Diseño y desarrollo de una aplicación web que permita conocer el nivel madurez en ciberseguridad para entidades pertenecientes al sector educativo.

María Angélica Serrano Mora

Trabajo de Grado para Optar al Título de Ingeniería de Sistemas e Informática

Directora

PhD. Lola Xiomara Bautista Rozo

Doctor en Ciencias y Tecnologías de la Comunicación y la Información

Universidad Industrial de Santander

Facultad de Ingenierías Fisicomecánicas

Escuela de Ingeniería de Sistemas e Informática

Bucaramanga

2023

Dedicado a

En primera instancia a Dios, por darme la sabiduría, paciencia y resiliencia ante todas las dificultades presentadas a lo largo de este camino universitario, así mismo las bendiciones recibidas durante este camino.

A mi madre, Geny Mora, por el apoyo y las palabras de aliento frente a cualquier dificultad presentada a largo de mi vida.

A mi padre, Juan Carlos Serrano, por estar presente y dispuesto a apoyarme en cualquier nuevo proyecto de vida.

A mi familia, mis hermanas, tías, madrinas y todos aquellos que se tomaron el tiempo de apoyarme en este camino.

A Herlinda Tarazona, por ser ejemplo de mujer resiliente, porque con su existencia y experiencias diarias me demostró que no hay impedimento más grande que uno mismo.

A mi prima, Yessica Serrano, por su apoyo en el desarrollo de este trabajo, gracias porque a pesar de las distancias siempre estaba dispuesta a ayudar.

A mis amigos UIS, especialmente a Juan, Kevin y Brayan, ya que sin ellos no hubiese vivido igual esta experiencia universitaria que ya ha llegado a su fin.

A Orlando Moncada y mi Sensei porque sin su compañía y apoyo no podría haber superado todas las dificultades que esta última etapa de mi carrera me presentó.

A mis amigos en general, ya que sin su apoyo y palabras de aliento no hubiese logrado salir de esos momentos de frustración que puede ocasionar la universidad.

Agradecimientos

A Lola Xiomara Bautista, por ser mi directora de proyecto, gracias por confiar en mí. Por el tiempo dedicado, las correcciones, sugerencias, conocimiento y demás aporte en este proyecto.

A mi familia, por ser el pilar fundamental de mi vida, por el apoyo incondicional, la paciencia y los consejos para terminar con éxito esta etapa.

A Sistemas Aplicativos S.A. (SISAP) por el conocimiento, tiempo, apoyo y dedicación brindado en las áreas de conocimiento pertinentes para realizar este proyecto y culminar de la mejor manera esta etapa.

A Irwin Samos, por su gran apoyo, por brindarme todas las herramientas y conocimientos necesarios para poder lograr este proyecto, por ser ese polo a tierra que me hacía pensar sin emociones y ser racional.

A la Universidad Industrial de Santander por permitirme formarme en ella y brindarme amigos, conocimiento y experiencias que serán de vital importancia para lo que sigue en mi vida.

Contenido

Lista de figuras

Lista de tablas

Resumen

Título: Diseño y desarrollo de una aplicación web que permita conocer el nivel madurez en ciberseguridad para entidades pertenecientes al sector educativo.[*]

Autor: María Angélica Serrano Mora[**]

Palabras clave: Ciberseguridad, NIST CSF, CIS Top 18, Ransomware, aplicación web, análisis de datos.

Descripción: Dado el avance tecnológico que ha venido transformando las maneras de concebir el mundo, la ciberseguridad y seguridad informática se ha convertido en uno de los pilares fundamentales para toda organización, siendo ésta la encargada de proteger y defender todos los activos en una compañía. La ciberseguridad es decisiva en cualquier sector, Verizon, una compañía de telecomunicaciones de Estados Unidos, desde el año 2008 ha emitido reportes de cómo se encuentra la ciberseguridad en el mundo, donde se ha visto una constante evolución de las ciber amenazas, este reporte clasifica los patrones de ataque más utilizados en diversos sectores, entre ellos el sector educativo. Hoy, millones de estudiantes están aprendiendo, a través de la tecnología en modalidades híbridas, atendiendo a clases, reuniones, conferencias y demás de forma remota o presencial, por lo que las redes del sector educativo se han extendido a las de los hogares, al dar acceso a la red interna del sector educativo. Es decir, si la computadora de un profesor o estudiante desde la red de su casa es atacada y ésta tiene acceso a los recursos internos de la entidad, dichos recursos podrían verse comprometidos por extensión.

Este proyecto, busca apoyar a estas instituciones a conocer su nivel de madurez actual en ciberseguridad según marcos de referencia como NIST y controles como los de CIS mediante una aplicación web inspirada en *stepper* para interactuar con el usuario de forma sencilla e interactiva.

[*] Trabajo de Grado

[**] Facultad de Ingenierías Fisicomecánicas. Escuela de Ingeniería de Sistemas e Informática. Directora: Lola Xiomara Bautista Rozo. Doctor en Ciencias y Tecnologías de la Comunicación y la Información.

Summary

Title: Design and development of a web application that allows to know the maturity level in cybersecurity for entities belonging to the education sector.[*]

Author: Maria Angélica Serrano Mora[**]

Keywords: Cybersecurity, NIST CSF, CIS Top 18, Ransomware, web application, data analysis.

Description: Given the technological progress that has been transforming the ways of conceiving the world, cybersecurity and computer security has become one of the fundamental pillars for any organization, being responsible for protecting and defending all assets in a company. Cybersecurity is decisive in any sector, Verizon, a telecommunications company in the United States, since 2008 has issued reports on how cybersecurity is in the world, where there has been a constant evolution of cyber threats, this report classifies the most used attack patterns in various sectors, including the education sector. Today, millions of students are learning, through technology in hybrid modalities, attending classes, meetings, conferences, and others remotely or in person, so the networks of the education sector have extended to those of homes, by giving access to the internal network of the education sector. That is, if the computer of a teacher or student from the network of his home is attacked and it has access to the internal resources of the entity, these resources could be compromised by extension.

This project seeks to support these institutions to know their current level of maturity in cybersecurity according to frameworks such as NIST and controls such as CIS through a web application inspired by *stepper* to interact with the user in a simple and interactive way.

[*] Degree work

[**] Faculty of Physic mechanical Engineering. School of Systems Engineering and Computer Science. Director: Lola Xiomara Bautista Rozo. Doctor of Science and Information Technologies.

Introducción

El proyecto, que se describe en este documento, tuvo el objetivo de desarrollar una aplicación web para ser utilizada por instituciones educativas y evaluar su nivel de madurez en ciberseguridad, adicionalmente le brinda una evaluación para verificar si se encuentra preparado ante un potencial ataque de ransomware. La herramienta utiliza el NIST Cybersecurity Framework (CSF) y el CIS Top 18 como sus principales marcos para evaluar las prácticas de ciberseguridad de una organización. La aplicación web utiliza un conjunto de 6 preguntas para evaluar la preparación de una institución ante un eventual ataque de ransomware, estas preguntas se realizan teniendo en cuenta las fases de un ataque de ransomware.

Al proporcionar una forma comprensiva y normalizada de medir la postura de ciberseguridad de una institución, incluyendo su preparación para defenderse contra el ransomware, la herramienta ayuda a los educadores y administradores a identificar áreas de mejora e implementar mejores prácticas para proteger sus redes y datos sensibles. El objetivo final del proyecto es entregar un recurso valioso para el sector educativo que ayude a las instituciones a proteger sus redes y datos contra amenazas cibernéticas cada vez más sofisticadas, incluyendo ataques de ransomware.

1. Marco Referencial

1.1. Marco Conceptual

1.1.1. Amenaza

En la seguridad informática, se considera amenaza cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de la organización (incluida la misión, las funciones, la Figura o la reputación), los activos de la organización, las personas, otras organizaciones o la Nación a través de un sistema de información a través del acceso no autorizado, la destrucción, la divulgación o la modificación de la información. y/o denegación de servicio (CSRC, 2022).

1.1.2. Brecha de datos

Una brecha de datos es una filtración de datos expone información confidencial, sensible o protegida a una persona no autorizada. Los archivos en una violación de datos se ven y/o comparten sin permiso. Cualquiera puede estar en riesgo de una violación de datos, desde individuos hasta empresas de alto nivel y gobiernos. Más importante aún, cualquiera puede poner en riesgo a otros si no está protegido. En general, las violaciones de datos ocurren debido a debilidades en tecnología y el comportamiento del usuario (Kaspersky, 2021).

1.1.3. Brecha de seguridad

Una brecha de seguridad es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Es decir, permite acceder sin autorización a información. Normalmente, se produce cuando un intruso logra sortear los mecanismos de seguridad.

Técnicamente, existe una diferencia entre una brecha de seguridad y una brecha o filtración de datos. Una brecha de seguridad comporta una intromisión, mientras que una brecha de datos consiste en la sustracción de información por parte de un ciberdelincuente. (Kaspersky, 2021)

1.1.4. Ciberataque

Un ciberataque es un intento de desactivar ordenadores, robar datos o utilizar un sistema informático infiltrado para lanzar ataques adicionales. Los ciberdelincuentes utilizan diferentes métodos para lanzar un ciberataque que incluye malware, phishing, ransomware, ataque de intermediario u otros métodos. (Unisys, 2021)

1.1.5. Ciberseguridad

La ciberseguridad, también llamada seguridad informática, es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. Kaspersky (2021) afirma que el término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

- Seguridad de red
- Seguridad de las aplicaciones
- Seguridad de la información
- Seguridad operativa
- Recuperación ante desastres y la continuidad del negocio
- Capacitación del usuario final

1.1.6. CIS

Proviene de las siglas en inglés *Center of Internet Security* (CIS., 2021) hace del mundo conectado un lugar más seguro para las personas, las empresas y los gobiernos a través de nuestras competencias básicas de colaboración e innovación. CIS cuenta con controles y puntos de referencia, para efectos de este trabajo de investigación se tendrán en cuenta los dieciocho controles del año 2022.

1.1.7. DBIR

Por sus siglas en inglés *Data Breach Investigations Report,* es un reporte como su nombre lo indica que es anualmente publicado por la compañía Verizon. De acuerdo con la compañía Improsec, es uno de los informes de seguridad cibernética más completos publicados públicamente en línea. Los profesionales de la seguridad utilizan DBIR para obtener perspectivas del mundo real sobre violaciones de datos potencialmente dañinas y basadas en análisis basados en datos (Wong, T, 2022).

1.1.8. Framework

Es un esquema o marco de trabajo que ofrece una estructura base para elaborar un proyecto con objetivos específicos, una especie de plantilla que sirve como punto de partida para la organización y desarrollo de software (Edix, R., 2021).

1.1.9. Incibe

El Instituto Nacional de Ciberseguridad trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España. Con una actividad basada en la investigación, la prestación de

servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional (INCIBE, 2022).

1.1.10. NIST Cybersecurity Framework

El marco de ciberseguridad del NIST es una poderosa herramienta para organizar y mejorar su programa de ciberseguridad. Es un conjunto de pautas con las mejores prácticas para ayudar a las organizaciones a construir, al igual que mejorar su postura de ciberseguridad. El marco presenta un conjunto de recomendaciones o estándares que permiten a las organizaciones estar mejor preparadas para identificar y detectar ataques cibernéticos; también proporciona pautas sobre cómo responder, prevenir, recuperarse de incidentes cibernéticos (Balbix, 2022).

1.1.11. Seguridad

La seguridad es un estado en el cual los peligros y las condiciones que pueden provocar daños de tipo físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos y de la comunidad.

1.1.12. Seguridad de la información

La seguridad de la información es el conjunto de medidas o técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización con el objetivo de asegurar que los datos no salgan del sistema que ha establecido la organización. Es una pieza clave para que las empresas puedan llevar a cabo sus operaciones, ya que los datos que maneja son esenciales para la actividad que desarrollan (Toro, 2021).

1.1.13. Verizon

Verizon es una empresa de telecomunicaciones estadounidense que ofrece servicios de telefonía móvil, internet y televisión por cable. Verizon ofrece servicios de internet y de red, por lo que es importante que implemente medidas de ciberseguridad para proteger a sus clientes y sus sistemas contra posibles amenazas cibernéticas (Verizon, 2022). Verizon es la empresa que pública el DBIR, por lo que se relaciona directamente con este informe. Además, como una empresa de telecomunicaciones, Verizon, también puede ser afectada por los incidentes de seguridad en la red que se analizan en el DBIR, por lo que puede utilizar el informe para identificar las áreas en las que necesita mejorar su propia seguridad y tomar medidas para protegerse contra posibles amenazas.

1.1.14. Riesgo

Es la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas (CIIFEN, 2022).

1.2. Estado del arte

Actualmente, existen diversos marcos de referencia que se pueden utilizar para medir el nivel de madurez de las prácticas de ciberseguridad de una organización. El NIST Cybersecurity Framework (CSF) es un ejemplo de un marco ampliamente utilizado para evaluar y mejorar la postura de ciberseguridad de una organización. El CSF proporciona un lenguaje común y un conjunto de normas para identificar, evaluar y mitigar los riesgos de ciberseguridad. Es utilizado por organizaciones de diversos sectores, incluyendo el sector educativo.

Otro ejemplo es el CIS Top 18, un conjunto de mejores prácticas para proteger la red y los datos de una organización. El CIS Top 18 es una lista completa de controles de ciberseguridad que las

organizaciones pueden utilizar para evaluar sus prácticas actuales e identificar áreas de mejora. Al igual que el NIST CSF, el CIS Top 18 es ampliamente utilizado por organizaciones de diversos sectores, incluyendo la educación.

También hay otras herramientas y marcos de referencia disponibles que se pueden utilizar para medir el nivel de madurez en ciberseguridad de una organización, como la norma ISO 27001 y COBIT. Estas herramientas y marcos de referencia pueden proporcionar información valiosa y ayudar a las organizaciones a implementar mejores prácticas para protegerse contra las amenazas cibernéticas.

1.3. Antecedentes del tema.

En esta sección se presentarán tres (3) herramientas de las cuales todas se puede encontrar en la web y una requiere instalación en el dispositivo. El origen de estas se encuentra fuera del país, donde se destaca CSET al ser desarrollada por CISA, la agencia de ciberseguridad y seguridad de infraestructura del gobierno de los Estados Unidos.

1.3.1. INCIBE

El instituto INCIBE (Instituto Nacional de Ciberseguridad) cuenta con diversas herramientas para apoyar a las organizaciones en ciberseguridad, entre ellas existe una herramienta para la medición del riesgo, en la cual mediante un cuestionario de 27 preguntas, donde se evalúan las tecnologías que se utilizan y las medidas de ciberseguridad que adopta la empresa para protegerlas. Esta herramienta viene orientada a diversos sectores, entre ellos educación. Al finalizar el cuestionario, se presenta el porcentaje del riesgo de la empresa distribuido en tres categorías (personas, procesos y tecnologías) cada uno con su respectivo puntaje de nivel de riesgo y su recomendación de mejora. Esta herramienta es bastante útil e intuitiva para el usuario, ya que

puede desplazarse con la facilidad de un solo clic y solo respondiendo preguntas con lenguaje no técnico.

Lo interesante de esta herramienta es que en la página de inicio, empieza a cuestionar al usuario sobre la importancia que le da a la información, ¿Qué pasaría si perdiera toda la información?, ¿Cuál es el nivel de ciberseguridad de su empresa? Y otras preguntas que curiosamente se han discutido en el planteamiento inicial del problema (INCIBE, 2022). Esta herramienta se encuentra basada en el RGPD (Reglamento General de Protección de Datos) de la Unión Europea.

1.3.2. Cybersecurity Capability Maturity Model (C2M2)

Es una herramienta gratuita que puede ser encontrada en formato web y PDF para ayudar a las organizaciones a evaluar sus capacidades de ciberseguridad y optimizar las inversiones en seguridad, la ejecución de esta se recomienda realizar a modalidad de taller, donde todas las áreas involucradas en los dominios específicos participen para tener un escenario más acertado. Utiliza un conjunto de prácticas de ciberseguridad examinadas por la industria centradas tanto en activos y entornos de tecnología de la información (TI) como en tecnología de operaciones (OT). (Cybersecurity Capability Maturity Model (C2M2), 2022). Esta herramienta evalúa diez (10) dominios, de los cuales en promedio por dominio son 35 preguntas para un total de 356.

El C2M2 puede ayudar a las organizaciones de todos los sectores, tipos y tamaños a evaluar y realizar mejoras en sus programas de ciberseguridad y fortalecer su resiliencia operativa. El C2M2 se centra en la implementación y gestión de prácticas de ciberseguridad asociadas con TI, OT y activos de información y los entornos en los que operan. (Cybersecurity Capability Maturity Model, 2022)

El modelo se puede utilizar para:

- Fortalecer las capacidades de ciberseguridad de las organizaciones.
- Permitir a las organizaciones evaluar y comparar de manera efectiva y consistente
- Capacidades de ciberseguridad.
- Compartir conocimientos, mejores prácticas y referencias relevantes entre organizaciones como un medio para mejorar las capacidades de ciberseguridad.
- Permitir a las organizaciones priorizar acciones e inversiones para mejorar capacidades de ciberseguridad.

1.3.3. CYBER SECURITY EVALUATION TOOL (CSET)

El Cyber Security Evaluation Tool (CSET®) es una aplicación de escritorio independiente que guía a los propietarios y operadores de activos a través de un proceso sistemático de evaluación de la tecnología operativa y la tecnología de la información. El 30 de junio de 2021, CSET se actualizó para incluir un nuevo módulo: Evaluación de preparación para ransomware (RRA). El RRA es una autoevaluación basada en un conjunto escalonado de prácticas para ayudar a las organizaciones a evaluar mejor qué tan bien están equipadas para defenderse y recuperarse de un incidente de ransomware.

Después de completar la evaluación, la organización recibirá informes que presentan los resultados de la evaluación de manera resumida y detallada. La organización podrá manipular y filtrar el contenido para analizar los hallazgos con diversos grados de granularidad. (CISA, 2021)

CISA (Hope, 2021) dice que la herramienta de evaluación de preparación para ransomware se basa en un conjunto de "prácticas escalonadas", ayudando a las organizaciones a evaluar su preparación para un posible ataque de ransomware de las siguientes maneras:

- Ayudar a las organizaciones a evaluar su postura de ciberseguridad, con respecto al ransomware, en comparación con los estándares reconocidos y las recomendaciones de mejores prácticas de manera sistemática, disciplinada y repetible. Este proceso podría ayudarles a detectar deficiencias y tomar medidas correctivas.
- Guiar a los propietarios y operadores de activos a través de un proceso sistemático para evaluar sus prácticas de seguridad de red de tecnología operativa (OT) y tecnología de la información (TI) contra la amenaza de ransomware.
- Presenta el análisis en un formato resumido y detallado en un panel enriquecido con gráficos y tablas.

2. Planteamiento y justificación del problema

A raíz de la inminente transformación digital, las organizaciones se han visto forzadas a estar en constante cambio (PowerData, 2022); este conlleva no solo a la modificación de las organizaciones, sino también de las personas que intentan ocasionarles daño, conocidas como cibercriminales. Para combatir a estos ciber atacantes, surge una ciencia derivada de esta necesidad, denominada ciberseguridad, la cual tiene diferentes métodos, herramientas y esfuerzos utilizados para proteger datos, redes y dispositivos digitales del acceso no autorizado.

La ciencia de la ciberseguridad engloba las salvaguardas y los procesos aplicados para asegurar no solo los activos físicos o personales, sino también los digitales; esto podría incluir procesos patentados, sistemas de acceso exclusivos, información personal, incluso información vital para las operaciones de una entidad o empresa, como planes futuros, diseños o resultados de investigación (Why Cybersecurity Matters, 2022).

Según Intel (2022), la ciberseguridad es decisiva en cualquier entorno empresarial, pero especialmente en el sector educativo. Los ataques cibernéticos no solo comprometen la seguridad de los profesores y el personal administrativo, sino también la privacidad de los estudiantes. Hoy, millones de estudiantes están aprendiendo, a través de la tecnología en modalidades híbridas, atendiendo a clases, reuniones, conferencias y demás de forma remota o presencial, por lo que las redes del sector educativo se han extendido a las de los hogares, al dar acceso a la red interna del sector educativo. Es decir, si la computadora de un profesor o estudiante desde la red de su casa es atacada y ésta tiene acceso a los recursos internos de la entidad, dichos recursos podrían verse comprometidos por extensión.

De acuerdo con el Data Breach Investigations Report (DBIR) de Verizon, en sus reportes desde el año 2017 al 2022 el promedio de la materialización de los incidentes en el sector de educación es del 25%, es decir una cuarta parte de los incidentes se están convirtiendo en exposición de datos. Es importante que las organizaciones conozcan su nivel de madurez y exposición a los vectores de ataque respecto a ciberseguridad, así pueden conocer que tan expuestos se encuentran en el amplio mar de la transformación digital (Data Breach Investigations Report, 2022).

Sufrir un ciberataque genera una pérdida para cualquier entidad, como por ejemplo, una exfiltración de datos conllevaría a una pérdida de credibilidad, afectando su reputación, buscar una solución a este ciberataque afecta la operación del negocio, si alguna persona afectada desea tomar medidas legales contra esta entidad está en su derecho de hacerlo y todas estas pérdidas conllevan a la más importante, que es la financiera, ya que el ejecutar contramedidas ante este ciberataque requerirá de dinero no presupuestado para responder. ¿Será que todo esto se pudo evitar al conocer cuáles eran las medidas de seguridad de la entidad? al tener tantas tecnologías disponibles al alcance de la mano, da la sensación de estar a la vanguardia tecnológicamente hablando pero ¿realmente tengo control de la tecnología que poseo? Es válido que como evaluador de este tema y perteneciente al sector de educación se pregunte ¿conozco el nivel de madurez y exposición a los vectores de ataques respecto a ciberseguridad de la escuela de ingeniería de sistemas? Es importante recordar que todo lo que no se conoce, no se puede medir y si no se puede medir, no se puede mejorar. Dicho esto, surge la pregunta más importante que envuelve este proyecto de grado ¿le interesaría conocer cómo mejorar su postura actual de ciberseguridad y además que tan eficaz sería para prevenir los vectores de ataque?

Para atender este problema, se diseñó un programa basado en la web que busca apoyar al sector de la educación a conocer su nivel de madurez y exposición a los vectores de ataque en ciberseguridad utilizando los últimos informes del DBIR de Verizon (2017-2022), el NIST Cybersecurity Framework y el CIS Top 18, adicionalmente podrá conocer cómo mejorar estos resultados. En este último año el ataque de ransomware se ha posicionado como uno de los más comunes, el cual es una forma de malware diseñado para secuestrar los datos y posteriormente exigir un rescate para liberar los datos secuestrados (Trellix, 2022). Es por esto, que se incluirá en este programa un módulo de Ransomware Readiness Assessment, con el fin de conocer si como entidad perteneciente al sector educativo se encuentra preparada para prevenir, detectar y responder o hasta recuperarse de un ataque de ransomware.

Haciendo uso de la ingeniería de software, bases de datos, programación en la web y análisis de datos, se realizará este programa para apoyar al sector educativo al conocer el nivel de madurez y exposición a los vectores de ataque, respecto a ciberseguridad y la capacidad de respuesta ante un eventual ataque de ransomware.

3. Objetivos

3.1. Objetivo general

Desarrollar una aplicación web para conocer el nivel de madurez y exposición a los vectores de ataque en ciberseguridad a organizaciones dentro del sector educativo.

3.2. Objetivos específicos

- Desarrollar módulos e interfaces que permitan hacer un mapeo para la captura de datos, de acuerdo con el marco de referencia NIST CSF y los controles del CIS Top 18.
- Implementar una rutina computacional para el análisis de datos que permita determinar el nivel de exposición a los vectores de ataque y madurez en ciberseguridad dentro del sector educativo.
- Proponer un protocolo para mejorar de la postura en ciberseguridad a cualquier organización perteneciente al sector educativo, creando un plan de acción a partir de la postura actual de la misma.

4. Metodología

Este trabajo se llevó a cabo para crear una aplicación web que determina el nivel de madurez en ciberseguridad para organizaciones o instituciones del sector educativo y consta de varios pasos. En primer lugar, se recopila información esencial sobre la institución, incluyendo su nombre, cantidad de empleados, dependencia tecnológica e ingreso financiero o *revenue* del año anterior, con el fin de tener contexto del negocio y apoyarse en el desarrollo de otros módulos.

A continuación, se presenta al usuario el módulo para conocer su nivel de madurez actual en ciberseguridad, el cual consta de 18 preguntas basadas en los 18 controles de CIS (Center for Internet Security), cada una de las cuales se encuentra mapeada según las 5 funciones de NIST (*National Institute of Standards and Technology*) y los patrones de ataque según el DBIR *(Data Breach Investigations Report*) del año 2022 para el sector educativo.

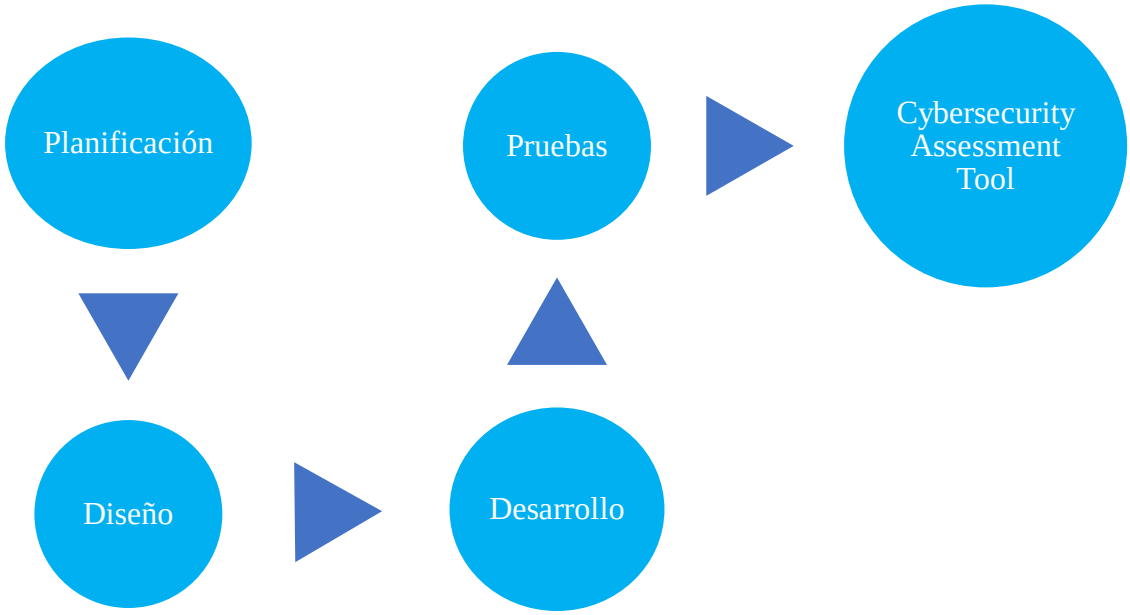
Posteriormente, se presenta al usuario 6 preguntas basadas en las 6 etapas de un ataque de ransomware, según el MITRE ATT&CK Framework, con el objetivo de evaluar si la organización se encuentra preparada para un eventual ataque de este tipo.

Una vez que el usuario ha completado las preguntas, se generan resultados que se muestran en un dashboard disponible para el usuario. Los resultados incluyen el nivel de madurez respecto al NIST CSF, el nivel de madurez de acuerdo con el CIS Top 18, el nivel de exposición ante ciberataques, un plan de mejora, hipótesis de ciberriesgo y los resultados del Ransomware Readiness Assessment. Estos resultados proporcionan una visión clara del estado actual de la organización en términos de ciberseguridad y ofrecen información valiosa para la toma de decisiones y la implementación de medidas de mejora en este ámbito.

A continuación, se detallará cómo se llega a cada uno de los módulos mencionados basándose en el SDLC (Ciclo de Vida del Desarrollo de Software), explicando de manera concisa cómo se logró a través de las distintas etapas del desarrollo de la aplicación web.

Figura 1

Metodología del desarrollo del proyecto



4.1. Planificación

La planificación es una etapa fundamental en cualquier proyecto, ya que sienta las bases para un desarrollo satisfactorio. Una parte clave de esta planificación es el diseño de requerimientos, que se elabora en función de los alcances y la problemática que dio origen al proyecto. Los requerimientos se clasifican en dos categorías: funcionales, que describen el comportamiento del sistema en relación con la funcionalidad establecida, y no funcionales, que consisten en las restricciones y funciones que se establecen para los servicios propuestos por el sistema.

El enfoque principal de este proyecto es la inminente transformación digital y cómo esta afecta a las organizaciones en todo el mundo desde el punto de vista de la ciberseguridad. Durante el desarrollo de este documento, Colombia enfrentó diversos ataques de ransomware en organizaciones de varios sectores. De hecho, según IBM (2023), Colombia fue el segundo país con el mayor número de brechas de seguridad, en las cuales tuvieron que intervenir, siendo superados únicamente por Brasil. Con lo anterior, se evidencia que cada vez cobra más sentido conocer el nivel de seguridad cibernética de cualquier institución educativa.

Se desarrolló una aplicación web basada en diversos controles y mejores prácticas de instituciones reconocidas a nivel mundial, como CIS y NIST, así como en el reporte anual de investigación de brechas de datos publicado por Verizon (DBIR), entre otros. Los usuarios deben registrarse en la aplicación para acceder a la evaluación. Una vez registrados, encuentran una aplicación inspirada en el concepto de *stepper*, que tuvo como objetivo brindarles una experiencia informativa sobre la importancia de realizar este tipo de evaluación y lo que se esperaba entregar al finalizarla.

Durante el registro, se recopiló información general, como el nombre de la organización educativa a la que pertenece, el ingreso del negocio en el último año, cantidad de empleados, dependencia tecnológica, entre otros detalles de la entidad. A continuación, se inicia la evaluación para conocer el nivel de madurez en ciberseguridad, la cual se basó en los dieciocho controles de CIS y las cinco funciones de NIST. Para cada pregunta de la evaluación, el usuario tuvo cinco opciones de respuesta.

Adicionalmente, la aplicación cuenta con un módulo de evaluación de preparación para *ransomware*, el cual consiste en seis preguntas basadas en las etapas que MITRE ATT&CK

identifica como puntos de entrada del *ransomware* en una organización y cómo recuperarse de ello. Una vez finalizada la evaluación, el usuario accede a un panel de control donde se muestra un resumen del estado actual de la organización, según las respuestas proporcionadas previamente mediante diferentes módulos, como por ejemplo, la madurez según CIS Top 18, la madurez según NIST CSF, la exposición a los vectores de ataque, la recomendación de un plan de mejora, la cuantificación o hipótesis de ciberriesgo y la evaluación de preparación para *ransomware*.

En el módulo de madurez según CIS Top 18, puede encontrar su nivel de madurez en porcentaje, los tres controles que debe mejorar y los tres mejores controles que implementa en la organización, estos los evidencia con la pregunta que fue respondida, teniendo en cuenta que las preguntas se encuentran en orden según los controles de CIS. En el módulo madurez según NIST CSF, encontrará un diagrama de barras, el cual le da una idea por función cual fue el resultado y el nivel de madurez en porcentaje de estos. Para la exposición de los vectores de ataque, dado que se tomaron los tres pertinentes que afectan al sector educativo (Ataque a aplicaciones web, intrusión del sistema y errores misceláneos) por cada uno de ellos encuentra que tan expuesto está actualmente la organización. Con los resultados anteriores, se visualiza un plan de mejora para su postura de ciberseguridad y la hipótesis de ciber-riesgo con la explicación de cuales fueron los datos utilizados para llegar a este resultado y finalmente, el resultado para determinar qué tan preparada se encuentra la institución ante un eventual ataque de *ransomware*. Todos estos resultados el usuario los puede visualizar cada vez que desee ingresar a la aplicación. Cabe resaltar que el usuario no puede modificar las respuestas a las preguntas respondidas una vez sean enviadas.

Con el planteamiento del proyecto previamente descrito, se procede a seleccionar los requerimientos funcionales este proyecto.

4.1.1. Levantamiento de requerimientos

Los requerimientos funcionales fueron seleccionados en base al propósito del proyecto y sus objetivos como se expuso anteriormente. Este proyecto es únicamente de software, lo cual significa que no tiene ninguna interacción con dispositivos hardware.

Tabla 1

Requerimiento funcional de autenticación y registro de usuarios

Prioridad	Alta
Identificación del Requerimiento	RF01
Nombre	Autenticación y registro de usuarios
Descripción	La aplicación permitirá a los usuarios registrarse e iniciar sesión.

Tabla 2

Requerimiento funcional de ingreso a consultar resultados

Prioridad	Alta
Identificación del Requerimiento	RF02
Nombre	Usuario podrá consultar sus resultados
Descripción	La aplicación permitirá al usuario ingresar a consultar los resultados obtenidos en la evaluación.

Tabla 3

Requerimiento funcional usuario realiza evaluación

Prioridad	Alta
Identificación del Requerimiento	RF03
Nombre	Usuario podrá contestar preguntas de la evaluación
Descripción	La aplicación permitirá al usuario responder las preguntas realizadas para completar la evaluación.

Tabla 4

Requerimiento funcional usuario visualiza nivel de madurez según CIS Top 18

Prioridad	Alta
Identificación del Requerimiento	RF04
Nombre	Usuario podrá visualizar su nivel de madurez CIS Top 18
Descripción	El usuario podrá visualizar su postura de ciberseguridad según las respuestas dadas y los controles de CIS Top 18

Tabla 5

Requerimiento funcional usuario visualiza nivel de madurez según NIST CSF

Prioridad	Alta
Identificación del Requerimiento	RF05
Nombre	Usuario podrá visualizar su nivel de madurez NIST CSF
Descripción	El usuario podrá visualizar su postura de ciberseguridad según las respuestas dadas y las funciones de NIST CSF

Tabla 6

Requerimiento funcional usuario visualiza exposición a los vectores de ataque

Prioridad	Alta
Identificación del Requerimiento	RF06
Nombre	Usuario podrá visualizar su exposición a los vectores de ataque
Descripción	El usuario podrá que tan expuesta se encuentra la organización a los vectores de ataque según el DBIR.

Tabla 7

Requerimiento funcional usuario visualiza exposición al ciber-riesgo

Prioridad	Alta
Identificación del Requerimiento	RF07
Nombre	Usuario podrá visualizar su exposición al ciber-riesgo
Descripción	El usuario podrá que en términos cuantitativos cuánto podría perder la organización en caso de que ocurra un incidente.

Tabla 8

Requerimiento funcional usuario visualiza plan de acción

Prioridad	Alta
Identificación del Requerimiento	RF08
Nombre	Usuario podrá visualizar su plan de mejora
Descripción	El usuario podrá conocer el plan propuesto para mejorar su nivel de ciberseguridad.

Tabla 9

Requerimiento funcional usuario visualiza preparación para un ataque de ransomware

Prioridad	Alta
Identificación del Requerimiento	RF09
Nombre	Usuario podrá visualizar preparación para un ataque de Ransomware
Descripción	El usuario podrá conocer que tan preparado se encuentra para responder ante un eventual ataque de ransomware.

Los requerimientos no funcionales se seleccionaron basados en las necesidades de los usuarios respecto al diligenciamiento de la evaluación y la consulta de los resultados de esta.

Tabla 10

Requerimiento no funcional disponibilidad

Prioridad	Alta
Identificación del Requerimiento	RNF01
Nombre	Disponibilidad
Descripción	El usuario podrá acceder a la aplicación en cualquier momento del día, todos los días del año.

Tabla 11

Requerimiento no funcional autenticación

Prioridad	Alta
Identificación del Requerimiento	RNF02
Nombre	Autenticación
Descripción	Se debe garantizar la protección sobre el acceso a la aplicación.

Tabla 12

Requerimiento no funcional integridad

Prioridad	Alta
Identificación del Requerimiento	RNF03
Nombre	Integridad
Descripción	Se debe garantizar la no modificación de los resultados obtenidos, una vez realizada la evaluación.

Tabla 13

Requerimiento no funcional capacidad de uso

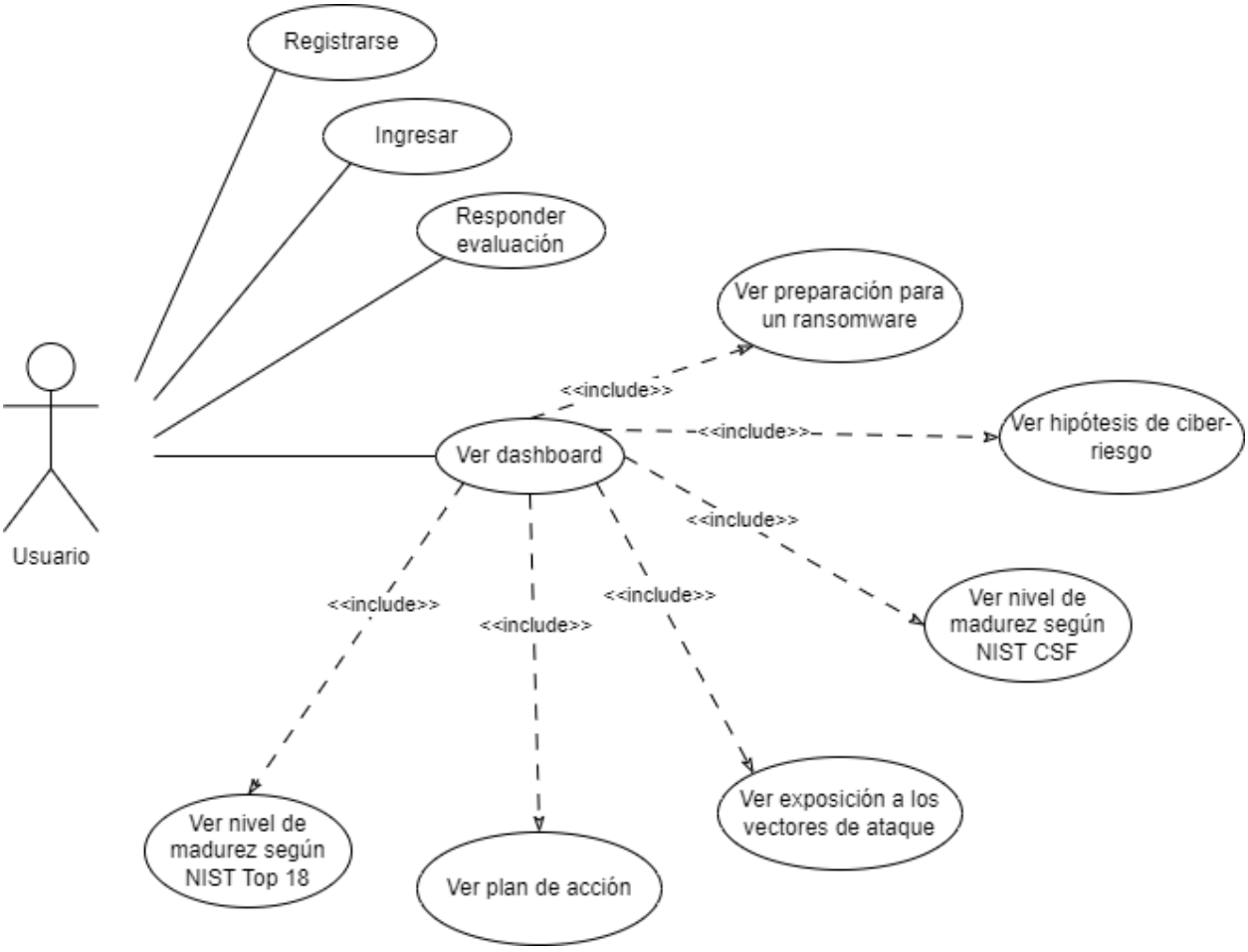
Prioridad	Alta
Identificación del Requerimiento	RNF04
Nombre	Capacidad de uso
Descripción	El sistema debe garantizar la usabilidad para todos los usuarios por lo tanto debe contar con una interfaz gráfica de fácil uso.

4.1.2. Casos de uso

El diagrama de casos de uso ofrece una vista general de todas las acciones que efectúa el usuario participante del sistema.

Figura 2

Diagrama de casos de uso

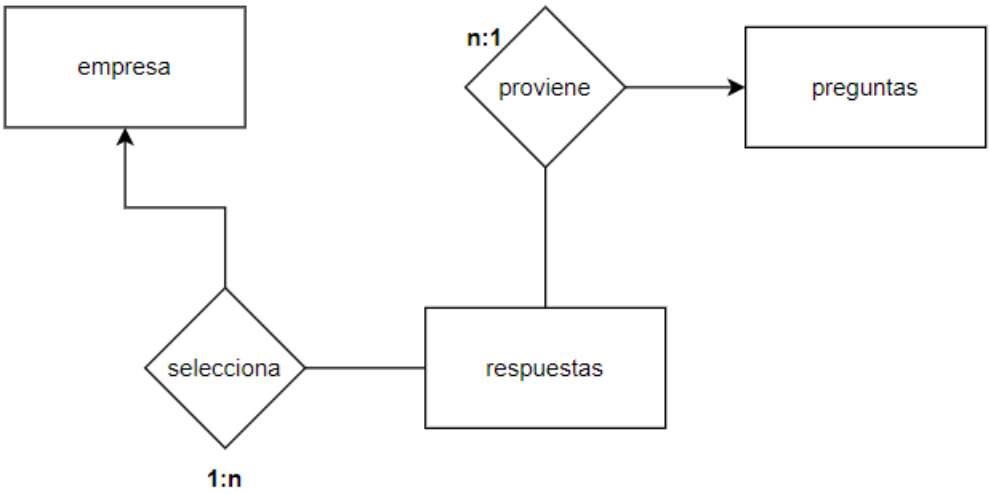


4.1.3. Diseño de diagrama entidad relación

Con el fin de entender el funcionamiento del proyecto y visualizar la interacción de la aplicación para obtener los resultados esperados, se utilizó un diagrama de entidad-relación.

Figura 3

Diagrama de entidad-relación



Como se puede observar en la figura anterior, para el funcionamiento del proyecto se utilizaron tres (3) entidades, las cuales se describen brevemente en la siguiente tabla.

Tabla 14

Descripción de entidades del proyecto

ENTIDAD	DESCRIPCIÓN
EMPRESA	Es la entidad que tiene información general sobre la empresa y la persona que está diligenciando la evaluación
PREGUNTA	Contiene las preguntas que se le realizarán al usuario junto con el tipo de ataque al que será asociada
RESPUESTA	Tendrá el valor asociado a cada opción de respuesta y las ordenará para conocer cuál es la mejor

A continuación, se enuncia cómo funcionan las relaciones presentadas en el diagrama entidad-relación de este proyecto:

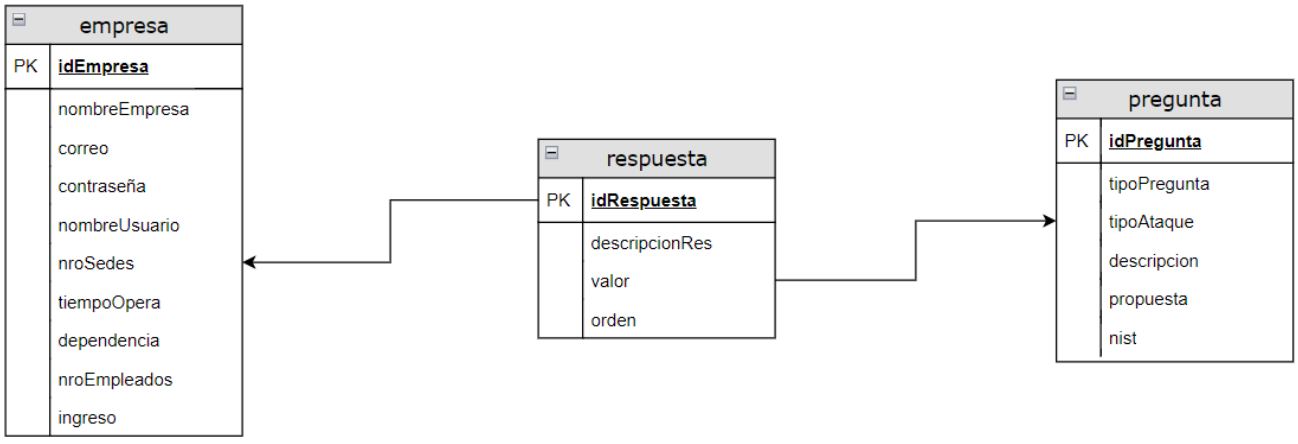
- Empresa – respuesta: Una única empresa selecciona una respuesta. Una respuesta pertenece a muchas empresas.
- Respuesta – pregunta: Una respuesta pertenece a una única pregunta. Una pregunta tiene varias opciones de respuesta.

4.1.4. Diseño de la base de datos

Al contar con el diagrama de entidad-relación, se realiza el diseño de la base de datos, donde se establecen los atributos necesarios para cada entidad

Figura 4

Diseño de la base de datos

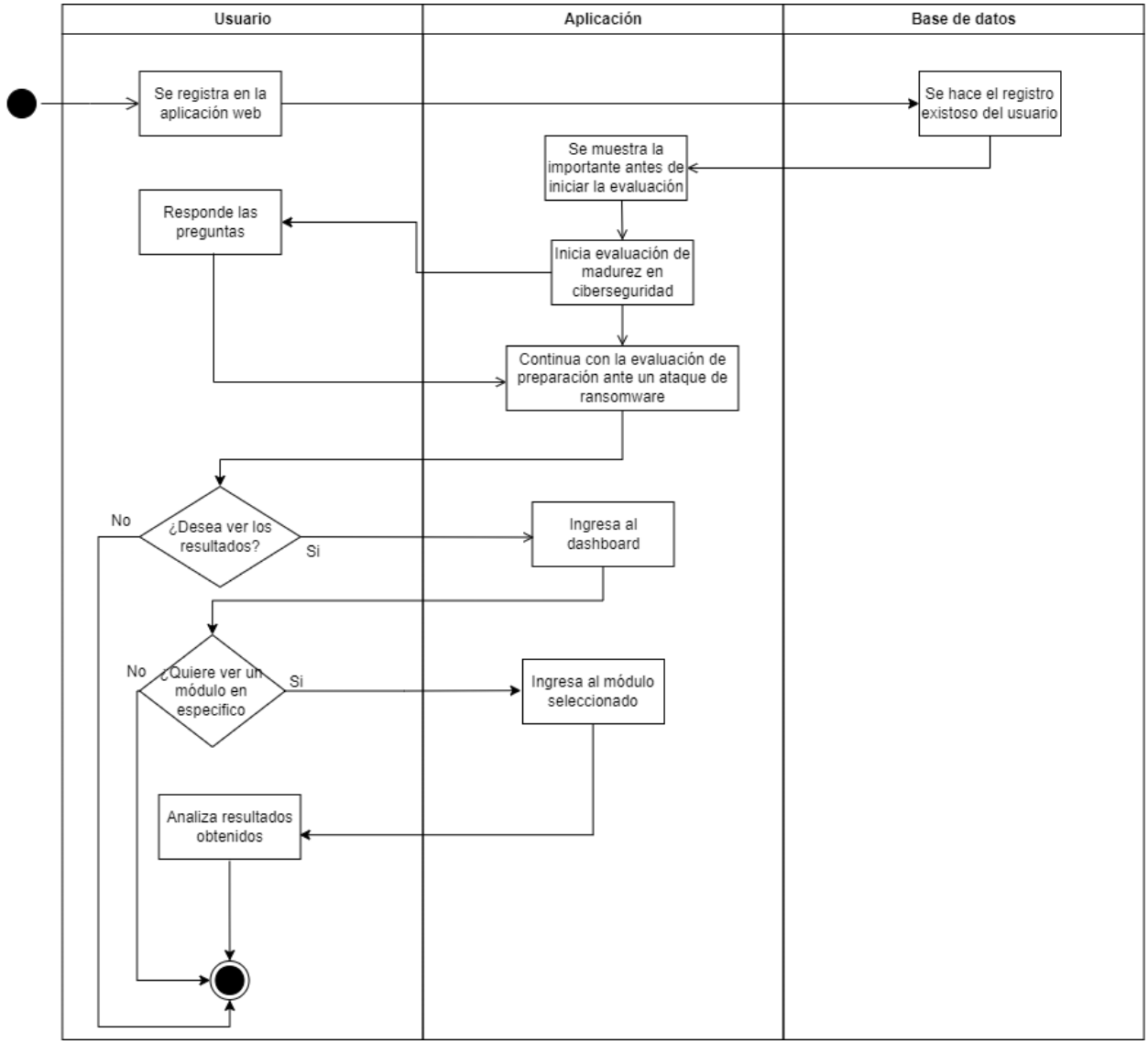


4.1.5. Diagrama de Actividades

Con el fin de comprender y describir las acciones implementadas en este proyecto, se utilizó un diagrama de actividades en lenguaje unificado de modelado (UML) para representar el funcionamiento del sistema.

Figura 5

Diagrama de actividades. Usuario utiliza por primera vez la aplicación.



4.1.6. Software

Actualmente existen diversas tecnologías y plataformas tecnológicas para trabajar al momento de desarrollar una aplicación web, teniendo en cuenta los requerimientos funcionales y no funcionales, se eligieron los siguientes elementos de software:

4.1.6.1. *Frontend*

En el mundo de la programación, hay una variedad de frameworks de JavaScript disponibles para los desarrolladores. Uno de los más populares es Angular, desarrollado por Google, que ofrece una amplia variedad de características avanzadas, como un sistema de módulos y componentes, un sistema de inyección de dependencias, un enrutador, una biblioteca de animaciones y una herramienta de pruebas unitarias. Aunque el aprendizaje de Angular puede ser más desafiante que algunos otros frameworks, como Blue JS, hay varias razones por las que podría ser una elección adecuada para una aplicación que se espera que sea inteligente y automatizada para futuros proyectos (Angular, 2023).

En particular, si se espera que la aplicación actualice automáticamente los datos de una base de datos, Angular puede ser utilizado para crear un sistema de inyección de dependencias que permita a la aplicación acceder a la base de datos de manera eficiente y sin errores. Además, la herramienta de pruebas unitarias de Angular garantiza que la aplicación funcione correctamente incluso después de futuras actualizaciones o cambios en los datos de la base de datos. En términos de escalabilidad, Angular está diseñado para manejar proyectos a gran escala con una arquitectura modular y una estructura clara (Angular, 2023).

Otro factor importante es la integración. Angular se integra bien con otras herramientas y tecnologías, como TypeScript, RxJS y Material Design. Esto lo hace ideal para proyectos que

requieren la integración con otras herramientas o para proyectos que necesitan utilizar una biblioteca específica de diseño. Además, Angular es ampliamente utilizado y tiene una comunidad activa que proporciona soporte y actualizaciones regulares. Esto significa que es fácil encontrar recursos y ayuda en línea para solucionar problemas o aprender nuevas características (U, 2022).

En resumen, aunque el aprendizaje de Angular puede ser un desafío, es una buena elección para una aplicación que se espera que sea inteligente y automatizada debido a sus características avanzadas, escalabilidad, facilidad de integración y amplio soporte comunitario. Con estas ventajas, los desarrolladores pueden crear aplicaciones más eficientes, confiables y escalables que pueden actualizarse y evolucionar con el tiempo.

Angular es un popular framework de desarrollo web de código abierto desarrollado y mantenido por Google. Está diseñado para facilitar la construcción de aplicaciones web dinámicas y de una sola página (SPA, por sus siglas en inglés), proporcionando una estructura organizada y modular para el desarrollo de componentes y servicios (Angular, 2023).

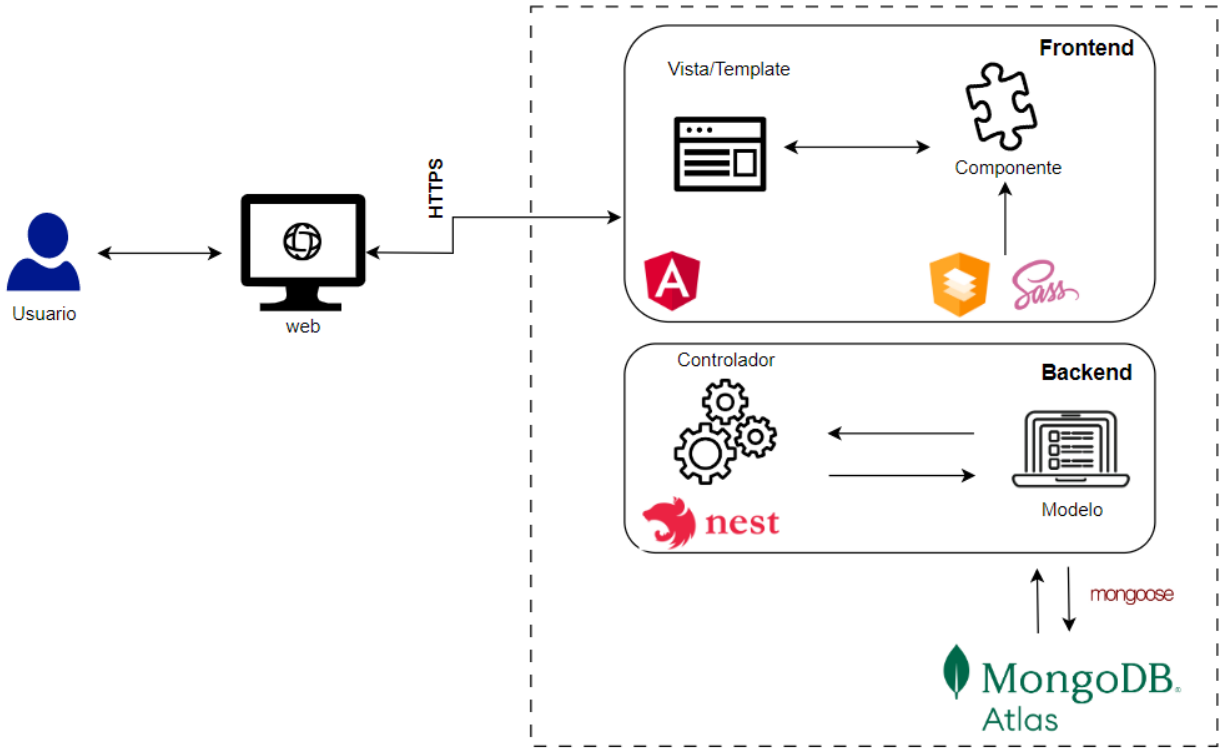
Angular está construido con TypeScript, un lenguaje de programación de tipado estático basado en JavaScript, que ofrece ventajas como la detección temprana de errores y una mejor autocompletado en los editores de código. Angular utiliza una arquitectura basada en componentes, lo que permite crear aplicaciones modulares y reutilizables, facilitando la organización y el mantenimiento del código.

El framework incluye una amplia variedad de herramientas y funcionalidades, como enlace de datos bidireccional (data binding), inyección de dependencias, directivas, manejo de eventos, rutas y navegación, así como integración con bibliotecas y servicios externos. Además, Angular cuenta

con una comunidad activa y en constante crecimiento, lo que garantiza un buen soporte, una amplia documentación y recursos para aprender y solucionar problemas.

Figura 6

Arquitectura del prototipo



4.1.6.2. Gestor de base de datos

Para elegir el gestor de base de datos para una aplicación que almacena respuestas dadas por el usuario e información de empresas, se consideró de primera mano MongoDB, ya que es una opción adecuada gracias a su flexibilidad, escalabilidad y capacidad de realizar consultas potentes. La naturaleza flexible de MongoDB, al ser una base de datos NoSQL basada en documentos, permite manejar fácilmente datos heterogéneos y esquemas dinámicos que pueden variar en formato y contenido. La escalabilidad de MongoDB, tanto horizontal como verticalmente, asegura

que la aplicación pueda manejar grandes cantidades de datos y crecer de manera eficiente conforme aumenta el número de usuarios y respuestas almacenadas. Por último, el lenguaje de consulta expresivo o versátil que ofrece MongoDB facilita la realización de consultas complejas, por medio de la búsqueda de datos específicos en función de diferentes criterios, lo que resulta útil al gestionar respuestas de usuarios e información de empresas y usuarios (MongoDB Atlas, 2023). Estas características convierten a MongoDB en una solución efectiva, adaptable para manejar y gestionar los datos de esta aplicación.

MongoDB es un sistema de gestión de bases de datos (DBMS) de código abierto, orientado a documentos y basado en la tecnología NoSQL. A diferencia de las bases de datos relacionales tradicionales, que utilizan tablas para almacenar datos, MongoDB utiliza una estructura basada en documentos JSON, lo que permite una mayor flexibilidad en la representación y almacenamiento de datos (MongoDB Atlas, 2023).

Algunas características principales de MongoDB son:

- Flexibilidad en el esquema: MongoDB no requiere que todos los documentos en una colección tengan la misma estructura, lo que permite almacenar datos con diferentes campos y estructuras sin tener que modificar un esquema predefinido.
- Escalabilidad: MongoDB es altamente escalable y admite la escalabilidad horizontal mediante la fragmentación (sharding) y la replicación de datos en múltiples servidores, lo que facilita el manejo de grandes cantidades de datos y el crecimiento de la aplicación.
- Rendimiento: MongoDB está optimizado para un alto rendimiento en operaciones de lectura y escritura, proporcionando una experiencia de usuario fluida al almacenar y recuperar datos.

- Consultas potentes: MongoDB ofrece un lenguaje de consulta expresivo y versátil que permite realizar consultas complejas y filtrar datos de manera eficiente.
- Comunidad y soporte: MongoDB cuenta con una comunidad activa y en constante crecimiento, lo que garantiza un buen soporte, una amplia documentación y recursos para aprender y solucionar problemas.

MongoDB es ampliamente utilizado en aplicaciones web y móviles modernas debido a su flexibilidad, escalabilidad y rendimiento. Es compatible con varios lenguajes de programación y se integra fácilmente con diferentes tecnologías y entornos de desarrollo (MongoDB Atlas, 2023).

5.1.6.3. Backend

Al diseñar el backend de la aplicación, se consideraron tres frameworks principales: Node.js, Nest y Django. Cada uno de estos frameworks ofrecían características y ventajas específicas, pero después de un análisis detenido, se tomó la decisión de utilizar Nest para el desarrollo del backend. La elección de Nest se basó en su facilidad de uso, así como en su capacidad para proporcionar una arquitectura sólida y modular que facilita la creación y el mantenimiento de la aplicación. Nest, construido sobre Node.js, combina elementos de programación orientada a objetos, programación funcional y programación reactiva, lo que resulta en un entorno de desarrollo versátil y eficiente para abordar las necesidades específicas del proyecto (Nest JS, 2023).

Nest es un framework de desarrollo backend de código abierto para aplicaciones Node.js que está construido sobre TypeScript (Nest JS, 2023). Fue diseñado para proporcionar una arquitectura escalable y modular para la creación de aplicaciones web y API eficientes y de alto rendimiento. Nest es conocido por su enfoque en la programación orientada a objetos, la programación funcional

y la programación reactiva, lo que permite a los desarrolladores crear aplicaciones bien estructuradas y organizadas.

Nest utiliza el patrón de diseño de inyección de dependencias, inspirado en *frameworks* como Angular, lo que facilita la separación de responsabilidades y la reutilización de código en toda la aplicación. Además, Nest es compatible con una amplia variedad de bibliotecas y herramientas de Node.js y JavaScript, lo que permite a los desarrolladores aprovechar el ecosistema existente y agregar funcionalidades adicionales según sea necesario.

El uso de TypeScript en Nest proporciona las ventajas del tipado estático, lo que facilita la detección temprana de errores y ofrece una mejor autocompletado en los editores de código. También ayuda a mejorar la legibilidad y el mantenimiento del código a medida que las aplicaciones crecen en tamaño y complejidad.

En resumen, Nest es un framework de desarrollo backend para Node.js que ofrece una arquitectura modular y escalable, facilitando la creación de aplicaciones web y API eficientes y bien organizadas.

4.1.7. Planteamiento de preguntas a realizar

Dado que esta etapa es la principal para el funcionamiento de la aplicación, se llevaron discusiones sobre cuál debe ser el documento guía para el cálculo de los resultados, se llegó a la conclusión de que se daría prioridad a los dieciocho controles de CIS, donde cada uno de estos se mapea de acuerdo las cinco funciones de NIST y los patrones de ataque. Adicionalmente, se crearon las preguntas que permiten determinar la preparación de las instituciones ante un eventual ataque de *ransomware*. Cabe destacar que uno de los resultados esperados de esta evaluación es la

creación de un mapa de ruta, para esto por cada uno de los controles se mapeó una propuesta específica. Para finalizar, la hipótesis del ciber-riesgo se calcula teniendo como base datos importantes para la funcionalidad de la institución, siempre teniendo en consideración que esta hipótesis se plantea para eventuales ataques de ciberseguridad. A continuación, se enuncia cuáles fueron los criterios realizar esta aplicación.

4.1.7.1. Información general

Antes de iniciar la evaluación de ciberseguridad, es importante contar con información general de la organización que es útil para los puntos que se tratan posteriormente. El usuario solo tiene que responder estas preguntas una vez y la aplicación se encarga del resto. La información necesaria es la siguiente:

1. Nombre de la institución.
2. Cantidad de sedes de la organización.
3. Tiempo de operación de la institución.
4. Horas que la organización puede operar sin tecnología.
5. Cantidad de empleados que forman parte de la organización.
6. Ingreso del último año.

Estas preguntas son de obligatoria respuesta para poder continuar con la evaluación. La información sobre la dependencia tecnológica y el ingreso del último año sirve para calcular la cuantificación del ciberriesgo.

4.1.7.2. Controles según CIS Top 18

El Centro para Internet Seguro (CIS), por sus siglas en inglés (Center for Internet Security), en su última versión ha combinado y consolidado los controles CIS por actividades, en lugar de por quién administra los dispositivos (Los 18 Controles Críticos de Seguridad CIS, 2021). A continuación se presenta la lista de dieciocho controles, junto con una breve descripción de su objetivo, lo cual nos brinda un total de dieciocho preguntas (18) para esta evaluación.

Tabla 15

Objetivos de los controles de CIS

No.	CONTROL	OBJETIVO
1	Inventario y control de los activos de la empresa	Administrar activamente (inventario, seguimiento y corrección) todos los activos de la empresa (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/Internet de las cosas (IoT); y servidores) conectados a la infraestructura física, virtual, remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también ayudará a identificar activos no autorizados y no administrados para eliminar o remediar.
2	Inventario y control de activos de software	Administrar activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) en la red para que sólo el software autorizado sea instalado y se pueda ejecutar, y que todo el software no autorizado y no administrado que se encuentre, inmediatamente se evite su instalación o ejecución.
3	Protección de datos	Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y disponer de forma segura los datos.
4	Configuración segura de activos y software de la empresa	Establecer y mantener la configuración segura de los activos de la empresa (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (sistemas operativos y aplicaciones).
5	Gestión de cuentas	Utilizar procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, los activos y el software de la empresa.
6	Gestión del control de acceso	Utilizar procesos y herramientas para crear, asignar, administrar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio para activos y software empresariales.

7	Gestión continua de vulnerabilidades	Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, a fin de remediar y minimizar la ventana de oportunidad para los atacantes. Supervise las fuentes de la industria pública y privada para obtener información nueva sobre amenazas y vulnerabilidades.
8	Administración del registro de auditoría	Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.
9	Protecciones de correo electrónico y navegador web	Mejorar las protecciones y las detecciones de amenazas del correo electrónico y los vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través del compromiso directo.
10	Defensas contra malware	Evitar o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en los activos de la empresa.
11	Recuperación de datos	Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales incluidos en el alcance a un estado de confianza y anterior al incidente.
12	Gestión de la infraestructura de red	Establecer, implementar y administrar activamente (rastree, informe, corrija) los dispositivos de red para evitar que los atacantes exploten los puntos de acceso y los servicios de red vulnerables.
13	Monitoreo y defensa de la red	Operar procesos y herramientas para establecer y mantener un monitoreo integral de la red y defensa contra amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.
14	Sensibilización sobre seguridad y capacitación en habilidades	Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de la fuerza laboral para que sea consciente de la seguridad y tenga las habilidades adecuadas para reducir los riesgos de seguridad cibernética de la empresa.
15	Gestión de proveedores de servicios	Desarrollar un proceso para evaluar a los proveedores de servicios que tienen datos confidenciales, o son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores estén protegiendo esas plataformas y datos de manera adecuada.
16	Seguridad del software de aplicación	Administrar el ciclo de vida de seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y remediar las debilidades de seguridad antes de que puedan afectar a la empresa.
17	Gestión de respuesta a incidentes	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (p. ej., políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para prepararse, detectar y responder rápidamente a un ataque.
18	Pruebas de penetración	Probar la eficacia y la resistencia de los activos de la empresa identificando y explotando las debilidades en los controles (personas, procesos y tecnología) y simulando los objetivos y las acciones de un atacante.

Teniendo claro cada uno de los objetivos de los controles, se plantea una única pregunta a realizar al usuario con el fin de que este cuente con cinco opciones de respuesta para cada pregunta.

En la Tabla 16 se muestra cual es la pregunta que se le plantea al usuario por cada control, mientras que en la Tabla 17 se muestra por cada control, cuál es la función de NIST CSF asociada y por qué, para finalizar con esta etapa de definición de preguntas se plantearon según las etapas de un ataque de ransomware, una evaluación que consta de catorce preguntas, que se puede encontrar en la Tabla 18

Tabla 16

Pregunta por control al usuario

No.	Control	Pregunta
1	Inventario y control de los activos de la empresa	¿Existe un inventario de activos detallado y actualizado?
2	Inventario y control de activos de software	¿Existe un inventario de software detallado y este mismo debidamente actualizado?
3	Protección de datos	¿Se implementa una solución de prevención de pérdida de datos (DLP) y sigue la política de proceso de clasificación de datos?
4	Configuración segura de activos y software de la empresa	¿Aplican guías de fortalecimiento a los activos empresariales (Endpoint, IoT, Servidores, Móvil, etc.)?
5	Gestión de cuentas	¿Cuenta con un directorio activo debidamente administrado?
6	Gestión del control de acceso	¿Implementa controles de acceso basado en roles (RBAC) para decidir el tipo de privilegios que se asignarán a los diferentes tipos de cuentas?
7	Gestión continua de vulnerabilidades	¿Realiza análisis de vulnerabilidades al menos dos veces al año y cuenta con un proceso para la mitigación de las vulnerabilidades encontradas?
8	Administración del registro de auditoría	¿Cuenta con un Centro de Operaciones de Seguridad (SOC) que está monitoreando eventos de seguridad 24x7 para anticipar, alertar y notificar sobre incidentes de ciberseguridad?
9	Protecciones de correo electrónico y navegador web	¿Cuenta con reglas de firewall para restringir la navegación a sitios web no confiables y/o correos de dudosa procedencia?
10	Defensas contra malware	¿Cuenta con un Endpoint Detection & Response (EDR) que esté constantemente monitoreando los endpoints para mitigar ciber-amenazas?

11	Recuperación de datos	¿Cuenta con un proceso debidamente comprobado para la recuperación de datos en caso de un ataque cibernético?
12	Gestión de la infraestructura de red	¿Aplican guías de endurecimiento a los dispositivos de red?
13	Monitoreo y defensa de la red	¿Cuenta con la tecnología Extended Detection & Response (XDR) desplegada en la red que recopila y correlaciona automáticamente datos en múltiples capas de seguridad?
14	Sensibilización sobre seguridad y capacitación en habilidades	¿Dentro de la organización se tiene establecido y se mantiene un programa de concientización a usuarios sobre seguridad de la información?
15	Gestión de proveedores de servicios	¿Mantiene monitoreada la dark y deep web, supervisando y evaluando la reputación de los proveedores de servicios?
16	Seguridad del software de aplicación	¿Desarrolla sus aplicaciones utilizando las mejores prácticas de ciberseguridad como OWASP Top 10 y las prueba antes de pasarlas a producción?
17	Gestión de respuesta a incidentes	¿Cuenta con un equipo y plan de respuesta a incidentes?
18	Pruebas de penetración	¿Realiza pruebas de penetración a la red interna, externa, wifi y aplicativos web y móviles que posee?

4.1.7.3. Funciones de NIST CSF mapeada a los controles

Antes de categorizar cada uno de los controles del CIS Top 18, es importante tener clara la definición de cada una de las funciones del marco de referencia NIST (National Institute of Standards and Technology, 2018). NIST define cada una de las funciones de la siguiente manera:

- **Identificar:** Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.
- **Proteger:** Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.
- **Detectar:** Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

- **Responder:** Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.
- **Recuperar:** 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 seguridad cibernética.

Tabla 17

Funciones de NIST según los controles de CIS Top 18

NIST CSF	CIS Top 18	¿Por qué?
ID	1: Inventario y control de los activos de la empresa	Es importante como parte inicial de cualquier evaluación tener definido el alcance, es decir tener un control sobre lo que se va a evaluar. En este caso toda la organización.
ID	2: Inventario y control de activos de software	Es importante como parte inicial de cualquier evaluación tener definido el alcance, es decir tener un control sobre lo que se va a evaluar. En este caso toda la organización.
PRO	3: Protección de datos	Como su nombre lo indica, se basa en la protección. Una vez la organización tiene conocimiento de lo que tiene, debe contar con un mecanismo para protegerlo
PRO	4: Configuración segura de activos y software de la empresa	Las herramientas por si solas no representan mayor seguridad, con un debido manejo de estas es posible proteger a la organización.
ID	5: Gestión de cuentas	Es importante como parte inicial de cualquier evaluación tener definido el alcance, es decir tener un control sobre lo que se va a evaluar. En este caso gestionar las cuentas de los usuarios, utilizando mejores prácticas de seguridad.
PRO	6: Gestión del control de acceso	Las cuentas deben contar con mejores prácticas como el mínimo privilegio, con el fin de que los usuarios tengan los permisos precisos para realizar cada una de sus labores.
PRO	7: Gestión continua de vulnerabilidades	Las herramientas por si solas no representan mayor seguridad, con un escaneo de cómo se encuentran los activos informáticos según todas las vulnerabilidades que salen diariamente en el mercado tendrá una mejor visión y estará protegido si realizó las debidas mitigaciones.
DET	8: Administración del registro de auditoría	El manejo de logs o registros es muy importante para detectar actividad anómala o fuera de lo común dentro de la red

PRO	9: Protecciones de correo electrónico y navegador web	Las herramientas por si solas no representan mayor seguridad, con un debido manejo de estas es posible proteger a la organización.
RES	10: Defensas contra malware	La protección en algunos casos no es suficiente, es por esto que si se detecta alguna anomalía o malware dentro de la organización, debe contar con la capacidad de responder para contener la expansión de este.
REC	11: Recuperación de datos	Si ocurre alguna brecha de seguridad, es importante la recuperación rápida de los datos ya que cada momento fuera de operación representa una pérdida monetaria significativa para la organización.
PRO	12: Gestión de la infraestructura de red	Las herramientas por si solas no representan mayor seguridad, con un debido manejo de estas es posible proteger a la organización.
RES	13: Monitoreo y defensa de la red	La protección en algunos casos no es suficiente, es por esto que si se detecta alguna anomalía o malware dentro de la organización, debe contar con la capacidad de responder para contener la expansión de este.
PRO	14: Sensibilización sobre seguridad y capacitación en habilidades	Los seres humanos son el eslabón más débil de toda organización y a su vez el más fundamental, es por esto por lo que una constante capacitación de seguridad de la información y ciberseguridad es vital para proteger a la organización.
DET	15: Gestión de proveedores de servicios	Es muy importante contar con conocimiento de cómo se encuentran actualmente los proveedores de servicios, con el fin de verificar que no exista ninguna fuga de información que pueda afectar la reputación y/o operación de la organización.
PRO	16: Seguridad del software de aplicación	Las herramientas por si solas no representan mayor seguridad, con un debido manejo de estas es posible proteger a la organización.
RES	17: Gestión de respuesta a incidentes	La protección en algunos casos no es suficiente, es por esto que si se detecta alguna anomalía o malware dentro de la organización, debe contar con la capacidad de responder para contener la expansión de este.
ID	18: Pruebas de penetración	La organización debe identificar si las líneas de defensa que tiene actualmente son suficientes para detectar, proteger y responder ante un eventual ataque cibernético.

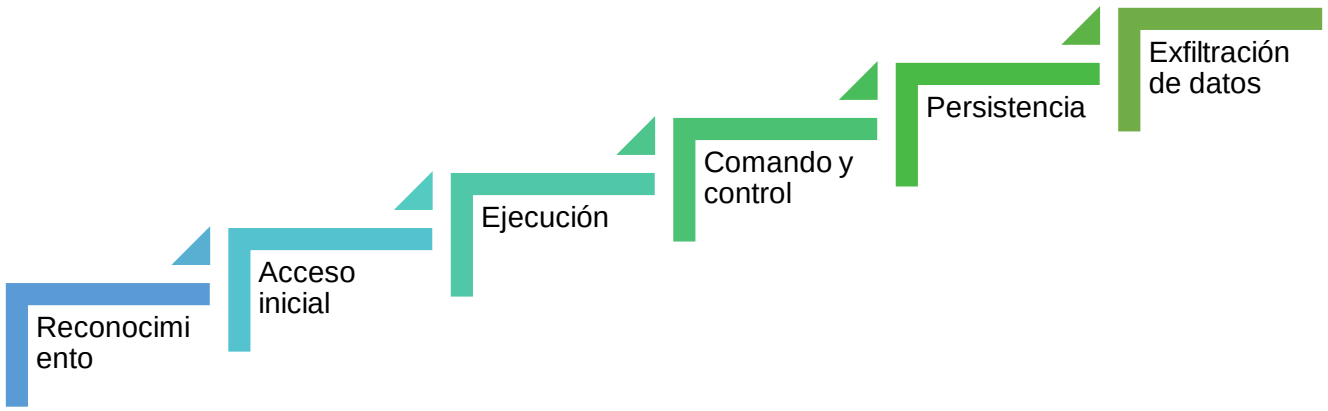
4.1.7.4. Preparación ante un ataque de *ransomware*

Un ataque de ransomware es un tipo de ciberataque sofisticado que busca cifrar la información y exigir un rescate a cambio de descifrarla (CISA, 2023). Se han identificado seis (6) etapas en un

ataque de ransomware, utilizando diversas fuentes como la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) de Estados Unidos, el FBI, la Agencia de Seguridad Nacional (NSA) y el Servicio Secreto de Estados Unidos (USSS). Estas etapas comienzan con una fase de reconocimiento y finalizan con la exfiltración de datos. Por lo tanto, es importante tener en cuenta la metodología que utiliza un ciber atacante para obtener el control de la red, cifrar los datos, exigir un rescate y, en algunos casos, exfiltrar los datos si no se recibe el pago solicitado, antes de plantear las preguntas al usuario.

Figura 7

Fases de un ataque de ransomware



- **Reconocimiento:** En esta etapa los actores maliciosos hacen uso de la ingeniería social, (como phishing) para llegar a sus víctimas.
- **Acceso inicial:** Utilizando las contraseñas débiles y la suplantación de identidad los actores maliciosos logran acceder a la red.
- **Ejecución:** Cuando las víctimas abren aquel correo malicioso, éste descarga malware y se realizan explotaciones de vulnerabilidades.

- **Comando y control:** En esta fase, ya los atacantes se encuentran dentro de la red y se comunican con dispositivos maliciosos.
- **Persistencia:** Utilizando un protocolo de escritorio remoto y credenciales robadas, los atacantes pueden obtener acceso a la red, donde proceden a cargar un DLL cifrado en la memoria y lo ejecutan.
- **Exfiltración de datos:** Los atacantes una vez dentro y con control sobre la red puede realizar múltiples daños, como buscar información sensible/valiosa y extraerla.

Teniendo ya claro cómo funciona un ataque de ransomware, se plantearon seis (6) preguntas y se utilizaron como base algunas de las planteadas según los controles de CIS Top 18. En la Tabla 18 se pueden encontrar todas las preguntas que harán parte de esta evaluación.

Tabla 18

Preguntas según la metodología de un ataque de ransomware

Metodología	**Pregunta**
Reconocimiento	¿Realiza pruebas de ingeniería social (como phishing) a sus usuarios? ¿Dentro de la organización se tiene establecido y se mantiene un programa de concientización a usuarios sobre seguridad de la información?
Acceso inicial	¿Tiene desactivadas cuentas de usuario dentro de la organización inactivas? ¿Cuenta con reglas de firewall para restringir la navegación a sitios web no confiables y/o correos de dudosa procedencia?
Ejecución	¿Su organización cuenta con actualizaciones automatizadas periódicamente para su software y sistemas? ¿Realiza análisis de vulnerabilidades al menos dos veces al año y cuenta con un proceso para la mitigación de las vulnerabilidades encontradas?

Comando y control	¿Cuenta con un Centro de Operaciones de Seguridad (SOC) que está monitoreando eventos de seguridad 24x7 para anticipar, alertar y notificar sobre incidentes de ciberseguridad en el EDR? ¿Aplican guías de fortalecimiento a los activos empresariales (Endpoint, IoT, Servidores, Móvil, etc.)? ¿Cuenta con un Endpoint Detection & Response (EDR) que esté constantemente monitoreando los endpoints para mitigar ciber-amenazas?
Persistencia	¿Cuenta con un Network Detection & Response (NDR) para detectar comportamientos anómalos en la red?
Exfiltración de datos	¿Su organización tiene una póliza de seguro cibernético que cubre los ataques de Ransomware? ¿Su organización tiene copias de seguridad programadas regularmente? ¿Cuenta con un proceso debidamente comprobado para la recuperación de datos en caso de un ataque cibernético? ¿Cuenta con un equipo y plan de respuesta a incidentes de ransomware?

Para cada una de las preguntas parte de este proyecto de investigación, se plantearon cinco (5) posibles opciones de respuesta, donde cada una de ellas hace referencia al nivel de funcionamiento de las medidas de seguridad actuales y se les asignó un valor que va desde el cero (0) hasta el cien (100) distribuido equitativamente. En la Tabla 19 se muestra cómo se plantean las opciones de respuesta.

Tabla 19

Opciones de respuesta

Valor	Respuesta	Comentario
0	No, inexistente.	No existe o no funciona, la herramienta no hace lo que debería
25	Si, en forma reactiva.	Sólo cuando lo piden altos mandos, por auditoría o cumplimiento
50	Si, algunas veces.	Existe pero no se hace lo que se debe
75	Si, en forma proactiva.	Si se hace pero no ayuda a prevenir incidentes
100	Si, en forma anticipatoria a futuros incidentes.	Si, se hace para prevenir incidentes

Con esta definición de opciones de respuesta se finaliza el planteamiento de las preguntas a realizar al usuario para poder dar paso a la lógica que da sentido a estas preguntas y es el apoyo para la institución al sugerir un plan de mejora por cada uno de los controles en los cuales se encuentra más vulnerable.

Dado que este proyecto también toma como base el reporte del DBIR de Verizon más actual, que para fecha de redacción de este documento y ejecución de este proyecto es el 2022 lanzado en mayo de este mismo año. Para el sector educativo se tienen mapeados tres (3) vectores de ataque que representan el 80% de las brechas, los cuales son, intrusión al sistema, ataques básicos a aplicaciones web y errores misceláneos. En la Tabla 20 se realiza un resumen de lo que dice el DBIR 2022 sobre los vectores de ataque que están afectando al sector educativo.

Tabla 20

Vectores de ataque en el sector educativo según el DBIR 2022

Vector de ataque	Descripción
Intrusión al sistema	Este patrón consiste en infracciones y ataques más complejos que aprovechan una combinación de varias acciones diferentes, como social, m*alware* y hacking.
Ataques básicos a aplicaciones web	Los ataques dentro de este patrón se dividen entre dos áreas. Los medios de acceso al servidor, como el uso de credenciales robadas, la explotación de vulnerabilidades y las contraseñas de fuerza bruta constituyen los primeros. El segundo representa la carga útil específica, como las puertas traseras, que se utilizan para mantener la persistencia o monetizar el acceso.
Errores misceláneos	Este patrón es basado en las personas internas de la organización que son susceptibles a cometer errores, bien sea de configuración o de entrega de información a personas no autorizadas.

4.1.7.5. Cuantificación del ciberriesgo

La aplicación también tiene como objetivo generar conciencia en los altos mandos de las instituciones educativas, y por ello incluye un apartado que aborda de manera cuantitativa el costo que podría conllevar para la organización en caso de materializarse el riesgo. Para determinar esto, se utilizan elementos clave, como el ingreso financiero del último año (RN) y el porcentaje de dependencia tecnológica (DT) del negocio. La combinación de estos elementos permite obtener una visión clara y precisa de los riesgos que enfrenta una organización en términos de ciberseguridad, lo que facilita la toma de medidas para protegerla de posibles ataques.

La fórmula planteada es la siguiente

$$CCR = \big((RN * DT)\big)$$

Esta fórmula permite calcular de manera precisa y detallada el costo que una organización puede enfrentar al sufrir un ataque cibernético, tomando en consideración los elementos previamente mencionados, como el ingreso financiero del último año (RN) y el porcentaje de dependencia tecnológica (DT) del negocio. Al calcular el CCR, las organizaciones pueden tomar decisiones informadas y eficaces en cuanto a la protección de su información y activos en línea.

4.2. Diseño

Con base en los pasos anteriores, se procede a diseñar la apariencia de la aplicación para que sea amigable e interactiva con el usuario. Se utiliza la plataforma Figma para crear un diseño UX/UI que sea sencillo y limpio, evitando sobrecargar al usuario con animaciones innecesarias y centrándose en lo que es importante. La página principal de la aplicación cuenta con el nombre de la aplicación y un botón para comenzar con la evaluación, como se muestra en la Figura 1. Dado que el acrónimo de la aplicación es CAT, se utiliza la representación de un gato como anfitrión de la aplicación, que está visible en momentos de interacción con el usuario.

Se eligió el diseño basado en stepper, ya que se buscaba mantener un enfoque claro y centrado en los pasos necesarios para llevar a cabo la evaluación y mejora de la postura de ciberseguridad. Cada paso o sección del stepper está diseñado de forma clara y concisa, con la información necesaria y los elementos de interacción relevantes para ese paso específico. Esto ayuda a evitar la sobrecarga de información y permite que el usuario se enfoque en cada aspecto de la evaluación de forma individual, lo que facilita la comprensión y toma de decisiones informadas.

En cuanto al diseño visual, se ha optado por un estilo sencillo y limpio, con un enfoque minimalista para evitar distracciones y mantener el enfoque en la información y acciones

importantes. El uso del nombre de la aplicación y un botón para comenzar con la evaluación en la página principal es claro y directo, lo que permite al usuario comenzar fácilmente el proceso de evaluación.

Además, la inclusión de un personaje animado, en este caso un gato, como anfitrión de la aplicación puede añadir un elemento lúdico y atractivo para el usuario, lo que puede hacer que la experiencia de la aplicación sea más interesante y agradable. El gato puede aparecer en momentos clave de interacción con el usuario, como ofrecer consejos o brindar retroalimentación, lo que puede ayudar a mantener el interés y la participación del usuario en la aplicación.

En resumen, el diseño basado en un stepper, junto con un estilo visual sencillo y limpio, y la inclusión de un personaje animado como anfitrión, proporciona una experiencia de usuario guiada, clara y atractiva para el usuario, fomentando la conciencia sobre la importancia de la ciberseguridad en el sector educativo y facilitando la evaluación y mejora de la postura de ciberseguridad de la institución.

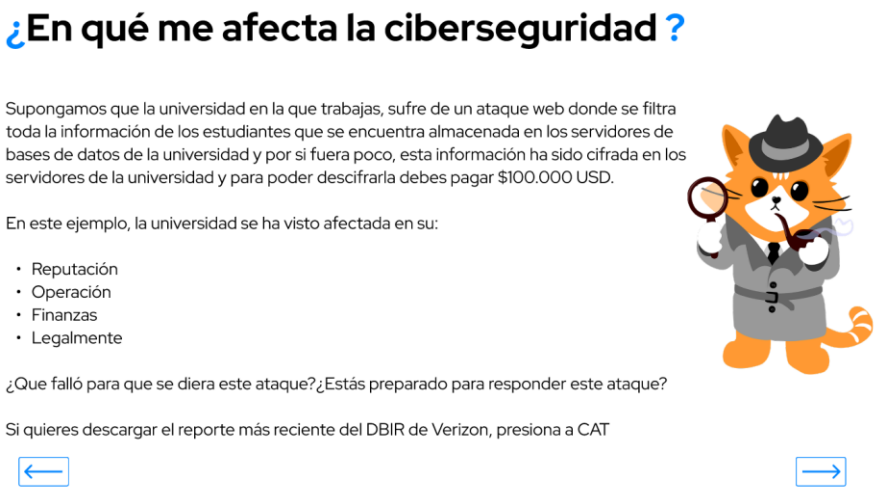
Figura 8

Prototipo página principal

Como fue mencionado anteriormente, en aquellos momentos en que sea necesario dar información importante, se utiliza un gato para captar la atención y curiosidad del usuario. En una de las etapas iniciales de la aplicación, se hizo referencia a la pregunta más escuchada en el área de ciberseguridad al momento de presentar su importancia ante una junta directiva e incluso ante el personal dentro de la organización: ¿esto en qué me afecta? Haciendo énfasis en que su única preocupación es no verse afectado o no tener nada que perder. En la Figura 2 se puede dar un rápido vistazo de lo que se aborda con esta pregunta y cómo un gato vestido de detective es aquel que explica la importancia de la ciberseguridad. Recordemos que lo que se está mostrando a continuación es el prototipo planteado, más no el producto final, teniendo en cuenta que para llegar al producto final es necesario tener el prototipo y evitar improvisar. Durante esta etapa inicial, informativa, se disponen de diversos enlaces con información interesante e importante que puede utilizar el usuario para instruirse y tener un conocimiento más amplio en este campo de la ciberseguridad.

Figura 9

¿En qué me afecta la ciberseguridad?



Una vez finalizada esta etapa informativa, se inicia la evaluación propiamente dicha, donde el usuario debe responder a las preguntas planteadas anteriormente. Esta vista busca no sobrecargar al usuario con información, pero es necesario que complete la información general básica para la evaluación. En la Figura 3 se encuentra la información catalogada como general, planteada en el apartado 4.1.7.1, y en la Figura 4 se encuentran las preguntas planteadas para toda la evaluación, que se encuentran en los apartados 4.1.7.2 y 4.1.7.4. Estas vistas son a nivel general de la aplicación, posteriormente se evidencia el panel de control donde el usuario puede consultar sus resultados cuando lo desee.

Figura 10

Información general

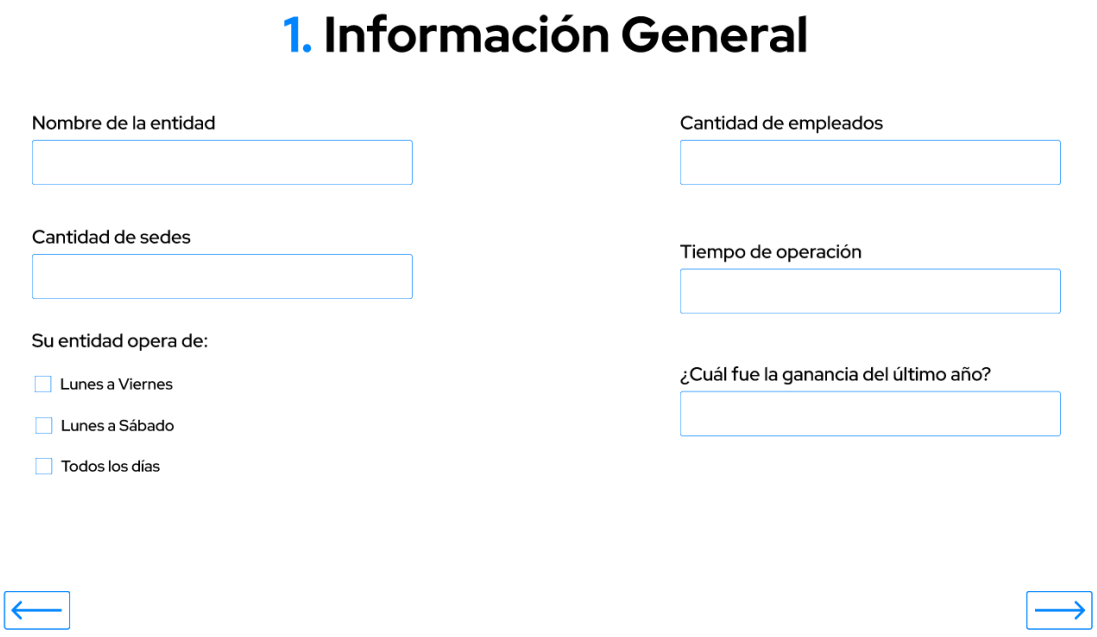
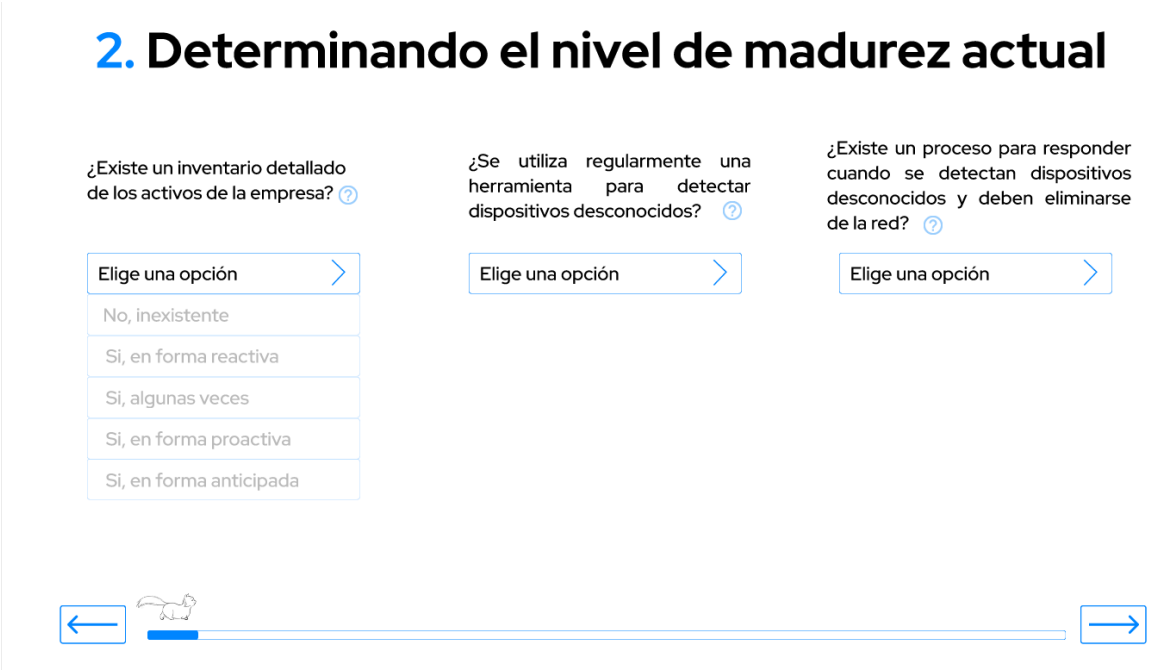


Figura 11

Determinando el nivel de madurez actual



4.2.1. Mapeo de resultados y recomendaciones

Una vez que se ha establecido la estructura de los marcos de referencia, controles y mejores prácticas en los cuales se basa este proyecto de grado, se procede a definir cómo se realizarán las mediciones de cumplimiento para cada uno de ellos. Para ello, se toman los dieciocho controles del Centro de Seguridad de Internet (CIS), las cinco funciones del Instituto Nacional de Estándares y Tecnología (NIST) mapeadas para cada uno de los controles, y se distribuyen en los vectores de ataque según el informe Verizon Data Breach Investigations Report (DBIR) de 2022, con especial énfasis en aquellos que representan la mayor cantidad de brechas en el sector.

La matriz de evaluación va tomando forma y se plantea una propuesta de mejora para cada uno de los controles, teniendo en cuenta el puntaje en los vectores de ataque de mayor peso (aquellos

que afectan al sector educativo). La Tabla 17 muestra cómo se propone una mejora para cada uno de los controles, y en la Tabla 21 se resaltan en color gris los vectores de ataque que representan la mayor cantidad de brechas en el sector. La asignación de pesos, según la respuesta del usuario, sirve como apoyo para priorizar las acciones y hacer recomendaciones al usuario al finalizar la evaluación. Es importante tener en cuenta que los valores (0-100) en la Tabla 21 son solo de referencia para tener en cuenta la distribución de cada uno de los vectores de ataque.

Tabla 21

Matriz de planteamiento del plan de mejora

NIST CSF	CIS Top 18	Basic Web App Attacks	DoS	Ransomware	Misc Errors	Priv. Misuse	Social Eng.	System Intrusion
ID	1: Inventario y control de los activos de la empresa				0%	0%		0%
ID	2: Inventario y control de activos de software					100%		100%
PRO	3: Protección de datos				25%	25%		

NIST CSF	CIS Top 18	Basic Web App Attacks	DoS	Ransomware	Misc Errors	Priv. Misuse	Social Eng.	System Intrusion
PRO	4: Configuración segura de activos y software de la empresa		25%	25%	25%	25%		25%
ID	5: Gestión de cuentas					100%		100%
PRO	6: Gestión del control de acceso				100%	100%		100%
PRO	7: Gestión continua de vulnerabilidades	25%	25%	25%	25%	25%		25%
DET	8: Administración del registro de auditoría	100%	100%	100%	100%	100%		100%
PRO	9: Protecciones de correo electrónico y navegador web			100%	100%	100%		100%
RES	10: Defensas contra malware			25%				25%
REC	11: Recuperación de datos			100%				100%

NIST CSF	CIS Top 18	Basic Web App Attacks	DoS	Ransomware	Misc Errors	Priv. Misuse	Social Eng.	System Intrusion
PRO	12: Gestión de la infraestructura de red		100%		100%	100%		100%
RES	13: Monitoreo y defensa de la red		25%		25%	25%		25%
PRO	14: Sensibilización sobre seguridad y capacitación en habilidades			100%	100%	100%	100%	100%
DET	15: Gestión de proveedores de servicios							25%
PRO	16: Seguridad del software de aplicación	100%			100%			100%
RES	17: Gestión de respuesta a incidentes	100%	100%	100%	100%	100%	100%	100%
ID	18: Pruebas de penetración	25%	25%		25%			25%

Teniendo en cuenta la distribución de esta tabla, se puede observar que existen en total cuatro (4) controles que pertenecen a la función de identificar, ocho (8) que pertenecen a la función de proteger, dos (2) que pertenecen a la función de detectar, tres (3) que pertenecen a la función de responder y uno (1) a la función de recuperar. Ahora bien, la forma en que se decidió elegir cuál sería el plan de mejora que el usuario debía seguir se basó en el control cuyo peso fuera más bajo para cada función de NIST CSF. En la Tabla 22 se puede apreciar por función de NIST el número del control perteneciente, con el fin de que sea más fácil para el lector identificar cómo se realizó este cálculo. Con esto, si para la primera categoría los controles que interactúan son el 1, 2, 5 y 18, el control con menor puntuación es el control recomendado. Se realizó de la misma forma para cada una de las funciones de NIST CSF, con el fin de recomendar al menos un control por función. En el caso de la función recuperar que solamente posee un control relacionado, se recomienda mejorar este control si su puntuación es menor a uno (1), es importante resaltar que en este caso el máximo puntaje es dos (2) dado que según la Tabla 22 en el control once (11) interactúan dos (2) patrones de ataque *ransomware* e intrusión al sistema.

Tabla 22

Controles por función de NIST

Controles por función de NIST	
Función	***Control***
Identificar	1,2,5,18
Proteger	3,4,6,7,9,12,14,16
Detectar	8,15
Responder	10,13
Recuperar	11

4.2.2. Generación del dashboard

Una vez el usuario finaliza de completar la evaluación, puede acceder a un *dashboard* de manera inmediata o ingresar a la aplicación para revisar los resultados cuando lo desee. Este *dashboard* busca darle una bienvenida a los resultados de la evaluación y la facilidad de consultar los resultados al interactuar con los módulos disponibles en la sección de la izquierda. En la Figura 12 se puede evidenciar el prototipo planteado para este *dashboard* y en la Figura 13 se puede ver el módulo de *Ransomware Readiness Assessment*, el cual es un módulo bastante interesante para la organización, ya que les indica que tan preparados se encuentran para un eventual ataque de *ransomware*, según los controles que tienen actualmente y le explica que este resultado es basado en las preguntas planteadas que están asociadas a las fases de un ataque de ransomware.

Figura 12

Dashboard de la aplicación

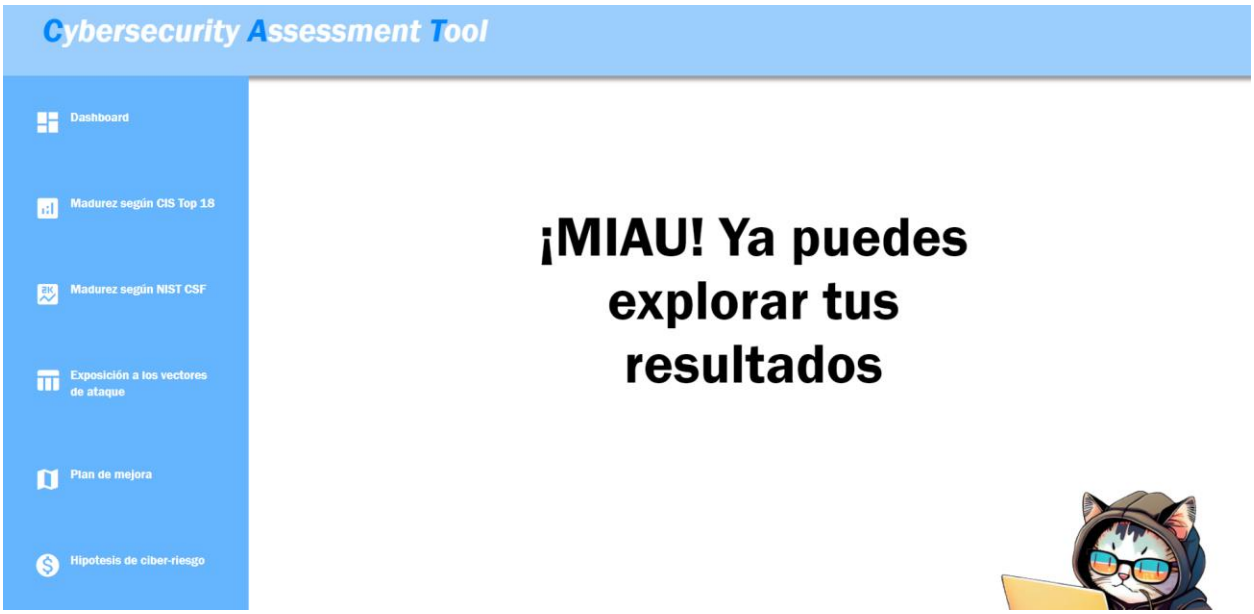
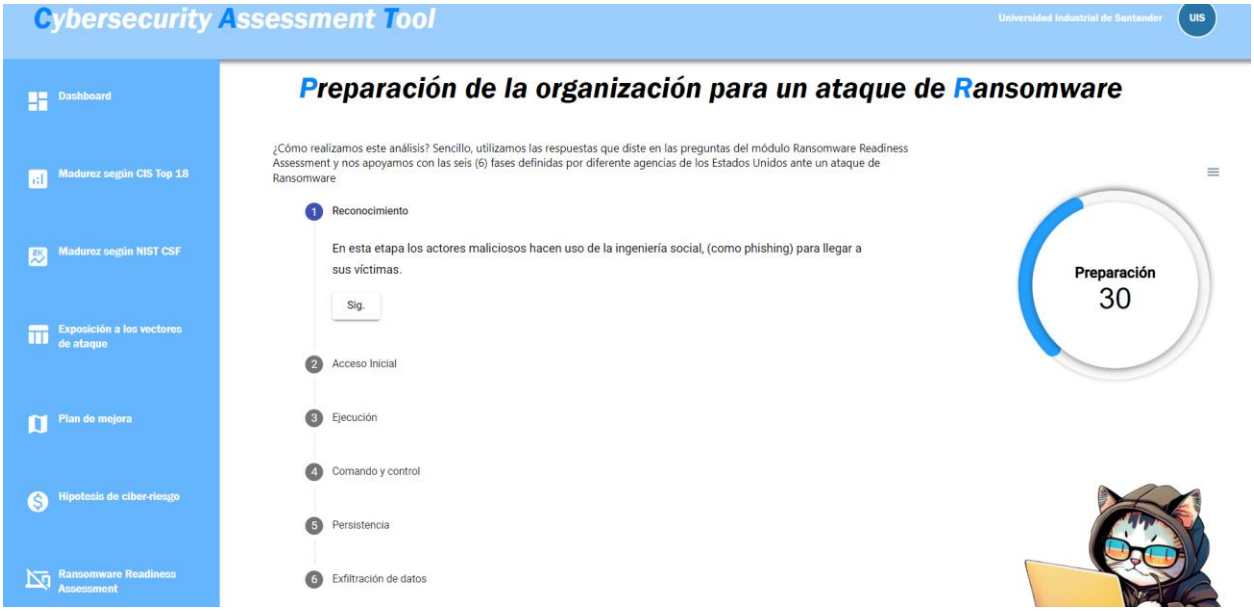


Figura 13

*Módulo de Ransomware Readiness Assessmen***t**



4.2.3. Diseño de la rutina computacional a utilizar para el cálculo de los módulos

A partir de lo que se planteó para realizar el mapeo de resultados, se diseñó la rutina que realiza el cálculo del nivel de madurez de NIST CSF y CIS Top 18, junto con los resultados para cada una de ellas.

4.2.3.1. Cálculo del nivel de madurez según CIS Top 18

Dado que se realizaron dieciocho preguntas en total, las cuales se encuentran en la El Centro para Internet Seguro (CIS), por sus siglas en inglés (Center for Internet Security), en su última versión ha combinado y consolidado los controles CIS por actividades, en lugar de por quién administra los dispositivos (Los 18 Controles Críticos de Seguridad CIS, 2021). A continuación se presenta la lista de dieciocho controles, junto con una breve descripción de su objetivo, lo cual nos brinda un total de dieciocho preguntas (18) para esta evaluación.. El cálculo se basa de acuerdo con la respuesta del usuario que varía según el estado de los controles, tal como se planteó en la Tabla

23, cuando se finalice la evaluación se realiza un promedio entre las respuestas dadas por el usuario, lo cual indica el nivel de madurez según los controles de CIS Top 18. En la Tabla 23 se plantea un escenario de ejemplo de lo que sería la respuesta del usuario a las preguntas realizadas en la evaluación, este escenario es utilizado para ejemplificar esta sección del documento.

Tabla 23

Ejemplo de cálculo nivel de madurez CIS Top 18

CIS Top 18	Respuesta
1: Inventario y control de los activos de la empresa	No, inexistente.
2: Inventario y control de activos de software	Si, en forma anticipatoria a futuros incidentes.
3: Protección de datos	Si, en forma reactiva.
4: Configuración segura de activos y software de la empresa	Si, en forma reactiva.
5: Gestión de cuentas	Si, en forma anticipatoria a futuros incidentes.
6: Gestión del control de acceso	Si, en forma anticipatoria a futuros incidentes.
7: Gestión continua de vulnerabilidades	Si, en forma reactiva.
8: Administración del registro de auditoría	Si, en forma anticipatoria a futuros incidentes.
9: Protecciones de correo electrónico y navegador web	Si, en forma anticipatoria a futuros incidentes.
10: Defensas contra malware	Si, en forma reactiva.
11: Recuperación de datos	Si, en forma anticipatoria a futuros incidentes.
12: Gestión de la infraestructura de red	Si, en forma anticipatoria a futuros incidentes.
13: Monitoreo y defensa de la red	Si, en forma reactiva.
14: Sensibilización sobre seguridad y capacitación en habilidades	Si, en forma anticipatoria a futuros incidentes.
15: Gestión de proveedores de servicios	Si, en forma reactiva.
16: Seguridad del software de aplicación	Si, en forma anticipatoria a futuros incidentes.

CIS Top 18	Respuesta
17: Gestión de respuesta a incidentes	Si, en forma anticipatoria a futuros incidentes.
18: Pruebas de penetración	Si, en forma reactiva.

Al realizar el respectivo promedio de cada uno de los puntajes, el usuario tendría un nivel de madurez del 65%, lo cual es un nivel medio, que podría ser mejor. Los puntajes donde menos se destaca, son los controles 1, 3 y 15. Dado que en estos puntajes sus respuestas fueron “No, inexistente” y “si, de forma reactiva” y su categorización según las funciones de NIST fueron las más bajas, obteniendo un resultado de 0, 0.06 y 0,13 respectivamente. Siguiendo la misma idea planteada anteriormente con la métrica de NIST CSF, los mejores controles o donde se destacaron fueron el 8, 11 y 17, con un puntaje de 3, 2 y 2.3 respectivamente. Algo curioso de este escenario es que en los controles donde se encuentra cierta debilidad, las funciones de NIST CSF asociadas son Identificar, Proteger y Detectar, mientras que en las destacadas se encuentra Detectar, Responder y Recuperar. De primera impresión se podría decir que esta organización, está enfocada en responder ante un ataque sin identificar que está protegiendo y que debería defender.

4.2.3.2. Cálculo del nivel de madurez según NIST CSF

Las funciones de NIST CSF como se mencionaron en la anterior sección de este documento, se encuentran categorizadas en cinco, identificar, proteger, detectar, responder y recuperar. En este proyecto, se realizó la distribución de estas funciones para cada uno de los controles, como se observó en la Tabla 24 haciendo uso del mismo ejemplo se va a ejemplificar el cálculo de este módulo.

Tabla 24

Ejemplo de cálculo NIST CSF

NIST CSF	CIS Top 18	Respuesta
ID	1: Inventario y control de los activos de la empresa	No, inexistente.
ID	2: Inventario y control de activos de software	Si, en forma anticipatoria a futuros incidentes.
PRO	3: Protección de datos	Si, en forma reactiva.
PRO	4: Configuración segura de activos y software de la empresa	Si, en forma reactiva.
ID	5: Gestión de cuentas	Si, en forma anticipatoria a futuros incidentes.
PRO	6: Gestión del control de acceso	Si, en forma anticipatoria a futuros incidentes.
PRO	7: Gestión continua de vulnerabilidades	Si, en forma reactiva.
DET	8: Administración del registro de auditoría	Si, en forma anticipatoria a futuros incidentes.
PRO	9: Protecciones de correo electrónico y navegador web	Si, en forma anticipatoria a futuros incidentes.
RES	10: Defensas contra malware	Si, en forma reactiva.
REC	11: Recuperación de datos	Si, en forma anticipatoria a futuros incidentes.
PRO	12: Gestión de la infraestructura de red	Si, en forma anticipatoria a futuros incidentes.
RES	13: Monitoreo y defensa de la red	Si, en forma reactiva.
PRO	14: Sensibilización sobre seguridad y capacitación en habilidades	Si, en forma anticipatoria a futuros incidentes.
DET	15: Gestión de proveedores de servicios	Si, en forma reactiva.
PRO	16: Seguridad del software de aplicación	Si, en forma anticipatoria a futuros incidentes.
RES	17: Gestión de respuesta a incidentes	Si, en forma anticipatoria a futuros incidentes.
ID	18: Pruebas de penetración	Si, en forma reactiva.

El programa realiza la suma por cada una de las funciones de NIST y la divide en la cantidad de controles que pertenecen a ella, es decir, para la función de identificar realiza la suma de las respuestas y es dividido entre cuatro (4), para el caso de proteger se divide entre ocho (8), para detectar entre dos (2), responder entre tres (3) y dado que la función de recuperar tiene una única respuesta, se toma únicamente este resultado, para finalizar el nivel de madurez de la organización según el NIST CSF se realizó calculando el promedio de estas cinco funciones. Siguiendo el ejemplo de la Tabla 24, se obtiene el resultado que se puede apreciar en la Figura 14, el usuario visualiza estos datos de una forma dinámica, similar a la que se puede apreciar en la Tabla 25.

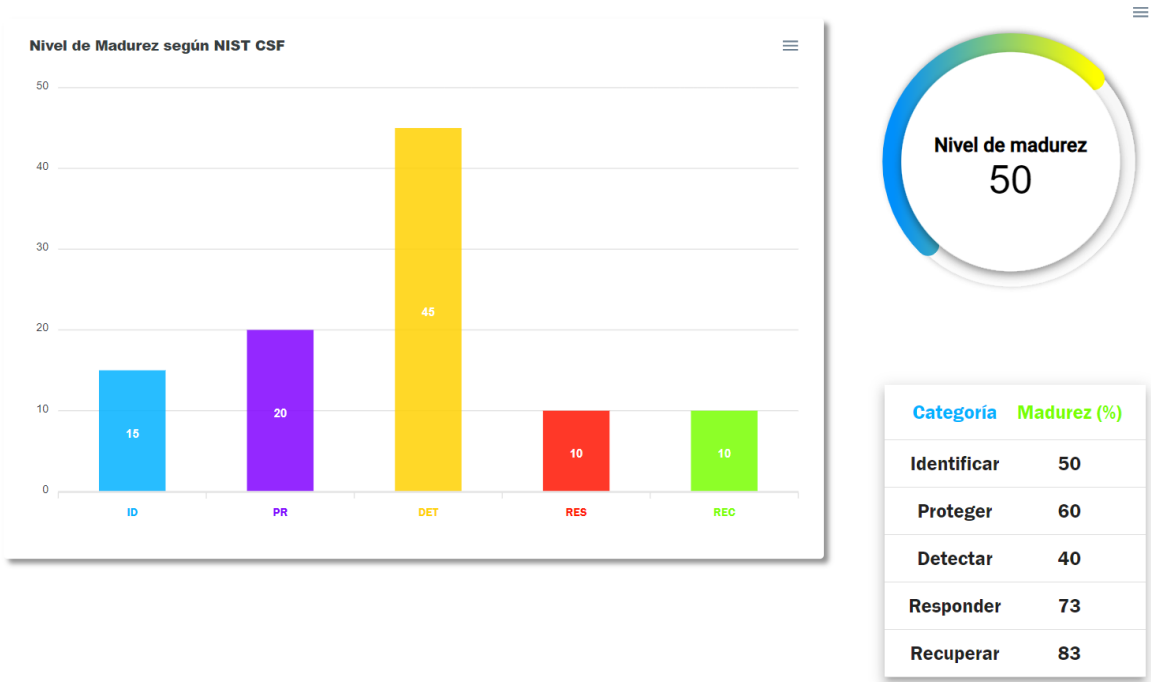
Tabla 25

Nivel de madurez por función de NIST CSF

Nivel de madurez según NIST	
ID	56%
PRO	72%
DET	63%
RES	50%
REC	100%
Nivel final	68%

Figura 14

Vista inicial del módulo NIST CSF



4.2.3.3. Cálculo del nivel de exposición a los patrones de ataque

Como se pudo apreciar en la Tabla 21 se mapearon siete (7) patrones de ataque según el DBIR 2022 de Verizon (2022 Data Breach Investigations Report, 2022) entre estos están:

- Ataques básicos a aplicaciones web
- Denegación de servicios
- Ransomware
- Errores misceláneos
- Abuso de privilegios
- Ingeniería social
- Intrusión al sistema

Donde, de estos siete (7) patrones de ataque, en el último año se registró que el 80% de las brechas en el sector educativo, se dio específicamente en ataques básicos a aplicaciones web, intrusión al sistema y errores misceláneos. Es por esto, que se realiza un mapeo total de todos los patrones de ataque, haciendo énfasis en solamente tres (3) que afectan directamente a este sector, es importante tener en cuenta que se está calculando el factor de exposición a estos vectores de ataque, es decir, que el resultado esperado es 0%, a diferencia de los resultados de los módulos anteriores, que el mejor escenario era 100%. Para realizar este cálculo se mapearon por controles, como se afecta a cada uno de los patrones, tal cual se evidencia en la Figura 15, para obtener el resultado del factor de exposición total, se realiza un promedio del nivel de exposición de cada uno de los patrones de ataque, mientras que para obtener el nivel de exposición para los tres (3) patrones de ataque que más afectó al sector educativo según el DBIR 2022, se calcula el promedio menos uno (1), dado que lo que buscamos es el nivel de exposición por lo tanto si los controles son los más adecuados, es decir que los aplican de forma anticipatoria, quiere decir que no se encuentran expuestos a este patrón de ataque, es por esto que es importante realizar la resta del mejor escenario (100%).

El usuario tiene una vista total de cuál es el nivel de exposición a todos los vectores de ataque y el detalle por cada uno de los vectores que afectan al sector educativo, la vista del usuario se puede apreciar en la Figura 15 donde no solamente se entrega el resultado de la evaluación, sino que se le da una vista rápida de por qué es importante tener estos datos en cuenta al momento de priorizar la ciberseguridad dentro de la institución.

Figura 15

Vista exposición a los vectores de ataque

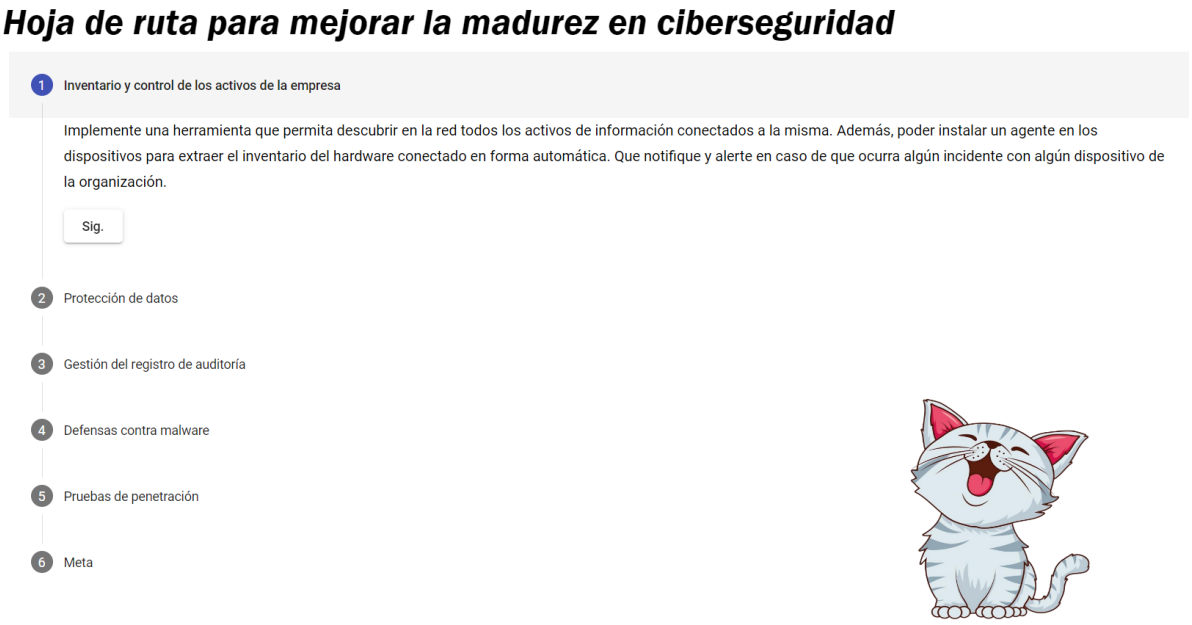
4.2.3.4. Establecimiento del plan de mejora

Todas las instituciones son diferentes, razón por la cual los planes de mejora deben estar hechos a la medida según las respuestas a las preguntas realizadas, aquí es donde entra la importancia de la honestidad al momento de realizar esta evaluación. Siguiendo la misma metodología que se utilizó para hacer el cálculo de los peores y mejores controles de CIS Top 18, este plan contiene un camino de mejora de cinco (5) pasos, donde se busca priorizar aquellos controles que se encuentran inexistentes o se realizan de forma reactiva. La idea de este plan de mejora es que sea una guía, más no una normativa cuya obligación es adoptarla, sin embargo es importante tener presente que está basado en la evidencia y su objetivo es reducir la exposición al ciberriesgo.

En el módulo correspondiente, el usuario observa un camino de cinco (5) pasos donde para continuar debe hacer clic en cada paso y ver la recomendación de lo que debería realizar, donde como nombre del camino se encuentra el control afectado. Una vista base del usuario es la que se visualiza en la Figura 16 la cual se diseñó teniendo en mente que el usuario no tiene mayor conocimiento de los controles de CIS Top 18 y se debe realizar lo más interactivo posible para que el usuario no veo únicamente una lista obligatoria a seguir.

Figura 16

Plan de mejora



4.2.3.5. Hipótesis de cuantificación del ciberriesgo

Los altos mandos de cualquier organización, no se preocupan por la operación como tal del negocio, sino en que el negocio esté funcionando y no se pierda dinero, es por esto por lo que es verdaderamente importante hablarle a la junta directiva en el lenguaje que ellos saben hablar: el dinero, mostrarles la cantidad de dinero que se puede perder si se ve afectada la parte tecnológica de la organización. A ellos no les importa el nivel de madurez que tienen, que tan expuestos se

encuentran según marcos de referencia y demás, solamente prestarán atención cuando se les vea afectado su activo más valioso (el dinero).

El módulo de cuantificación del ciberriesgo fue explicado en secciones anteriores, donde se ejemplifica como se utiliza esta ecuación para demostrar la cantidad diaria, en tres, cinco y diez días donde no funcione la operación tecnológica de la organización. Todos los componentes utilizados para calcular la cuantificación del ciberriesgo fueron datos anteriormente por el usuario, el objetivo de este resultado es demostrar según la dependencia tecnológica y la rentabilidad del negocio la pérdida que podrían llegar a sufrir en cuestión de que un incidente se materialice. Recordando un poco, la ecuación a utilizar es:

$$CCR = \big((RN * DT)\big)$$

Donde cada componente hace referencia a:

RN = Ingreso financiero del último año

DT = Porcentaje de dependencia tecnológica del negocio

En la Figura 17 el usuario finalmente tiene una vista donde se le explica lo que significa este módulo y de donde sale la cantidad estimada como pérdida en caso de que una brecha afecte a la institución.

Figura 17

Cuantificación del ciberriesgo

Cabe destacar que el valor de un día es el valor resultado que se muestra en el *dashboard*. Dado que las imágenes que se están mostrando son vistas, los resultados no son los mismos pero debería mostrarse aquel valor en los dos lugares correspondientes.

4.2.3.6. Ransomware Readiness Assessment

Para lograr este resultado se utilizaron las preguntas planteadas en la Tabla 18 con la metodología de respuesta, cuyo objetivo final es conocer en qué porcentaje se encuentra lista la organización para un eventual ataque de Ransomware. Este cálculo se realizó de forma sencilla, al hacer un promedio de las respuestas dadas por el usuario por cada una de las fases, donde en el módulo, por cada una de las fases se explica que busca hacer un atacante en cada una de ellas.

4.3. Desarrollo

El proyecto en cuestión siguió un enfoque disciplinado y metódico basado en el *Software Development Life Cycle (*SDLC). En las primeras fases del proyecto, la planificación y el análisis se fusionaron en una sola fase para definir los objetivos, los requisitos del usuario final y la arquitectura de la aplicación web.

Una vez completada la fase de análisis y diseño, se llevó a cabo la fase de desarrollo en la cual se procedió a la codificación de la aplicación web, comenzando con el desarrollo del frontend y continuando con la creación de la base de datos. Finalmente, se programó el backend de la aplicación, que contiene la lógica y es la base del funcionamiento de la aplicación.

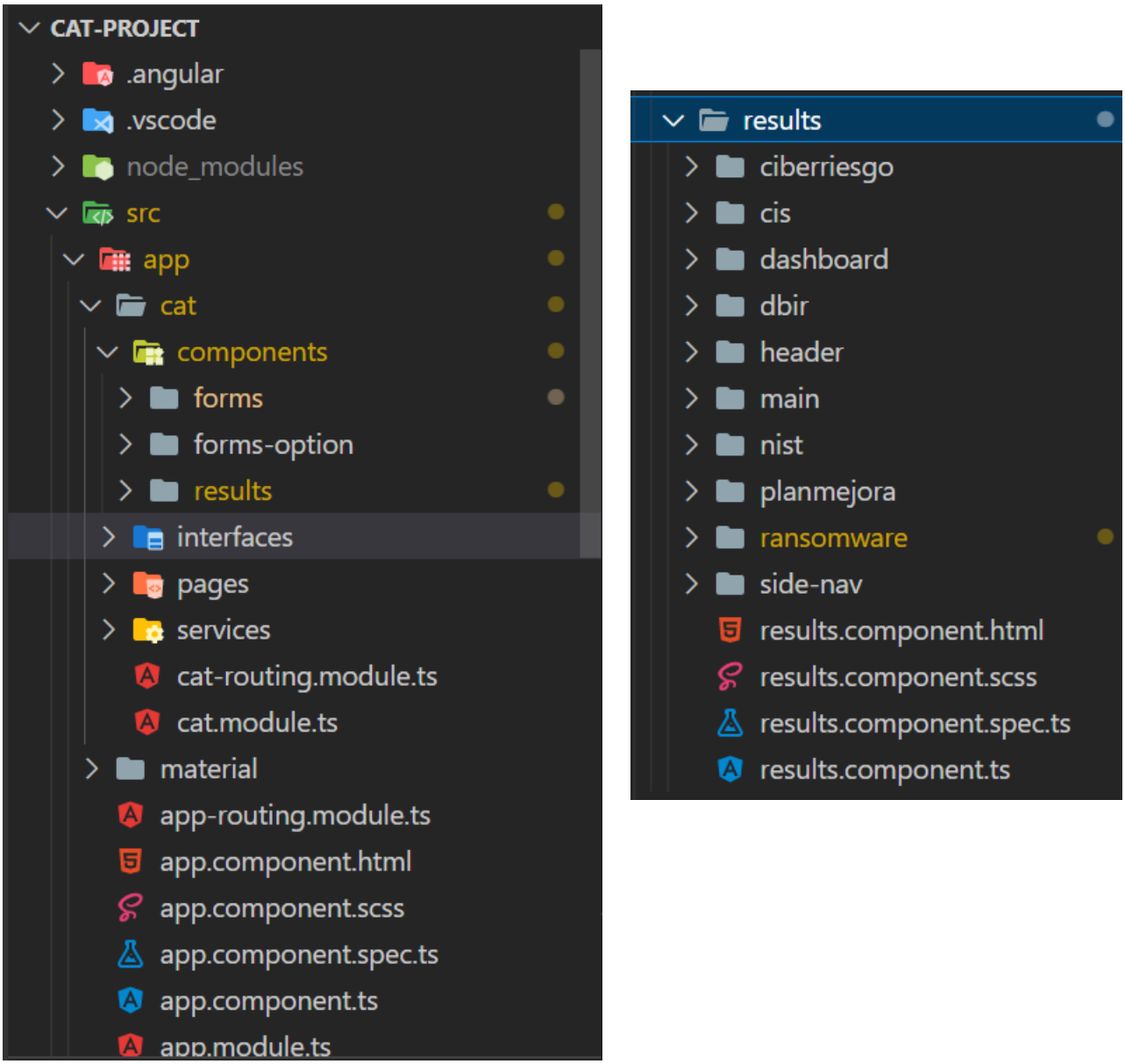
Gracias al éxito en la ejecución de las fases previas del proyecto, se ha sentado una base sólida para la fase de codificación. Esto ha permitido que se aborde con confianza la implementación del proyecto, asegurando que el desarrollo de la aplicación web cumpla con los requisitos del usuario final y garantizando un rendimiento óptimo. Con el frontend, la base de datos y el backend de la aplicación, se creó una estructura completa que permite que la magia de la aplicación ocurra.

4.3.1. Creación del proyecto en Angular

El proyecto Frontend fue modularizado, buscando tener como resultado un proyecto funcional, eficaz, fácil de interpretar y escalable. Asimismo, se aplicó un modelo de ruteo donde solamente la página web lee las rutas existentes y aquellas que no correspondan, son redirigidas a la página principal, esto con el fin de minimizar la exposición a ataques de inyección SQL. En cuanto al diseño, se utilizó la librería de componentes web de Angular Material para darle un *look & feel* amigable al usuario y cumplir con las vistas propuestas en la fase de diseño.

Figura 18

Proyecto Frontend



En la Figura 12, se puede observar la distribución de la interfaz de la página, la cual cuenta con formularios que ofrecen diversas opciones y la sección de resultados, descrita en apartados anteriores de este documento, con el fin de garantizar la consistencia y la cohesión visual en todos los módulos de la página, se ha implementado un componente de header y side-nav que se

mantiene constante, independientemente del módulo que se esté visualizando. Este enfoque asegura una experiencia de usuario uniforme y familiar en todos los componentes del dashboard.

Además, se puede apreciar cómo los módulos restantes de la página están diseñados para proporcionar resultados relevantes y útiles al usuario. Estos módulos están cuidadosamente diseñados para ofrecer información clara y concisa, presentada de manera atractiva y fácil de entender. Cada uno de ellos cumple una función específica y se integra armoniosamente en la página del dashboard.

Cabe destacar que la implementación de la funcionalidad de navegación entre páginas se ha llevado a cabo utilizando un módulo de ruteo, lo que permite una navegación fluida y eficiente dentro de la aplicación. Asimismo, se ha utilizado la popular librería de Angular Material, que proporciona un conjunto de componentes de interfaz de usuario predefinidos y estilizados, lo que contribuye a una apariencia moderna y atractiva en la página.

En resumen, la Figura 12 muestra claramente la estructura y el diseño de la página, con formularios, opciones y resultados, así como la integración de módulos de header y side-nav para mantener la consistencia visual. Además, se evidencia el cuidado en la presentación de resultados y la implementación de funcionalidades de navegación y diseño utilizando la librería de Angular Material, lo que contribuye a una experiencia de usuario agradable y eficiente en el dashboard.

4.3.2. Creación de la base de datos

Dado que la base de datos se creó en MongoDB, el cuales un gestor de base de datos NoSQL, la interacción con estas es más sencillo y encaja justamente con lo que se necesita de la aplicación. Estas bases de datos se caracterizan por ser flexibles, escalables y de alto rendimiento, lo cual permite el almacenamiento y recuperación eficiente de datos en formatos como documentos,

columnas, gráficos o clave-valor, entre otros. Recordemos que el término NoSQL hace referencia a Not Only SQL, es decir que no utiliza este lenguaje de consulta SQL como SELECT, sino que utiliza el formato de la creación de las tablas (json) y se realiza mediante el formato de JavaScript, tal como se puede apreciar en la Figura 19 se tiene una colección llamada empresa que contiene ID, nombre de la empresa, correo, contraseña, entre otros. Donde lo que se almacena son todos los datos necesarios de una empresa y en especial para esta aplicación, como lo son el tiempo de operación y el porcentaje de dependencia tecnológica.

Figura 19

Colección empresa


```
_id: ObjectId('6429fd9ce1c6c031b07d6a6b')
nombreEmpresa: "Empresa"
correo: "some@smt.com"
contrasena: "12341234"
__v: 0
dependencia: "3213123"
ingreso: 31231231
nroEmpleados: 31231
nroSedes: 3213123
tiempoOpera: 40
```


A continuación, se ejemplifica como es una consulta en esta base de datos, donde se busca encontrar todas las empresas llamadas Empresa cuyo tiempo de operación sea mayor que 24.

```
db.empresa.find({
  "nombreEmpresa": "Empresa"
  "tiempoOpera": { $gt: 24 }, });
```

4.3.3. Creación del backend y rutina computacional

Ahora bien, se procede a programar la rutina computacional que tiene la lógica planteada en el módulo anterior, utilizando el lenguaje de TypeScript, donde se declaran tipos de datos para variables, parámetros y resultados de las funciones.

4.3.3.1. Cálculo de madurez según CIS Top 18

Según la descriptiva que se dio en el apartado de diseño, de lo que se espera haga esta aplicación para este módulo en específico se crea la rutina computacional, cuyo objetivo es filtrar, ordenar y realizar cálculos en los datos de respuestas para su posterior visualización en gráficos o visualizaciones de datos en el componente, utilizando una función de comparación (el método sort() en este caso) para determinar el orden relativo de los elementos del arreglo de respuestas en función del valor del campo denominado orden en la base de datos. Esto se realizó mediante los siguientes pasos:

1. Se ordenan las respuestas filtradas en función del valor del campo orden, de menor a mayor, utilizando el método sort() de JavaScript con una función de comparación y dentro de esta se realiza una resta de los valores del campo orden de dos elementos (a y b) para determinar su orden relativo en el arreglo resultante.
    a. Si el valor de a.orden es menor que el valor de b.orden, a se coloca antes que b en el arreglo resultante.
    b. Si el valor de a.orden es mayor que el valor de b.orden, a se coloca después que b en el arreglo resultante.
    c. Si los valores de a.orden y b.orden son iguales, su orden relativo no importa en el arreglo resultante.

2. Para finalizar, se realizan cálculos en las respuestas filtradas, como calcular el promedio de los valores numéricos de un campo específico.
3. Se configuran opciones de visualización de gráficos o datos.

4.3.3.2. Cálculo de madurez según NIST CSF

A continuación se presenta cuáles fueron los pasos a seguir para realizar este cálculo:

1. Se obtiene las preguntas y se calculan las cantidades de NIST:
    a. Se llama a una función para obtener datos de preguntas desde algún lugar.
    b. Luego, se realiza un cálculo en base a estas preguntas para determinar la cantidad de NIST (un tipo de medida de seguridad) para cada pregunta.
    c. Los resultados de estos cálculos se almacenan en una variable.
2. Obtención de respuestas y cálculo de exposición NIST
    a. Se llama a una función para obtener datos de respuestas desde algún lugar.
    b. Luego, se filtran las respuestas para obtener solo aquellas que cumplan con ciertas condiciones.
    c. Después, se realiza un cálculo en base a las preguntas y respuestas obtenidas para determinar la exposición de NIST en base a los datos de las respuestas.
    d. Los resultados de estos cálculos se almacenan en variables como respuestas, preguntas y nist.
3. Actualización de datos para el gráfico de barras y la tabla:
    a. Se actualizan los datos del gráfico con los resultados de los cálculos anteriores.
    b. Se actualiza la variable con los datos de exposición de NIST.
4. Actualización de datos para el gráfico de madurez total:
    a. Se actualiza una variable con datos adicionales calculados en base a la variable nist.

b. Estos datos se obtienen a partir de un cálculo de suma de valores en la variable nist y se dividen por las cinco funciones de NIST.

4.3.3.3. Cálculo del módulo de exposición a los patrones de ataque

Dentro de este módulo se busca calcular el factor de exposición a los vectores de ataque, teniendo en cuenta que para este, se calculó el promedio para cada uno de los patrones de ataque que afecta al sector educativo y se le restó el 100% de exposición, ya que su objetivo es conocer la exposición a ciberatacantes, esto por medio de los siguientes pasos:

1. Se declara una lista de los tres patrones de ataque ('BWAA', 'SI', 'MISC') que son los asociados al sector educativo.
2. Se recorre por cada pregunta que busque el vector de ataque perteneciente a la lista definida anteriormente, si lo encuentra suma el valor de la respuesta.
3. Finalmente, este valor le resta 100 que hace referencia al factor de exposición mayor y lo divide entre la cantidad de cada vector de ataque.
4. Este valor se posiciona en la tabla en cada una de las celdas correspondientes y para encontrar el factor de exposición total, se suman los resultados del paso 3 y se divide entre 3.

4.3.3.4. Cálculo del módulo de cuantificación del ciberriesgo

Este probablemente es el módulo más sencillo de crear de todos, ya que solamente se necesitan los datos provistos por el usuario al inicio de la evaluación y realizar una operación matemática, así:

1. Actualiza los valores de ingreso y dependencia de la empresa obtenidos. Estos valores se utilizan posteriormente en el cálculo del valor del día.

2. Se calcula el valor del día multiplicando la dependencia de la empresa por su ingreso y lo utiliza para actualizar la propiedad data de la serie del gráfico. Los valores calculados se multiplican por diferentes factores (3, 5 y 10) para obtener diferentes puntos en el gráfico.
    a. Se asigna el valor del día calculado a la propiedad denominada ccr (Coeficiente de Capital de Riesgo) del componente. Este valor se utiliza para mostrar información adicional en el componente y se obtiene a partir del cálculo realizado en el paso anterior.

4.3.3.5. Cálculo de la preparación para un ataque de *Ransomware*

El cálculo de este módulo es sencillo pero bastante significativo, ya que la idea de este es dar un diagnóstico a alto nivel de cómo se encuentra la organización para responder ante un eventual ataque de Ransomware, para esto se creó una función que se encarga de hacer lo siguiente:

1. Recorre las preguntas y se buscan aquellas que tengan en su tipo de ataque 'RN' que hace referencia a Ransomware.
2. Una vez se localizan estas respuestas son sumadas y divididas en la cantidad de preguntas encontradas, en este caso 14.
3. Con este dato, ya se procede a colocarlo dentro del *series_bar* para desplegarlo en la plataforma.

4.3.3.6. Cálculo del plan de mejora

Con la creación de la función de CIS Top 18, donde se hizo el ordenamiento de aquellos controles de menos a mayor se toma esta misma lógica, con la diferencia de que se tomaran los cinco primeros controles con menor puntaje y se somete a una búsqueda de la propuesta previamente definida. Lo anterior se logró realizando los siguientes pasos:

1. Se ordenan las respuestas filtradas en función del valor del campo orden, de menor a mayor, utilizando el método sort() de JavaScript con una función de comparación y dentro de esta se realiza una resta de los valores del campo orden de dos elementos (a y b) para determinar su orden relativo en el arreglo resultante.
    a. Si el valor de a.orden es menor que el valor de b.orden, a se coloca antes que b en el arreglo resultante.
    b. Si el valor de a.orden es mayor que el valor de b.orden, a se coloca después que b en el arreglo resultante.
    c. Si los valores de a.orden y b.orden son iguales, su orden relativo no importa en el arreglo resultante.
2. Una vez tiene el orden, procede a buscar en las preguntas la propuesta respectiva que está definida en la base de datos y es colocada de forma ordenada en el *stepper*.

Con la implementación de este último método de búsqueda, donde se filtran las preguntas y respuestas, se completan los módulos de apoyo al usuario para mejorar su postura de ciberseguridad. Estos módulos proporcionan herramientas esenciales para defender la importancia de la ciberseguridad y reducir los riesgos asociados. Con la capacidad de acceder y manipular datos de preguntas y respuestas de forma eficiente, los usuarios tienen a su disposición una solución completa para gestionar y mejorar su seguridad en línea. Estos módulos ofrecen un enfoque integral para ayudar a los usuarios a tomar decisiones informadas y a implementar medidas efectivas de seguridad cibernética en su institución.

4.4. Etapa de pruebas

Se creó una empresa de prueba que se llamó “Para que estudies con dedicación” la cual cuenta con los siguientes datos:

- Dependencia tecnológica:"100"
- Ingreso del año anterior: 9876543210
- Número Empleados: 4400
- Número de Sedes: 123
- Tiempo de operación: 168

Se diligenció la evaluación de forma aleatoria y se guardaron las opciones de respuesta colocadas, en la Tabla 26 para ejemplificar únicamente se colocó el número de la pregunta con la opción de respuesta, teniendo presente que cada pregunta hace referencia a un control de CIS y se encuentran en orden.

Tabla 26

Respuestas de empresa de prueba

Pregunta	Respuesta
1: Inventario y control de los activos de la empresa	Si, en forma reactiva.
2: Inventario y control de activos de software	Si, en forma proactiva.
3: Protección de datos	Si, en forma anticipatoria a futuros incidentes.
4: Configuración segura de activos y software de la empresa	Si, en forma anticipatoria a futuros incidentes.
5: Gestión de cuentas	Si, en forma proactiva.
6: Gestión del control de acceso	Si, algunas veces.
7: Gestión continua de vulnerabilidades	Si, en forma anticipatoria a futuros incidentes.
8: Administración del registro de auditoría	Si, algunas veces.
9: Protecciones de correo electrónico y navegador web	No, inexistente.
10: Defensas contra malware	Si, en forma anticipatoria a futuros incidentes.
11: Recuperación de datos	Si, en forma proactiva.
12: Gestión de la infraestructura de red	Si, en forma reactiva.
13: Monitoreo y defensa de la red	No, inexistente.
14: Sensibilización sobre seguridad y capacitación en habilidades	Si, en forma reactiva.
15: Gestión de proveedores de servicios	Si, algunas veces.

16: Seguridad del software de aplicación	Si, en forma proactiva.
17: Gestión de respuesta a incidentes	Si, en forma anticipatoria a futuros incidentes.
18: Pruebas de penetración	Si, en forma anticipatoria a futuros incidentes.

A continuación, se muestra el comportamiento esperado con unas tablas planteadas en Excel, con la lógica de la aplicación vs. El resultado de la aplicación.

4.4.1. Prueba al módulo CIS Top 18

Este módulo tuvo la mayor complejidad, ya que no solamente arroja resultados numéricos sino que también realiza el ordenamiento y priorización de los controles a mejorar. Es por esto que se realizaron estas pruebas en primer lugar, en la Tabla 27 se puede observar cual es el resultado esperado global, respecto al nivel de madurez actual y en la Tabla 28 se encuentra el ordenamiento esperado por cada uno de los controles por control CIS Top 18. En la Figura 20 se puede verificar que efectivamente, el programa está realizando los cálculos esperados.

Tabla 27

Nivel de madurez de CIS Top 18

CIS Top 18	% RTA
1: Inventario y control de los activos de la empresa	25%
2: Inventario y control de activos de software	75%
3: Protección de datos	100%
4: Configuración segura de activos y software de la empresa	100%
5: Gestión de cuentas	75%
6: Gestión del control de acceso	50%
7: Gestión continua de vulnerabilidades	100%
8: Administración del registro de auditoría	50%
9: Protecciones de correo electrónico y navegador web	0%

10: Defensas contra malware	100%
11: Recuperación de datos	75%
12: Gestión de la infraestructura de red	25%
13: Monitoreo y defensa de la red	0%
14: Sensibilización sobre seguridad y capacitación en habilidades	25%
15: Gestión de proveedores de servicios	50%
16: Seguridad del software de aplicación	75%
17: Gestión de respuesta a incidentes	100%
18: Pruebas de penetración	100%
Nivel de madurez	62%

Tabla 28

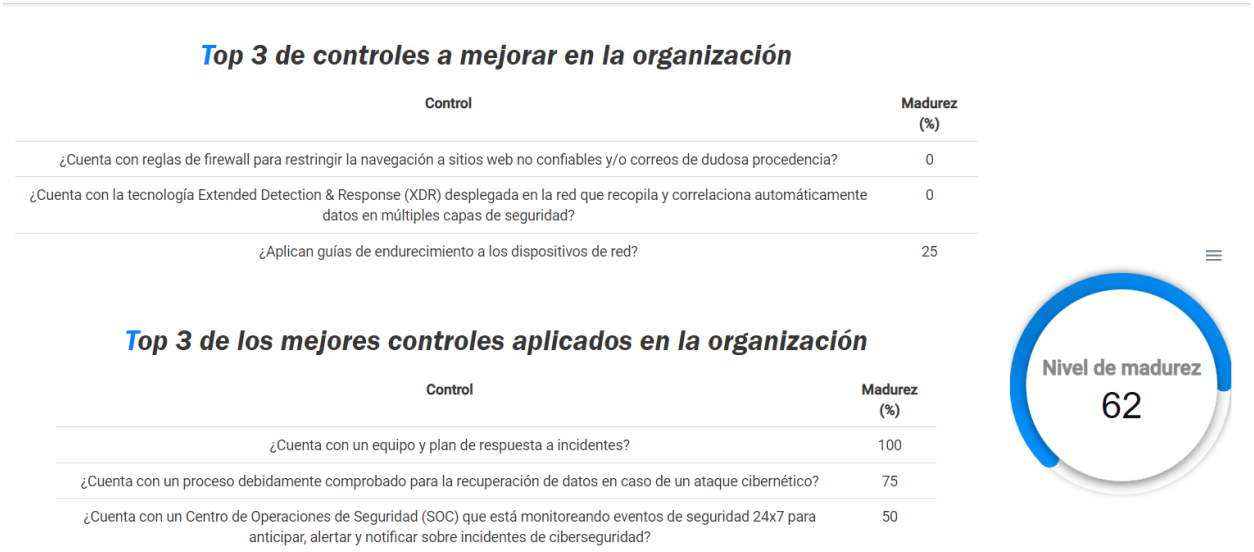
Orden esperado para los mejores y peores controles

Pregunta	Puntaje	Orden
¿Cuenta con reglas de firewall para restringir la navegación a sitios web no confiables y/o correos de dudosa procedencia?	0	1
¿Cuenta con la tecnología Extended Detection & Response (XDR) desplegada en la red que recopila y correlaciona automáticamente datos en múltiples capas de seguridad?	0	2
¿Aplican guías de endurecimiento a los dispositivos de red?	0,125	3
¿Dentro de la organización se tiene establecido y se mantiene un programa de concientización a usuarios sobre seguridad de la información?	0,15625	4
¿Existe un inventario de activos detallado y actualizado?	0,1875	5
¿Implementa controles de acceso basado en roles (RBAC) para decidir el tipo de privilegios que se asignarán a los diferentes tipos de cuentas?	0,1875	6
¿Se implementa una solución de prevención de pérdida de datos (DLP) y sigue la política de proceso de clasificación de datos?	0,25	7
¿Mantiene monitoreada la dark y deep web, supervisando y evaluando la reputación de los proveedores de servicios?	0,25	8
¿Desarrolla sus aplicaciones utilizando las mejores prácticas de ciberseguridad como OWASP Top 10 y las prueba antes de pasarlas a producción?	0,28125	9
¿Existe un inventario de software detallado y este mismo debidamente actualizado?	0,375	10
¿Cuenta con un directorio activo debidamente administrado?	0,375	11

¿Aplican guías de fortalecimiento a los activos empresariales (Endpoint, IoT, Servidores, Móvil, etc.)?	0,625	12
¿Cuenta con un Endpoint Detection & Response (EDR) que esté constantemente monitoreando los endpoints para mitigar ciber-amenazas?	0,666667	13
¿Realiza análisis de vulnerabilidades al menos dos veces al año y cuenta con un proceso para la mitigación de las vulnerabilidades encontradas?	0,75	14
¿Realiza pruebas de penetración a la red interna, externa, wifi y aplicativos web y móviles que posee?	1	15
¿Cuenta con un Centro de Operaciones de Seguridad (SOC) que está monitoreando eventos de seguridad 24x7 para anticipar, alertar y notificar sobre incidentes de ciberseguridad?	1,5	16
¿Cuenta con un proceso debidamente comprobado para la recuperación de datos en caso de un ataque cibernético?	1,5	17
¿Cuenta con un equipo y plan de respuesta a incidentes?	2,333333	18

Figura 20

Resultado de la aplicación según CIS Top 18



4.4.2. Prueba al módulo NIST CSF

Para este módulo, el resultado esperado era que el nivel de madurez total de NIST fuese 63% y los niveles por funciones como se muestran en la Tabla 29 y como se puede observar en la Figura 21 son los mismos dados en la aplicación.

Tabla 29

Resultados esperados para NIST

Nivel de madurez según NIST	
ID	69%
PRO	59%
DET	50%
RES	67%
REC	75%
Madurez Total	63%

Figura 21

Resultados de la aplicación para NIST

4.4.3. Prueba al módulo exposiciones a los patrones de ataque

Para este módulo, el resultado esperado era que el factor de exposición fuese de un 32% y los patrones de ataque que afectan al sector educativo se muestran en la Tabla 30 y como se puede observar en la Figura 22 son los mismos dados en la aplicación.

Tabla 30

Resultados esperados para los patrones de ataque

Patrón de ataque	***Exposición***
Ataques básicos a sitios web	15%
Errores misceláneos	42%
Intrusión del sistema	40%
Exposición total	32%

Figura 22

Resultado de la aplicación para los patrones de ataque

4.4.4. Prueba al módulo de cuantificación del ciberriesgo

Para este módulo, el resultado esperado para la hipótesis del ciberriesgo era de $ 987.654.321.000,00 como se muestra en la Tabla 31 y como se puede observar en la Figura 23 son los mismos dados en la aplicación.

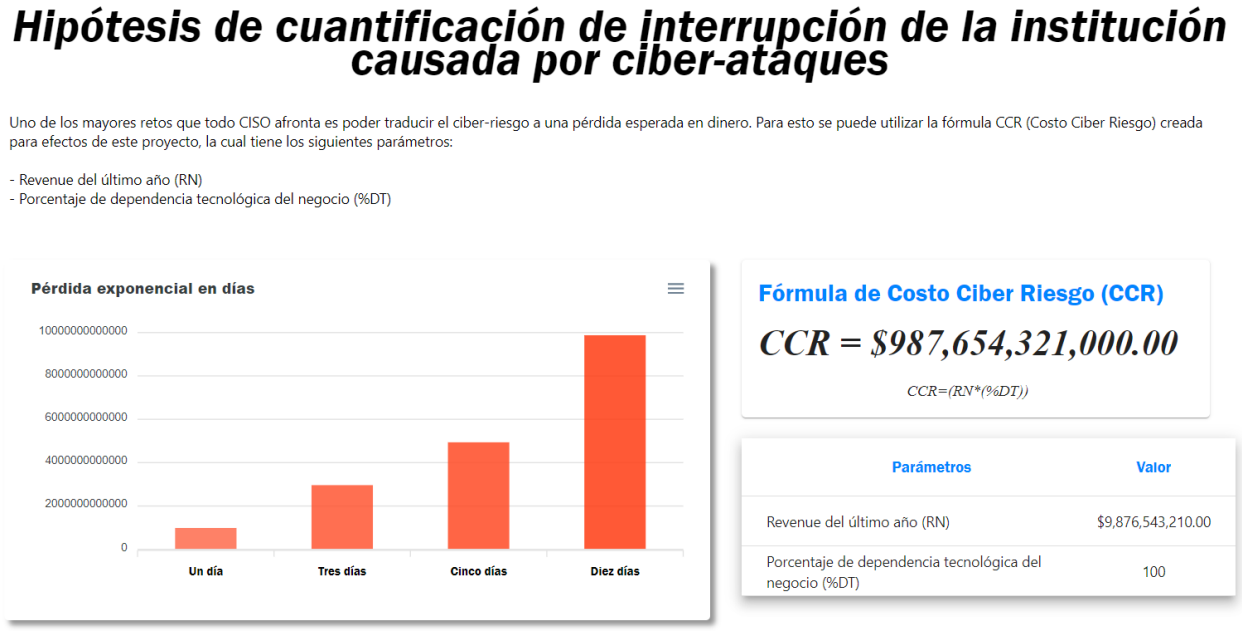
Tabla 31

Resultado esperado para la cuantificación del ciberriesgo

Ingreso del último año	Dependencia tecnológica	Hipótesis del ciberriesgo
$ 9.876.543.210,00	100	$ 987.654.321.000,00

Figura 23

Resultado de la aplicación para la cuantificación del ciberriesgo



4.4.5. Prueba al módulo de Ransomware Readiness Assessment

Tomando las respuestas que dio este usuario de prueba, apreciadas en la Tabla 32 se espera una respuesta de 87% y este resultado concuerda con el que se evidencia en la Figura 24.

Tabla 32

Resultado esperado para RRA

Pregunta	Valor	Preparación
¿Realiza pruebas de ingeniería social (como phishing) a sus usuarios?	100	87
¿Cuenta con tecnologías de gestión de identidad y accesos (IAM) y gestión de privilegios (PAM)?	100	
¿Su organización cuenta con actualizaciones automatizadas periódicamente para su software y sistemas?	100	
¿Su organización tiene copias de seguridad programadas regularmente?	75	
¿Desarrolla escenarios para evaluar cuánto tiempo llevaría recuperar datos críticos y sus servicios?	75	
¿Su sistema tiene una póliza de seguro cibernético que cubre los ataques de Ransomware?	75	

Figura 24

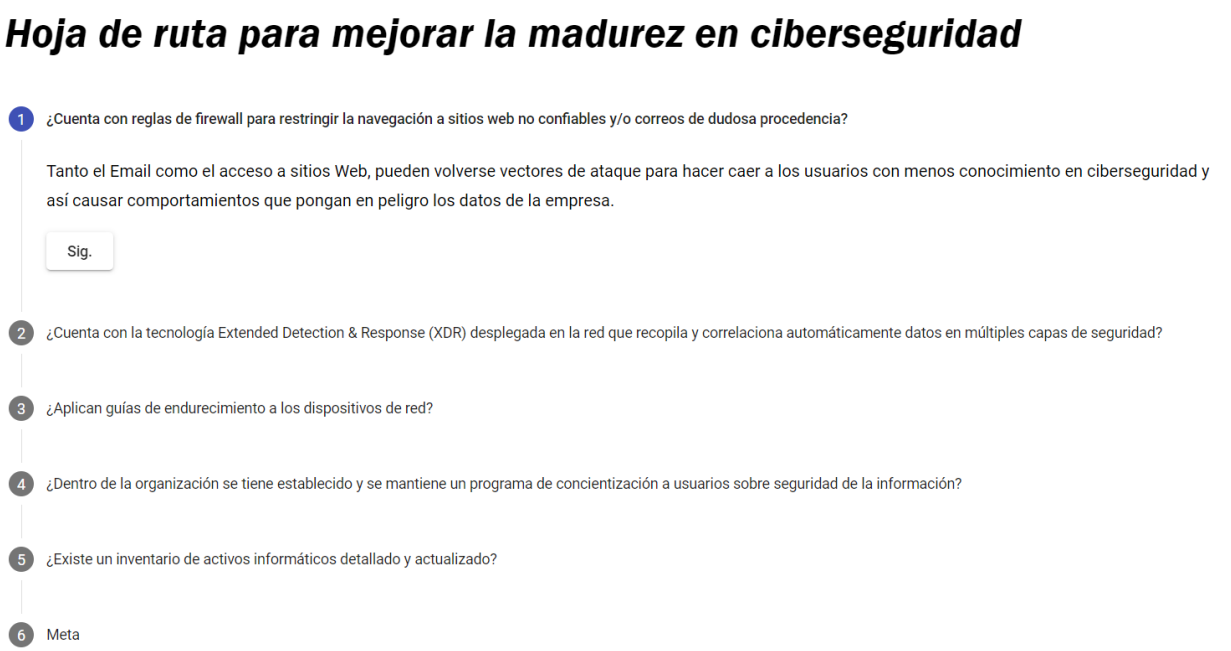
Resultado de la aplicación para RRA

4.4.6. Prueba al plan de mejora

La última prueba realizada a este proyecto fue al plan de mejora, que como se mostró en la Tabla 28 se encuentra ya el ordenamiento, donde ahora únicamente se muestran los cinco primeros controles (los de peor puntaje). Como se aprecia en la Figura 25 el resultado es el esperado.

Figura 25

Resultado de la aplicación para el plan de mejora



5. Entrega

Para finalizar este documento y el ciclo de la carrera de ingeniería de sistemas se hace la entrega del aplicativo web desarrollado, que se puede encontrar en el siguiente repositorio de GitHub https://github.com/MariaASerrano/CAT---PROJECT para el *Frontend* y https://github.com/MariaASerrano/CAT-Project-Back para el *BackEnd* donde para poder iniciar a hacer uso de la aplicación desde su computador loca, debe tener instalado Docker y Mongo Atlas. Para iniciar a hacer uso de la aplicación, se debe registrar y responder la evaluación que le sirve como apoyo para mejorar la postura de ciberseguridad de la institución.

Como se mostró en secciones anteriores, para iniciar a hacer uso de la aplicación, es necesario el registro, donde lo únicamente necesario es el nombre de la empresa, correo electrónico y contraseña. Una vez se encuentra a dentro puede realizar la evaluación e inmediatamente poder ver los resultados, de igual forma estos resultados se encontrarán disponibles todo el tiempo, donde para acceder a ellos, el usuario debe ingresar a la aplicación con el nombre de la empresa y la contraseña, a partir de ahí se muestra el mismo *dashboard* que se mostró al finalizar la evaluación.

6. Conclusiones

Este proyecto se desarrolló con el fin de apoyar a las instituciones educativas a mejorar su postura en ciberseguridad, ya que como se ha podido evidenciar en los últimos reportes de Verizon, el sector educativo ha sido blanco de una gran cantidad de incidentes y una buena parte se ha convertido en brechas.

Un importante paso para lograr la construcción de esta aplicación fue el diseño y el desarrollo de módulos, basados en marcos de referencia y controles, como lo son NIST CSF en su primera versión y el CIS Top 18. Con estos módulos, el usuario tiene una vista amplia y realista de cómo se encuentra según lo que dictan estas mejores prácticas.

Para definir las preguntas que se plantearían al usuario para cada uno de los controles, se realizó una amplia investigación de cuál era el objetivo de cada uno de los controles, para poder basado en esto construir una única pregunta, donde el usuario pudiese responder de forma sencilla, siempre teniendo como base que las respuestas deben ser dadas con toda honestidad.

Ya con las fases anteriores, se pudo proceder al desarrollo de una forma ágil, ya que solamente se debían seguir los pasos previamente predeterminados, donde se buscaba compartir cual es la postura actual de la organización y que debería realizar para mejorarla. En esta fase de buscó realizar la mejor implementación para brindarle a la institución el mejor apoyo posible, no solamente diciéndole en que estaba fallando, sino una vista rápida de cómo puede mejorarlo.

Se realizaron múltiples pruebas a la aplicación, donde se buscaba afinar los detalles de la rutina computacional creada, verificando que realmente estuviese dando los resultados esperados según la lógica planteada, con el fin de apoyar a las organizaciones a mejorar su nivel de madurez en ciberseguridad.

Teniendo en cuenta todo lo anterior, se logró exitosamente al escenario planteado, donde se tiene una aplicación que es fácil de manejar por el usuario, informativa, útil y confiable. Ya que todo lo que se realiza dentro de esta aplicación está basado en la evidencia y en la experiencia de las grandes compañías como Verizon y sus diversos estudios. Esta aplicación, da respuesta a la problemática planteada al iniciar este proyecto.

Se logró desarrollar una aplicación web para que las instituciones educativas, puedan conocer el nivel de madurez y exposición a los vectores de ataque en ciberseguridad a organizaciones dentro del sector educativo.

7. Trabajo futuro

- Creación de un usuario administrador que se encargue de actualizar los reportes de Verizon, año con año.
- Utilizar inteligencia artificial, para que basado en la experiencia, la aplicación pueda proponer mejores planes de mejora
- Automatización de la herramienta para que cuando exista una nueva versión de los controles de CIS, NIST CSF y los reportes de Verizon, se puedan actualizar las preguntas y como los puntajes son calculados.
- Implementar un asistente virtual, que pueda resolver las dudas del usuario inmediatamente y no dependa de un experto en el área.
- Realizar este mismo proyecto y ejercicio para todos los sectores planteados en el DBIR, donde se debe tener en cuenta el historial de ellos y los patrones de ataque que los afecta.
- En caso de que se presente una falla en la aplicación al momento de realizar la evaluación debería existir la posibilidad de que las respuestas sean recuperadas una vez se restablezca el servicio.

Referencias Bibliográficas

2022 Data Breach Investigations Report. (28 de Octubre de 2022). *Verizon*. Obtenido de Verizon Business: https://www.verizon.com/business/resources/reports/dbir/

Angular. (Febrero de 2023). *Angular Docs.* Obtenido de Angular: https://angular.io/docs

Balbix. (31 de Enero de 2022). *Balbix*. Obtenido de What is the NIST Cybersecurity Framework?: https://www.balbix.com/insights/nist-cybersecurity-framework/

CIIFEN. (29 de Julio de 2022). *Definición del riesgo*. Obtenido de CIIFEN: https://ciifen.org/definicion-de-riesgo/

CIS. (24 de Julio de 2021). *About us*. Obtenido de CIS: https://www.cisecurity.org/about-us

CISA. (Julio de 2021). *Cyber Security Evaluation Tool (CSET®).* Obtenido de CISA: https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

CISA. (2023). *Stop Ransomware.* Obtenido de Cybersecurity and Infrastructure Security Agency CISA: https://www.cisa.gov/stopransomware

Cybersecurity Capability Maturity Model (C2M2). (12 de Diciembre de 2022). *Cybersecurity Capability Maturity Model (C2M2)*. Obtenido de Energy.gov: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Cybersecurity Capability Maturity Model. (Junio de 2022). *Cybersecurity Capability Maturity Modell, Version 2.1*. Obtenido de Energy: https://www.energy.gov/sites/default/files/2022-06/C2M2+Version+2.1+June+2022.pdf

Edix, R. (13 de Septiembre de 2021). *Edix España.* . Obtenido de Framework: qué es, para qué sirve y algunos ejemplos: https://www.edix.com/es/instituto/framework/

Hope, A. (9 de Julio de 2021). *CISA Releases Ransomware Readiness Assessment Tool for Assessing Organizations' Cybersecurity Posture.* Obtenido de CPO Magazine: https://www.cpomagazine.com/cyber-security/cisa-releases-ransomware-readiness-assessment-tool-for-assessing-orga

IBM. (Enero de 2023). *IBM Security X-Force Threat Intelligence Index 2023.* Obtenido de IBM: https://www.ibm.com/reports/threat-intelligence

INCIBE. (25 de Abril de 2022). *¿Conoces tus riesgos?* Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos

INCIBE. (3 de Febrero de 2022). *Qué es*. Obtenido de INCIBE: https://www.incibe.es/que-es-incibe

MongoDB Atlas. (Febrero de 2023). *What is MongoDB Atlas?* Obtenido de MongoDB: https://www.mongodb.com/docs/atlas/

National Institute of Standards and Technology. (16 de Abril de 2018). *Framework for Improving.* Obtenido de National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nest JS. (Febrero de 2023). *Nest JS Documentation.* Obtenido de Nest JS: https://docs.nestjs.com/

The 18 CIS Critical Security Controls. (28 de Octubre de 2021). Obtenido de Center for Internet Security: https://www.cisecurity.org/controls/cis-controls-list

Toro, R. (11 de Marzo de 2021). *PMG SSI - ISO 27001*. Obtenido de ¿Qué es la seguridad de la información y cuantos tipos hay?: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

U, H. (29 de Julio de 2022). *7 razones para usar Angular para sus aplicaciones web en 2022.* Obtenido de Cynoteck: https://cynoteck.com/es/blog-post/reasons-to-use-angular-for-your-web-app/

Verizon. (24 de Octubre de 2022). *Company Purpose & Mission Statement.* Obtenido de About Verizon: https://www.verizon.com/about/our-company

Wong, T. (7 de Junio de 2022). *Data Breach Investigation Report DBIR 2022*. Obtenido de Improsec | improving security: https://improsec.com/cyber-blog/data-breach-investigation-report-dbir-2022