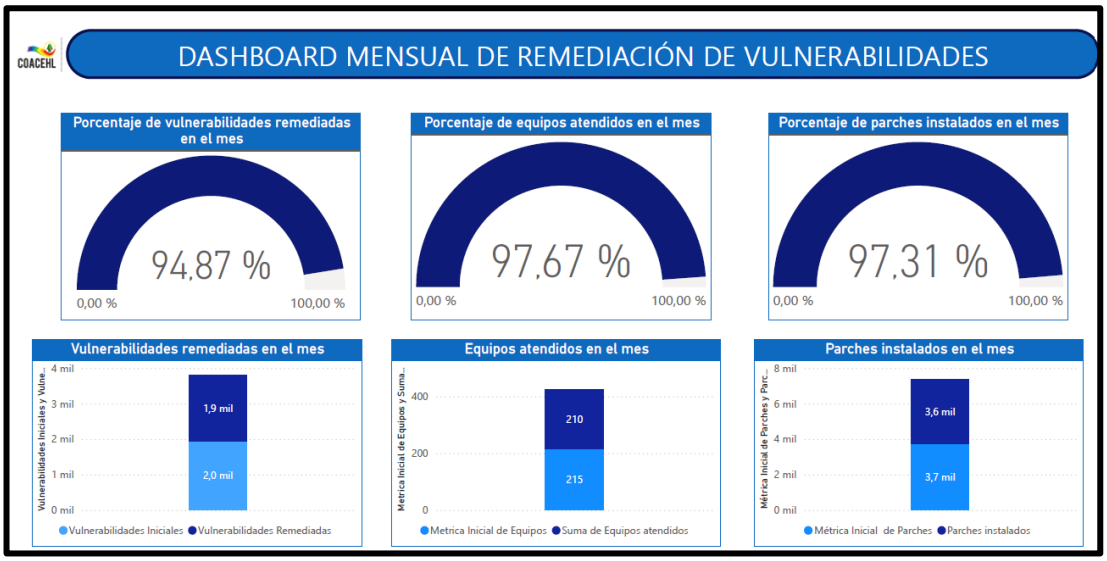


Medias	Bajas	Vulnerabilidades Remediadas	Críticas	Altas	Medias	Bajas	Metrica Inicial Parches	Parches instalados	Metrica Inicial de Equipos	Equipos atendidos
80	10	120	20	10	80	10	750	750	50	50
50	20	90	5	15	50	20	1500	1500	100	100
1450	50	1600	100	100	1350	50	1350	1250	35	30
20	10	40	3	7	20	10	123	123	30	30

Nota: Elaboración propia.

– **Indicadores clave de desempeño (KPI)**: Como buena práctica se recomienda hacer este ejercicio de forma mensual y definir un valor meta a cumplir (Por ejemplo: Mantener un indicador mínimo de 95% en la aplicación de actualizaciones o parches). Ya se explicó previamente en la etapa de: “Evaluar y aprender”, que es posible construir algunos indicadores utilizando las diferentes métricas (iniciales y finales) obtenidas desde el escáner de vulnerabilidades o mediante la herramienta para la aplicación de parches., y en base a ello, generar algunos informes del proceso tal y como se muestra en el siguiente ejemplo:

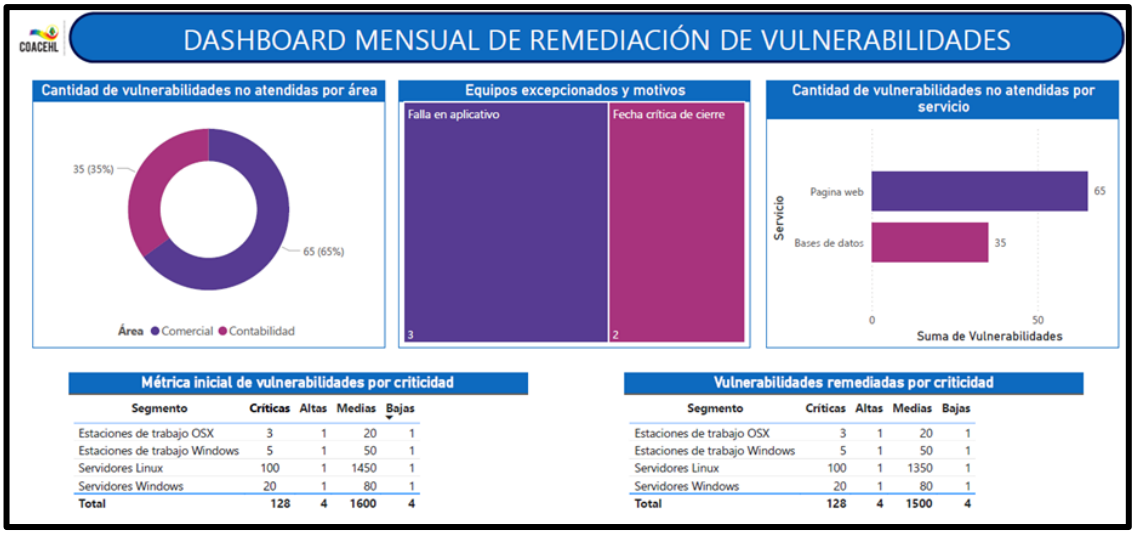
Figura 65 *Ejemplo de indicadores con el resumen de actividades de remediación de vulnerabilidades*



Nota: Elaboración propia.

En la medida que el inventario está conectado con los servicios, áreas y objetivos estratégicos del negocio es posible ampliar las mediciones e incorporar nuevas dimensiones que contribuyan a profundizar la corresponsabilidad en la gestión oportuna de vulnerabilidades y visualizar con mayor facilidad el impacto de la no atención de estas brechas.

Figura 66 *Ejemplo de indicadores de vulnerabilidades remediadas por área y servicio*



Segmento	Criticas	Altas	Medias	Bajas
Estaciones de trabajo OSX	3	1	20	1
Estaciones de trabajo Windows	5	1	50	1
Servidores Linux	100	1	1450	1
Servidores Windows	20	1	80	1
Total	**128**	**4**	**1600**	**4**

Segmento	Criticas	Altas	Medias	Bajas
Estaciones de trabajo OSX	3	1	20	1
Estaciones de trabajo Windows	5	1	50	1
Servidores Linux	100	1	1350	1
Servidores Windows	20	1	80	1
Total	**128**	**4**	**1500**	**4**

Nota: Elaboración propia.

Como ya se ha descrito estos indicadores pueden publicarse periódicamente como informes o boletines para las diferentes áreas involucradas, los altos mandos y entes auditores, a fin de reflejar el rendimiento y avance en la remediación de vulnerabilidades.

6.8 CRONOGRAMA DE IMPLEMENTACIÓN

La planificación de las actividades del proceso puede realizarse de forma mensual. Aquí es importante hacer mención de la forma en que se actualizan las bases de conocimiento de las herramientas considerando sus pros y contras pues este es un aspecto con impacto directo en la planificación y ejecución de las actividades.

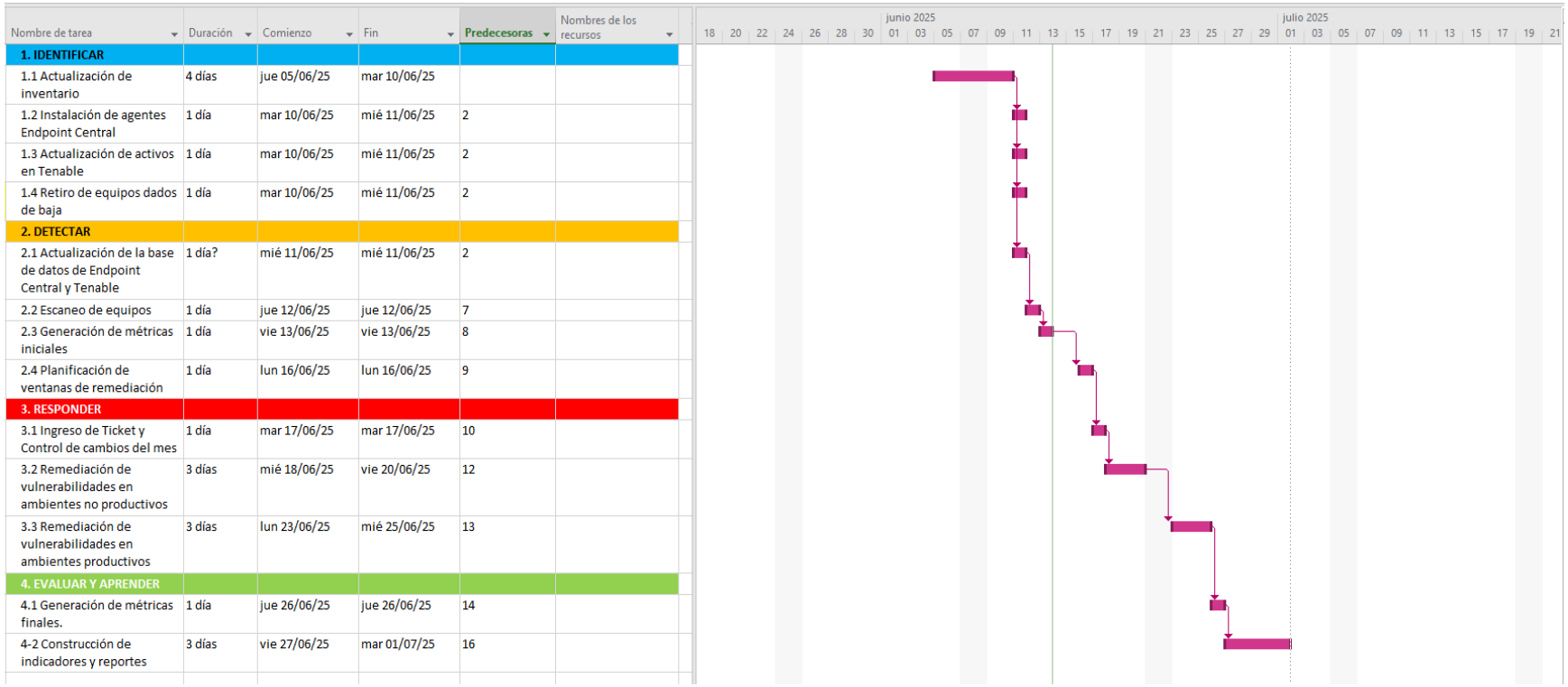
Tabla 62 *Comparativa entre formas de actualización de bases de conocimientos de las herramientas para la detección de vulnerabilidades*

Actualización automática	Actualización manual
Las bases de conocimiento de vulnerabilidades se actualización automáticamente una vez se publican las CVE correspondientes.	La actualización se ejecuta hasta que el equipo de seguridad de la información realiza la tarea.
Puede ser más difícil establecer puntos de medición por la constante sobreescritura de las vulnerabilidades si estas no se remedian a la brevedad.	Permite un mayor control y holgura en los tiempos de atención de las vulnerabilidades identificadas en los activos. Sin embargo, se corre el riesgo de perder de vista vulnerabilidades más recientes a la fecha de la última actualización.

Nota: Elaboración propia.

Se propone realizar la actualización manual considerando las fechas de liberación de parches por parte de Microsoft (segundo martes de cada mes) para tratar de alinear las actividades en base a ese punto de referencia. A razón de ello se presenta como ejemplo el siguiente cronograma general de actividades.

Figura 67 *Ejemplo de cronograma mensual de remediación de vulnerabilidades*



Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1. IDENTIFICAR					
1.1 Actualización de inventario	4 días	jue 05/06/25	mar 10/06/25		
1.2 Instalación de agentes Endpoint Central	1 día	mar 10/06/25	mié 11/06/25	2	
1.3 Actualización de activos en Tenable	1 día	mar 10/06/25	mié 11/06/25	2	
1.4 Retiro de equipos dados de baja	1 día	mar 10/06/25	mié 11/06/25	2	
2. DETECTAR					
2.1 Actualización de la base de datos de Endpoint Central y Tenable	1 día?	mié 11/06/25	mié 11/06/25	2	
2.2 Escaneo de equipos	1 día	jue 12/06/25	jue 12/06/25	7	
2.3 Generación de métricas iniciales	1 día	vie 13/06/25	vie 13/06/25	8	
2.4 Planificación de ventanas de remediación	1 día	lun 16/06/25	lun 16/06/25	9	
3. RESPONDER					
3.1 Ingreso de Ticket y Control de cambios del mes	1 día	mar 17/06/25	mar 17/06/25	10	
3.2 Remediación de vulnerabilidades en ambientes no productivos	3 días	mié 18/06/25	vie 20/06/25	12	
3.3 Remediación de vulnerabilidades en ambientes productivos	3 días	lun 23/06/25	mié 25/06/25	13	
4. EVALUAR Y APRENDER					
4.1 Generación de métricas finales.	1 día	jue 26/06/25	jue 26/06/25	14	
4-2 Construcción de indicadores y reportes	3 días	vie 27/06/25	mar 01/07/25	16	

Nota: Elaboración propia.

6.9 PRESUPUESTO E IMPACTO DEL PROYECTO

Para la puesta en marcha del proceso en la Cooperativa no se incurrirá en costos adicionales, sino que más bien, se optimizará el uso de las herramientas y recursos ya adquiridos bajo licencia por parte de COACEHL. Sin embargo, para fines meramente ilustrativos se agregan algunas estimaciones tanto para dimensionar valores económicos o para conocer soluciones alternativas en caso de que a futuro alguien tenga interés en implementar este proceso.

Los precios de referencia en moneda nacional se calculan tomando la tasa de cambio vigente (L. 26.19) del Lempira con relación al dólar americano, por lo que los montos reflejados pueden variar con el tiempo.

Tabla 63 *Estimación de costos de implementación del proceso*

Concepto	Costo	Valor de mercado
Licencias Manage Engine Endpoint Central	0.00	L. 853,290.20
Licencias Tenable	0.00	L. 185.242,99
Licencias Power BI	0.00	L. 8,799.84
Total	**0.00**	**L. 1,047,333.03**

Nota: Elaboración propia.

Para el cálculo de costos de Manage Engine Endpoint Central se han tomado los precios de mercado de su página web oficial considerando las siguientes características utilizadas en la Cooperativa.

Tabla 64 *Costos de Manage Engine Endpoint Central*

Características	Detalle	Costo Unitario (Por técnico)	Cantidad de técnicos	Costo Total	Moneda nacional
Tipo de infraestructura	On-Premise				
Licenciamiento	Enterprise				
Estaciones de trabajo (anual)	1000	$10,795,00	2	$ 21,590	L 565,462.10
Servidores (anual)	250	$5,495.00	2	$ 10,990	L. 287,828.10
Total				**$ 32,580**	**L. 853,290.20**

Nota: Elaboración propia a partir de página web oficial (Ver enlace).

Existen en el mercado otras opciones para la administración y despliegue de actualizaciones como:

- Ninja One.
- Atera.
- Ivanti Endpoint Manager,
- Action1 (Gratuito para los primeros 200 activos).

En el caso de Tenable se recomienda la edición Expert ya que cuenta con una amplia parametrización para el análisis de vulnerabilidades y puede evaluar servicios web, endurecimiento (hardening) entre otros.

Tabla 65 *Costos de Tenable*

Versión	Alojamiento	Costo Total
Tenable Nessus Expert (anual)	On-Premise	L. 185,242.99

Nota: Elaboración propia a partir de página web oficial (Ver enlace).

Alternativamente en el mercado existen otras muy buenas soluciones para escanear vulnerabilidades mismas que se pueden considerar en base a la disponibilidad presupuestaria como, por ejemplo:

- Qualys.
- Rapid7.
- Batuta
- Vicarius.
- OpenVas (GreenBone), etc.

Este último posee una versión gratuita, pero con limitaciones en cuanto a profundidad de escaneos y soporte, pero puede resultar útil en escenarios con bajos recursos o para comenzar con

las etapas tempranas de madurez en el proceso de gestión de vulnerabilidades.

Finalmente, en este caso se considera la opción de Power BI como herramienta para la elaboración de indicadores y reportes porque el mismo ya viene incluido dentro del licenciamiento de Microsoft Office 365. Sin embargo, también se ofrece la opción de paga por separado.

Tabla 66 *Costos de Power BI*

Versión	Costo unitario (facturado anualmente)	Cantidad de técnicos	Costo Total	Moneda nacional
Power BI Pro	$ 168.00	2	$. 336.00	L. 8,799.84

Nota: Elaboración propia a partir de página web oficial (Ver enlace).

Alternativamente, existen otras opciones para la elaboración de tableros de indicadores y reportes tales como: <

- Tableu.
- Loker Studio.
- Apache Superset (sin costo).

Como se puede observar, la propuesta del proceso no está atada a una solución de software en especial. Por el contrario, es flexible a adaptarse a lo que se disponga según el contexto de la organización Y para la mayoría de herramientas, existen buenas alternativas de bajo o ningún costo lo que puede contribuir a su adopción en diferentes escenarios.

6.10 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 67 *Concordancia de los segmentos de la tesis con la propuesta*

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título de Investigación	**Objetivo general**	**Objetivos específicos**	**Metodologías**	**Variables**	**Población**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos de la propuesta**
Análisis de madurez del proceso para la gestión de vulnerabilidades basado en el marco de ciberseguridad del NIST CSF 2.0 para la Cooperativa de Ahorro y Crédito Educadores de Honduras (COACEHL).	Diseñar un proceso adaptando componentes del Marco de Ciberseguridad NIST CSF 2.0, para gestionar las vulnerabilidades presentes en los sistemas de información de COACEHL.	Analizar la gestión de vulnerabilidades vigente para diagnosticar la situación actual del proceso.	Cualitativa	Procesos, políticas.	1 proceso, 2 personas.	Entrevista semiestructurada. Lista de verificación basada en Control 8.8 de ISO 27002:2022. Matriz de perfilamiento NIST. Notas de campo.	En base a los resultados del perfilamiento NIST CSF 2.0 se concluye que el proceso actual se encuentra mayormente en un nivel: Repetible. Sin embargo, el control ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades se encuentra en una etapa de conocimiento lo que denota que la forma en que de recibe, procesa y canaliza la información sobre vulnerabilidades debe ajustarse para consolidar y	Proceso para la gestión de vulnerabilidades basado en el marco de ciberseguridad del NIST CSF 2.0 para la Cooperativa de Ahorro y Crédito Educadores de Honduras (COACEHL).	Demostrar y caracterizar el flujo de gestión que se puede aplicar a las vulnerabilidades de los sistemas de COACEHL, desde su reporte inicial a través de diversas fuentes hasta su resolución final, con el fin de comprender y describir el proceso completo.

							estandarizar el tratamiento y respuesta de la organización para las brechas de seguridad identificadas. Esto coincide de alguna manera con el contexto de país pues como se describió en el Microentorno y Marco Legal existen pocas iniciativas y un bajo avance en la adopción de mejores prácticas de ciberseguridad en las organizaciones.		
		Determinar que herramientas se usan en COACEHL para la detección y atención de vulnerabilidades de sus activos tecnológicos a fin de modelar como optimizar el aprovechamiento de estos		Metodologías y herramientas.			Considerando los hallazgos encontrados mediante la Lista de verificación de ISO 27002:2022 y la Matriz de Análisis FODA, se ha podido constatar que la entidad cuenta con un cierto grado de		Exponer cómo documentar de manera más eficiente y estructurada las actividades de gestión de vulnerabilidades, facilitando

		recursos.					automatización del proceso, utilizando algunas soluciones de software ya implementadas para la aplicación de parches de seguridad y escaneo de vulnerabilidades. Sin embargo, se evidente la desconexión entre las herramientas y el proceso de gestión de vulnerabilidades lo que representa una posible mejora en el proceso. La mayoría de los marcos de referencia (incluido el NIST CSF 2.0) están recomendando a las organizaciones a conectar: Personas, procesos y herramientas de modo que todo		el seguimiento, la auditoría y la comunicación dentro del equipo y con otras partes interesadas.

							contribuya al cumplimiento de los objetivos estratégicos del negocio.		
		Identificar el grado de conocimiento y uso de estándares de Seguridad de la Información y Ciberseguridad en COACEHL para validar la utilización de mejores prácticas en la organización.		Estándares y marcos de referencia (NIST, ISO 27002, COBIT 2019, etc.).			A través de la Entrevista Semiestructurada se logró establecer que el personal de seguridad de la información cuenta con un alto nivel de conocimiento sobre marcos de referencia como: COBIT 2019, la familia ISO 27000 o el Marco de Seguridad Cibernética del NIST CSF 2.0 lo que permite garantizar la comprensión del propósito de la investigación, así como reconocer el valor y la relevancia de la propuesta con las mejoras identificadas. Al		Ejemplificar cómo se pueden usar Indicadores Clave de Desempeño (KPI) para medir de forma efectiva el rendimiento del proceso de gestión de vulnerabilidades, permitiendo una toma de decisiones informada y la mejora continua..

							contar con el criterio de un equipo de expertos en esta unidad, se ha comprobado que es necesaria una mayor utilización de este tipo de estándares para dar más consistencia y vigencia a los procesos de la institución. Definir los procesos en base a mejores prácticas contribuye a que las organizaciones puedan realizar estudios más precisos para reconocer mejoras, medir sus avances en madurez de manera más concreta e incluso prepararse para certificaciones organizacionales.		
		Establecer cómo la mejora del		Eficacia en la gestión de			Finalmente, el proceso de		.

		proceso de gestión de vulnerabilidades basada en el Marco de Ciberseguridad del NIST CSF 2.0 puede ser de beneficio en COACEHL para robustecer su postura de ciberseguridad.		vulnerabilidades.			gestión de vulnerabilidades se encuentra en su estado de madurez actual por la influencia que han ejercido las normativas emitidas por entidades como: El Congreso Nacional, la Comisión Nacional de Bancos y Seguros, el Consejo Superior de Cooperativas, etc., por los esfuerzos de mejora continua planteados en el Plan Operativo Anual de COACEHL y por la iniciativa del equipo de seguridad de la información quienes de una forma empírica definieron las etapas del proceso vigente..		

Nota: Elaboración propia.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar Antonio, Juan Manuel (2024). *Rezago y asimetrías de la política nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: retos de cooperación para Norteamérica*, Revista Académica del CISAN-UNAM, 19(1), 5, p. 30. https://dialnet.unirioja.es/servlet/articulo?codigo=9396821
Fecha de consulta: 14/03/2025

Aguirre Segura, Carla Vivian (2023). *Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud* [Tesis de grado, Universidad Nacional Pedro Ruiz Gallo], Repositorio Institucional Universidad Pedro Ruiz Gallo, Perú. https://repositorio.unprg.edu.pe/handle/20.500.12893/11406
Fecha de consulta: 16/02/2025

Alanis, Macedonio (2021) *Administración Estratégica y Gobierno de Tecnologías de Información*, Tecnológico de Monterrey, ISBN-13: 9798475090350, p. 67. https://www.amazon.com/Macedonio-Alanis-ebook/dp/B09PJMMCPS?ref_=ast_author_dp_rw&dib=eyJ2IjoiMSJ9.WnbhG_RVZ6ik-Ic2xuKErbSRwR7GFT3T5u4joeQyzpTtxCFWFvCYirNG0dGhB2S-3jDqifKHhNg0fK3bQZ95Bw1ddp1enh-S8kEKFgsM-6XNNuFBe8Pok2z9EOobLeIIp_rujDQtCYZ2d73q9GqdeAGTsrvC9C-rqK2unluqu87qoBMOAoNWnMYgZH_4p3cT3VoOnTcnyx9Xabit7rJMSA.KQ9Yfrv08HGRQPPcFYGuCsFl_tIKQng2wBzFtJXWaw8&dib_tag=AUTHOR
Fecha de consulta: 22/02/2025

Arciniegas, Jaime y González, Oscar (2016). *Sistemas de gestión de calidad: teoría y práctica bajo la norma ISO 2015*: (1 ed.). Bogotá, Ecoe Ediciones, p. 29. https://elibro.net/es/ereader/unitechn/114366?page=29
Fecha de consulta: 03/03/2025

Arispe Alburqueque, C. M. (Il.), Yangali Vicente, J. S. (Il.) y Guerrero Bejarano, M. A. (Il.) (2020). *La investigación científica: una aproximación para los estudios de posgrado*: (1 ed.). Guayaquil, Universidad Internacional del Ecuador, p. 64. https://elibro.net/es/ereader/unitechn/171469?page=64
Fecha de consulta: 17/03/2025

Asociación de Auditoría y Control de Sistemas de Información [ISACA] (2018). *Marco de Referencia COBIT® 2019: Introducción y metodología*, ISBN 978-1-60420-788-0, p. 39.
Fecha de consulta: 18/02/2025

Asociación de Auditoría y Control de Sistemas de Información [ISACA] (2018). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión*, ISBN 978-1-60420-790-3, p. 12, 18 – 19.
Fecha de consulta: 18/02/2025

Astudillo, B. Karina (2018). *Hacking Ético: ¡Cómo convertirse en hacker ético en 21 días o menos!*: (3 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 20, 72. https://elibro.net/es/ereader/unitechn/222677?page=72

Fecha de consulta: 16/02/2025
Ayjón, Miguel Marcos (2020). *La protección de datos de carácter personal en la justicia penal: (1 ed.)*. Barcelona, J.M. Bosh Editor, p. 94 – 95. https://elibro.net/es/ereader/unitechn/130486?page=94
Fecha de consulta: 20/02/2025
Baena Paz, Guillermina (2017). *Metodología de la investigación*: 3 ed. México, D.F, México: Grupo Editorial Patria, p. 83. https://elibro.net/es/ereader/unitechn/40513?page=83
Fecha de consulta: 12/03/2025
Baker, Jessica. (2025). *Hackeados: los secretos detrás de los ciberataques*: (1 ed.). Ediciones Granica, p. 70 – 79. https://elibro.net/es/ereader/unitechn/280510?page=70
Fecha de consulta: 21/02/2025
Banco Interamericano de Desarrollo [BID], Organización de Estados Americanos [OEA] (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, p. 42 – 44, 118 – 119. https://observatoriociberseguridad.org/#/final-report
Fecha de consulta: 18/02/2025
Banco Interamericano de Desarrollo [BID] (2019). Proyecto: *Transformación Digital para una Mayor Competitividad*. https://www.iadb.org/es/proyecto/HO-L1202
Fecha de consulta: 18/02/2025
Barbosa Ramírez, David H. (2024). *Derecho y economía digital: perspectivas y desafíos*: (1 ed.), p. 57. Editorial Universidad del Rosario. https://elibro.net/es/ereader/unitechn/273475?page=57
Fecha de consulta: 27/02/2025
Bautista Cárdenas, Nelly Patricia (2021). *Proceso de la investigación cualitativa: epistemología, metodología y aplicaciones*, 2 ed. Bogotá, Colombia, Editorial El Manual Moderno Colombia, p. 29. https://elibro.net/es/ereader/unitechn/219449?page=29.
Fecha de consulta: 21/03/2025
Beltrán, Marta, Sevillano Fernando (2021). *Ciberseguridad industrial e infraestructuras críticas*: (1 ed.), p. 58, 284. RA-MA Editorial. https://elibro.net/es/ereader/unitechn/222659?page=284
Fecha de consulta: 16/02/2025
Bernal Torres, Cesar (2022). *Metodología de la investigación*. 1 ed. Pearson Educación, p. 58, 141. https://www.ebooks7-24.com:443/?il=19299
Fecha de consulta: 16/02/2025
Burzaco Samper, María (2020). *Protección de datos personales*: (1 ed.). Madrid, Dykinson, p. 26. https://elibro.net/es/ereader/unitechn/160010?page=26
Fecha de consulta: 16/02/2025
Caballero Quezada, Alonso E. (2022). *Kali Linux: curso práctico*: (1 ed.). Madrid, RA-MA Editorial, p. 38 – 155. https://elibro.net/es/ereader/unitechn/222673?page=38
Fecha de consulta: 27/02/2025
Camisón, César, González Cruz, Tomás, Cruz, Sonia (2006). *Gestión de la calidad: conceptos, enfoques, modelos y sistemas*. Pearson Educación, p. 16. https://www.ebooks7-24.com:443/?il=4338
Fecha de consulta: 15/02/2025

Cano, Jeimy (2017). *Manual de un CISO: Reflexiones no convencionales sobre la gerencia de la seguridad de la información en un mundo VICA (Volátil, Incierto, Complejo y Ambiguo)*: (1 ed.). Madrid, RA-MA Editorial, p. 126. https://elibro.net/es/ereader/unitechn/230297?page=126
Fecha de consulta: 19/02/2025

Carhuancho Mendoza, Irma Milagros, Nolazco Labajos, Fernando Alexis (2019). Metodología de la investigación holística: (1 ed.). Guayaquil, Universidad Internacional del Ecuador, p. 22. https://elibro.net/es/ereader/unitechn/131261?page=22.
Fecha de consulta: 02/03/2025

Centro de Escritura Javeriano (2020). Normas APA, séptima edición. Pontificia Universidad Javeriana, seccional Cali. https://www.javerianacali.edu.co/sites/default/files/2022-06/Manual%20de%20Normas%20APA%207ma%20edicio%CC%81n.pdf
Fecha de consulta: 15/02/2025

Certiprof (2022). ISO 27001 Foundation, Versión 112022, p. 74, 86, 87.
Fecha de consulta: 22/02/2025

Comisión Nacional de Bancos y Seguros [CNBS] (2023, 29 de mayo) *Lineamientos mínimos para prevenir y mitigar la ocurrencia de fraudes y estafas cibernéticas en contra del usuario financiero*. Circular No. 008, p. 8.
https://circulares.cnbs.gob.hn/Archivo/Viewer/2555/C008-2023.pdf
Fecha de consulta: 16/02/2025

Comisión Nacional de Bancos y Seguros [CNBS] (2022, 19 de diciembre). *Normas para la Gestión de Tecnologías de Información, Ciberseguridad y Continuidad del Negocio*. Circular No 025, p. 3, 4, 12, 11 – 14.
https://circulares.cnbs.gob.hn/Archivo/Viewer/2520/025-2022%20NORMAS%20GESTION%20TECNOLOGIAS%20INFORMACION.pdf
Fecha de consulta: 16/02/2025

Comisión Nacional de Bancos y Seguros [CNBS] (2005, 22 de noviembre). *Normas para regular la Administración de Tecnologías de la Información y Comunicaciones en las Instituciones del Sistema Financiero*. Circular No 119.
https://circulares.cnbs.gob.hn/Archivo/Viewer/1016/CIR119_05.pdf
Fecha de consulta: 16/02/2025

Congreso Nacional de Honduras (2023, 31 de agosto). *Ley del Sistema Nacional de Bases de Datos de ADN*. Diario Oficial La Gaceta No. 36,322. Decreto No. 57-2023, Sección A, p. 6. https://www.tsc.gob.hn/web/leyes/Decreto-57-2023.pdf
Fecha de consulta: 18/02/2025

Congreso Nacional de Honduras (2019, 10 de mayo). *Código Penal*. Diario Oficial La Gaceta No. 34,940. Decreto No. 130-2017, Sección A, p. 93, 94, 131.
https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf
Fecha de consulta: 18/02/2025

Congreso Nacional de Honduras (2016, 06 de diciembre). *Acuerdo Marco de Cooperación entre el Gobierno de la Republica de Honduras y el Gobierno del Estado de Israel*. Diario Oficial La Gaceta No. 34,205. Decreto No. 139-2016, Sección A, p. 9.
https://tzibalnaah.unah.edu.hn/bitstream/handle/123456789/4698/20161206.pdf?sequence=2&isAllowed=y

Fecha de consulta: 18/02/2025

Congreso Nacional de Honduras (2013, 24 de enero). *Reformas Constitucionales*. Diario Oficial La Gaceta No. 33,033. Decreto No. 237-2012, Sección A, p. 17 – 18. https://www.tsc.gob.hn/web/leyes/Reformas_varios_consitucion_2013.pdf
Fecha de consulta: 17/02/2025

Congreso Nacional de Honduras (2006, 30 de diciembre). *Ley de Transparencia y Acceso a la Información Pública*. Diario Oficial La Gaceta No. 31,193. Decreto No. 170-2006, Sección A, p. 57 – 58. https://www.onadici.gob.hn/wp-content/uploads/2024/01/Decreto-Legislativo-170-2006-Ley-de-Transparencia-y-Acceso-a-la-Informacion-Publica.pdf
Fecha de consulta: 19/02/2025

Congreso Nacional de Honduras (1982, 20 de enero). *Constitución de la Republica*. Diario Oficial La Gaceta No. 23,612. Decreto No. 131, p. 5 – 6. https://www.cree.gob.hn/wp-content/uploads/2019/02/Ley-de-la-Constitucion-de-la-Republica.pdf
Fecha de consulta: 17/02/2025

Consejo Superior de Cooperativas de Honduras [CONSUCOOP] (2023, 01 de febrero). *Norma para la Administración de Tecnologías de Información y Comunicaciones (TIC), para las Cooperativas de Ahorro y Crédito (CAC´S)*. Diario Oficial La Gaceta No. 36,144, Acuerdo No 002-15-12-2022, Sección A, p. 27 – 51. https://consucoop.hn/sdm_downloads/normativa-para-la-administracion-de-tecnologias-de-tecnologias-de-informacion-y-comunicacion-tic/
Fecha de consulta: 18/02/2025

Cooperativa de Ahorro y Crédito Educadores de Honduras Limitada [COACEHL] (2023). Memoria Anual 2023, p. 75. https://www.coacehl.com/wp-content/uploads/2019/01/INFORME-COACEHL-2023-V1-FINAL.pdf
Fecha de consulta: 16/02/2025

Coronado García, Beatriz. (2024). *Seguridad en equipos informáticos. MF0486*: (1 ed.). Logroño, Editorial Tutor Formación, p. 42 – 45, 61. https://elibro.net/es/ereader/unitechn/276624?page=61
Fecha de consulta: 25/02/2025

Costas Santos, Jesús (2021). *IFCT050PO. Gestión de la seguridad informática en la empresa*: (1 ed.). Madrid, RA-MA Editorial, p. 24. https://elibro.net/es/ereader/unitechn/248798?page=24
Fecha de consulta: 18/02/2025

Costas Santos, Jesús. (2015). *Seguridad informática:* (1 ed.). Madrid, Spain: RA-MA Editorial, p. 27. https://elibro.net/es/ereader/unitechn/62452?page=27
Fecha de consulta: 18/02/2025

Cruz del Castillo, Cinthia, Olivares Orozco, Socorro (2014). *Metodología de la investigación*: (1 ed.). Grupo Editorial Patria, p. 133. https://elibro.net/es/ereader/unitechn/39410?page=133
Fecha de consulta: 04/03/2025

Davalos Guillen, A. J., Mujica Sánchez, M. L. (2024). *Ciberseguridad y vulneración de datos personales en entidades financieras* [Tesis de grado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú. https://repositorio.autonoma.edu.pe/handle/20.500.13067/3512

Fecha de consulta: 16/02/2025
Deutsch, Víctor Eduardo (2022). Ciberseguridad para directivos: riesgos, control y eficiencia de las tecnologías de la información: (1 ed.), p. 152, 154. Córdoba, LID Editorial España. https://elibro.net/es/ereader/unitechn/269669?page=152
Fecha de consulta: 15/02/2025
Diego, Isaac Martin De y Fernández Isabel, Alberto. (2020). *Ciencia de datos para la ciberseguridad: (1 ed.)*. Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 67 – 68. https://elibro.net/es/ereader/unitechn/222714?page=67
Fecha de consulta: 28/04/2025
Dirección de Gestión por Resultados [DIGER] (2023). *Plan Nacional de Gobierno Digital 2023 – 2026, Gobierno de Honduras*. p. 21 – 54. https://www.diger.gob.hn/centro-de-documentos
Fecha de consulta: 19/02/2025
Echeverria Pérez, Ángel Alonso, Martínez Soria, Juan Cristian (2024). *Gestión de vulnerabilidades y obsolescencia en la empresa MAPFRE Perú* [Tesis de grado, Universidad San Ignacio de Loyola]. Repositorio de la Universidad San Ignacio de Loyola, Perú. https://repositorio.usil.edu.pe/entities/publication/d983a6d0-1a36-4266-8d16-f6eacb219118
Fecha de consulta: 28/02/2025
Fernández Sánchez, Carlos Manuel (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*: (1 ed.). Madrid, Spain: AENOR - Asociación Española de Normalización y Certificación, p. 21. https://elibro.net/es/ereader/unitechn/53581?page=21
Fecha de consulta: 24/02/2025
Fuentes Diaz, Walter Marcelo, Macas Carrasco, Mayra Alexandra (2023). *Ciberseguridad: del ciber-crimen a los ataques ciber-físicos, (1 ed.)*, Universidad de las Fuerzas Armadas-ESPE, Ecuador, p. 26.
Fecha de consulta: 17/02/2025
Gascón Marcén, Ana (2021). *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. Cuadernos de Derecho Transnacional*, Vol. 13, No. 2, p. 231. https://e-revistas.uc3m.es/index.php/CDT/article/view/6256
Fecha de consulta: 16/02/2025
Gaseta, Edson Roberto, Motta Alexandre Cesar, Boca Picollini Jacomo Dimmit (s.f.), *Gobierno de las Tecnologías de Información*, Red Nacional de Tecnología Avanzada – RENATA, Colombia, p. 19. https://cedia.edu.ec/docs/efc/GTI4.pdf
Fecha de consulta: 05/03/2025
Gibbs, Graham (2014). *El análisis de datos cualitativos en investigación cualitativa*: (1 ed.). Ediciones Morata, S. L., p. 22, 194. https://elibro.net/es/ereader/unitechn/51842?page=22
Fecha de consulta: 06/03/2025
Gómez Hervás, Nuria del Carmen (2021). *Normativa de Ciberseguridad*: (1 ed.). Madrid, RA-MA Editorial, p. 144 – 147. https://elibro.net/es/ereader/unitechn/222663?page=144
Fecha de consulta: 21/02/2025
Gómez, Marcelo (2009). *Introducción a la metodología de la investigación científica*: (2 ed.). Córdoba, Argentina: Editorial Brujas, p. 102. https://elibro.net/es/ereader/unitechn/78021?page=102.
Fecha de consulta: 06/03/2025

Gómez Vieites, Á. (2015). *Seguridad en equipos informáticos*: (1 ed.). Madrid, Spain: RA-MA Editorial, p. 40 – 65, 72. https://elibro.net/es/ereader/unitechn/62466?page=72
Fecha de consulta: 27/02/2025

Greco, Orlando (2009). *Diccionario de finanzas: (2 ed.)*. Buenos Aires, Argentina, Argentina: Valletta Ediciones, p. 370. https://elibro.net/es/ereader/unitechn/66816?page=370
Fecha de consulta: 24/02/2025.

Gregorio Rojas, N. (2023). *Metodología de la investigación para anteproyectos*: (1 ed.). Santiago de los Caballeros, Universidad Abierta para Adultos (UAPA), p. 148, 150, 157 – 160. https://elibro.net/es/ereader/unitechn/229656?page=148
Fecha de consulta: 05/03/2025

Guerra Soto, Mario (2023). *Ciberinteligencia de la amenaza en entornos corporativos*: (1 ed.). Madrid, RA-MA Editorial, p. 41. https://elibro.net/es/ereader/unitechn/235055?page=41
Fecha de consulta: 19/02/2025

Gutiérrez Salazar, Pablo (2019). *El libro blanco del Hacker*: (2 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 127, 132 – 133. https://elibro.net/es/ereader/unitechn/222683?page=132
Fecha de consulta: 05/04/2025

Guzmán Solano, Sandra Liliana (2019). *Guía para la implementación de la Norma ISO 27032* [Tesis de grado, Universidad Católica de Colombia]. Repositorio de la Universidad Católica de Colombia. https://repository.ucatolica.edu.co/entities/publication/16c44c07-b5d2-4fb1-83de-853b5d13e48a
Fecha de consulta: 22/02/2025

Hernández López, José Miguel (2023). *¿Por qué debemos proteger la privacidad? Cronología, textos y notas sobre intimidad, vida privada y protección de datos: (1 ed.)*. Barcelona, J.M. Bosch Editor, p. 264 – 266. https://elibro.net/es/ereader/unitechn/249512?page=264
Fecha de consulta: 16/02/2025

Hernández Sampieri, Roberto, Mendoza Torres, Christian Paulina (2023*). Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana, *(2 ed.),* p. 9, 447. https://www.ebooks7-24.com:443/?il=31455
Fecha de consulta: 04/03/2025

Hernández-Sampieri, Roberto, Fernández Collado, Carlos, Baptista Lucio, Pilar (2014). *Metodología de la Investigación*. 6ta. edición. México. McGraw-Hill ISBN 978-1-4562-2396-0, p. 127, 152-162, 402. https://esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf
Fecha de consulta: 12/03/2025

Hernández-Sampieri, Roberto, Fernández Collado, Carlos, Baptista Lucio, Pilar (2010). *Metodología de la Investigación*. 5ta. edición. México. McGraw-Hill ISBN: 978-607-15-0291-9, p. 149 – 152.
Fecha de consulta: 12/03/2025

Herrero Pérez, Luis (2021). *Hacking ético de redes y comunicaciones: curso práctico*: (1 ed.). Madrid, RA-MA Editorial, p. 15. https://elibro.net/es/ereader/unitechn/222667?page=15
Fecha de consulta: 20/02/2025

HLB (2024). *Informe de Ciberseguridad de HLB 2024*, p. 5, 13, 15. https://www.hlbhonduras.com/wp-content/uploads/2024/10/HLB-Reporte-de-Ciberseguridad-2024.pdf

Fecha de consulta: 21/02/2025
Instituto de Acceso a la Información Pública [IAIP] (2021). *Ley de Protección de Datos Personales*, p. 3 – 6. https://cei.iaip.gob.hn/doc/Anteproyecto%20de%20Ley%20de%20Proteccion%20de%20Datos%20Personales%20y%20Accion%20de%20Habeas%20Data%20de%20Honduras%20%20Final%2021%2001%2014.pdf
Fecha de consulta: 21/02/2025
Instituto de Auditores Internos [IAP] (2025, febrero). *Requisito Temático Ciberseguridad*, p. 2 – 4. https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement_spanish.pdf
Fecha de consulta: 21/02/2025
Instituto Nacional de Estadística [INE] (2024). *Conectividad en Honduras: Explorando el acceso y uso de las TIC en los hogares*, p. 6. https://www.ine.gob.hn/Documentacion/ConectividadenHonduras2024.pdf
Fecha de consulta: 24/02/2025
Jordi José (2023, abril 23). La ciberdelincuencia sigue en aumento: los ciberataques se multiplican, *EY España*. https://www.ey.com/es_es/insights/cybersecurity/la-ciberdelicuencia-sigue-aumento-los-ciberataques-se-multiplican
Fecha de consulta: 16/02/2025
Joyanes Aguilar, Luis (2017). *Industria 4.0: la cuarta revolución industrial*. Alpha Editorial. p. XVII – XVI, 14. https://books.google.hn/books?hl=es&lr=&id=QyN1EAAAQBAJ&oi=fnd&pg=PR7&dq=la+cuarta+revoluci%C3%B3n+industrial+&ots=kjyhtsdIJb&sig=H3Zln3VFgK8nn5ZYpfN9vcTMyro&redir_esc=y#v=onepage&q=la%20cuarta%20revoluci%C3%B3n%20industrial&f=false
Fecha de consulta: 18/02/2025
Joyanes Aguilar, Luis (2015). *Sistemas de Información en la Empresa. El impacto de la nube, la movilidad. y los medios sociales*. Alpha Editorial, p. 524, 531.
Fecha de consulta: 18/02/2025
Llanes-Font, Mariluz, Lorenzo-Llanes, Ernesto (2021). *La cuarta revolución industrial y una nueva aliada: calidad 4.0*. Ciencias Holguín, 27(2), p. 68. https://www.redalyc.org/journal/1815/181566671006/181566671006.pdf
Fecha de consulta: 16/02/2025
López, Antonio (2015, 21 de julio). *Métricas de evaluación de vulnerabilidades: CVSS 3.0*. Instituto Nacional de Ciberseguridad. https://www.incibe.es/incibe-cert/blog/cvss3-0
Fecha de consulta: 19/02/2025
López-Tarruella Martínez, Aurelio (2021). *Propiedad intelectual e innovación basada en los datos: (1 ed.)*. Madrid, Dykinson, p. 67. https://elibro.net/es/ereader/unitechn/209966?page=67
Fecha de consulta: 26/02/2025
Maíllo Fernández, Juan Andrés (2020). *Hackers: técnicas y herramientas para atacar y defendernos*: (1 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 240. https://elibro.net/es/ereader/unitechn/222726?page=240
Fecha de consulta: 11/03/2025
Mata, Arturo Enrique (2024). *Ciberseguridad: curso práctico* (1ra ed.), Madrid, RA-MA Editorial, p. 12, 173. https://elibro.net/es/ereader/unitechn/273939?page=173

Fecha de consulta: 16/02/2025
Mata García, Arturo (2023). *Kali Linux para Hackers: Técnicas y metodologías avanzadas de seguridad informática ofensiva: (1 ed.)*. Madrid, RA-MA Editorial, p. 239. https://elibro.net/es/ereader/unitechn/230295?page=239
Fecha de consulta: 16/02/2025
Mata, Arturo Enrique (2022). *Curso de programación Bash Shell: fundamentos teóricos y prácticos para el reconocimiento, evaluación y explotación de vulnerabilidades informáticas*: (1 ed.). Madrid, RA-MA Editorial, p. 152. https://elibro.net/es/ereader/unitechn/222671?page=152
Fecha de consulta: 18/02/2025
Markovski, Veni, Trepykhalin, Alexey (2022). *Informe de enfoque por países: leyes e iniciativas de políticas relacionadas con Internet en China*. Corporación para la Asignación de Nombres y Números en Internet [ICANN], p. iv, 8, 11 – 24. https://itp.cdn.icann.org/es/files/government-engagement-ge/ge-010-31jan22-en.pdf
Fecha de consulta: 21/02/2025
Maxwell, Joseph A. (2019). *Diseño de investigación cualitativa*: (1 ed.). Barcelona, Editorial Gedisa. https://elibro.net/es/ereader/unitechn/127783?page=211
Fecha de consulta: 23/03/2025
Menéndez Arantes, Silvia Clara (2022). *Auditoría de seguridad informática: curso práctico*: (1 ed.). Madrid, RA-MA Editorial, p. 118 – 217. https://elibro.net/es/ereader/unitechn/222672?page=118
Fecha de consulta: 17/02/2025
Molina Marín, Yeison, Orozco, Luis Guillermo (2020). *Vulnerabilidades de los Sistemas de Información: una revisión* [Trabajo de grado, Tecnológico de Antioquia, Institución Universitaria]. Repositorio Digital TDA. Colombia, p. 4. https://dspace.tdea.edu.co/handle/tdea/1398
Fecha de consulta: 19/02/2025
Monroy Mejía, María de los Ángeles, Nava Sanchezllanes, Nelisahuel (2018). *Metodología de la investigación*: (1 ed.). México, D.F., Grupo Editorial Éxodo, p. 103. https://elibro.net/es/ereader/unitechn/172512?page=103
Fecha de consulta: 24/03/2025
Morera Carballo, Mario (2022). *Los sistemas de información gerencial y su evolución hacia la cuarta revolución industrial*. Revista Nacional de Administración, 13(1), (p. 96). https://www.scielo.sa.cr/scielo.php?pid=S1659-49322022000100006&script=sci_arttext
Fecha de consulta: 02/03/2025
Moya, Javier Guaña (2023). *Revolución de la ciberseguridad en la cuarta revolución industrial*. Revista Ingeniería e Innovación del Futuro, 2(2), p. 7. https://editorialscientificfuture.com/index.php/riif/article/view/11/13
Fecha de consulta: 02/03/2025
National Institute of Standards and Technology [NIST] (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST*, p. 1, 5, 6, 8, 11, 24 – 26. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf
Fecha de consulta: 16/02/2025
National Institute of Standards and Technology [NIST] (2016). *Small Business Information Security: The Fundamentals*, NISTIR 7621. Revisión 1. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf

Fecha de consulta: 16/02/2025
Niño Rojas, Víctor Miguel (2019). *Metodología de la Investigación: diseño, ejecución e informe*: (2 ed.). Bogotá, Ediciones de la U, p. 27, 53.} https://elibro.net/es/ereader/unitechn/127116?page=27
Fecha de consulta: 13/03/2025
Nolasco Valenzuela, Jorge Santiago, Gamboa Cruzado, Javier, Dextre Alarcon, Jymmy Stwart (2023). *Tecnologías disruptivas: comprende las herramientas de la sociedad digital*: (1 ed.). Madrid, RA-MA Editorial, p. 336. https://elibro.net/es/ereader/unitechn/235058?page=336
Fecha de consulta: 20/02/2025
Observatorio de la Ciberseguridad en América Latina y el Caribe (2020). *Reporte Ciberseguridad 2020 del Observatorio de la Ciberseguridad en América Latina y el Caribe*, Organización de Estados Americanos (OEA), Banco Interamericano de Desarrollo (BID), p. 117 – 119. https://observatoriociberseguridad.org/#/final-report
Fecha de consulta: 07/03/2025
Organismo de Certificación Global [NQA] (s.f.). *ISO 27001:2022 Guía de Implementación de Sistemas de Gestión de Seguridad de la Información*, p. 6, 13. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf
Fecha de consulta: 07/03/2025
Organización de las Naciones Unidas [ONU] (1990). *Resolución 45/95. Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales*, p. 198. https://digitallibrary.un.org/nanna/record/105299/files/A_RES_45_95-ES.pdf?withWatermark=0&withMetadata=0&registerDownload=1&version=1
Fecha de consulta: 07/03/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 25010:2023. https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-2:v1:en
Fecha de consulta: 20/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 27001:2022, Anexo 12.6.1. https://www.iso27000.es/iso27002_12.html
Fecha de consulta: 20/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 27002:2022. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-3:v2:en
Fecha de consulta: 20/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 27005:2022. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en
Fecha de consulta: 23/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 29147:2018. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29147:ed-2:v1:en
Fecha de consulta: 18/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 30111:2019. https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-2:v1:en
Fecha de consulta: 15/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 45001:2018. https://www.iso.org/obp/ui/#iso:std:iso:45001:ed-1:v1:es

Fecha de consulta: 21/02/2025
Organización Internacional de Normalización [ISO] (s.f.). ISO 9241-11:2019. https://www.iso.org/obp/ui/es/#iso:std:iso:9241:-11:ed-2:v1:en
Fecha de consulta: 17/02/2025
Organización Mundial de la Propiedad Intelectual [OMPI] (2022). *Tratado de Budapest sobre el reconocimiento internacional del depósito de microorganismos a los fines de procedimiento en materia de patentes*, p.1. https://www.wipo.int/export/sites/www/treaties/es/registration/budapest/pdf/wo_inf_12.pdf
Fecha de consulta: 16/02/2025
Páramo Morales, Dagoberto, Campo Sierra, Shester Jesus, Maestre Matos, Leydis Marcela (2020). *Métodos de investigación cualitativa: fundamentos y aplicaciones*: (1 ed.). Editorial Unimagdalena. https://elibro.net/es/ereader/unitechn/174940?page=35
Fecha de consulta: 21/03/2025
Pérez, Luciano, Pérez, Rubén y Seca, María Victoria (2020). *Metodología de la investigación científica*: (1 ed.). Ituzaingó, Editorial Maipue, p. 213. https://elibro.net/es/ereader/unitechn/138497?page=213
Fecha de consulta: 21/03/2025
Piattini Velthuis, Mario. G., Ruiz González, Francisco. (2020). *Gobierno y gestión de las tecnologías y los sistemas de información*: (1 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 103. https://elibro.net/es/ereader/unitechn/222724?page=103
Fecha de consulta: 18/02/2025
Poder Ejecutivo de la República de Honduras (2020, 26 de septiembre). *Reglamento Sobre Gobierno Electrónico*. Diario Oficial La Gaceta No. 35,383. Decreto Ejecutivo No. PCM-086- 2020, Sección A, p. 1 – 42. https://www.tsc.gob.hn/web/leyes/PCM-086-2020.pdf
Fecha de consulta: 02/03/2025
Portantier, Fabián (2013). *Gestión de la seguridad informática: (1 ed.)*, p .45, Ciudad Autónoma de Buenos Aires: Fox Andina; Buenos Aires: Dalaga.
Fecha de consulta: 19/02/2025
Pulido Varón, Heidi Smith, Quintero Arango, Luis Fernando y Gutiérrez Avendaño, Jairo (2024). *Investigación cualitativa: claves para estudiantes universitarios: (1 ed.)*. Medellín, Universidad Católica Luis Amigó, p. 49, 53, 76. https://elibro.net/es/ereader/unitechn/277320?page=49
Fecha de consulta: 21/03/2025
Quirós Carvajal, Carlos Daniel (2024). *Análisis y descubrimiento de vulnerabilidades en múltiples superficies de ataque en entornos de seguridad informática*, Semestre de Industria, Ingeniería de sistemas, Universidad de Antioquia, Medellín. https://bibliotecadigital.udea.edu.co/handle/10495/38586
Fecha de consulta: 01/04/2025
Ramírez Pascual, B. (Coord.) (2023). *La ciberseguridad en la era de la Inteligencia Artificial: dilemas y retos empresariales: (1 ed.)*, p. 66 – 67, Madrid, LA LEY Soluciones Legales S.A. https://elibro.net/es/ereader/unitechn/248924?page=66 .
Fecha de consulta: 19/02/2025
Redacción (2017, octubre 10). Unas 16 instituciones serán protegidas de los cibercriminales en Honduras, *El Heraldo*. https://www.elheraldo.hn/honduras/unas-16-instituciones-seran-protegidas-de-los-cibercriminales-en-honduras-PVEH1115813

Fecha de consulta: 16/02/2025
Rodríguez, Luis (2024, julio 11). ¿Cuánto aumentó la inversión en ciberseguridad bancaria en Honduras?, *El Heraldo*. https://www.elheraldo.hn/economia/inversion-ciberseguridad-bancaria-honduras-CA20317849
Fecha de consulta: 16/02/2025
Romero Egusquiza, Navidad Helen (2023). *Diseño de un Programa de Ciberseguridad basado en el Cyber Security Framework (CSF) del National Institute of Standards and Technology (NIST), usando ISO/IEC 27001: 2013 para empresas de distribución eléctrica en Perú* [Tesis de grado, Universidad Peruana de Ciencias Aplicadas], Repositorio Académico UPC.
https://repositorioacademico.upc.edu.pe/handle/10757/672985
Fecha de consulta: 18/02/2025|
Sánchez Huerta, David (2020). *Análisis FODA o DAFO: el mejor y más completo estudio con 9 ejemplos prácticos*: (1 ed.). Madrid, Bubok Publishing S.L., p. 16.
https://elibro.net/es/ereader/unitechn/189293?page=16.
Fecha de consulta: 22/03/2025
Santiesteban Naranjo, Ernan (2014). *Metodología de la investigación científica*: (1 ed.). Las Tunas, Editorial Académica Universitaria (Edacun), p. 114, 122.
https://elibro.net/es/ereader/unitechn/151737?page=114
Fecha de consulta: 20/03/2025
Schwab, Klaus (2020). *La Cuarta Revolución Industrial*. Futuro Hoy. Vol. 1. Nro. 1, p. 06, Fondo Editorial de la Sociedad Secular Humanista del Perú.
http://futurohoy.ssh.org.pe/wp-content/uploads/2020/12/Schwab-Klaus-2020.-La-Cuarta-Revolucion-Industrial.-Futuro-Hoy.-Vol.1-Nro.1.pdf
Fecha de consulta: 19/02/2025
Sevillano, Fernando, Beltrán, Marta (2020). *Dirección de seguridad y gestión del ciber riesgo*: (1 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 54 – 56.
https://elibro.net/es/ereader/unitechn/222733?page=54
Fecha de consulta: 16/02/2025
Staff, Redacción (2024, abril 16). IHTT sufrió ataque cibernético, revela Rafael Barahona, *El Heraldo*. https://www.elheraldo.hn/honduras/ihtt-sufrio-ataque-cibernetico-revela-comisionado-rafael-barahona-II18671081
Fecha de consulta: 17/02/2025
Stallings, William (2004). *Fundamentos de seguridad en redes: aplicaciones y estándares*. Pearson Educación, p. 5. https://www.ebooks7-24.com:443/?il=3241
Fecha de consulta: 01/04/2025
Suarez Campos, Jorge Luis (2022). Vigencia ontológica de la ciberseguridad en el marco de la seguridad informática chilena. Convenio de Budapest, Universidad Mayor, Santiago de Chile, Revista Aula Virtual, Vol. 3, No, 6, p. 141. https://biblat.unam.mx/es/revista/aula-virtual/articulo/vigencia-ontologica-de-la-ciberseguridad-en-el-marco-de-la-seguridad-informatica-chilena-convenio-de-budapest
Fecha de consulta: 20/02/2025
Tejerina, Ofelia, Beltrán, Marta (2020). *Aspectos jurídicos de la ciberseguridad: (1 ed.)*. Paracuellos de Jarama, Madrid, RA-MA Editorial, p. 117.
https://elibro.net/es/ereader/unitechn/222712?page=117
Fecha de consulta: 05/04/2025

Trejo Sánchez, Karina (2021). *Fundamentos de metodología para la realización de trabajos de investigación*: (1 ed.). Ciudad de México, Editorial Parmenia, Universidad La Salle México, p. 76. https://elibro.net/es/ereader/unitechn/183470?page=76.
Fecha de consulta: 15/03/2025/02/2025

Urcuqui López, Christian Camilo, Navarro Cadavid, Andrés (2023). *Ciberseguridad: los datos, las semillas del caos: (1 ed.)*. Cali, Editorial Universidad Icesi, p. 49. https://elibro.net/es/ereader/unitechn/278897?page=49
Fecha de consulta: 15/04/2025

Urcuqui López, Christian Camilo, García Peña, Melissa y Osorio Quintero, José Luis (2018). *Ciberseguridad: un enfoque desde la ciencia de datos*: (1 ed.). Editorial Universidad Icesi, p. 23. https://elibro.net/es/ereader/unitechn/120435?page=23
Fecha de consulta: 09/04/2025

Uribe Macías, Mario Enrique (2011). *Los sistemas de gestión de la calidad: el enfoque teórico y la aplicación empresarial*: (1 ed.). Ibagué, Colombia: Sello Editorial Universidad del Tolima, p. 45. https://elibro.net/es/ereader/unitechn/71132?page=45
Fecha de consulta: 17/02/2025

Useche, Alejandro J. Juárez, Fernando. y Ramírez Restrepo, Álvaro. (2022). *Tecnologías de la cuarta revolución industrial y su aplicación en la Armada Nacional de Colombia*: (1 ed.) p. 19 – 20. Bogotá, Editorial Universidad del Rosario. https://elibro.net/es/ereader/unitechn/219907?page=19
Fecha de consulta: 23/02/2025

Valencia Gómez, José Daniel (2025). *Diseño del Sistema de Gestión de Seguridad de la Información según el marco de trabajo internacional NIST CSF 2.0 en la empresa Skynet*, Universidad del Bosque, Facultad de Ingeniería, Especialización en Seguridad de Redes Telemáticas, Bogotá. https://repositorio.unbosque.edu.co/bitstreams/33f26b64-05df-4dbf-88f9-ff1aa28fe73e/download
Fecha de consulta: 18/02/2025

Vásquez Vergara, Henry Anthonny (2024) *Guía de buenas prácticas de seguridad informática basado en la norma internacional ISO 27002:2022 para una entidad financiera, Chepén - La Libertad* [Tesis de grado, Universidad Nacional de Trujillo], Perú. https://dspace.unitru.edu.pe/server/api/core/bitstreams/051f804c-b180-4e7c-bde9-52154efe9e33/content
Fecha de consulta: 19/02/2025

Villa Crespo, Enrique y Morales Alonso, Ismael (2017). *Ciberseguridad IoT y su aplicación en Ciudades inteligentes*: (1 ed.). Madrid, RA-MA Editorial, p, 268 – 270. https://elibro.net/es/ereader/unitechn/230294?page=268
Fecha de consulta: 20/02/2025

Zapata, David (2024, agosto 10). Instituciones del Estado, las más vulnerables a los ciberataques, *El Heraldo*. https://www.elheraldo.hn/honduras/instituciones-estado-vulnerables-ciberataques-honduras-HL20818492
Fecha de consulta: 19/02/2025

ANEXOS

SECCIÓN 1: INSTRUMENTOS TEMÁTICOS

ANEXO 1 CUADRO COMPARATIVO DE ESCÁNER DE VULNERABILIDADES

Criterio	Herramienta 1	Herramienta 2	Herramienta 3
Tipo de infraestructura.			
Límite de periodo de prueba.			
Funcionalidades en versión de prueba.			
Equipos administrables en versión de pruebas.			
Método de gestión de activos.			
Soporte de múltiples versiones de Sistemas Operativos (Windows, Linux, OSX).			
Formato de reportes.			
Base de datos de vulnerabilidades actualizable.			
Segmentación de activos por ambiente.			
Profundidad de análisis configurable (Superficial o exhaustivo).			
Análisis multicapa (Red, sistema operativo, bases de datos, aplicaciones web, configuraciones, etc.).			
Automatización de correos y notificaciones.			
Aplicar remediación automática de vulnerabilidades.			
Proveedor en Honduras			

ANEXO 2 MATRIZ DE PERFILAMIENTO ORGANIZATIVO NIST

COMPONENTES DEL NÚCLEO			PERFIL ACTUAL	PERFIL OBJETIVO
FUNCIÓN	CATEGORÍA	SUBCATEGORÍA	NIVEL	NIVEL

ANEXO 3 LISTA DE VERIFICACIÓN BASADA EN ISO 27002: CONTROLES EN LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

Controles	Aplicado		Observaciones.
	SI	NO	
I. Identificación de vulnerabilidades técnicas.			
1. Se tiene definidas las funciones y responsabilidades asociadas a la gestión técnica de vulnerabilidad, incluida supervisión de vulnerabilidad, evaluación de riesgo de esta, actualización, monitoreo de activos y cualquier responsabilidad de coordinación necesaria.			
2. Se tiene identificados los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento de las mismas, en el caso de programas informáticos y otras tecnologías.			
3. Se usan herramientas de exploración de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y verificar si la aplicación de parches a las vulnerabilidades fue exitosa;			
4. Se realizan pruebas de penetración o evaluaciones de vulnerabilidad planificadas, documentadas y repetibles por personas competentes y autorizadas para apoyar la identificación de vulnerabilidades.			
5. La organización cuenta con procedimientos y capacidades para detectar existencia de vulnerabilidades en sus productos y servicios.			
II. Evaluación de vulnerabilidades técnicas.			
6. Se analizan y verifican los informes para determinar qué actividad de respuesta y reparación es necesaria.			
7. Se identifican los riesgos asociados y las acciones a realizar, una vez identificada una posible vulnerabilidad técnica. Estas acciones pueden consistir en la			

actualización de los sistemas vulnerables o en la aplicación de otros controles.			
I**II. Medidas apropiadas para hacer frente a las vulnerabilidades técnicas.**			
8. Se cuenta con un proceso de gestión de actualizaciones de “software” para garantizar que se instalan los parches y actualizaciones de aplicaciones más recientes para todo el “software” autorizado.			
9. Se define un calendario para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes.			
10. Se prueban y evalúan actualizaciones antes de instalarlas para garantizar que son eficaces y no provocan efectos secundarios que no se puedan tolerar.			
IV. Otras consideraciones.			
11. Se mantiene un registro de auditoría para todos los pasos realizados en gestión de vulnerabilidades técnicas.			
12. El proceso de gestión de vulnerabilidad técnica se debería supervisar, evaluar periódicamente para garantizar su eficacia y eficiencia.			

SECCIÓN 2: INSTRUMENTOS METODOLÓGICOS

ANEXO 4 MATRIZ DE REVISIÓN DOCUMENTAL

N°	Año	Autores	Titulo	Tipo de recurso	Referencia

ANEXO 5 MATRIZ DE ANÁLISIS FODA

ANEXO 6 FORMATO PARA NOTAS DE CAMPO

PROPUESTA DE PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL) PREGUNTAS DE ENTREVISTA PARA EMPLEADOS DE SEGURIDAD DE LA INFORMACIÓN

FORMATO PARA NOTAS DE CAMPO

Fecha:	
Lugar:	
Hora Inicio:	
Hora Final:	
Tipo:	☐ Evento ☐ Idea ☐ Actividad
Descripción:	

ANEXO 7 MATRIZ DE ANÁLISIS DE DATOS

Sección del instrumento	Pregunta	Participante 1	Participante 2

ANEXO 8 PREGUNTAS DE ENTREVISTA PARA PERSONAL DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN

MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTA DE PROCESO PARA LA GESTIÓN DE VULNERABILIDADES BASADO EN EL MARCO DE CIBERSEGURIDAD NIST PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE HONDURAS LIMITADA (COACEHL)

PREGUNTAS DE ENTREVISTA PARA EMPLEADOS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:
Diseñar un proceso adaptando el Marco de Seguridad Cibernética del NIST, para gestionar las vulnerabilidades presentes en los sistemas de información de COACEHL, mejorando con ello sus estándares de ciberseguridad.

Contexto:
Su participación y respuestas como entrevistado son sumamente importantes por lo que se requiere de usted la mayor colaboración y que sus respuestas sean transparentes y claras.

Participación Voluntaria:
Su participación es completamente voluntaria. Usted puede optar por no responder a cualquier interrogante o retirarse de la entrevista sin objeción alguna.

Duración:
La entrevista tendrá una duración aproximada de 45 a 60 minutos.

Confidencialidad:
La información compartida durante la entrevista será de carácter confidencial y utilizada únicamente para los propósitos de esta investigación. Se mantendrá el anonimato de los participantes.

Beneficios y Riesgos:
No se contemplan riesgos directos para usted al participar en este ejercicio. Y entre los beneficios podemos mencionar: La posibilidad de definir una propuesta que mejore los procesos existentes en COACEHL

Consentimiento:
Se solicita que firme este documento para confirmar que comprende los detalles descritos, que está conforme con la información proporcionada, que acepta participar en la misma y que autoriza el uso de los datos recopilados para los fines expuestos previamente.

Firma del Participante: _____ Fecha: _____

Datos Demográficos:

1. Edad:

- ☐ 21 – 30 años.
- ☐ 31 – 40 años.
- ☐ 41 – 50 años.
- ☐ 51 – 60 años.
- ☐ 61 o más.

.

2. Género:

- ☐ Hombre.
- ☐ Mujer.

3. Último grado de escolaridad culminado:

- ☐ Doctorado.
- ☐ Posgrado.
- ☐ Pregrado.
- ☐ Educación Media.
- ☐ Educación Básica.
- ☐ Ninguno.

4. Profesión: _____

Sección: Introducción.

5. ¿Puede por favor describirme su rol y responsabilidades dentro de COACEHL?

_____

_____

6. ¿Qué es lo que más le agrada de trabajar en COACEHL y en el área de seguridad de la información?

_____

_____

7. De acuerdo a su experiencia y objetivos trazados en el Plan Operativo Anual (POA) ¿Qué retos enfrentan como Seguridad de la Información en el contexto actual?

_____

Sección: Gobierno y alineamiento estratégico.

8. ¿Qué marcos conoce relacionados con Gobierno de TI, Seguridad de la Información y Ciberseguridad? (Márquelos).

- ☐ Familia ISO 27000 (27001, 27002, 27005, etc.).
- ☐ COBIT 2019.
- ☐ NIST.
- ☐ OCTAVE.
- ☐ ITIL.
- ☐ COSO.
- ☐ Otros: _____
- ☐ Ninguno.

9. ¿Cuál de los siguientes marcos se aplican en la empresa? (Márquelos).

- ☐ Familia ISO 27000 (27001, 27002, 27005, etc.).
- ☐ COBIT 2019
- ☐ NIST
- ☐ OCTAVE
- ☐ ITIL
- ☐ COSO
- ☐ Otros: _____
- ☐ Ninguno.

10. ¿La empresa cuenta con un Sistema de Gestión de Seguridad de la Información?

- ☐ Si.
- ☐ No.

11. ¿Cuál de las siguientes políticas se aplican en la empresa? (Puede marcar varias opciones).

- ☐ Política de Seguridad de la Información.
- ☐ Política de gestión de activos tecnológicos (o equivalente).
- ☐ Política para la gestión de actualizaciones (o parches).
- ☐ Política para la gestión de vulnerabilidades.
- ☐ Política para la separación de ambientes (Pruebas, Calidad, Producción).
- ☐ Política de gestión de cambios en activos tecnológicos.
- ☐ Política de respaldo y recuperación frente a desastres.

12. ¿Cuál de los siguientes procesos se aplican en la empresa? (Puede marcar varias opciones).

☐ Proceso de configuración de activos tecnológicos.
☐ Proceso de aplicación de parches.
☐ Proceso de remediación de vulnerabilidades.
☐ Proceso de implementación de cambios en activos tecnológicos.
☐ Política de respaldo y recuperación frente a desastres.

13. ¿Cuál de los siguientes aspectos se cumplen en cuanto a la política de Seguridad de la Información y Ciberseguridad? (Puede marcar varias opciones):

☐ Estas políticas son establecidas, comunicadas y aplicadas.
☐ Las políticas se establecen en base al contexto organizativo, la estrategia de ciberseguridad y los objetivos estratégicos del negocio.
☐ Estas políticas se revisan, actualizan, comunican y aplican para reflejar los cambios en los requisitos legales /normativos, las amenazas, la tecnología y la misión de la organización.

14. Al considerar el tema de la supervisión o seguimiento. ¿Qué descripciones coinciden con las prácticas de la institución? (Puede marcar varias opciones):

☐ Los resultados de las actividades de Seguridad de la Información y Ciberseguridad en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.
☐ La estrategia de gestión de Seguridad de la Información y Ciberseguridad, se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización.
☐ El rendimiento de la gestión de Seguridad de la Información y Ciberseguridad de la organización se evalúa y revisa para realizar los ajustes necesarios.

15. Como parte de las actividades de seguimiento y cumplimiento de políticas y procesos. ¿Se genera alguno de los siguientes reportes o indicadores de desempeño (KPI) para los Altos Mandos? (Puede seleccionar varias opciones).

☐ Indicadores de aplicación de parches.
☐ Indicadores de remediación de vulnerabilidades.
☐ Indicadores de cobertura de agentes de seguridad en activos tecnológicos.
☐ Otros: _____

Sección: Identificación y Gestión de Activos.

16. Sobre los activos (Por ejemplo: Datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos (Puede marcar varias opciones).

☐ Se mantienen inventarios del hardware gestionado por la organización.
☐ Se mantienen inventarios de software, servicios y sistemas gestionados por la organización.
☐ Se mantienen inventarios de los servicios prestados por los proveedores.
☐ Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.
☐ Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida.

17. ¿Con qué periodicidad se actualiza el inventario de activos?

☐ Diariamente.
☐ Semanalmente.
☐ Mensualmente.
☐ Bimestralmente.
☐ Trimestralmente.
☐ Semestralmente.
☐ Anualmente.

18. ¿La organización comprende el riesgo de seguridad cibernética para la misma, los activos y los individuos por medio de algunas de estas prácticas? (Puede marcar varias opciones):

☐ Se identifican, validan y registran las vulnerabilidades de los activos.
☐ Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades.
☐ Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento.
☐ Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades.

Sección: Detección y Gestión de vulnerabilidades técnicas.

19. Describa como se gestionan las vulnerabilidades en los activos tecnológicos actualmente.

_____

_____

20. Describa como se mantiene un registro de auditoria o documentan todos los pasos dados en la gestión de vulnerabilidades técnicas.

_____

_____

21. ¿De dónde se reciben informes sobre vulnerabilidades en los activos tecnológicos (Puede marcar una o ambas)?

☐ Fuentes internas.
☐ Fuentes externas.

22. Al considerar como se monitorean los activos para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos. ¿Cuáles de las siguientes opciones describen a la organización?

☐ Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos.

☐ Se monitorea el entorno físico para detectar posibles acontecimientos adversos.
☐ Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.
☐ Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar acontecimientos potencialmente adversos.
☐ Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles acontecimientos adversos.

23. Sobre el análisis de eventos adversos (Seleccione aquellas que se practican en la organización):
☐ Se analizan anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos para caracterizarlos y detectar incidentes de seguridad cibernética.
☐ Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas.
☐ Se comprende el impacto estimado y el alcance de los acontecimientos adversos.
☐ La información sobre acontecimientos adversos se proporciona al personal y a las herramientas autorizadas.
☐ La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis.
☐ Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos.

24. ¿Se dispone de los siguientes ambientes (Puede marcar varias opciones)?
☐ Pruebas (o Desarrollo).
☐ Calidad (o QA).
☐ Pre-Producción.
☐ Producción.

Sección: Exploración de Herramientas.

25. ¿Actualmente se cuenta con algunas de estas herramientas? (Puede marcar varias opciones).
☐ Herramienta de parcheo.
☐ Escáner de vulnerabilidades.
☐ Software para la remediación automática de vulnerabilidades.

26. ¿Se emplea alguno de estos productos?
☐ OpenVas (o Greenbone).
☐ Nessus (o Tenable).
☐ Manage Engine Endpoint Central.
☐ Manage Engine Patch Vulnerability Plus.
☐ Otros: _____

27. ¿Qué beneficios encuentra usted en estas herramientas? (Puede seleccionar varias opciones).
☐ Mayor visibilidad de la superficie de ataque.

☐ Claridad con respecto a activos más vulnerables.
☐ Automatización de tareas manuales.
☐ Otros: _____

28. Las actualizaciones de software se obtienen y despliegan desde (Puede marcar varias opciones).
☐ Sitios oficiales de los fabricantes.
☐ Herramienta de gestión de parches.
☐ Repositorios locales.

Sección: Desafíos y oportunidades de mejora.

29. ¿Cómo se identifican mejoras en los procesos, procedimientos y actividades de gestión de seguridad de la información y ciberseguridad? (Puede marcar varias opciones).
☐ Las mejoras se identifican a partir de evaluaciones.
☐ Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.
☐ Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativas.
☐ Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de seguridad de la información y ciberseguridad que afectan a las operaciones.

30. Desde su experiencia: ¿Cuáles son los principales desafíos que enfrenta la empresa en temas de Seguridad de la Información y Ciberseguridad? (Seleccione 2).
☐ La obsolescencia de los activos tecnológicos.
☐ Desarrollar mayor agilidad en el cierre de brechas de seguridad.
☐ Alcanzar más madurez en procesos y controles basados en mejores prácticas.
☐ Automatización de procesos.
☐ Mayor complejidad de los ciberataques.
☐ Otros: _____

31. ¿Cuáles pueden ser los principales obstáculos para la mejora de los procesos de Seguridad de la Información en la empresa?
☐ Resistencia al cambio.
☐ Limitaciones presupuestarias.
☐ Falta de apoyo por parte de los altos mandos.
☐ Infraestructura tecnológica.
☐ Otros: _____

32. ¿Qué tanto interés tiene en esta propuesta de proceso para la gestión de vulnerabilidades basado en el Marco de Ciberseguridad del NIST?
☐ Ninguno.
☐ Poco.

☐ Moderado.
☐ Mucho.

33. En un escenario ideal ¿Qué estrategias cree que serían más efectivas para asegurar que se adopte el proceso de manera exitosa?

☐ Capacitación inicial.
☐ Comunicación de los beneficios del proceso.
☐ Acompañamiento en la adopción del proceso.
☐ Otra: _____

Sección: Cierre de la entrevista.

34. ¿Hay algún aspecto relevante que considere importante mencionar sobre el desarrollo de la propuesta de este proceso y que no hayamos cubierto aún?

SECCIÓN 3: INSTRUMENTOS DE MONITOREO Y CONTROL

ANEXO 9 DIAGRAMA DE GANTT