Universidad CENFOTEC

Facultad de Ingeniería en Sistemas

Maestría Profesional en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

EVALUACIÓN DEL SISTEMA DE GESTIÓN DE RESILIENCIA Y DE CIBERSEGURIDAD EN UN PROVEEDOR DE INTERNET, UTILIZANDO EL "MARCO PARA LA MEJORA DE LA SEGURIDAD DEL INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA NIST 1.1"

Elaborado por:

Artavia León, José Andrés

Soto Sotelo, Marvin G.

Marzo 2023

2 Declaratoria de derechos de autor

Declaramos que la investigación realizada en este proyecto es absolutamente original, auténtica, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes. Las ideas, doctrinas, resultados y conclusiones a las que hemos llegado son de nuestra absoluta responsabilidad.

Además, todos los datos personales que pudieran identificar tanto a una persona física, como a la empresa objeto de esta investigación han sido anonimizados con el fin de autorizar la consulta de esta investigación y uso con fines exclusivamente académicos.

Dedicatorias

Como co-autor, José Andrés Artavia León, dedico este proyecto final de graduación a:

A Dios, quien ha sido mi guía y mi fortaleza desde el primer momento en quien puse toda mi confianza, para poder realizar un proyecto exitoso. A Katherinne Alvarado Ramírez, mi esposa, quien con amor, paciencia y esfuerzo ha sido un apoyo incondicional y mi pilar fundamental para lograr esta meta tan importante para nuestra familia.

A Sara Artavia y Andrés Artavia, mis dos hijos, quienes aún son muy pequeños para comprender la importancia de este logro, sin embargo, con cada

beso y abrazo que me dan a diario han sido mi motor y mi principal motivo para seguir adelante, especialmente en los momentos más difíciles y de mayor cansancio.

Como co-autor, Marvin Giovanni Soto Sotelo, dedico este proyecto final de graduación:

Al Supremo, quien en las vertiginosas y escarpadas sendas de la vida me ha provisto de piernas, de brazos y de manos fuertes para aferrarme a tantos imposibles hoy posibles, quien ha provisto sandalias para lidiar con los guijarros filosos de las vicisitudes y limitaciones, quien me ha dado vigor para sostenerse erguido en los severos huracanes de las pruebas y en las amargas horas en que he querido claudicar.

A mi madre, tan fuerte, tan sabia, llena de coraje y una indecible energía vital. Sos el génesis de mi nada, me has guiado e inspirado, me amas incluso más de lo que yo mismo me amaría y me has forjado, me has protegido, me has alumbrado

incesantemente en tus brazos de diosa a través de los abismos, los valles y las cimas de tu propia vida.

A mi Esposa María Gabriela, mástil que sostiene mis velas en las apacibles y también en las bravías tormentas de mi vida, refugio sereno cuando lucho contra mis demonios internos, mana que me nutre cuando mis fuerzas decrecen, mi pedacito de cielo cual oasis en los desiertos de este viaje que es la vida. ¡A vos, mi Negrita, ¡a vos que me llenas de eternidad!

A mis hijos, combustible que mueve mi maquinaria de carne, tendones y huesos. Quienes ponen coto a mis ansias de renuncia porque sé que me ven y me

siguen. A ustedes, que llevan en sus venas el indomable e incansable espíritu de su padre, de su abuelo, de mis ancestros.

Agradecimientos

Agradecemos profundamente a todas las autoridades y personal docente y administrativo que hacen de la Universidad CENFOTEC un grato lugar para desarrollarse, tanto como profesionales, como personas; con lo cual hemos obtenido un conocimiento invaluable que nos potencia a ser mejores profesionales en el campo de la ciberseguridad.

Expresamos nuestra más grande admiración y sincero agradecimiento al Dr. Luis Carlos Naranjo Zeledón, nuestro tutor durante esta investigación, quien con su

dirección, conocimiento, enseñanza y colaboración fue una pieza fundamental para el éxito de este proyecto.

Nuestra inconmensurable gratitud a nuestras familias, incluso a aquellos que viven inmaterialmente en nuestros corazones hasta el día final.

Gracias a la vida por este viaje afortunado y apasionante por las letras y el conocimiento, durante el cual incluso tuvimos el privilegio de coincidir con seres humanos extraordinarios.

De hinojos agradecemos el amor y la gracia que brilla en el rostro de quienes nos aman, nos admiran y nos ven donde nosotros aun solo vemos nieblas.

Hoja de aprobación del proyecto

Hoja de aprobación del proyecto, firmada por los miembros del Tribunal Examinador (Aprobación Tribunal). Sin este documento, la tesis NO ES VÁLIDA.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad**, requisito para optar por el título de grado de **Maestría**, para los estudiantes: **Artavia León José Andrés y Soto Sotelo Marvin.**

LUIS CARLOS NARANJO ZELEDON (FIRMA) — Firmado digitalmente por LUIS CARLOS NARANJO ZELEDON (FIRMA) Fecha: 2023.03.17 10:25:18 -06'00'

Dr. Luis Carlos Naranjo Zeledón
Tutor

Alonso Ramírez — Digitally signed by Alonso Ramírez Date: 2023.03.20 15:13:42 -06'00'

M.Sc. Luis Alonso Ramírez Jiménez
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA) — Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA) Fecha: 2023.03.20 20:40:57 -06'00'

M.Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 16 de marzo de 2023

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

Tabla de Contenidos

Tabla de Figuras

Tabla de Tablas

1 Resumen Ejecutivo

En esta nueva era de la hiperconectividad, la digitalización y del ciberespacio, las empresas inmersas en el mundo de la tecnología han visto un importante crecimiento del cibercrimen, el cual ha aumentado tanto en el grado de sofisticación, como en la cantidad de eventos que se ejecutan, y es tanto así, que el ciber crimen organizado es hoy en día, el tipo de crimen más rentable; se dice que el 80% de los ciberataques fueron coordinados por anillos de crimen organizado (Security Intelligence, 2015) en los cuales los datos, herramientas y experiencia fueron ampliamente compartidos entre ellos, otorgándoles un poder inigualable.

Según el reporte anual de datos publicado por IBM (Cost of a Data Breach Report 2021), para este año 2021 los costos promedio de una filtración fueron los

más altos de la historia, ascendiendo a los $4,24 millones, al respecto señalaron lo siguiente:

(...) Estos costos fueron significativamente más bajos para algunas de las organizaciones con una postura de seguridad más madura, sin embargo, para aquellas organizaciones que se quedaron atrás en áreas de la seguridad, tales como; inteligencia artificial, automatización, adopción de modelos de “confianza cero” y seguridad en la nube, están teniendo una repercusión muy alta en términos financieros. (...)

En este mismo reporte de IBM, se muestra que la pérdida de negocios representó el 38% del promedio general con un costo promedio de $1.59 millones. Los costos comerciales perdidos incluyeron una mayor rotación de clientes, pérdida de ingresos debido al tiempo que los sistemas estuvieron fuera de servicio y el costo creciente de adquirir nuevos negocios debido a la disminución de la reputación.

Solo un 10% de las compañías tienen un plan de gestión de incidentes, lo cual tiene sentido, desde el punto de vista financiero, ya que elaborar un plan de gestión requiere una alta inversión tanto en recurso humano especializado como en equipo tecnológico y si a esta le añadimos el desconocimiento o falta de interés de las altas gerencias da como resultado que sea tan alto el número de empresas que no cuentan con dicho plan y esto bien lo saben los cibercriminales que han hecho “El gran negocio de hackear a los pequeños negocios”.

Es un reto para la ciberseguridad mostrar a las empresas los riesgos a los que se encuentran expuestos desde la transformación digital, la necesidad de blindar el corazón de las empresas que es su información, ya que los activos físicos

dejaron de ser importantes para los negocios y ahora todo lo importante está en la red, por ende, si antes se contrataba seguridad para cuidar una planta física, ahora más que nunca, debe invertirse en seguridad informática y en un robusto Sistema de Gestión de Resiliencia y Ciberseguridad.

En este trabajo final de graduación, se desarrollará un Sistema de Gestión de Resiliencia y Ciberseguridad, el cual será una combinación de diferentes metodologías que servirá de guía para que pueda ser utilizado por empresas de cualquier tamaño e industria con el fin de lograr implementaciones de sistemas de gestión de resiliencia y ciberseguridad de forma efectiva y sencilla.

En definitiva, esta investigación recopila un conjunto de metodologías y herramientas necesarias para lograr satisfactoriamente la implementación de un robusto sistema de resiliencia y ciberseguridad en UN PROVEEDOR DE INTERNET y que adicionalmente, se apoya en la experiencia de sus autores, gracias a sus años de ejercicio profesional en el campo de la ciberseguridad tanto en, posiciones

gerenciales, como también en funciones de consultores especializados, es que se logra la combinación perfecta para desarrollar este sistema de gestión. La construcción inicia con una fase diagnostica, un inventario de activos tecnológicos y un análisis de riesgo, en los cuales definiremos brechas, activos críticos y riesgos de mayor impacto y/o probabilidad; para luego enfocarnos en la construcción de planes de seguridad de la información, ciberseguridad, gestión continua de incidentes, planes de acción, de continuidad del negocio, de recuperación ante desastres, así de como de toda la instrumentación necesaria para blindar el mejor posicionamiento posible a cualquier empresa.

1 Capítulo I. Introducción

La cuarta revolución industrial estará marcada por los robots integrados en sistemas ciber físicos, la digitalización y la automatización de los procesos, Internet de las cosas con su horda de dispositivos conectados, los cuales serán sin duda los responsables de esta transformación radical.

En palabras simples; hemos venido migrando muy aceleradamente todas nuestras interacciones físicas al mundo virtual. El vehículo para movilizar esta transformación son las comunicaciones y el vasto universo que se sustenta en la

tecnología en todas sus formas, en una paranoia interminable, porque como sabemos, los avances no cesan.

Por lo tanto, las amenazas que antes conocíamos en el mundo físico han comenzado su migración hacia la virtualidad haciendo inevitable la necesidad de educarnos digitalmente y, además; de gestionar todas las tecnologías que usamos en este nuevo universo.

Así pues, hemos visto florecer la seguridad de la información y la ciberseguridad como nuevos campos de conocimiento derivados de las tecnologías y su disruptivo emerger.

1.1 Generalidades

Las metodologías, estándares y normas que conforman la base y el fundamento de este documento, son de carácter público, sin menosprecio de que se ameriten en el caso de las acreditaciones, las certificaciones respectivas. Sin embargo, la acción de evaluar la Resiliencia en Ciberseguridad en una empresa específica como lo es en UN PROVEEDOR DE INTERNET, e interactuar con un campo que explora información sensible, privada y de uso interno, conlleva que sea

necesario la expresa suscripción de cláusulas de confidencialidad, a través de la que se ha solicita anonimizar los datos, a fin de que los datos reales no se vuelvan de dominio público.

1.2 Antecedentes del Problema

Las buenas prácticas de implementación de sistemas de resiliencia, seguridad de la información y ciberseguridad son tan diversas, como complejas; debiéndose invertir enormes esfuerzos en entender dichas prácticas, para luego

definir cuales componentes de estos posibles marcos, atienden el contexto organizacional.

Algunos de estos marcos están diseñados para atender industrias específicas, como, por ejemplo: ISO/IEC 27000, ISO/IEC 27032, NIST CSF, BS31111, ISO/IEC 22301, PCI DSS, SOX, HIPPA, entre otros.

Esta investigación pretende evidenciar que la aplicación de normativas está direccionada a dar un tratamiento sesgado a temas asociados con el giro de negocios y no necesariamente a una metodología transversal; por lo que, considerando el nivel de complejidad de estos temas, el presente proyecto se centra únicamente en evaluar el sistema de gestión de resiliencia de ciberseguridad de las empresas, utilizando el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1.

1.3 Definición y Descripción del Problema

Dado el alto nivel de especialización que se requiere, tanto en materia de tecnológica, protección, prevención, defensa y respuesta ante amenazas, continuidad de negocios, recuperación ante desastres, etc., las empresas se

enfrentan a un gran reto de defenderse efectivamente de ataques cibernéticos, lo que deben hacer con limitados recursos humanos, técnicos y financieros, y en la mayoría de los casos, con un nivel mínimo de conocimiento en materia de ciberseguridad.

Los costos promedio de una filtración de datos tal y como se mencionó anteriormente, ascendieron a $4,24 millones para el año 2021, el costo total

promedio más alto en la historia. Una realidad que ninguna empresa puede obviar y es necesario tomar acciones de forma inmediata, lo cual representa otro reto aún mayor.

El mayor riesgo de una organización es no conocer sus riesgos y por ende no prepararse para afrontarlos, y es a través de la planificación, que muchas empresas logran garantizar la disponibilidad en sus sistemas y con la menor superficie de ataque en los servicios que brindan, para ofrecer un mejor servicio a sus clientes -*quienes son cada vez más exigentes*- y es que para todas las personas su necesidad es la más importante, y eso lo experimentamos todos sea cual sea nuestra posición, sólo bastaría con realizar el pago con una tarjeta de crédito y que el sistema no funcione cuando estamos realizando la transacción, para que se nos vuelva una urgencia saber si el pago se realizó o no, si debo reclamar por una transacción duplicada, etc.

1.4 Justificación

La industria ha enfocado sus esfuerzos en crear marcos de mejores prácticas focalizados en normas para mejor la seguridad de la Información, y especialmente enfocadas en los servicios financieros, hospitalarios y otros, con el cual se da un tratamiento y gestión de riesgos, continuidad de negocio y recuperación ante

desastres, no obstante, digerir esos volúmenes de datos, controles, políticas y luego consolidarlos a las empresas de manera agnóstica, suele ser una hipérbole. La experiencia en el mercado de la ciberseguridad, de la seguridad de la información y especialmente del gobierno de la tecnología, ha dejado a la vista la carencia de herramientas simples aplicables transversalmente a las empresas sin distingo de

tamaño y presupuestos.

Lo que se plantea es la construcción de un sistema de gestión de resiliencia y ciberseguridad para simplificar las complejidades, reducir los tiempos de implementación y lograr que sea económicamente accesible para cualquier empresa, enrumbarse con certidumbre en el cumplimiento de las regulaciones y estándares esenciales en materia de ciberseguridad, mientras se logra que la empresa sea resiliente.

En resumen; se busca mejorar la capacidad defensiva, mejorar la respuesta ante incidentes, generar una cultura de ciberseguridad mediante la alfabetización digital transversal y garantizar la continuidad de las operaciones y/o su rápida respuesta y vuelta a producción ante eventos graves. Todo a partir de este primer ejercicio.

1.5 Viabilidad

El marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1, es un conjunto de mejoras prácticas que se puede adquirir de manera gratuita en el sitio web oficial del instituto. Lo que facilita la viabilidad del proyecto, al existir los recursos necesarios para su desarrollo.

1.5.1 Punto de Vista Técnico.

Los autores, quienes son profesionales en ciberseguridad, cuentan con el conocimiento y experiencia en la implementación y evaluación de diferentes estándares asociados a la seguridad de la información, la ciberseguridad, la gestión

de riesgos, la continuidad de negocios, la recuperación ante desastres e inteligencia de amenazas empleando diversas tácticas, técnicas y procedimientos. Igualmente se espera que, como parte del proceso investigativo, se recopile la experiencia de diversos autores en la resolución de problemas similares, que puedan ser aplicados al problema que se pretende abordar.

1.5.2 Punto de Vista Operativo.

La empresa que vaya a realizar la evaluación de su sistema de gestión -*en este caso la empresa UN PROVEEDOR DE INTERNET*-, necesita poner a disposición de los consultores un equipo interdisciplinario con el fin de proveer la información necesaria para realizar el análisis y diagnóstico.

En el caso de no contar con un consultor, y por el contrario se pretenda hacer con personal interno, será necesario seguir paso a paso las guías dispuestas por el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1, tal cual como se describe a lo largo de este documento.

1.5.3 Punto de Vista Económico.

La realización de este trabajo es posible, desde el punto de vista económico, ya que solamente se necesita de las horas de trabajo de los consultores, para realizar el análisis y diagnóstico, lo cual generará un resultado final que podrá ser usado para las empresas para iniciar con un plan estratégico para mejorar su postura de defensa en ciberseguridad.

Además, al tratarse de una evaluación basada en un conjunto de normas disponibles para ser utilizadas sin ningún costo económico, no es necesario hacer ningún tipo de inversión económica adicional para esta evaluación.

1.6 Objetivos

1.6.1 Objetivo General.

Evaluar el sistema de gestión de resiliencia de ciberseguridad de la empresa UN PROVEEDOR DE INTERNET, utilizando el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1.

1.6.2 Objetivos Específicos.

- Revisar el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1. a fin de determinar si es necesario disponer de instrumentos que faciliten la evaluación de los sistemas de gestión de resiliencia de ciberseguridad.

- Aplicar una evaluación al sistema de gestión de resiliencia de ciberseguridad de la empresa UN PROVEEDOR DE INTERNET, desarrollada con base en el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1.
- Emitir recomendaciones relacionadas con la ciberseguridad a la empresa UN PROVEEDOR DE INTERNET, con base en los resultados obtenidos en la evaluación.

1.7 Alcances y Limitaciones

En esta sección se pretender asignar correctamente las expectativas de todos los involucrados.

1.7.1 Alcances.

El proyecto comprende la evaluación del sistema de gestión de resiliencia de ciberseguridad de la empresa UN PROVEEDOR DE INTERNET, utilizando como referencia el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1.

1.7.2 Limitaciones.

No se considera como parte del desarrollo de este proyecto, implementar ningún proceso ni herramienta en empresas, así como, tampoco ninguna modificación a alguno existente.

Este proyecto se limita a evaluar el estado actual del plan de resiliencia y ciberseguridad en las empresas, esto con base en el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1.

1.8 Marco de Referencia Organizacional y Socioeconómico

Costa Rica cuenta con una economía que intenta escalar en el ranking global de la ciberseguridad, ubicándose actualmente en el puesto número 39, esto no quiere decir que esté preparada o que sea resiliente, sino que ha tomado medidas a nivel estatal para mejorar el nivel de compromiso del país con la Agenda de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (ITU).

El índice en cuestión busca colaborar con recomendaciones para la mejora de la ciberseguridad a nivel mundial desde el contexto de cada país. En este caso, las recomendaciones van orientadas a facilitar que cualquier empresa pueda realizar una evaluación fiable de su sistema de gestión de resiliencia y ciberseguridad.

Debido al aumento en las amenazas cibernéticas el 89% de las organizaciones le asigna una importancia muy alta a la gestión de ciber riesgos en un contexto cada vez más digital de los negocios. Sin embargo, sólo un 31% de las organizaciones realiza inteligencia de amenazas y comparte información con otras organizaciones (CAMTIC, 2019). Lo que significa que, aunque se hacen esfuerzos estos no son transversales; o bien, no cubren todos los contextos de la ciberseguridad.

Ante esta realidad, parece ser que el entramado para lograr fortalecer la ciberseguridad en las empresas es un esfuerzo unilateral en el cual cada organización debe ingeniárselas para alcanzar. A fin de simplificar este enorme desafío, nuestro objeto de estudio consiste en ofrecer una guía simple, fácil de seguir y amigable con la diversidad de verticales de negocio en el ecosistema país.

1.8.1 Contexto Organizacional

UN PROVEEDOR DE INTERNET es un proveedor costarricense de Internet y conectividad especializada en servicios por fibra óptica con más de 12 años de experiencia en el sector, y su misión es ofrecer una experiencia excepcional de

conexión, manteniendo a sus clientes altamente disponibles y conectados con sus mercados. Cuenta con experiencia en desarrollo e implementación de proyectos de telecomunicaciones en Centro América, a través de servicios de Conectividad

Avanzada IP, Internet Dedicado, Voz Corporativa e integrando soluciones especializadas de hardware, software y tecnologías de información.

1.8.1.1 Oferta de Servicios:

Administrativos: Con material humano altamente calificado, UN PROVEEDOR DE INTERNET tiene la capacidad para formar parte de la operación y soporte técnico de sus clientes, siendo una extensión de su compañía para brindar servicios de atención, soporte, monitoreo o procesos relacionados con su operación de TI.

Conectividad: Las exigencias de las compañías en el ámbito de las Tecnologías de la Información y las Comunicaciones dentro de un mercado cada día más competitivo plantean nuevos desafíos, requiriendo del apoyo y experiencia de una empresa líder como UN PROVEEDOR DE INTERNET.

UN PROVEEDOR DE INTERNET brinda su conectividad a través de su propia Red de Fibra Óptica de última generación, con el fin de garantizar alta capacidad y baja latencia para el rendimiento óptimo de los servicios de sus clientes. Las redes son construidas con base en los más altos estándares de la Industria para garantizar el mayor tiempo de disponibilidad.

1.8.1.2 Misión

Ofrecer una experiencia excepcional de conexión al mundo. Ayudamos a nuestros clientes a lograr sus objetivos, manteniéndolos altamente disponibles y

conectados a sus mercados.

1.8.1.3 Visión

Liderar la provisión de soluciones innovadoras de telecomunicaciones e infraestructuras de redes en el mercado corporativo costarricense y latinoamericano.

21
22

1.9 Estado de la Cuestión

A pesar de que hay muchos estándares y normas, se carece de una guía metodológica que permita a las empresas de cualquier vertical de mercado o tamaño evaluar con éxito su sistema de resiliencia y ciber seguridad.

El concepto de ciber resiliencia, surge a partir de la aparición de lo que conocemos resiliencia organizacional, es decir, de la capacidad de una organización para afrontar adversidades, y por ende su capacidad para recuperar su estado inicial. Dicho en palabras simples, la fortaleza de una organización para enfrentar y adaptarse a los continuos cambios de su entorno en todas las áreas.

Pues bien, siendo que las empresas han tenido que emigrar al ciberespacio, se ha acuñado la palabra ciber resiliencia. En este sentido, el Instituto Nacional de Ciberseguridad de España (INCIBE), define la resiliencia como la *"Capacidad de una organización de resistir ante una situación adversa, como, por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.".*

Es por lo expuesto, que en el presente proyecto se pretende realizar una

evaluación del sistema de gestión de resiliencia y de ciberseguridad en UN PROVEEDOR DE INTERNET utilizando una guía metodológica que simplifique el camino desde la insipiencia hasta el mejor nivel de ciber resiliencia posible en cualquier organización, según sus mismas aspiraciones.

1.9.1 Planificación de la revisión.

Se realiza una búsqueda de la documentación existente sobre el objeto de estudio, con el fin de explorar y conocer los aportes académicos que se hayan emitido

al respecto, identificando, las áreas débiles y oportunidades de mejora. Finalmente, y una vez realizado el análisis de dicha documentación, se procede a desarrollar una guía que sea simple, flexible y de fácil implementación en UN PROVEEDOR DE INTERNET.

1.9.1.1 Formulación de la pregunta

Con el objetivo de encontrar respuestas que demuestren el aporte de información e investigación a este trabajo, se realiza la formulación de la pregunta, la cual nos va a ayudar a delimitar los esfuerzos de búsqueda de información. 1.9.1.1.1 Enfoque del a pregunta

Se determina para esta investigación, que la búsqueda de información se debe realizar con base en documentos técnicos que detallen el uso y aplicación del marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se define en esta sección la pregunta de investigación que se desea

responder de forma clara y concisa, basados en un problema a resolver. Para la cual se realiza un listado de términos clave relevantes para la búsqueda de información y se consideran componentes fundamentales como son la población específica, capacidad técnica y guías de interés. Se definen medidas a utilizar para medir el efecto con base en la pregunta a responder y el diseño de los estudios. **1. Problema.**

Dado el alto nivel de especialización que se requiere, tanto en materia de continuidad de negocios, como en tecnología, las empresas se enfrentan a un gran reto de defenderse efectivamente de ataques cibernéticos.

2. Pregunta.

Dado el problema anterior, se plantea la siguiente pregunta de investigación: ¿Qué guías técnicas se han publicado en el área de seguridad de la información para realizar una efectiva evaluación e implementación del marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1.? **3. Palabras claves y sinónimos.**

Se hace un listado de palabras claves que se van a utilizar para la búsqueda e identificación de documentos y trabajos relacionados con la investigación. En su gran mayoría, estas palabras están en el idioma inglés debido a que existe una gran cantidad de trabajos relaciones y publicaciones en este idioma, las cuales se muestran en la tabla 1.

Tabla 1-1. Listado de palabras.

Palabra	Equivalente en ingles
Ciberseguridad	Cybersecurity
Niveles de implementación	Tiers

Marco	Framework
NIST	NIST
Madurez	Maturity
Modelo	Model
Evaluación	Evaluation
Riesgo	Risk

4. Intervención

Ver los resultados de como la utilización del marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1. contribuye a las empresas a mejorar su resiliencia en ciberseguridad.

5. Control

Al iniciar la investigación, no se cuenta con ninguna base de información. Se empieza con una búsqueda de cero a partir de las palabras clave definidas.

6. Efectos

Se espera tener documentación suficiente con las búsquedas realizadas para entender cuales guías practicas existen para realizar una evaluación del sistema de gestión con base en el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1.

7. Medida de salida

Para la documentación encontrada se realiza una revisión de la calidad de esta en sitios web especializados para tal fin.

8. Población

La población de esta investigación, son los altos gerentes de la empresa UN PROVEEDOR DE INTERNET quienes tienen a cargo la responsabilidad de mantener segura su infraestructura.

9. Aplicación

Esta investigación será de mucha utilidad para ingenieros a cargo de administrar equipos de tecnología y telecomunicaciones, así como también administradores de bases de datos, quienes deben resguardar el activo más valioso de una organización, y que deseen realizar una evaluación de su estado actual de resiliencia y ciberseguridad.

10.Diseño experimental

Durante el diseño experimental se hace un análisis y clasificación de los estudios obtenidos basándose en la calidad del contenido y relevancia para la investigación. Con lo anterior, se garantiza no solo contar con la documentación de mayor confianza para la investigación sino también la suficiente, para evitar tener un rango muy amplio de estudios que pudieran generar resultados no deseados.

1.9.1.2 Selección de fuentes

Se especifican en esta sección las fuentes para la identificación de estudios primarios que se utilizarán para la investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes.

Se han tomado en cuenta para la selección de fuentes, en general, varios aspectos como la popularidad entre investigadores y el respaldo teórico con que cuenta la fuente. También se consideran fuentes que cuenten con gran variedad de

documentación y con relevancia vigente.

1.9.1.2.2 Lenguaje de estudio.

Con respecto a las búsquedas, se utiliza para el estudio tanto el idioma español como el inglés, de esta manera se puede incrementar el rango posible de resultados para obtener recursos de mayor valor.

1.9.1.2.3 Identificación de fuentes

Se describe en este apartado la selección de fuentes para la documentación primaria, además se hace una descripción de la formo como se obtuvieron los resultados y se realizar una lista de fuentes.

1. Método de selección de fuentes:

El método de selección de fuentes se basa principalmente en el respaldo con el que cuenta la fuente en el área de tecnología con respecto a la publicación de estudios y documentos investigativos. Además se considera la facilidad de acceso al documento y en la mayoría de los casos que estos no tengan ningún costo. 2. Cadena de búsqueda.

La cadena de búsqueda se basa en Google hacking, también conocida como “dorks” con la cual se logra hacer una búsqueda con mejor criterio para obtener

resultados más precisos según la necesidad de esta investigación. En esta búsqueda se utilizaron los operadores “intitle”, “AND” y “OR”, definiendo el criterio de búsqueda de la siguiente manera.

"intitle":(evaluation OR Review AND NIST Framework AND Cybersecurity)

3. Lista de Fuentes

a. IEEE

b. ProQuest

c. EBSCO Host

1.9.1.2.4 Selección de fuentes después de la evaluación

Los elementos para refinar la lista de fuentes dependen de la facilidad de aplicación de las cadenas de búsqueda y la confiabilidad de los documentos brindados.

1.9.1.2.5 Comprobación de las fuentes

En este momento no se cuenta con criterio experto para la selección de las fuentes; sin embargo, se escogieron las más utilizadas para obtener documentación relacionada con tecnología

1.9.1.3 Selección de los estudios

Una vez con las fuentes definidas, se han seleccionado los artículos que tenga relación con el marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1. o bien que evidencie la existencia de algún riesgo latente por no tener dicho marco.

1.9.1.3.1 Definición de criterio de inclusión y exclusión de estudios. Se utilizan los criterios detallados en la tabla 2, para incluir o excluir un documento. Los artículos que cumplan los requisitos son candidatos para incluir.

Tabla 1-2 Criterio de inclusión y exclusión de estudios

Pregunta de Investigación	Termino principal para Criterio de inclusión	Criterio de Inclusión

¿Qué guías técnicas se han publicado en el área de seguridad de la información para realizar una efectiva evaluación e implementación del marco para la mejora de la seguridad del instituto nacional de estándares y tecnología nist 1.1.?	“Ciberseguridad”, “Cybersecurity”, “Niveles de implementación”, “Tiers”, “Marco Framework”, “NIST”, “Madurez”, “Maturity”, “Modelo”, “Model”, “Evaluación”, “Evaluation”, “Riesgo”, “Risk”	• Documentos de ciberseguridad que tengan relación con la madurez del sistema de gestión. • Documentos que muestren alguna vulnerabilidad en el sistema de resiliencia de alguna industria. • Estudios que muestren algún grado de automatización para realizar procesos de reconocimiento y análisis de vulnerabilidades. • Documentos que detallen como realizar análisis de riesgos de Ciberseguridad.

Fuente: Elaboración Propia.

1.9.1.3.2 Definición de tipos de estudio

La definición de los tipos de estudios está relacionada con la pregunta de investigación, por lo cual se crea la tabla 3 para determinar los requisitos para definir los artículos.

Tabla 1-3 Tipos de Estudio

Pregunta	**¿Quién?**	**¿Qué?**	**¿Cómo?**	**¿Dónde?**
¿Qué guías técnicas se han publicado en el área de seguridad de la	Personal técnico calificado en ciberseguridad	El Marco para la mejora de la seguridad.	Evaluación, Identificación, Implementación	Empresa de cualquier industria que cuenta con tecnología y datos.

información para realizar una efectiva				

29

evaluación e implementación del marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST?				

Fuente: Elaboración propia.

1.9.1.3.3 Procedimiento para la selección de estudios

Se ha hecho un proceso iterativo por cada fuente para la selección de los estudios relevantes.

1. Utilizar la opción de búsqueda avanzada en las fuentes seleccionadas.
2. Con base en la cantidad de resultados obtenidos, se pone en uso la cadena de búsqueda aplicable para obtener resultados que se consideran de interés.
3. En aquellos casos que el resultado obtenido sea mayor de 50, entonces se aplican filtros adicionales para disminuir dicha lista.
4. Evaluar los resultados obtenidos y aplicar los criterios de exclusión basados en el resumen ejecutivo y las palabras claves del artículo. 5.

Seleccionar los resultados considerados relevantes para la fuente consultada y repetir el proceso con las demás fuentes disponibles.

1.9.2 Ejecución de la revisión

A continuación, se muestra el proceso de selección que se ha llevado a cabo para las diferentes fuentes.

1.9.2.1 Ejecución de la selección en la fuente IEEE

1.9.2.1.1 Selección de estudios iniciales

Para la selección de estudio con la fuente IEEE se realiza la búsqueda de la siguiente manera:

Búsqueda basada en los siguientes parámetros:

- NIST
- Cybersecurity
- Framework

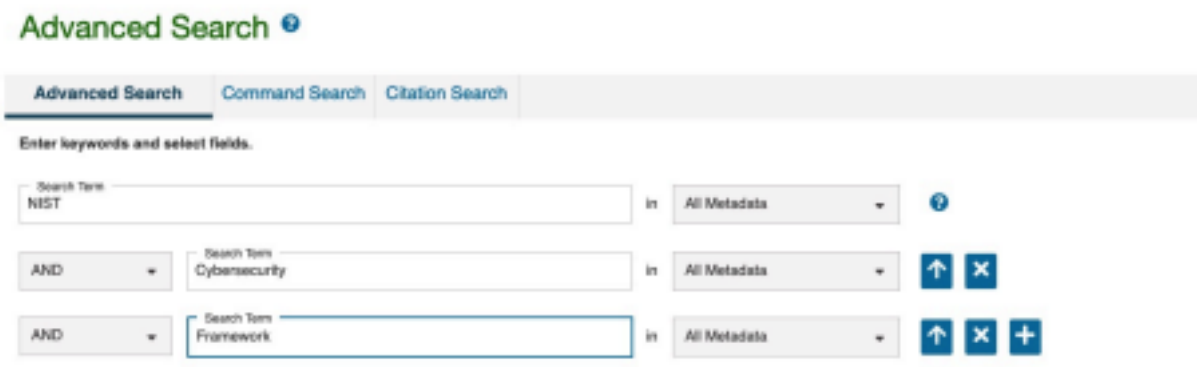

Figura 1-1 Ejecución se la selección, fuente IEE

Una vez realizada la búsqueda utilizando los parámetros mencionados se encontraron sesenta y tres resultados, los cuales fueron seleccionados solamente tres tras aplicar el método de exclusión propuesto (principalmente aquellos artículos

que tenga acceso libre). A continuación, se presenta el detalle de los artículos seleccionados:

#	Titulo	Autores	Año	URL
1	Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a	Fernando Rocha Moreira; Demétrio Antônio Da Silva Filho;	2021	https://ieeexplore.ieee.org/document/9540950/

	Constructivist Multicriteria Methodology	Georges Daniel Amvame Nze; Rafael Timóteo de Sousa Júnior; Rafael Rabelo Nunes		
2	A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method	Angelito Gabriel; Juan Shi; Cagil Ozansoy	2017	https://ieeexplore.ieee.org/document/7954946/
3	Cyberthreats and Security	Morris Chang; Rick Kuhn; Tim Weil	2018	https://ieeexplore.ieee.org/document/8378978/

Tabla 1-4 Estudios encontrados IEEE

1.9.2.1.2 Evaluación de la calidad de los estudios

Se presume la calidad de los artículos mencionados, con base en la cantidad de filtros y evaluaciones realizadas por IEEE.

1.9.2.1.3 Revisión de la selección

La selección de estudios primarios se realiza tras llevar a cabo una revisión de los resúmenes y contenido incluido en cada artículo. Para la revisión de estos artículos, los mismos fueron ordenados con base en la relevancia de los artículos.

1.9.2.1.4 Extracción de la información

Para la extracción de la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación, se consideran los siguientes elementos:

• Evaluación de Riesgos de ciberseguridad.

• Aplicación del marco para la mejora de infraestructura critica. •

Análisis de Resultados.

Fuente	**IEEE**
Titulo	Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology
Autores	Fernando Rocha Moreira; Demétrio Antônio Da Silva Filho; Georges Daniel Amvame Nze; Rafael Timóteo de Sousa Júnior; Rafael Rabelo Nunes

Referencia	[1] D. Pedriali, C. H. Arima, and F. J. Piacente, ‘‘Segurança da informação na Logística 4.0: Bibliométrico,’’ Res., Soc. Develop., vol. 9, no. 2, Jan. 2020, Art. no. e38921949, doi: 10.33448/rsd v9i2.1949. [2] F. B. Bancos, ‘‘Pesquisa febraban de tecnologia Bancária 2019,’’ FEBRABAN-Federação Brasileira de Bancos, São Paulo, Brazil, Tech. Rep., 2019. [3] F. R. Moreira, R. R. Nunes, W. F. Giozza, and G. A. Nze, ‘‘Optimization of the performance of an online payment application by the improve- ment of its infrastructure,’’ in Proc. 15th Iberian Conf. Inf. Syst. Technol. (CISTI), Seville, Spain, 2020, pp. 1–2, doi: 10.23919/CISTI49556.2020. 9140895.
Área	NIST Cybersecurity Framework
Resumen	Este artículo tiene como objetivo mostrar cómo se puede resolver la creación de un plan de riesgos con la ayuda del método multicriterio constructivista. Se aplicó un caso de estudio utilizando “Multicriteria Decision Aid Constructivist” (MCDA-C), tomando como referencia los controles del framework de

	ciberseguridad. El estudio se realizó en un banco brasileño. La relevancia de este trabajo radica en la necesidad de mostrar que la aplicación de métodos multicriterio se puede aplicar en el contexto de la seguridad de la información, por lo que se recomienda el uso de dichos métodos para ayudar en el análisis de riesgos. La metodología utilizada en este estudio fue tanto cuantitativa como cualitativa, obteniendo datos primarios a través de lluvia de ideas con los tomadores de decisiones y formularios respondidos por expertos. Los datos secundarios se obtuvieron a través del Framework for Improving Critical Infrastructure Cybersecurity, creado por NIST - el Instituto Nacional de Estándares y Tecnología de los Estados Unidos. El problema se estructuró según el método constructivista, y los datos recogidos fueron procesados y calculados. El estudio concluyó que la categoría de controles de Monitoreo Continuo de Seguridad se destacó en comparación con otras categorías. También muestra la importancia de aplicar el método constructivista para la gestión de riesgos cibernéticos al desentrañar un problema y proporcionar una base para la toma de decisiones. Nuestro trabajo contribuye a una mejor comprensión de la gestión de riesgos, fomentando la adopción del método constructivista como una forma de mejores prácticas de gestión de riesgos.
Aspectos Por Destacar	Digital Object Identifier 10.1109/ACCESS.2021.3113178

Tabla 1-5 Extracción articulo 1, fuente IEEE
Fuente: Elaboración propia.

Fuente	**IEEE**
Titulo	A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method
Autores	Angelito Gabriel;Juan Shi;Cagil Ozansoy
Referencia	[1] BBC News. (May 15, 2017). WannaCry Ransomware Cyber-Attacks Slow But Fears Remain, accessed on May 18, 2017. [Online]. Available: http://www.bbc.com/news/technology-39920141#_=_ [2] (Jun. 2014). Oil and Gas Cyber Security Conference. Oslo, Norway. accessed on Jul. 6, 2017. [Online]. Available: http://www.Smi online.co.uk/energy/europe/conference/Oil-and-Gas-Cyber- Security Nordics?utm_source=E-046&utm_medium=oilandgas cybersecurity7.asp&utm_campaign=GOTO&o=login&dl=br&p1=451 5# tab_overview [3] L. Pièтre-Cambacèdés and M. Bouissou, ‘‘Cross-fertilization between safety and security engineering,’’ Rel. Eng. Syst. Safety, vol. 110, pp. 110– 126, Feb. 2013.
Área	NIST Cybersecurity Framework

Resumen	La operación segura y protegida de la infraestructura crítica depende de las respuestas apropiadas a las prioridades operativas y de seguridad en los sistemas integrados de control y seguridad (ICSS), en la etapa de diseño y durante toda la vida útil del sistema. La digitalización, así como las infraestructuras de automatización y control en red, han aumentado en los últimos años y están dando lugar a notables riesgos de seguridad potenciales. Las noticias recientes sobre incidentes de seguridad graves, como el ransomware WannaCry, que afectan a todo el mundo, se escuchan con más frecuencia. El objetivo de este documento es generar un marco de evaluación integrado y optimizado para el ICSS y los

	subsistemas relacionados que tengan en cuenta la seguridad y la ciberseguridad. Esto se puede lograr mediante la alineación del marco de ciberseguridad formulado por el Instituto Nacional de Estándares y Tecnología con los estándares de seguridad y protección ISA84 (IEC 61511) e ISA99 (IEC 62443), y el novedoso método de gráfico de riesgo de embudo. La comunidad de investigación, la industria y la Sociedad Internacional de Automatización (ISA) han reconocido la necesidad de tal alineación entre seguridad y protección.
Aspectos Por Destacar	Digital Object Identifier 10.1109/ACCESS.2017.2718568

Tabla 1-6 Extracción articulo 2, fuente IEEE

Fuente: Elaboración propia.

Fuente	IEEE
Titulo	Cyberthreats and Security
Autores	Morris Chang;Rick Kuhn;Tim Weil
Referencia	[1] BBC News. (May 15, 2017). WannaCry Ransomware Cyber-Attacks Slow But Fears Remain, accessed on May 18, 2017. [Online]. Available: http://www.bbc.com/news/technology-39920141#_=_ [2] (Jun. 2014). Oil and Gas Cyber Security Conference. Oslo, Norway. accessed on Jul. 6, 2017. [Online]. Available: http://www.Smi online.co.uk/energy/europe/conference/Oil-and-Gas-Cyber- Security Nordics?utm_source=E-046&utm_medium=oilandgas cybersecurity7.asp&utm_campaign=GOTO&o=login&dl=br&p1=451 5# tab_overview

	[3] L. Pièтre-Cambacèdés and M. Bouissou, ‘‘Cross-fertilization between safety and security engineering,’’ Rel. Eng. Syst. Safety, vol. 110, pp. 110– 126, Feb. 2013.
Área	NIST Cybersecurity Framework

Resumen	La operación segura y protegida de la infraestructura crítica depende de las respuestas apropiadas a las prioridades operativas y de seguridad en los sistemas integrados de control y seguridad (ICSS), en la etapa de diseño y durante toda la vida útil del sistema. La digitalización, así como las infraestructuras de automatización y control en red, han aumentado en los últimos años y están dando lugar a notables riesgos de seguridad potenciales. Las noticias recientes sobre incidentes de seguridad graves, como el ransomware WannaCry, que afectan a todo el mundo, se escuchan con más frecuencia. El objetivo de este documento es generar un marco de evaluación integrado y optimizado para el ICSS y los subsistemas relacionados que tengan en cuenta la seguridad y la ciberseguridad. Esto se puede lograr mediante la alineación del marco de ciberseguridad formulado por el Instituto Nacional de Estándares y Tecnología con los estándares de seguridad y protección ISA84 (IEC 61511) e ISA99 (IEC 62443), y el novedoso método de gráfico de riesgo de embudo. La comunidad de investigación, la industria y la Sociedad Internacional de Automatización (ISA) han reconocido la necesidad de tal alineación entre seguridad y protección.
Aspectos Por Destacar	Digital Object Identifier 10.1109/ACCESS.2017.2718568

Tabla 1-7 Extracción articulo 3, fuente IEEE

Fuente: Elaboración propia.

1.9.2.2 Ejecución de la selección en la fuente ProQuest

1.9.2.2.1 Selección de estudios iniciales

Para la selección de estudio con la fuente ProQuest se realiza la búsqueda de la siguiente manera:

Búsqueda basada en los siguientes parámetros:

• NIST

• Cybersecurity

• Framework

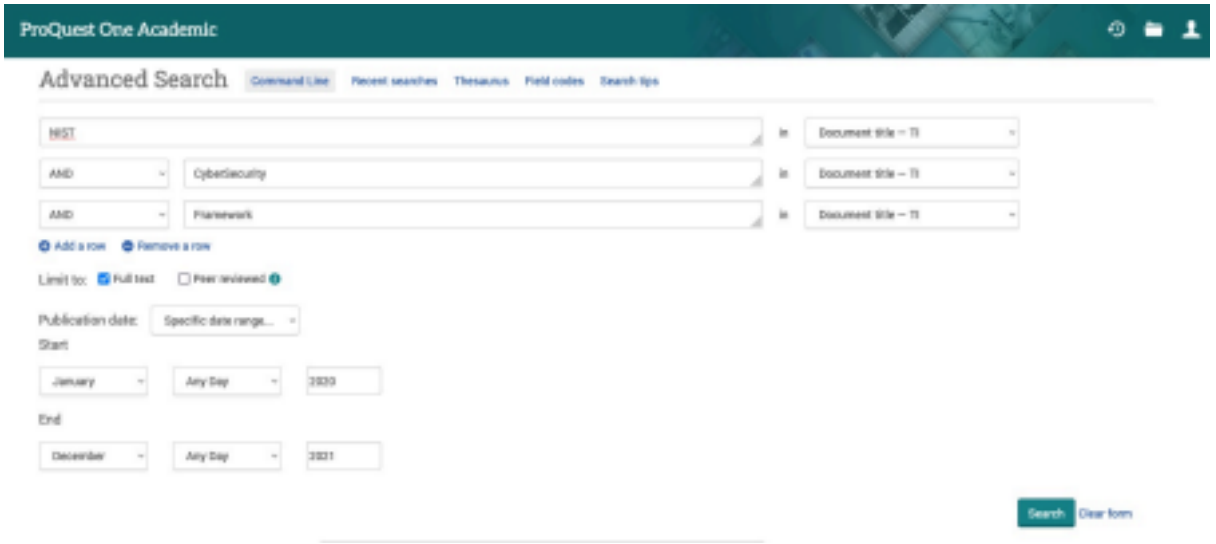

Figura 1-2 Ejecución de la selección ProQuest

Una vez realizada la búsqueda utilizando los parámetros mencionados se encontraron veintiún resultados, los cuales fueron seleccionados solamente tres tras aplicar el método de exclusión propuesto (principalmente aquellos artículos que tenga acceso libre). A continuación, se presenta el detalle de los artículos seleccionados:

#	Titulo	Autores	Año	URL
1	Methodology based on the NIST Cybersecurity Framework as a proposal for cybersecurity management in government organizations	Delgado, Maurice Frayssinet; Esenarro, Doris; Regalado, Francisco Fernando Juárez; Reátegui, Mónica Díaz.	2021	https://www.proquest.com/pq1 academic/docview/270001200 8/fulltextPDF/A2C6CB8EDB2A 47E9PQ/5?accountid=32236
2	Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework	ALDhanhani, Mohamed Jumah; Jizat, Jessnor Elmy Mat.	2021	https://www.proquest.com/pq1 academic/docview/262391827 5/CAB63F2BC20140F4PQ/8? accountid=32236
3	The Need for a Financial Sector Legal Standard to Support the Nist Framework for Improving Critical Infrastructure Cybersecurity	Goodwin, Susan.	2020	https://www.proquest.com/pq1 academic/pagepdf/247972927 4/Record/86CE8002029646C9 PQ/13?accountid=32236

Tabla 1-8 Estudios encontrados ProQuest

1.9.2.2.2 Evaluación de la calidad de los estudios

Se presume la calidad de los artículos mencionados, con base en la cantidad de filtros y evaluaciones realizadas por ProQuest.

1.9.2.2.3 Revisión de la selección

La selección de estudios primarios se realiza tras llevar a cabo una revisión de los resúmenes y contenido incluido en cada artículo. Para la revisión de estos artículos, los mismos fueron ordenados con base en la relevancia de los artículos.

1.9.2.2.4 Extracción de la información

Para la extracción de la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación, se consideran los siguientes elementos:

- Evaluación de Riesgos de ciberseguridad.
- Aplicación del marco para la mejora de infraestructura critica. •

Análisis de Resultados.

Fuente	**ProQuest**
Titulo	Methodology based on the NIST Cybersecurity Framework as a proposal for cybersecurity management in government organizations
Autores	Delgado, Maurice Frayssinet; Esenarro, Doris; Regalado, Francisco Fernando Juárez; Reátegui, Mónica Díaz.

Referencia	Almagro, L. (2019). NIST Cybersecurity Framework (CSF) / A comprehensive approach to cybersecu- rity. White paper series, Issue 5. http://www.itsd.gov.vc/itsd/images/pdf_documents/OAS_AWS_ NIST_Cybersecurity_Framework_CSF_ENG.pdf Alvarez, D. (2018). Cybersecurity in Latin America and cyber defense in Chile. Chilean journal of law and technology, 7(1). https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416 Ayala, C., & Lopez, E. (2019). Design and implementation of ISO 27035 (information security incident ma- nagement) for the service platform area of a Peruvian state entity. http://repositorio.utp.edu.pe/handle/ UTP/2477
Área	NIST Cybersecurity Framework
Resumen	Esta investigación tiene como objetivo proponer el uso de la metodología basada en el Marco del NIST para una gestión adecuada de la ciberseguridad en las organizaciones gubernamentales en el marco de la prestación de servicios digitales. Muchas organizaciones gubernamentales han estado gestionando

	la ciberseguridad sin un proceso definido; esto genera que la gestión sea deficiente y sin indicadores. En cuanto a si están implementando la metodología basada en el marco de ciberseguridad del NIST», muestra que el 36,8% de los encuestados presenta un nivel de desacuerdo, el 31,6% (6) un nivel de indeciso, el 15,8% (3) un nivel de acuerdo, el 10,5% (2) un nivel totalmente en desacuerdo y el 5,3% (1) un nivel totalmente de acuerdo. Mientras tanto, la variable «La gestión de la ciberseguridad» muestra que el 36,8% (7) de los ministerios encuestados presentan un nivel de desacuerdo; el 36,8% (7) un nivel indeciso, el 15,8% (3) un nivel de acuerdo y el 10,5% (2) un nivel totalmente en desacuerdo. En conclusión: se ha demostrado que el uso de la metodología basado en el marco de ciberseguridad del NIST influye en la gestión de la ciberseguridad en las organizaciones gubernamentales y está claro que actualmente no lo utilizan, lo que provoca un nivel relativamente bajo de liderazgo en la implementación de medidas de seguridad relacionadas con la gestión de la ciberseguridad.
Aspectos Por Destacar	ISSN: 2254 – 6529

Tabla 1-9 Extracción articulo 1, fuente ProQuest
Fuente: Elaboración propia.

Fuente	**ProQuest**
Titulo	Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework
Autores	ALDhanhani, Mohamed Jumah; Jizat, Jessnor Elmy Mat.

Referencia	[1] Abdullahi, S. (2020). Measuring Co-Movements and Linkages between Nigeria and the UAE Stock Exchanges: Is there Opportunity for Portfolio Building.

41

	[2] Al Neaimi, A., Ranginya, T., &Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). International Journal of Cyber Security and Digital Forensics (IJCSDF), 4(1), 290-301. [3] Al Restar. (2019). Half Of The Cyber Attacks In The Middle East Targeted Oil And Gas Companies. Z6 Mag. Retrieved Dec 03, 2019, from https://z6mag.com/2019/06/18/middle-east hackers-targets-oil-companies/
Área	Revisión de la seguridad cibernética en la industria del petróleo y el gas.

Resumen	En vista del aumento de los ciberataques, la adopción de un marco de seguridad eficaz es esencial para cualquier organización que participe en sectores críticos, como el sector del petróleo y el gas, para garantizar el más alto nivel de seguridad y cumplimiento. En este sentido, como uno de los principales productores y exportadores de petróleo, los Emiratos Árabes Unidos (EAU) necesitan emplear un marco de seguridad eficaz para proteger las infraestructuras críticas de su sector de petróleo y gas. Como tal, este estudio se lleva a cabo para examinar los posibles daños de los ciberataques centrándose en los elementos del marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología. La metodología de investigación utilizada en esta investigación se basa en una revisión sistemática de la literatura actual sobre ciberseguridad y marcos. La revisión revela que el marco de ciberseguridad del NIST tiene ciertas características que aparentemente lo hacen más efectivo que otros. Básicamente, este marco tiene tres componentes principales, a saber, el núcleo del marco, los niveles de implementación y el perfil, que se definen en función del negocio de la organización. Específicamente, el núcleo del marco tiene

	cinco funciones, a saber, identificar, proteger, detectar, responder y recuperar. Los hallazgos de esta investigación pueden ayudar a guiar a los responsables políticos de la industria del petróleo y el gas de los Emiratos Árabes Unidos a tomar decisiones informadas sobre la mejor manera de mitigar las ciberamenazas contra las compañías petroleras. En particular, los hallazgos pueden ayudar a los responsables políticos a determinar si el marco de ciberseguridad del NIST puede desempeñar un papel esencial en el fortalecimiento de la ciberseguridad en el sector del petróleo y el gas de los Emiratos Árabes Unidos. Además, los hallazgos pueden ayudar a los profesionales a recomendar medidas prácticas adecuadas para reforzar la preparación y las respuestas de las compañías de petróleo y gas de los Emiratos Árabes Unidos ante los ciberataques.
Aspectos Por Destacar	Artículo de Investigación. Recibido: 11 de enero de 2021; Revisado: 12 de febrero de 2021; Aceptado: 27 de marzo de 2021; Publicado en línea: 10 de mayo de 2021

Tabla 1-10 Extracción articulo 2, fuente ProQuest
Fuente: Elaboración propia.

Fuente	**ProQuest**
Titulo	The Need for a Financial Sector Legal Standard to Support the Nist Framework for Improving Critical Infrastructure Cybersecurity
Autores	Goodwin, Susan.
Referencia	[1] Bank of America (2020a). Governance. Retrieved on January 25, 2020 from https://about.bankofamerica.com/en-us/what-guides-us/governance.html

	[2] Bank of America (2020b). Bank of America 4Q19 Financial Results. Retrieved on January 25, 2020, from http://investor.bankofamerica.com/static-files/8eec43d6-4cee-48a3-bcfe e5a47b00e200 [3] Bitglass (2019). The financial matrix: Bitglass' 2019 financial breach report. Retrieved from https://pages.bitglass.com/CD FY19Q4TheFinancialMatrixBitglass2019FinancialBreachReport_LP.html
Área	NIST Framework

Resumen	El Instituto Nacional de Estándares y Tecnología (NIST) publicó el Marco NIST para mejorar la ciberseguridad de la infraestructura crítica de 2014, seguido de una versión actualizada en 2017. El Marco, que fue desarrollado como un esfuerzo conjunto entre el gobierno federal y el sector privado, sirve solo como una guía y no es obligatorio por ninguna autoridad legal. Actualmente, la adopción del Marco es voluntaria. El Sector Financiero, uno de los dieciséis sectores de infraestructura crítica del Departamento de Seguridad Nacional, debe recibir el mandato de adoptar el marco, basado en la inconsistencia y responsabilidad de la implementación de las mejores prácticas en todo el sector. Los oportunistas de ataques cibernéticos globales utilizaron la pandemia de COVID-19 de 2020 para explotar las vulnerabilidades y brechas de seguridad cibernética en el sector financiero de EE. UU. El marco de seguridad cibernética del NIST proporciona pautas para fortalecer la seguridad cibernética e identifica las áreas de impacto potencial de los ataques cibernéticos. Este estudio incluye la investigación y el análisis de los riesgos, fallas e impactos informados del sector financiero debido a la debilidad o falta de controles de seguridad cibernética. El estudio también proporciona un análisis de las historias de éxito del sector financiero y otras entidades que han adoptado

	el marco de seguridad cibernética del NIST, como los ejemplos publicados en el informe de National Law Review "GAO Reports Challenges and Successes in Cybersecurity Framework Adoption" (Fleming, Richmond, Farber, Singh y Nuzum, 2018).

Aspectos Por Destacar	

Tabla 1-11 Extracción articulo 3, fuente ProQuest
Fuente: Elaboración propia.

1.9.2.3 Ejecución de la selección en la fuente EBSCO Host

1.9.2.3.1 Selección de estudios iniciales

Para la selección de estudio con la fuente EBSCO Host se realiza la búsqueda de la siguiente manera:

Búsqueda basada en los siguientes parámetros:

• NIST

• Cybersecurity

• Framework

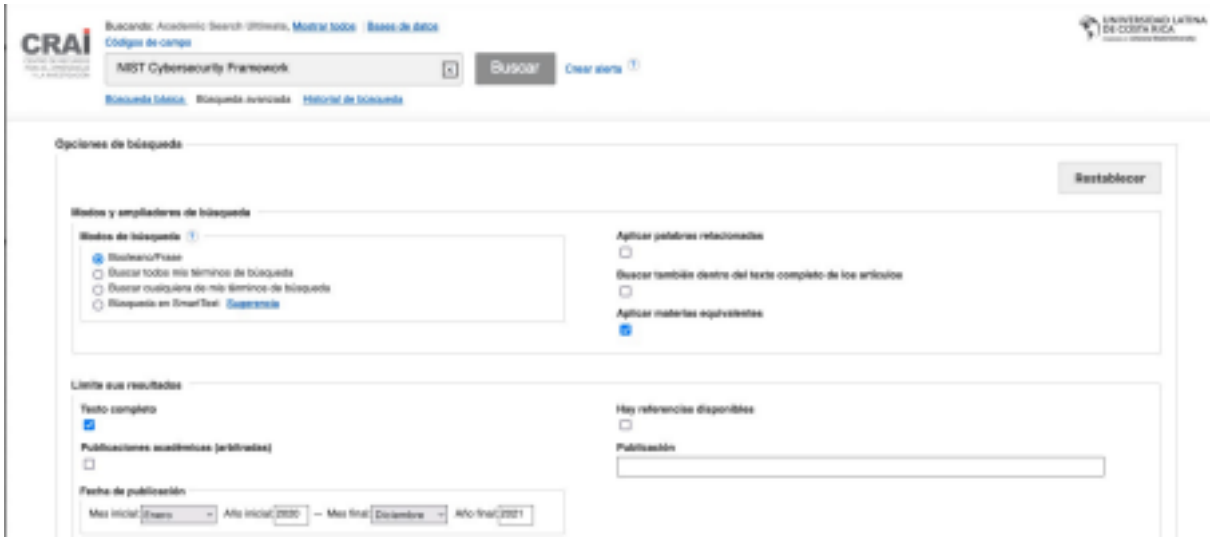

Figura 1-3 Ejecución de la selección EBSCO Host

Una vez realizada la búsqueda utilizando los parámetros mencionados se encontraron diez resultados, los cuales fueron seleccionados solamente tres tras

aplicar el método de exclusión propuesto (principalmente aquellos artículos que tenga acceso libre). A continuación se presenta el detalle de los artículos seleccionados:

#	Titulo	Autores	Año	URL
1	Methodology based on the NIST Cybersecurity Framework as a proposal for cybersecurity management in government organizations	Frayssinet Delgado, Maurice Esenarro, Doris Juárez Regalado, Francisco Fernando Díaz Reátegui, Mónica	2021	https://web.s.ebscohost.com/ehost/detail/detail?vid=0&sid=c91f81ae-807e-4b96-9734-28eccc29c86c%40redis&bdata=JkF1dGhUeXBlPXNzbyZsY W5nPWVzJnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=1516 03467&db=iih
2	Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model.	Gordon, Lawrence; Loeb, Martin; Zhou, Lei1	2020	https://web.s.ebscohost.com/ehost/detail/detail?vid=25&sid=6787a6c5-ab62-4aeb-a8d4-4da1ce7210cb%40redis&bdata=JkF1dGhUeXBlPXNzbyZsY W5nPWVzJnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aps&A N=151369196

Tabla 1-12 Estudios encontrados EBSCO Host

1.9.2.3.2 Evaluación de la calidad de los estudios

Se presume la calidad de los artículos mencionados, con base en la cantidad de filtros y evaluaciones realizadas por EBSCO Host.

1.9.2.3.3 Revisión de la selección

La selección de estudios primarios se realiza tras llevar a cabo una revisión de los resúmenes y contenido incluido en cada artículo. Para la revisión de estos artículos, los mismos fueron ordenados con base en la relevancia de los artículos.

1.9.2.3.4 Extracción de la información

Para la extracción de la información relevante de los estudios primarios y el cumplimiento de los objetivos de la investigación, se consideran los siguientes elementos:

• Evaluación de Riesgos de ciberseguridad.

• Aplicación del marco para la mejora de infraestructura critica. •

Análisis de Resultados.

Fuente	**EBSCO Host**
Titulo	Methodology based on the NIST Cybersecurity Framework as a proposal for cybersecurity management in government organizations
Autores	Frayssinet Delgado, Maurice Esenarro, Doris Juárez Regalado, Francisco Fernando Díaz Reátegui, Mónica
Referencia	[1] Almagro, L. (2019). NIST Cybersecurity Framework (CSF) / A comprehensive approach to cybersecu- rity. White paper series, Issue 5. http://www.itsd.gov.vc/itsd/images/pdf_documents/OAS_AWS_ NIST_Cybersecurity_Framework_CSF_ENG.pdf [2] Alvarez, D. (2018). Cybersecurity in Latin America and cyber defense in Chile. Chilean journal of law and technology, 7(1). https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416 [3] Ayala, C., & Lopez, E. (2019). Design and implementation of ISO 27035 (information security incident ma- nagement) for the service platform area of a Peruvian state entity. http://repositorio.utp.edu.pe/handle/ UTP/2477

Área	National Institute of Standards & Technology (U.S.)
Resumen	Esta investigación tiene como objetivo proponer el uso de la metodología basada en el Framework NIST para una adecuada gestión de la ciberseguridad en las organizaciones gubernamentales en el marco de la entrega de servicios digitales. Muchas organizaciones gubernamentales han estado

	gestionando la ciberseguridad sin un proceso definido; esto genera que la gestión sea deficiente y sin indicadores. En cuanto a si están implementando la metodología basada en el marco de ciberseguridad del NIST", muestra que el 36,8% de los encuestados presenta un nivel en desacuerdo, el 31,6% (6) un nivel indeciso, el 15,8% (3) un nivel de acuerdo, el 10,5% (2)) un nivel totalmente en desacuerdo y el 5,3% (1) un nivel totalmente de acuerdo. Por su parte, la variable "La gestión de la ciberseguridad" muestra que el 36,8% (7) de los Ministerios encuestados presentan un nivel en desacuerdo, el 36,8% (7) un nivel indeciso, 15.8% (3) un nivel de acuerdo, y 10.5% (2) un nivel totalmente en desacuerdo En conclusión: Se ha demostrado que el uso de la metodología basada en el marco de ciberseguridad del NIST influye en la gestión de la ciberseguridad en las organizaciones gubernamentales y es claro que actualmente no lo están utilizando lo que provoca un nivel de liderazgo relativamente bajo en la implementación de medidas de seguridad en materia de gestión de la ciberseguridad.
Aspectos Por Destacar	ISSN: 2254-6529

Tabla 1-13 Extracción articulo 1, fuente EBSCO Host
Fuente: Elaboración propia.

Fuente	**EBSCO Host**
Titulo	Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model.
Autores	Gordon, Lawrence; Loeb, Martin; Zhou, Lei1

Referencia	1. Agrarafiotis I, Nurse J, Goldsmith M et al. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propa- gate. J Cybersecur 2018;4:1–15. 2. Campbell K, Gordon LA, Loeb MP et al. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 2003;11:431– 48. 3. Gordon LA, Loeb MP, Zhou L. The impact of information security breaches: has there been a downward shift in costs? J Comput Secur 2011; 19:33–56.
Área	Marco NIST

Resumen	El marco de seguridad cibernética del Instituto Nacional de Estándares y Tecnología (NIST) se ha convertido rápidamente en un enfoque ampliamente aceptado para facilitar la gestión de riesgos de seguridad cibernética dentro de las organizaciones. Un aspecto revelador del marco de seguridad cibernética del NIST es su reconocimiento explícito de que las actividades asociadas con la gestión del riesgo de seguridad cibernética son específicas de la organización. El Marco NIST también reconoce que las organizaciones deben evaluar su gestión de riesgos de seguridad cibernética sobre una base de costo-beneficio. El Marco NIST, sin embargo, no brinda orientación sobre cómo llevar a cabo dicho análisis de costo-beneficio. Este artículo proporciona un enfoque para integrar el análisis de costo beneficio en el marco de ciberseguridad del NIST. El modelo Gordon-Loeb (GL) para inversiones en seguridad cibernética se propone como base para obtener un nivel rentable de gasto en actividades de seguridad cibernética y para seleccionar el nivel de implementación NIST adecuado. El análisis muestra que el modelo GL proporciona un enfoque lógico para usar al

	considerar los aspectos de costo-beneficio de las inversiones en seguridad cibernética durante el proceso de una organización de seleccionar el nivel de implementación NIST más apropiado. Además, el enfoque de costo-beneficio proporcionado en este artículo ayuda a identificar las condiciones bajo las cuales existe un incentivo para pasar a un nivel de implementación NIST más alto.
Aspectos Por Destacar	Recibido el 10 de septiembre de 2019; revisado el 14 de diciembre de 2019; aceptado el 23 de enero de 2020

Tabla 1-14 Extracción articulo 2, fuente EBSCO Host
Fuente: Elaboración propia.

2 Capítulo II. Marco Conceptual

2.1 Conceptos técnicos

Sistema de Gestión de resiliencia y de ciberseguridad: Comprende la capacidad de las organizaciones de recuperarse tras haber sido víctimas de un ataque por parte de ciberdelincuentes.

Marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1: La Organización de los Estados Americanos (OEA) en su documento “Ciberseguridad Marco NIST, Un abordaje integral de la

ciberseguridad” define el Marco de **Ciberseguridad** o Cybersecurity Framework del Instituto Nacional de Estándares y Tecnología, **NIST** por sus siglas en inglés, como una herramienta para la gestión de riesgos asociados a la seguridad de la información y si bien es un marco de adopción voluntaria, ofrece muchas ventajas. Es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información. El Cybersecurity Framework (CSF) consta de tres componentes principales: • Framework Core

- Niveles de implementación (Tiers)
- Perfiles

Y en el mismo documento define estos componentes como:

Framework Core: Conjunto de actividades y resultados de ciberseguridad deseados, organizados en categorías y alineados con Referencias Informativas a estándares aceptados por la industria. Está diseñado para ser intuitivo y actuar como una capa de traducción para permitir la comunicación entre equipos multidisciplinarios mediante el uso de lenguaje simplista y no técnico. El Core consta

de tres partes: Funciones, Categorías y Subcategorías. Incluye cinco funciones de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar. **Niveles de implementación del CSF:** Describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el Marco. Los niveles van desde Parcial (Nivel 1) a Adaptativo (Nivel 4) y describen un grado cada vez mayor de rigor, y qué tan bien integradas están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, y el grado en que la organización comparte y recibe información de ciberseguridad de

fuentes externas.

Perfiles: Los perfiles son la alineación única de una organización de sus requisitos y objetivos organizacionales, la tolerancia al riesgo y los recursos con respecto a los resultados deseados del Framework Core. Los perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de ciberseguridad comparando un perfil “actual” con un perfil “objetivo”.

2.2 Conceptos generales

El marco conceptual está compuesto de referencias a sucesos y situaciones pertinentes, a resultados de investigación, incluyendo, un marco de antecedentes, definiciones, supuestos, relacionados con resiliencia, ciberseguridad y las NIST. Se creó la siguiente nube de conceptos con el objetivo de identificar los más relevantes, mencionados en los diversos artículos incluidos como parte del estado de la cuestión.

Figura 2-1 Nube de palabras.

Fuente: Elaboración Propia, utilizando el sitio https://www.nubedepalabras.es

Considerando las diferentes terminologías resultantes de esta guía metodológica, que pueden ser complejas, se realiza el siguiente mapa conceptual que contempla las 5 funciones del Cybersecurity Framework (CFS) como una guía para cubrir todos los conceptos relacionados y de conformidad con el mapa, se proceden a desarrollar cada uno de los conceptos.

Figura 2-2 Mapa Conceptual.
Fuente: Elaboración Propia.

Para desarrollar cada concepto que se presenta a continuación, se han consultado diversas fuentes a fin de dar una definición con mayor comprensión y de fácil análisis brindando un panorama al profesional que desarrollará los temas. Por lo que se aclara que, dichos conceptos son producto de diversas fuentes y de la redacción de los autores del presente proyecto, no siendo completa la autoría.

2.2.1 Identificación

Esta es la primera etapa del Marco para la mejora de la ciberseguridad y consiste en desarrollar una comprensión organizacional para administrar el riesgo de ciber seguridad tanto para los sistemas, como las personas, activos, datos y capacidades.

2.2.1.1 Entorno Empresarial

El entorno empresarial engloba todas las variables que pueden afectar directa o indirectamente a la organización.

Este entorno además se caracteriza por ser cambiante en el tiempo y muchas veces difícil de predecir. Puede ser, por ejemplo, que, ante la entrada en gestión de un nuevo gobierno, el marco legal sobre el cual trabaja la empresa varíe. **2.2.1.2 Gobernanza**

El término gobernanza se usa desde la década de los 90 para designar la eficacia, calidad y buena orientación de la intervención del Estado, que proporciona buena parte de su legitimidad en lo que a veces se define como una "nueva forma de gobernar" en la globalización del mundo posterior a la caída del muro de Berlín (1989).

Con respecto al marco de para la mejora de la ciber seguridad, la gobernanza, se refiere a como la compañía va a intervenir de forma eficaz, con calidad y buena orientación la gestión de los riesgos.

2.2.1.3 Gestión de Riesgos

Proceso mediante el cual se identifican, analizan, clasifican las probabilidades de que suceda un evento y la forma de enfrentarlos de forma efectiva.

2.2.1.4 Gestión de activos

El término gestión de riesgos hace referencia al proceso que se utiliza para identificarlos y evaluarlos, y a la creación de un plan para disminuir o controlar no solo dichos riesgos, sino también el efecto que podrían tener en la empresa. Un riesgo implica una posible pérdida o daño. Los riesgos pueden originarse por distintas causas, como la responsabilidad legal, los desastres naturales, los accidentes, los errores de gestión o las amenazas de ciberseguridad. **2.2.1.5 Riesgos Organizacionales**

Cada organización sufre de diferentes y múltiples problemas de riesgo independientemente del sector, campo y tamaño de la organización. La toma de decisiones sobre cómo proceder con la sospecha de un caso de riesgo para la organización, generalmente está estrictamente relacionada con la consideración del costo del riesgo, de modo que, al no identificar el núcleo del riesgo, el resultado tiende y puede convertirse en una escalada mayor del riesgo, que puede causar daños graves o dimensiones devastadoras para una organización.

2.2.1.6 Riesgos en la Cadena de Suministros

Los grandes avances en las comunicaciones y la capacidad en procesamiento de datos han permitido el incremento exponencial en la complejidad

de las cadenas de suministro, así como en el aumento de los Riesgos en la Cadena de Suministro. Los beneficios potenciales de esta complejidad son incuestionables, sin embargo, el incremento en interdependencias multiplica y fragmentan los puntos de riesgo y dificultan enormemente la ubicación y evaluación de estos. Las operaciones de la cadena de suministro se vuelven particularmente vulnerables ante

eventos ocasionados por Riesgos en la Cadena de Suministro y son de difícil predicción.

2.2.2 Protección

La protección es la segunda etapa del Marco para la mejora de la ciberseguridad, y pretende ofrecer herramientas que faciliten el proceso de protección de los datos.

2.2.2.1 Capacitación

Proporcionar al trabajador las habilidades y conocimientos que lo hagan más apto y diestro en la ejecución de los planes de respuesta a incidentes de ciberseguridad, con el fin de que, sin importar su rol, cada uno sepa con claridad como actuar en caso de una emergencia.

2.2.2.2 Procesos y procedimientos

Un proceso es una secuencia de tareas que se llevan a cabo una detrás de la otra. Todas las organizaciones trabajan bajo procesos por lo tanto los procesos en las empresas representan el eje principal sobre el que giran todas las actividades que se llevan a cabo en un negocio.

Un procedimiento es una descripción detallada de cómo se debe llevar a cabo un proceso. Este procedimiento podrá estar documentado (escrito en papel o

formato digital) o no estar escrito en ningún sitio, pero conocerse por parte de todos los integrantes de una empresa.

Siempre que existe un proceso en una empresa existe un procedimiento, podrá estar documentado o no pero siempre existirá una descripción detallada de cómo se lleva a cabo una actividad en una organización.

Así mismo siempre que existe un procedimiento en una empresa es porque existe un proceso detrás.

2.2.2.3 Control de Accesos

Un sistema de control de accesos se puede entender desde una vertiente física. En este sentido, se podría definir como aquel mecanismo o dispositivo que autoriza la entrada de personas o vehículos a determinadas instalaciones.

Por ejemplo, se puede instalar un control de acceso en puertas para permitir el paso a determinadas áreas de instalaciones como almacenes, oficinas o departamentos a determinados empleados de una organización.

Por otro lado, el control de acceso también se puede entender desde el punto de vista de la ciber seguridad. En este caso, se define como aquellas herramientas o aplicaciones cuyo objetivo es gestionar quién está autorizado para acceder a determinados sistemas informáticos y a los recursos que contienen. **2.2.2.4 Seguridad de Datos**

Se define como seguridad de datos la práctica de proteger la información digital de acceso no autorizado, corrupción o robo en todo su ciclo de vida. Es un concepto que abarca todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las

aplicaciones de software. También incluye políticas y procedimientos organizacionales.

Cuando se implementan correctamente, las estrategias sólidas de seguridad de datos protegerán los activos de información de una organización contra las actividades de los ciberdelincuentes, pero también protegen contra las amenazas internas y los errores humanos, que sigue siendo una de las principales causas de brechas de seguridad de datos en la actualidad. La seguridad de los datos implica la implementación de herramientas y tecnologías que mejoran la visibilidad de la

organización sobre dónde residen sus datos críticos y cómo se utilizan. Idealmente, estas herramientas deberían poder aplicar protecciones como el cifrado, el enmascaramiento de datos y la redacción de archivos confidenciales, y deberían automatizar los informes para agilizar las auditorías y cumplir con los requisitos regulatorios.

2.2.2.5 Tecnología de Protección

Se refiere a diferentes mecanismos, tanto de software como de hardware que se ponen en práctica para proteger la información de la compañía. Una compañía que quiera construir defensas confiables y fuertes necesita varias capas de seguridad y no puede depender de una sola tecnología de protección.

2.2.2.6 Mantenimiento

El mantenimiento y las reparaciones de los componentes del sistema de información y control industrial se realizan de acuerdo con las políticas y los procedimientos.

Se realizan y registran el mantenimiento y reparación de los activos de la organización, con herramientas aprobadas y controladas.

El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de una manera que evita el acceso no autorizado.

2.2.3 Detección

Acción y resultado de detectar, descubrir o darse cuenta de una cosa o un evento.

2.2.3.1 Detección de Intrusos

Un sistema de detección de intrusos tiene como objetivo evitar conexiones indeseadas. Básicamente se encargan de bloquear la entrada de intrusos en una

red o equipo, alertando en cuanto detectan que hay algo extraño y que debemos tener cuidado.

Son herramientas que tienen como misión monitorear el tráfico de red y de esta forma detectar amenazas. Está constantemente escaneando las conexiones que entran y salen de un equipo o de una red, para detectar cualquier anomalía.

2.2.3.2 Monitoreo

El monitoreo, es la acción de vigilar de cerca las acciones o actividades de alguien o algo.

En el caso de la ciberseguridad, esta vigilancia se debe hacer constante e ininterrumpida tanto a dispositivos de dentro de la red, así como, también al tráfico que se transporta en ella.

2.2.3.3 Detección de Intrusiones

La detección de intrusiones se refiera al proceso de detectar accesos no autorizados a una computadora, dispositivo IoT (internet of things) o a una red. Existen sistemas de software especializado para este fin los cuales se basan en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es

comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El sistema de detección de intrusos no solo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

2.2.4 Respuesta

Una brecha de seguridad puede paralizar la funcionalidad operativa, causar fugas de datos, dañar la reputación de una empresa y causar complicaciones regulatorias. Y para las amenazas que superan las defensas, las organizaciones necesitan las

herramientas y los conocimientos para responder de forma rápida y eficaz. Desafortunadamente, la mayoría de las organizaciones se basan en procesos antiguos para investigar incluso los incidentes cibernéticos más sencillos, como los ataques de phishing a los empleados. Solo el 26 % de las organizaciones tienen un plan de respuesta a incidentes en toda la empresa. Los planes de respuesta a incidentes y la automatización de la seguridad distinguen a los de alto rendimiento y debido a la brecha de habilidades, las organizaciones con las herramientas y la tecnología adecuadas podrían tener dificultades para encontrar suficientes recursos para gestionar la avalancha de incidentes de manera eficiente.

2.2.4.1 Proceso de Respuesta

La respuesta a incidentes es un enfoque sistemático para ayudar a los equipos de TI a prepararse y planificar incidentes de TI, incluida una interrupción del servicio, una violación de la seguridad de una organización o un ataque cibernético.

Ninguna organización es completamente inmune a los incidentes de TI, particularmente los incidentes de seguridad dada la situación actual de trabajo remoto adoptada por las empresas. Cuando ocurren incidentes de seguridad, lo hacen con fuerza, provocando la destrucción de datos, violando la confidencialidad e induciendo pérdidas significativas en términos de productividad y finanzas, lo que implica un gran esfuerzo para recuperarse. Sin embargo, con un plan de respuesta a incidentes constructivo, hace posible manejar estas situaciones de manera más efectiva y restaurar la normalidad más rápido.

2.2.4.2 Análisis de Incidentes

El hecho de reconstruir lo que ha sucedido en un sistema informático tras un incidente de seguridad es posible a partir de una innovadora ciencia que se conoce

como análisis forense, de la cual podemos extraer información valiosa para comprender el origen y la naturaleza del incidente.

2.2.4.3 Mitigación de Incidentes

Cuando se detecta un incidente grave de seguridad es necesario reaccionar con rapidez. Si no es posible contactar con la institución implicada en el incidente, se procederá a aplicar el procedimiento para tratar de solucionar el problema lo antes posible de tal manera que los efectos de este sean menores.

Para esto se debe planificar con antelación la forma en cómo se va a reaccionar ante un incidente de seguridad, y con esto lograr una mitigación más efectiva.

2.2.4.4 Comunicación de Incidentes

Los incidentes o emergencias son eventos que ocurren en una organización

que generalmente son de naturaleza crítica y requieren atención urgente para remediar el problema. Cada empresa tendrá su idea de lo que constituye un incidente importante, pero en general, pueden ser cosas como cortes de TI, cortes de energía, fallas de sistemas, inclemencias del tiempo y cualquier otra cosa que pueda dañar sus operaciones comerciales.

Comunicarse eficazmente con sus empleados durante un incidente es importante, puede ayudar a minimizar el impacto que tendrá.

2.2.4.5 Mejora al Proceso de Respuesta

Al igual que con cualquier otro plan puesto en práctica, es esencial trabajar siempre para mejorar a medida que transcurre el tiempo. El primer plan de respuesta a incidentes que se implementa probablemente no sea ni parecido al plan número 100 que se ponga en práctica luego. Con el tiempo, las se aprenden otras

formas de ser más eficiente y detectar más fácil los incidentes antes de que se transformen en problemas.

Si bien la práctica hace a la perfección, hay otras maneras en las se puede ampliar los conocimientos. Entre ellas se incluyen seguir capacitándose y dar seguimiento a las métricas de rendimiento. Asistir a talleres, escuchar expertos y leer artículos pueden ser todas fuentes de inspiración para aportar ideas nuevas al equipo. Además, el seguimiento de proyectos y el análisis de las métricas de rendimiento pueden ser muy útiles para que, con el equipo, aprendan de los errores.

2.2.5 Recuperación

La recuperación ante desastres es el método que utiliza una organización para recuperar el acceso y la funcionalidad de su infraestructura de TI tras un desastre

natural o humano, como una avería de los equipos o un ciberataque

2.2.5.1 Proceso de Recuperación

Un buen plan de recuperación ante desastres incluye documentación sobre los sistemas y datos esenciales para la continuidad del negocio, así como indicaciones sobre los pasos necesarios para recuperar los datos. El plan debe incorporar un objetivo de punto de recuperación (RPO) que establezca la frecuencia de las copias de seguridad y un objetivo de tiempo de recuperación (RTO) que defina el tiempo de inactividad máximo admisible tras un desastre. Estos parámetros crean límites para guiar la elección de la estrategia de TI, los procesos y los procedimientos que componen el plan de recuperación ante desastres de una organización. La estrategia de recuperación ante desastres debe reflejar el tiempo de inactividad que una organización puede soportar y la frecuencia con la que se realizan copias de seguridad de sus datos. Por último, es importante poner el plan a

prueba con regularidad para comprobar que funciona antes de que se produzca un desastre.

2.2.5.2 Comunicación de la Recuperación

Cuando las malas noticias llegan es esencial comunicar el mensaje correct y para esto se debe planificar de previo y saber quién, qué, dónde y por qué ocurrieron los hechos antes de realizar una comunicación oficial. Mejora al proceso de Recuperación.

Designar un portavoz, esta persona generalmente es el CEO o fundador de la empresa, pero si tiene otro ejecutivo en el equipo que pueda manejar preguntas difíciles, también puede ser una opción.

Una vez que haya designado a su portavoz, debe ser capacitado en el manejo medios. Los entrenadores de medios pueden simular situaciones de crisis relevantes para su marca e industria, y proporcionar orientación sobre la mensajería que su equipo puede elaborar de antemano para combatir diferentes escenarios de crisis.

2.2.5.3 Mejora del proceso de recuperación

La mejora del proceso de recuperación incorpora lecciones aprendidas de incidentes anteriores al propio proceso con el fin de garantizar una mejor respuesta. Estas lecciones se utilizan como insumo para desarrollar una estrategia con la cual se pueda actualizar el actual proceso de recuperación.

3 Capítulo III - Marco Metodológico

3.1 Tipo de Investigación

El presente proyecto utilizó una investigación aplicada que sirve para generar conocimientos que se puedan poner en práctica en el sector productivo, con el fin de impulsar un impacto positivo en la vida cotidiana, permitiendo establecer estrategias de mejora institucional, permitiendo a la empresa conocer su situación y establecer acciones de control en términos de resiliencia en ciberseguridad.

Asimismo, esta investigación tendrá un agente evaluador externo, el cual

aporta mayor objetividad y credibilidad.

3.2 Alcance Investigativo

Esta investigación tiene un alcance de tipo explicativo, el cual va más allá de las descripciones y busca establecer las causas de los eventos o fenómenos y pretende generar mayor entendimiento de estos.

3.3 Enfoque

El enfoque es cualitativo y sigue un método de inferencia de resultados llamado “ideográfico”, en el cual no se comprueban leyes universales. Se usa el método inductivo (de lo específico a lo general). Esto marca una diferencia muy grande en cuanto al nivel de generalización que se puede alcanzar, más parecido a las posibilidades que al alto umbral de certeza del enfoque cuantitativo. El paradigma base es el naturalismo.

3.4 Diseño

Dado que esta investigación tiene un enfoque cualitativo se concentra en dar sentido y valor a las categorías de análisis.

3.4.1 Categorías de Análisis

3.4.1.1 Identificación

Desarrollar una comprensión organizacional para administrar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades. **3.4.1.2 Protección:**

Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

3.4.1.3 Detección:

Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

3.4.1.4 Respuesta:

Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de ciberseguridad.

3.4.1.5 Recuperación:

Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad.

3.5 Población y Muestreo

En este proyecto se entiende como población la empresa costarricense UN PROVEEDOR DE INTERNET.

3.6 Instrumentos de Recolección de Datos

Los instrumentos de recolección de datos permiten conseguir datos “crudos”, que deberán ser analizados, para fines de conteos y mediciones, o bien para ser sujetos de un proceso de interpretación. En este caso, los instrumentos de evaluación utilizados fueron los siguientes:

Entrevista: Se realizó una entrevista por videollamada con el Sr. Gerente

General de UN PROVEEDOR DE INTERNET.

Aplicación de la plantilla de evaluación: el otro instrumento de recolección utilizado fue la plantilla realizada con base en el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

3.7 Técnicas de Análisis de Información

Las técnicas de análisis de información toman los datos recolectados y les dan un sentido útil para efectos de la investigación. Para el proyecto, se emplearon las siguientes técnicas:

- Mapas conceptuales
- Mapas mentales.

3.8 Fundamento teórico

El mercado de la ciberseguridad ha venido al alza después del despliegue global del acceso a Internet a mediados de la década de los 90, catapultando la aparición de marcos y estándares de todo tipo, direccionados estos a múltiples áreas del saber en el campo de la tecnología.

La sociedad ha sido testigo del surgimiento de una malla tecnológica alrededor de la ciberseguridad, que involucra la ciencia de datos (Big Data) y la

Inteligencia Artificial (ML especialmente) para procesar enormes pantanos de datos, que son ingeridos y procesados, y que terminan convertidos en lagos de datos correlacionados y en todo tipo de métodos de inteligencia de amenazas.

Incluso, en una aproximación al tiempo real este híper procesamiento nos

permite hoy en día desplegar labores de cacería de amenazas automatizadas en gran parte, diseccionando indicadores de ataque y eliminando los sesgos de los falsos positivos.

El aumento de la resiliencia y las capacidades ofensivas suelen ser tan complejas que suelen frustrar y/o agotar a las organizaciones antes de que logren alcanzar sus objetivos. La razón es simple; el recorrido demanda muchos recursos y mucho tiempo y no hay un camino bien señalado hacia su objetivo.

Por ello, en este proyecto se desarrolla una esta guía metodológica para evaluación, en la que se examina el contexto integral de las organizaciones, del mercado y de la industria, para extraer una visión panorámica, pragmática y holística que rotule y señale adecuadamente el sendero para que empresas y organizaciones logren alcanzar su destino, a decir; la ciber resiliencia.

Esta guía busca ser de utilidad tanto para la empresa UN PROVEEDOR DE INTERNET como para organizaciones de cualquier tamaño, en cualquier vertical del mercado y con agnosticismo respecto a la geolocalización de la empresa; para lo cual deberán definir su apetito respecto a la resiliencia que deseen alcanzar.

3.9 Marco NIST 1.1

Para la puesta en escena de esta “Evaluación del sistema de gestión de resiliencia de ciberseguridad”, se usará el Marco para la mejora de la seguridad del instituto nacional de estándares y tecnología NIST 1.1., para la aplicación de este

Marco es necesario reconocer aspectos trascendentales con los que se debería contar para su correcto funcionamiento, entre los que destaca que, el patrocinio de la Junta Directiva, la Mesa Directiva y/o quienes gobiernan las empresas, deben

conocer la importancia de la constitución de un órgano en la política de seguridad de la información, de ciberseguridad o de ciber resiliencia.

3.9.1 Separación de funciones.

La organización debe procurar la separación de funciones a nivel organizacional, no se debe ser juez y parte. Por ejemplo, el área de tecnologías de información no debe ser el que opere lo pertinente a los controles sobre la seguridad de la información, o bien quien establezca las líneas estratégicas en lo relacionado con riesgos. Las decisiones de esta separación de funciones se rigen desde el nivel más alto de la organización y se expresan en los organigramas y procesos estratégicos organizacionales.

3.9.2 Comunicación y socialización interna

La socialización de las estrategias y quienes están al frente de estas, es una de las labores que más incide en el éxito o el fracaso del camino hacia la madurez organizacional, mantener a los colaboradores al tanto del rumbo organizacional es sin duda una de las apuestas ganadoras de toda organización. Esto aplica para toda actividad o esfuerzo lanzado en procura de mayor seguridad física, clima laboral, mercado, y por supuesto; a las acciones dirigidas a mejorar la ciber resiliencia.

Las acciones informativas y de socialización promueven además la transparencia y la rendición de cuentas. La guía metodológica de este proyecto aporta ideas alrededor de los marcos que se proponen como base de esta en cada

fase, no obstante; no ofrece herramientas desarrolladas, lo que sí expone es las ideas centrales de cómo lograr que cada fase se desarrolle con fluidez y con un

norte claro alrededor del objetivo de lograr ciber resiliencia.

3.10Descripción operativa detallada de las fases del proyecto.

3.10.1 Primera fase: Determinación del perfil actual de la empresa. La primera fase, denominada “determinación del perfil actual de la empresa”, focaliza un entendimiento del estado actual de la organización en ciber-resiliencia. Esta fase, es de suma importancia, toda vez que, se requiere conocer la experiencia y acciones que ha desarrollado la empresa en materia de Ciberseguridad esto a través de la aplicación de un documento de autoevaluación basado en el marco NIST 1.1. El resultado esperado es un porcentaje que permitirá determinar el perfil actual de la empresa en materia de Ciberseguridad.

La ponderación del nivel de madurez de la empresa que es obtenido con la aplicación del formulario de autoevaluación basado en NIST, y se desglosa en un rango de preguntas por nivel de la siguiente forma: si se obtiene de 0 -24 puntos será **Nivel 1**, de 25 – 49 puntos **Nivel 2**, de 50 – 74 puntos **Nivel 3** y de 75 a 100 puntos **Nivel 4** siendo este último el más alto.

Es importante destacar que, la ponderación se basa en los resultados obtenidos en las funciones establecidas en el marco, que son: Identificar, Proteger, Detectar, Responder y recuperar; por lo que también se tendrá una evaluación específica de cada uno de estos aspectos.

3.10.1.1 Resultado esperado

Formulario de autoevaluación aplicado, el porcentaje de Nivel de madurez de la Empresa UN PROVEEDOR DE INTERNET y el resultado individual de las funciones.

3.10.2 Segunda fase: Resultados obtenidos por función y Detalle del Perfil Objetivo

En esta fase desarrollaremos análisis basados en el marco NIST 1.1., ampliando el esquema operativo de cada estándar, en el caso de NIST CSF; este marco de trabajo está conformado principalmente por un marco base con sus funciones, a decir: identificar, proteger, detectar, responder y recuperar, las cuales a su vez se dividen en categorías y subcategorías.

De acuerdo con el nivel de madurez, se puede aspirar a diferentes niveles los cuales son: parcial, riesgo informado, repetible y adaptativo. Si bien es cierto, la propuesta de plan de acción no está contemplada en el presente proyecto, la evaluación será el insumo para realizarlo. En la siguiente ilustración se muestra el marco de trabajo de ciberseguridad NIST 1.1.:

Figura 3-1 Arquitectura de NIST 1.1

Fuente: Sitio Web de PCI Hispano 2022.

La herramienta que se aplicará permite verificar las funciones del marco de trabajo, dividiendo la tarea en categorías y subcategorías. Las opciones de respuesta se presentan en concordancia con los niveles que maneja el marco de trabajo, donde 1 equivale a un cumplimiento “parcial”, 2 equivale a “cumplimiento con riesgo informado”, 3 significa que el cumplimiento es “repetible” y 4 equivale a un cumplimiento “adaptativo”, dicha gradualidad se muestra a continuación:

● **Nivel 1 – Parcial:** Gestión de riesgos ad hoc (para esto). Conocimiento limitado de riesgos de ciberseguridad. Baja participación externa. ● **Nivel 2 – Riesgo informado:** Algunas prácticas de gestión de riesgos. Aumento de la conciencia. Participación de terceros informal.

● **Nivel 3 – Repetible:** Gestión de riesgos formalizada. Programas transversales a la organización. Se gestiona la información de terceros. ● **Nivel 4 – Adaptativo:** Prácticas basadas en lecciones aprendidas. Mejora continua. Colaboración activa con terceros.

Los niveles están destinados a respaldar la toma de decisiones organizacionales sobre cómo gestionar el riesgo de seguridad cibernética, así como qué dimensiones de la organización son de mayor prioridad y podrían recibir recursos adicionales.

3.10.2.1 Resultados esperados

Porcentaje obtenido por función (perfil actual) y el perfil objetivo de la empresa.

3.10.2.2 Factores de éxito y fracaso.

Esta fase es fundamental para el resto del ejercicio, por lo que es vital que quien atiende la aplicación de la herramienta sea honesto, objetivo y apegado a la realidad de la organización.

Hay que considerar que los resultados no constituyen un arma forjada contra nadie, sino un instrumento de promoción de las oportunidades de mejora a la luz de los resultados obtenidos.

4 Capítulo IV. Resultados del Proyecto

4.1 Resultados Fase 1: Aplicación de fórmula de autoevaluación.

De conformidad con la aplicación de la herramienta denominada “Determinación del perfil actual de la empresa”, el nivel de madurez en seguridad con el que cuenta UN PROVEEDOR DE INTERNET es **de 87 puntos,** lo que

significa que se encuentra en un **Nivel 4-Adaptable**, esto según se muestra en el formulario del ANEXO 1 del presente documento. En el gráfico que se muestra a continuación, se representan las dimensiones del NIST CSF aplicadas y que desencadenan el desglose de la nota obtenida de la empresa según las funciones del NIST 1.1.

Figura 4-1 Nota General Ciber resiliencia UN PROVEEDOR DE INTERNET

Fuente: Elaboración propia.

El Nivel 4 se interpreta como qué; se cuenta con un amplio manejo de prácticas **de gestión de riesgos**, así como un **aumento de conciencia** de parte del nivel directivo de la organización. No obstante, la madurez en ciberseguridad está en un plano aparte y depende esencialmente de la materialización de un adecuado cumplimento del plan de acción.

4.2 Resultados Fase 2: Porcentaje por función y Detalle del Perfil Objetivo

4.2.1 Porcentajes obtenido por función:

Las preguntas aplicadas en el formulario son contestadas con un rango del 1 a 4 siendo 4 el más valor más alto, y van dirigidas a determinar lo siguiente:

1. Si la misión, visión y objetivos de la empresa, elementos esenciales de la misma, están establecidos y los conocen todos quienes deben conocerlos.
2. Si hay definido un proceso de Gestión de Riesgo alineado con los procesos críticos que permiten cumplir la misión, visión y objetivos. 3. Si los activos de la empresa están identificados.
4. Si los riesgos de los activos críticos se monitorean.
5. Si los riesgos de la cadena de suministros se monitorean.

4.2.1.1 Identificar:

Esta función abarca el entorno empresarial, los temas de gobernanza de las TIC, la gestión de riesgos en el contexto de TI, la gestión de activos de información, los riesgos desde el contexto de la organización y los riesgos asociados con terceros o de la cadena de suministros. En esta función, se realizaron 29 preguntas divididas en Subcategorías según el siguiente detalle:

Subcategoría	Cantidad de Preguntas
Entorno Empresarial	5
Gestión de Activos	6
Gestión de Riesgo	3

Gobernanza	4
Riesgos en Cadena Suministros	5
Riesgos Organizacionales	6

75
Fuente: Elaboración propia.

Una vez aplicadas las preguntas, la evaluación arrojó que la función identificar UN PROVEEDOR DE INTERNET es **de un 88**, a continuación, se muestran los resultados obtenidos por cada subcategoría:

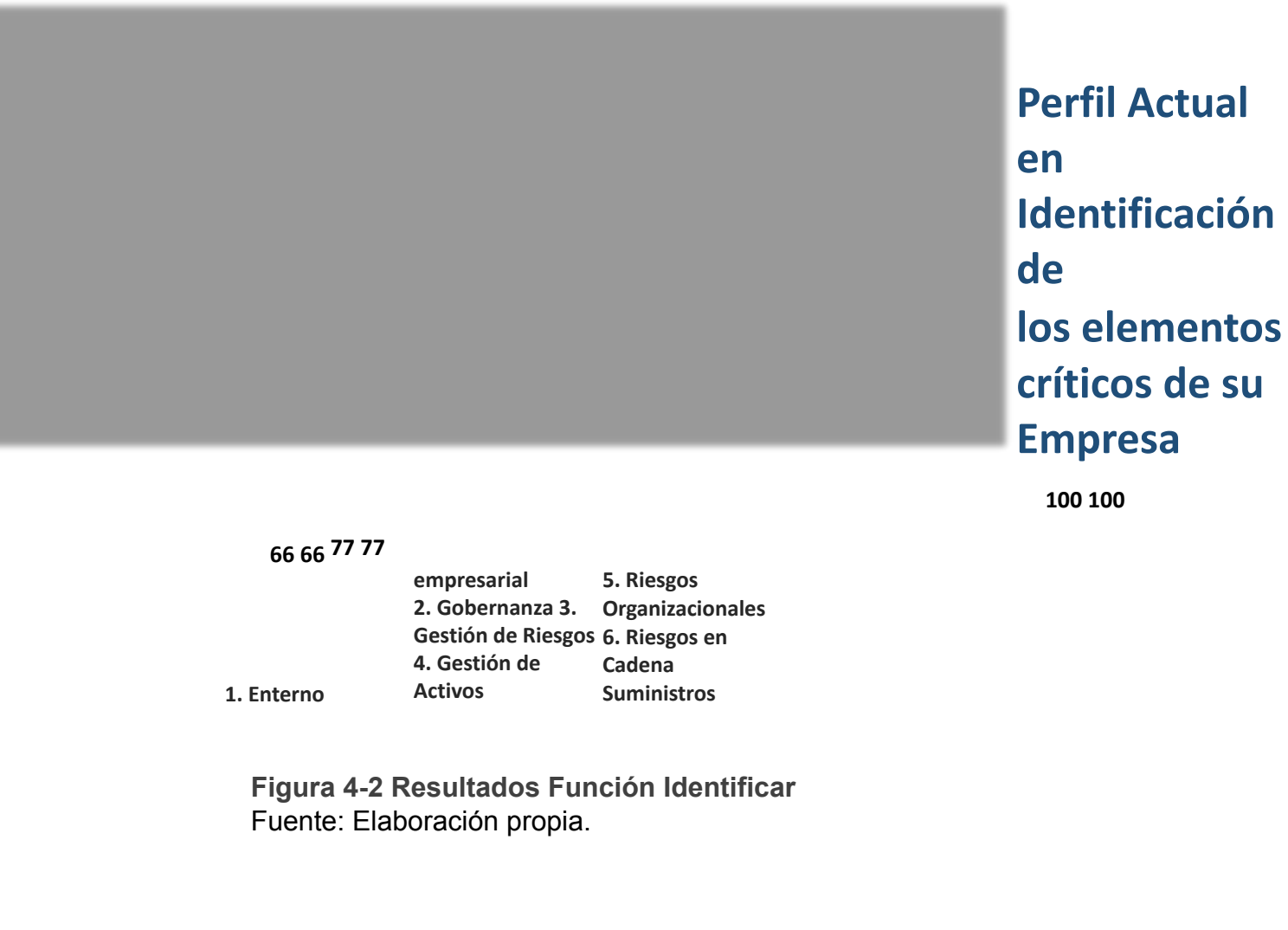

Figura 4-2 Resultados Función Identificar
Fuente: Elaboración propia.

El resultado anterior, lo que demuestra es que en la función **Identificar** aún hay oportunidades de mejorar en la Gobernanza de las TIC, Riesgos organizacionales y Riesgos en cadena suministros, se deben implementar procesos apropiados de gobernanza de la ciberseguridad, identificando y catalogando la información sensible que se posea. Sumado, deben identificarse y catalogarse los servicios operacionales clave que se despliegan atendiendo la necesidad de que los usuarios accedan a información sensible o servicios operacionales clave, la cual debe ser entendida y administrada continuamente.

Por otro lado, en el caso del análisis de los resultados de las subcategorías se tiene lo siguiente:

i) En el caso del **entorno organizacional** se evidencia una calificación de **66** de **100**, lo que deviene en temas relacionados con la articulación de acciones y la fluidez de la comunicación a lo largo y ancho de la organización.

ii) La **gobernanza** contextualiza la cobertura por un lado y la capacidad de actuar como una sola masa al margen de las acciones desplegadas. En cuyo caso la calificación fue de **66** de **100**.

iii) Tanto la gestión del **riesgo a nivel de TI**, como la gestión del **riesgo a nivel general de la organización y gestión de cadena de suministros** parecen haber alcanzado el puntaje más alto al menos en la teoría, dado que este ejercicio no se eleva hasta su aplicación en la práctica.

iv) El proceso de tratamiento de decomiso, baja y desecho de activos y/o gestión integral de la seguridad de la información, denominado **gestión**

de activos de TI alcanzó un **93** de **100**.

4.2.1.2 Proteger:

En el contexto de aplicación de la función **proteger**, el acceso a información sensible y servicios operativos clave sólo se proporcionará a usuarios o sistemas identificados, autenticados y autorizados.

Los sistemas que manejan información sensible o servicios operacionales clave deben estar protegidos contra la explotación de vulnerabilidades conocidas y las cuentas altamente privilegiadas no deben ser vulnerables a ataques cibernéticos comunes.

Como queda a la vista, esta función agrupa temas de capacitación y cultura en seguridad de la información, aplicación de procesos, procedimientos y buenas prácticas, provisión y accionables para el control de acceso, provisión y accionables

para la protección de datos así como de tecnologías para la protección de la red y equipos servidores, de usuario final y de otros servicios, y finalmente, todo lo relacionado con el mantenimiento, soporte, actualización y buenas prácticas alrededor de ellos.

En la función proteger se realizaron 40 preguntas divididas en Subcategorías según el siguiente detalle:

Subcategoría	Cantidad de Preguntas
Capacitación	5
Control de Accesos	8
Mantenimiento	2
Procesos y Procedimientos	12
Seguridad de Datos	8

Tecnología de Protección	5

El resultado granulado sobre la autoevaluación y el análisis de resultados sobre la función **proteger** queda de la siguiente forma:

Figura 4-3 Resultados Función Proteger