Revista Brasileira de Informática na Educação – RBIE
Brazilian Journal of Computers in Education
(ISSN online: 2317-6121; print: 1414-5685)
http://br-ie.org/pub/index.php/rbie

Submission: 19/Feb/2021; 1st round notif.: 05/May/2021; New version: 25/May/2021; 2nd round notif.: 29/Jun/2021;
Camera ready: 15/Jul/2021; Edition review: 23/Jul/2021; Available online: 06/Aug/2021; Published: 06/Aug/2021;

Desarrollo de plataforma digital para la prevención y atención de casos de ciberacoso en niñas, niños y adolescentes

Title: Development of digital platform for the prevention and attention of cyberbullying cases in children and adolescents

Ana Teresa Morales Rodríguez
Laboratorio Nacional de Informática Avanzada
ana.morales@lania.edu.mx

Juan Fidel Ortiz Fernández
Laboratorio Nacional de Informática Avanzada
jortiz.mca17@lania.edu.mx

Resumen

Este este trabajo se presenta el desarrollo de una plataforma web para la prevención y atención de casos de ciberacoso contra Niñas, Niños y Adolescentes (NNA), quienes en la actualidad debido al confinamiento por la pandemia del COVID19, se encuentran en mayor contacto con medios digitales, ya que de acuerdo con estadísticas a nivel internacional y nacional (en México), éstos están hiperconectados, con poca supervisión en el uso de medios y con escasa o nula orientación en el uso seguro y responsable de la tecnología. Se está aprendiendo desde casa y las aulas escolares ahora han trascendido a medios digitales, por lo que los estudiantes de primaria, secundaria y nivel medio superior, no están exentos de ser víctimas de ataques como ciberacoso, sextorciones, phishing y grooming, entre otros, que desafortunadamente afectan su integridad física y psicológica. En coordinación con una instancia encargada de la procuración de los derechos de las y los NNA (el Sistema de Protección Integral de Niñas Niños y Adolescentes SIPINNA, de un gobierno local), se trabajó en el análisis, diseño, desarrollo y pruebas de una plataforma que permita, principalmente tres cosas: 1) informar y prevenir a través de contenido digital acerca riesgos en línea; 2) diagnosticar la vulnerabilidad de las y los NNA para tomar decisiones e implementar acciones focalizadas en escuelas donde haya mayor vulnerabilidad; y finalmente, proveer un mecanismo de reporte, a través del cual, las y los NNA podrán reportar a SIPINNA si son víctimas de algún tipo de ciberacoso y la organización pueda atender y/o canalizar con las autoridades correspondientes.

Palabras clave: *Sistema web; Niñas; Niños; Adolescentes; Bullying; Cyberbullying; Grooming; Phishing.*

Abstract

This paper presents the development of a web platform for the prevention and attention of cases of cyberbullying against Children and Adolescents, who currently due to the confinement by the COVID19 pandemic, are in greater contact with digital media. According to international and national statistics (in Mexico), children and adolescents are hyperconnected, with little supervision in the use of media and with out guidance in the safe and responsible use of technology. They are learning from home and school classrooms are now on digital media, so elementary, middle and high school students are not exempt from being victims of attacks such as cyberbullyng, sextortions, phishing and grooming, among others, which unfortunately affect their physical and psychological integrity. In coordination with an agency responsible for the protection of the rights of children and adolescents (the System for the Comprehensive Protection of Children and Adolescents of a local government), we worked on the analysis, design, development and testing of a platform that allows, mainly three things: 1) inform and prevent through digital content about online risks; 2) diagnose the vulnerability of children and adolescents to make decisions and implement targeted actions in schools where there is greater vulnerability; and finally, provide a reporting mechanism, through which children and adolescents can report to SIPINNA if they are victims of any type of cyberbullying and the organization can address or channel with the pertinent authorities.

Keywords: *Web system; Children; Adolescents; Bullying; Cyberbullying; Grooming; Phishing.*

Cite as: Morales Rodríguez, A. T., & Ortiz Fernández, J. F. (2021). Desarrollo de plataforma digital para la prevención y atención de casos de ciberacoso en niñas, niños y adolescentes. Revista Brasileira de Informática na Educação, 29, 903-927. DOI: 10.5753/RBIE.2021.29.0.903

1 Introducción

De acuerdo con la Ley General de los Derechos de las Niñas, Niños y Adolescentes, decretada en el año 2014, en México, las Niñas, Niños y Adolescentes (NNA) son titulares de 20 derechos, entre los cuales se encuentra el derecho de acceso a las Tecnologías de la Información y Comunicación (TIC), así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Las y los NNA tienen derecho a acceder a las TIC, sin embargo, se debe considerar que son un grupo que puede estar en mayor grado de vulnerabilidad, por lo que es primordial fomentar en ellos un uso consiente, seguro y responsable de dispositivos digitales e Internet, es decir desarrollar habilidades de Ciudadanía Digital. Si las niñas, niños y adolescentes no conocen los riesgos a los que son susceptibles en línea, éstos no serán capaces de tomar las medidas de seguridad necesarias y algunas de las vulnerabilidades a las que ya son sujetos, pueden expandirse o magnificarse. En Internet, existen diversos tipos de ataques como el ciberacoso, grooming, sextorsión, robo de identidad, porno venganzas, entre otros.

El cyberbullying, según Smith (2000), es un acto agresivo e intencionado llevado a cabo de manera repetida y constante a lo largo del tiempo, mediante el uso de formas de contacto electrónicas por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente; el grooming, es el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través del Internet con el fin último de obtener concesiones de índole sexual (Sánchez, 2014); el phishing, es una forma conocida de ciberdelincuencia con el objetivo de intentar adquirir información confidencial del usuario, como sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc., reduciendo todos los datos posibles para luego ser usados de forma fraudulenta (Guerrero Luque, 2015). Estos y otros riesgos hacen que las y los NNA, vivan circunstancias que van desde la intimidación, pérdida de autoestima, hasta situaciones que atentan contra su integridad. Entonces, es fundamental que antes de permitir que las niñas, niños y adolescentes tengan contacto con redes sociales o cualquier otro medio electrónico, se les enseñe y oriente en buenas prácticas de ciudadanía digital.

En el 2018, México contaba con alrededor de 82.7 millones de internautas, de los cuales aproximadamente el 26% tiene una edad inferior a los 18 años; El 67% de internautas se conectan durante las 24 horas, resaltando los momentos de hora de comida (84%) y noche (83%) con más personas conectadas. Así mismo, el incremento en acceso tecnológico a los medios digitales ha permeado en la popularidad de las redes sociales como Tiktok, Facebook, WhatsApp y YouTube que son de las más usadas por los jóvenes. A esto se suma, que desde el inicio de la pandemia del COVID19, el consumo diario de contenido en redes sociales se incrementó (Statista, 2020).

La violencia a través de medios digitales contra niñas, niños y adolescentes, es un problema que recobró importancia debido a la pandemia por el COVID-19, ya que incrementó el tiempo en pantallas sin orientación o acompañamiento para el uso seguro y responsable de Internet, así como poco conocimiento de los riesgos en línea y cómo operan. En este sentido, existen algunas herramientas que promueven la protección de niñas, niños y adolescentes ante riesgos en línea, por ejemplo: “Protégete”, una aplicación que permite realizar una denuncia anónima sobre un contenido ilegal o nocivo y determina el nivel de conocimientos sobre la seguridad y uso responsable de las TIC por medio de cuestionarios (Balaguer, 2014); “Basta de Bullying”, que ofrece recursos didácticos sobre temas relacionados con el bullying, cuenta con evaluaciones, consejos a los jóvenes y un juego (Llorca, 2016); “Dinantia”, es una aplicación enfocada a padres y alumnos, lo que permite mantener comunicaciones frecuentes entre el alumnado, profesores y los padres, además, incluye un mecanismo de alertas que permite tener al día a los padres mediante notificaciones y recordatorios (Dinantia, 2018).

En este trabajo de desarrollo de tecnología aplicada a la educación, se presenta la implementación de una plataforma web, que tiene como objetivo principal: coadyuvar a la

prevención de violencias digitales (en sus diversos modos) contra niñas, niños y adolescentes (NNA). Mediante esta herramienta: a) se provee contenido que sensibilice, concientice y promueva el uso responsable de las redes sociales e Internet, mediante recomendaciones de buenas prácticas de ciudadanía digital; y por otro lado, se facilitan mecanismos para que estudiantes de niveles primaria, secundaria y preparatoria, puedan reportar incidentes o ataques en línea a un organismo encargado de la garantía de sus derechos, en este caso, el Sistema de Protección Integral de Niñas, Niños y Adolescentes (SIPINNA) del Ayuntamiento de Xalapa, Veracruz, México, y esta dependencia se encargará de atender, canalizar o dar seguimiento a estas situaciones en que se ve afectada la seguridad de las y los estudiantes de escuelas que estén bajo su jurisdicción.

2 Marco teórico y metodológico

2.1 Problemática que atiende la plataforma #NNASegur@s

Según el INEGI (2017), en México se tiene un alto grado de ciberacoso, este trabajo se desarrolla en el estado de Veracruz, México, el cual se posiciona en primer lugar a nivel nacional con un 25.6% de víctimas. En Xalapa, ciudad capital de Veracruz, han incrementado los incidentes de ciberacoso y de acuerdo con Juanz (2018), el cyberbullying ha impactado en los ámbitos educativos, especialmente en el nivel de secundaria, esto generó el involucramiento de organizaciones como el Consejo Estatal de Seguridad en Veracruz y la Secretaría de Seguridad Pública, mismas que a partir del 2017 han implementado, un programa de seguridad ciudadana donde se involucró a docentes y a padres o tutores.

Por su parte, el Sistema de Protección Integral de Niñas, Niños y Adolescentes, es un organismo que tiene como objetivo garantizar los lineamientos de la Ley General de Derechos de Niñas, Niños y Adolescentes, haciendo conocer, valer, y respetar los derechos humanos (SIPINNA Ciudad de México, 2016). Esta organización trabaja en temas como la violencia de género, desigualdad, el acoso escolar, entre otros. En el SIPINNA-Xalapa, se han realizado proyectos como el buzón de reportes anónimos en las escuelas, cuya finalidad era obtener históricos sobre hechos de violencia, acoso, hostigamiento, en las niñas, niños y adolescentes. En este buzón, se detectaban problemas para poder canalizar y/o brindar seguimiento acorde a las necesidades de las víctimas. Las principales limitaciones de este proyecto fueron que: a) los reportes eran generados en hojas de papel; b) no se tenían datos del autor del reporte, lo que genera dificultad de brindar seguimiento directo con la persona; y c) el registro del seguimiento era generado mediante documentos, lo que hacía más complejo llevar un control eficiente.

2.2 Los riesgos en línea que afectan a niñas, niños y adolescentes

Antes del 2020, las y los NNA ya eran vulnerables a ciertos riesgos o ataques en línea, sin embargo, con la pandemia del COVID-19, el confinamiento y la necesidad de que aprendan desde casa, el uso de medios digitales se intensificó sin considerar que habría que preparar a las y los NNA para poder desenvolverse en ellos, de forma segura y responsable y es que algo crucial es que reconozcan el modus operandi de los ataques para que ellos los distingan y puedan cuidarse. A continuación, algunos de los riesgos más comunes y algunas de sus principales características.

El ciberbullying es un tipo de hostigamiento que se da a través de los medios digitales como WhatsApp, Facebook, Tiktok, Instagram, entre otros. Las consecuencias de este tipo de violencia son mucho mayores, ya que el alcance de las burlas u ofensas rompe barreras escolares e incluso geográficas, y se pueden derivar otro tipo de situaciones como: amenazas, venganzas, agresiones físicas, pensamientos suicidas, fracaso o absentismo escolar; consumo de sustancias; ansiedad y depresión, entre otros (Zapata, Soriano, González, Márquez, y López, 2015).

El grooming es un ataque en línea, donde un adulto endulza, enamora, engaña y convence por medio de los medios digitales a un menor para persuadirlo y que realice actividades con fines sexuales (Cambridge Dictionary, 2018). Éste regularmente, funciona de la siguiente manera: 1) Un adulto establece contacto con un menor, en la mayoría de los casos haciendo uso de perfiles falsos, 2) el adulto inicia una supuesta amistad con el menor ganándose su confianza, 3) Convence al menor de enviar contenido íntimo (por medio de engaños, o amenazas). En algunos casos, este ataque deriva en delitos graves como: abuso sexual, pornografía infantil y juvenil, sextorciones y tráfico de menores (Pereira, 2017).

El Phishing es una técnica de ingeniería social donde un individuo con conocimiento de hacking suplanta la identidad de una persona o institución de confianza como bancos, aseguradoras, financieras etc., con la finalidad de extraer o utilizar de alguna forma, su información personal.

Aunque el acoso escolar no es un ataque en línea, es preciso considerarlo porque las y los NNA, están confinados, aprendiendo desde casa y el ámbito escolar está ahora mediado por tecnología. Entonces, el acoso escolar ahora no se presenta en las aulas o en las instalaciones escolares, sino a través de todas aquellas plataformas que están siendo utilizadas para la enseñanza y aprendizaje. De acuerdo con López 2012, el acoso escolar se define como el acoso físico, psicológico verbal de manera deliberada que implica un desequilibrio de poder o de fuerza y regularmente se determinan motivos como la raza, religión, por su aspecto, su forma de hablar, etc.; algunas de sus principales características son las siguientes:

1) Persistencia de tiempo: esta situación provoca pérdidas emocionales constantemente, debido a que se genera de manera inventiva y periódica sobre el afectado, esto se logra mediante agresiones culminantes provocadas por la desigualdad de poder.
2) Desequilibrio entre el acoso y el acosador: ambos participantes tienen cualidades diferentes unos inferiores a otros que provocan desigualdad física, psicológica o social. Estos rasgos generan que la víctima se sienta intimidada e incompetente en habilidades o virtudes.
3) Ausencia de provocación de la víctima: la víctima se severa ser una persona pasiva que no provoca problemas con el agresor, este acto se considera una característica muy distinguida de acoso donde la inocencia siempre es del acosado.
4) Indefensión de la víctima: el agresor genera acorralamiento e intimidación cada cierto tiempo, ya sea porque la víctima se muestra pasiva, indefensa, indeficiente, por ser menor de edad, color de piel e incluso género.
5) Complicidad, pasividad o ignorancia del entorno: la generación de estos tres sucesos es provocadas por los individuos que acontecen de manera inconsciente un apoyo a las faltas del agresor, esto puede darse por diversas razones como el miedo o bien por la falta de conocimiento que presentan los padres, compañeros o maestros al no darse cuenta el problema que provoca (Del Pera y Navarro, 2015).

2.3 Aplicaciones para la prevención y atención del ciberacoso

Ante la problemática y los efectos en la integridad física y mental de las y los NNA, existen ahora, diversas maneras de prevenir y atender el ciberacoso, desde tratamientos psicológicos y legales para corregir y eliminar huella de aquellos problemas generados en la víctima. En lo que refiere a la prevención, existen diferentes proyectos que buscan coadyuvar a la prevención de estas amenazas en línea e incluso a brindar una posible solución a incidentes. Este tipo de plataformas, ofrecen contenido audiovisual, juegos serios, aplicaciones con control parental, o botones de pánico etc. A continuación, se muestra un comparativo de 11 plataformas que fomentan la prevención del ciberacoso (Tabla 1).

Tabla 1: Cuadro comparativo de aplicaciones para la prevención del ciberacoso

	Aplicaciones para la prevención del ciberacoso					
	Características funcionales					
Aplicación	**Público que atiende**	**Información sobre ciberacoso**	**Permite reportar problemas**	**País de origen**	**Es gratis**	**Alcance**
MSpy	Padres y tutores	No	Si	EE. UU.	No	Internacional
Appvise	Profesores, padres y alumnos	Si	Si	España	No	Internacional
Eset parental control	Padres y niños	No	Si	Eslovaquia	Gratis/Pago	Internacional.
Qustodio	Familias, escuelas y empresas	No	Si	España	No	Internacional
Dinantia	Colegios, profesores, padres y alumnos	Si	No	España	No	Internacional
Protegete	Hijos	No	Si	España	Si	España
KnowBullying by SAMHSA	Padres e hijos	Si	No	España	Si	EE. UU.
Keepers Child Safety	Padres e hijos	No	Si	EE. UU.	No	EE. UU.
BullySemáforo	Hijos	Si	No	México	Si	México
Anonymous Alerts	Padres e hijos	Si	Si	EE. UU.	Si	EE. UU.
CyberBully Hotline Mobile App	Hijos	Si	Si	EE. UU.	Si	EE. UU.

Nota: Elaboración propia.

Como se puede observar en la Tabla 1, existen varias aplicaciones que atienden al mismo problema, sin embargo, la mayor parte aplicaciones son extranjeras, elaboradas por empresas privadas lo cual implica un costo para las niñas, niños y adolescentes. No obstante, es notable que las aplicaciones extranjeras gratuitas son desarrolladas y puestas en marcha por entidades gubernamentales. En el caso específico de México, no se cuenta con muchas aplicaciones que atiendan el problema, lo que indica que no se han tomado medidas de este tipo como lo han hecho otros países.

Al observar aspectos más técnicos (Tabla 2), se encontró que la aplicación de México es la que menos descargas tiene y además al momento de la revisión, ésta no contaba con servicio de soporte técnico y reportaba fallos en operatividad. Por otro lado, se observa que todas las aplicaciones tienen un espacio en memoria inferior a 50 megabytes, lo que hace que no se requiera

de un equipo con muchas características técnicas. Sin embargo, aquellas que cuentan con control parental y recolección de información, incrementan el uso de espacio en memoria. Con base en lo anterior, se concluyó que es viable y pertinente desarrollar un sistema web adaptable a dispositivos móviles para contribuir en la prevención del ciberacoso.

Tabla 2: Características técnicas de aplicaciones para la prevención del ciberacoso

	Aplicaciones para la prevención del ciberacoso							
	Características técnicas							
Aplicación	Número de descargas	Plataforma	Tamaño de la aplicación		Consumo de batería	Consumo de RAM	Cuenta con soporte técnico	Técnicas de I.A.
MSpy	500,000+	Aplicación Android, IOS, macOS y Windows	12.86MB	Si	120 mAh	493 KB	Si	No aplica
Appvise	500+	Android y IOS	31.66MB	No	230 mAh	326 KB	Si	No aplica
Eset parental control	100,000+	Android y IOS	22.02MB	No	1319 mAh	40 MB	Si	No aplica
Qustodio	500,000+	Aplicación Android, IOS, macOS, Kindle y Windows	29.89MB	No	134 mAh	666 KB	Si	No aplica
Dinantia	10,000+	Android y IOS	15.28MB	No	126 mAh	107 MB	Si	No aplica
Protegete	227	Android y IOS	No disponible	No disponible	No disponible	No disponible	No	No aplica
KnowBullying by SAMHSA	5,000+	Android y IOS	Varia con el dispositivo	No	No disponible	No disponible	Si	No aplica
Keepers Child Safety	10,000+	Android y IOS	45.20MB	No	567 mAh	341 KB	Si	Algoritmo de procesamiento de lenguajes naturales (NLP)
BullySemáforo	100+	Aplicación Android, IOS, macOS, web y Windows	4.57MB	No funciona	No funciona	No funciona	No	No aplica

Anonymous Alerts	5.000+	Android	7.5 MB	No	42 mAh	162 KB	Si	No aplica
CyberBully Hotline Mobile App	No aplica	Android y IOS	No aplica	No	No aplica	No aplica	Si	No aplica

Nota: Elaboración propia.

2.4 Metodología

La ingeniería de software es un método que incluye todos los procedimientos del ciclo de vida del software, aplicando un conjunto de prácticas automatizadas que infieren desde la especificación del sistema hasta el mantenimiento (Ingeniería del Software 7ma. Edición). Para el desarrollo de la plataforma web, se requirió de la aplicación de metodologías y modelos para simplificar procesos, así también de manera inherente se aplicó un conjunto de herramientas CASE que comprenden un amplio abanico de tecnologías que ayudan a la realización de tareas en todo el proceso de software. Es preciso señalar que, para la construcción de la plataforma, se trabajó con dos metodologías Scrum, e Iconix, esto debido a que por la naturaleza del proyecto, los tiempos de desarrollo y la necesidad de trabajar con el equipo de trabajo de especialistas de SIPINNA, Xalapa, fue preciso integrar ambas metodologías para ajustarse fácilmente a cambios de requerimientos, pues el cambio de requerimientos es considerado en sí un requerimiento y por otro lado, se esperaba realizar entregas y retroalimentaciones constantes y periódicas al cliente. De esta forma, el proceso de desarrollo se mejoró de manera continua y el cliente podía verificar el estado del desarrollo, familiarizarse con las funcionalidades del producto de manera progresiva y de esta manera revisar que #NNASegur@s cumpliese con sus requerimientos.

La metodología de desarrollo implementada se resume en lo siguiente:

1. Análisis de otros temas relacionados con el problema: se realizó una investigación documental acerca de temas relacionados con la prevención de violencias contra niñas, niños y adolescentes, a través de medios digitales.
2. Recolección de requerimientos a la institución SIPINNA Xalapa: se agendaron citas semanales o quincenales con la institución para obtener los requerimientos necesarios para el desarrollo de los casos de uso de la etapa de análisis.
3. Elaboración y entrega del Software Requirements Specification (SRS): consistió en la entrega de un documento donde incluyó toda la documentación y especificaciones del producto de software.
4. Diseño y construcción del prototipo no funcional: se plasmaron los casos de uso al diseño de las interfaces de usuario.
5. Reunión de planificación de Sprint (iteración): en esta fase se definieron las fechas de reunión de manera mensual, y se aterrizó la forma de organización con el equipo de SIPINNA Xalapa para cada uno de los Sprints, también se elaboraron las estimaciones de tiempo y esfuerzo, y éstas se representaron mediante listas de tareas priorizadas (Sprint Backlog).
6. Desarrollo del sistema: aquí se trabajó en las tareas del Sprint Backlog para evaluar el progreso que tuvo el Sprint cada dos semanas, para ello se utilizó a menudo un Scrumboard (tablero de información) para realizar el seguimiento del trabajo y de actividades que se

llevaron a cabo para el desarrollo de cada componente del sistema y verificar los inconvenientes que se presentasen.

7. Revisión del Sprint: esta reunión se llevó a cabo al finalizar cada iteración. Se hizo una demostración de todos los requerimientos finalizados dentro del Sprint para inspeccionar el incremento y adaptar, si es necesario, el producto de software.
8. Pruebas: en esta fase se probó el sistema en cuanto a rendimiento, seguridad y funcionalidad de cada componente desarrollado, las pruebas se hicieron de manera interna y externa por parte del cliente. Durante el proceso de pruebas se aplicaron métricas para llevar un control del porcentaje de requerimientos funcionales y no funcionales, cuales se cumplen o no, en qué nivel de exactitud, y cuáles son las debilidades y fallas en las que se tuvo que trabajar para su corrección. Al terminar las correcciones se anotaron en las métricas, y se procedió a una segunda evaluación de pruebas, al concluir el proceso de pruebas se desarrolló los casos de pruebas unitarias e integrales. Por último, al finalizar el sistema se le entrega a SIPINNA una versión beta de todos módulos desarrollados, para que se pueda verificar y validar la funcionalidad de los módulos simulando un ambiente real con usuarios definidos por SIPINNA.

3 Desarrollo

3.1 Análisis

El análisis es la primera etapa de un proceso de software, esta etapa consiste en el acercamiento con lo Stakeholders para la recolección de las necesidades, en este caso el SIPINNA Xalapa, que es un organismo encargado de supervisar la garantía de los derechos de las niñas, niños y adolescentes y que trabaja de manera coordinada con las escuelas privadas y públicas del municipio. Durante su proceso de operación, aquí se trabajó de la siguiente manera: Se hizo un estudio de modalidades de ciberacoso y acoso (cyberbullying, grooming, phishing, bullying y acoso escolar); por otro lado, se aplicó un estudio exploratorio sobre diversas aplicaciones que atiendan problemas de acoso escolar y riesgos digitales; se mantuvieron reuniones de trabajo con psicólogos y personal del SIPINNA Xalapa; y se trabajó de manera directa con estudiantes de cuarto, quinto y sexto de primaria y primero, segundo y tercero de secundaria. Así mismo, se realizó una investigación documental, en la que se revisaron diferentes modalidades de violencia, orientada en reconocer su definición, quiénes son regularmente sus víctimas, quiénes suelen ser los atacantes, cómo opera, qué lo ocasiona, sus consecuencias, así como las medidas de prevención y detención implementadas por diversas organizaciones públicas y privadas que atienden estos tipos de violencias (Cambridge Dictionary, 2018; Fundación UNAM, 2018; Cussiánovich, Tello y Sotelo, 2016; Domenech, 2016; Moisés, 2018; DAS, 2017; López, Finalé, Villén, Mora, y Ortega, 2013; Zapata, Soriano, González, Márquez, y López, 2015; Herrera, 2017; UNICEF, 2018). De esta revisión, se definió que la plataforma debía abordar tres temas primordiales: a) información de los tipos de riesgos en línea, el modo en que operan y la forma de prevenirlos, b) diagnósticos que permitan reconocer si las y los niños ya fueron víctimas de alguno, y c) proveer mecanismos para reportar incidentes y que la organización encargada de procurar su protección pueda dar seguimiento y atender estos casos.

A partir de lo anterior, se definieron los requerimientos funcionales, atributos de calidad y reglas de negocio. Se diseñaron varios modelos marcados por la metodología de desarrollo de

software utilizada. En la Figura 1, se presenta el modelo de contexto que contiene el panorama general y funcional del sistema como un todo, destacando las principales funcionalidades y la interacción con los usuarios en un entorno de trabajo.

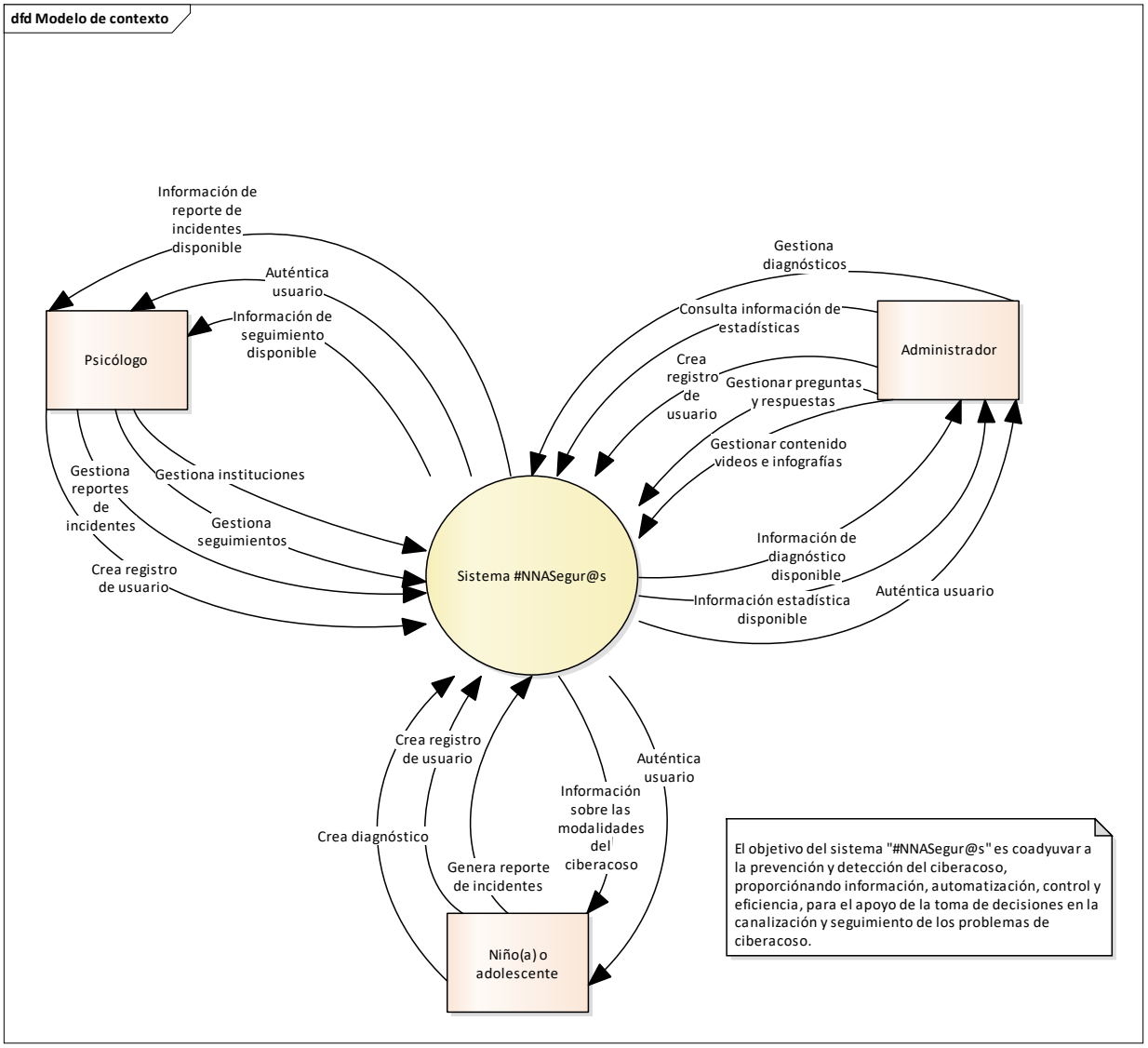

Figura 1. Modelo de Contexto de la Plataforma #NNASeguros.

Así mismo, se desarrollaron otros modelos como: el modelo de procesos de negocio, el modelo de dominio y los casos de uso, entre otros.

3.2 Diseño

Durante la fase de diseño, se definieron las tecnologías para el desarrollo del software. Las tecnologías elegidas para el desarrollo del Backend fueron: PostgreSql para la base de datos y Spring Framework 5; para el desarrollo del Frontend, se utilizó Angular 7, HTML, CSS, JavaScript y Bootstrap. Una vez definidas las herramientas de desarrollo, se trabajó en la estructura del sistema, se definió un modelo de componentes para identificar aquellos elementos indicados que representan la estructura física del sistema. Esto permitió diseñar el diagrama de arquitectura del software, tomando como base la arquitectura Modelo Vista Controlador (MVC)

y la arquitectura Cliente-Servidor, implementando un patrón de diseño llamado Representational State Transfer (REST), que consiste en una API (Servidor) que será consumida mediante peticiones de Hypertext Transfer Protocol (HTTP) por un cliente (Frontend). Para dar continuidad, se implementaron los diagramas de robustez resultantes del análisis preliminar de los casos de uso, así también se definió el modelo de datos correspondiente partiendo del modelo de dominio definido en la fase de análisis.

Partiendo de unos Sketch obtenidos en la fase de análisis y ya haber definido la interacción del usuario con el sistema mediante flujos básicos y flujos alternos, y se diseñó el prototipo no funcional con un correspondiente diagrama de arquitectura de información que muestra la jerarquía de las interfaces (Figura 2) y el flujo de navegación que se debe seguir para realizar las tareas en el sistema.

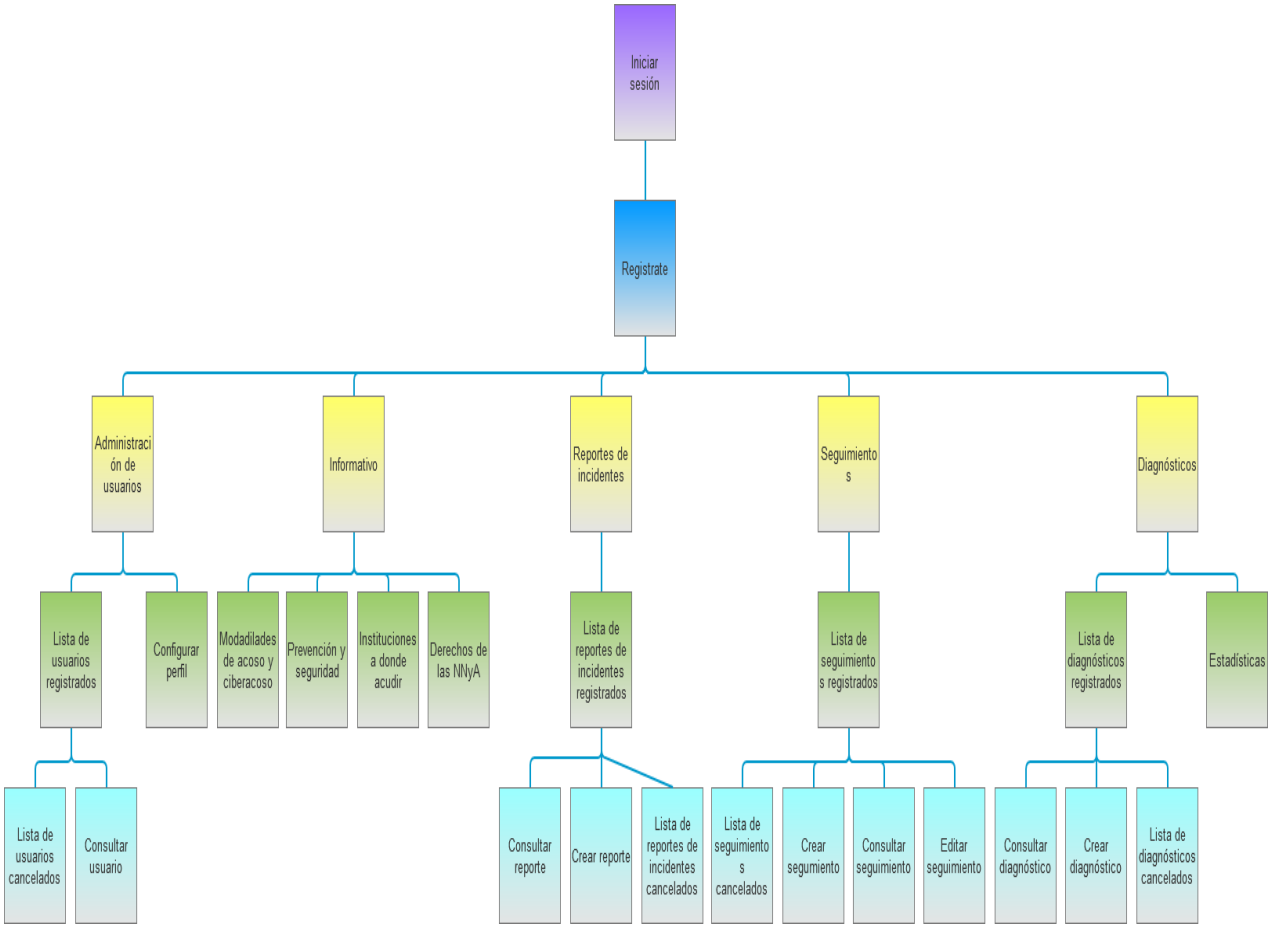

Figura 2. Jerarquía de interfaces.

En lo que corresponde a la arquitectura de software, se tomo como base los Frameworks utilizados (Angular, Spring MVC y Bootstrap), tal como se muestra en el siguiente modelo (Figura 3).

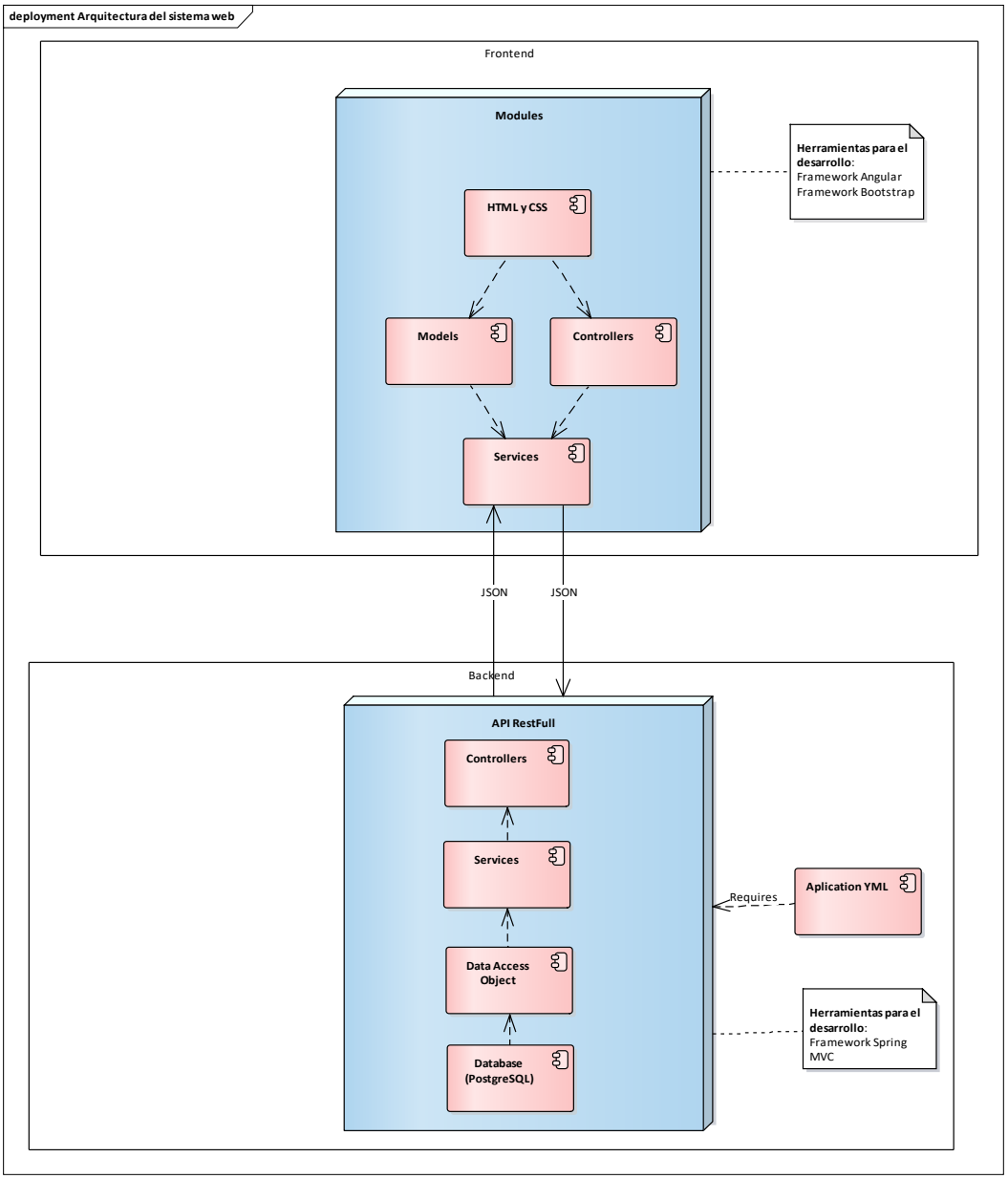

Figura 3. Arquitectura del Sistema #NNASegur@s.

Es preciso señalar que el diseño de la plataforma incluyó también la generación de contenido digital que se desarrolló en conjunto con un equipo de psicólogos y especialistas en la atención de niñas, niños y adolescentes del Sistema para la Protección Integral de Niñas, Niños y Adolescentes de Xalapa. Todo el contenido se generó bajo la licencia *Creative Commons*. A continuación, un ejemplo de las infografías diseñadas (Figura 4):

Figura 4. Ejemplo de infografía incluida en #NNASegur@s.

3.3 Desarrollo

El desarrollo de la plataforma denominada #NNASegur@s, implicó la aplicación de tecnologías que permitiesen la implementación de API REST, que constan de separar completamente una aplicación de manera que el Backend se convierte en un servicio REST que puede ser consumido por una aplicación cliente como Angular. En esta implementación, se utilizó Sprint Framework tomando todas las restricciones de la arquitectura MVC para desarrollar la API.

En Spring se tiene desarrollado los servicios necesarios para que el Frontend pueda hacer peticiones HTTP, mostrar, insertar, actualizar y eliminar información de la base de datos. Para realizar las peticiones necesarias se requiere de autenticación, por lo tanto, se usó el protocolo de autorización (OAuth) en su versión 2.0, este estándar se basa en la implementación de tokens que permiten encriptar la información del usuario autenticado de manera que esta quede resguardada y pueda ser validada únicamente por el usuario que genera el token al momento de iniciar sesión en el sistema.

En la Figura 5, se muestra un ejemplo de peticiones realizadas y probadas con una herramienta de testeo llamada Postman (software para probar sistemas con API REST, a través de peticiones HTTP). En este caso, se trata de la generación del token de acceso al sistema una vez que el usuario ingresa y el sistema valida que existe en la base de datos.

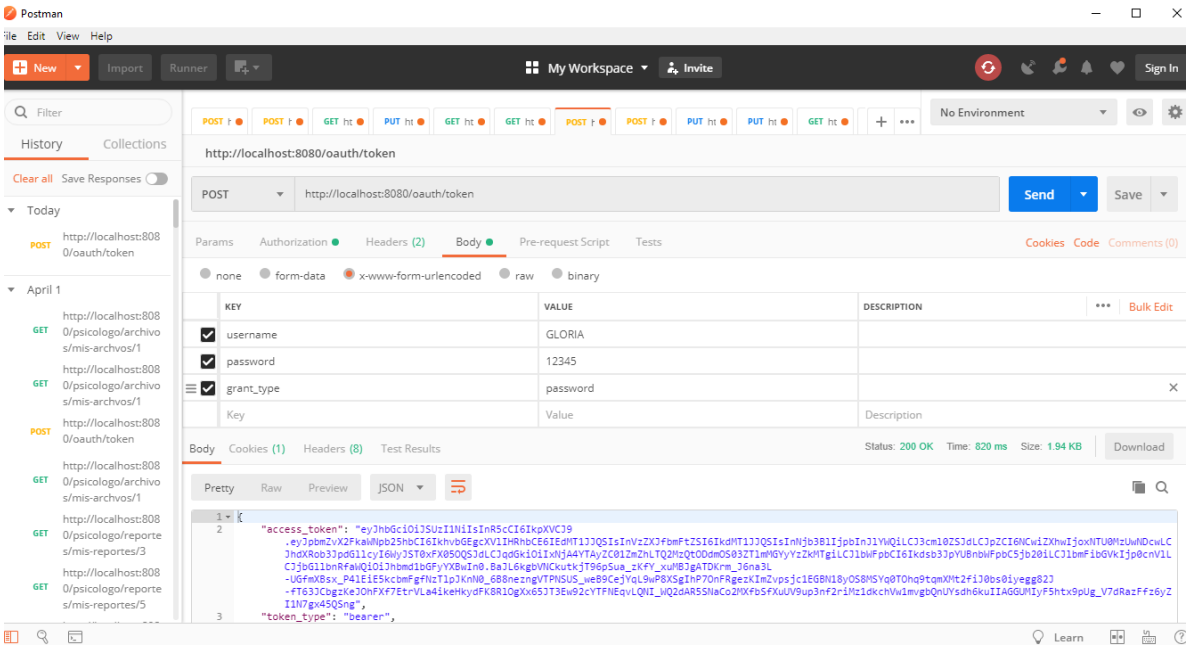

Figura 5. Petición al sistema, utilizando Postman.
Nota: Elaboración propia.

4 Resultados

4.1 La Plataforma #NNASegur@s

La plataforma denominada #NNASegur@s, tiene como objetivo, coadyuvar a la prevención y atención de casos de ciberacoso a niñas, niños y adolescentes. A continuación, se detallan los principales módulos que la conforman.

Módulo informativo

Este módulo tiene la finalidad de brindar contenido digital a niñas, niños y adolescentes, para poder informarlos acerca de riesgos en línea y medidas de seguridad. Algunos de los temas abordados, son: cyberbullying, grooming, phishing, acoso escolar y sexting. Es importante recalcar que el contenido está formado por infografías y videos, diseñados en colaboración con los psicólogos de SIPINNA. El contenido agregado es completamente dinámico, ya que se generó un apartado en el sistema para que el administrador pueda subir y actualizar la información cuando sea necesario, en este apartado se tienen ciertas características en los archivos que SIPINNA podrá modificar y que serán brindadas en un instructivo, el cual se puede ver más sobre este, en la sección de apéndices. En la Figura 6 se muestra un ejemplo de pantalla del módulo informativo.

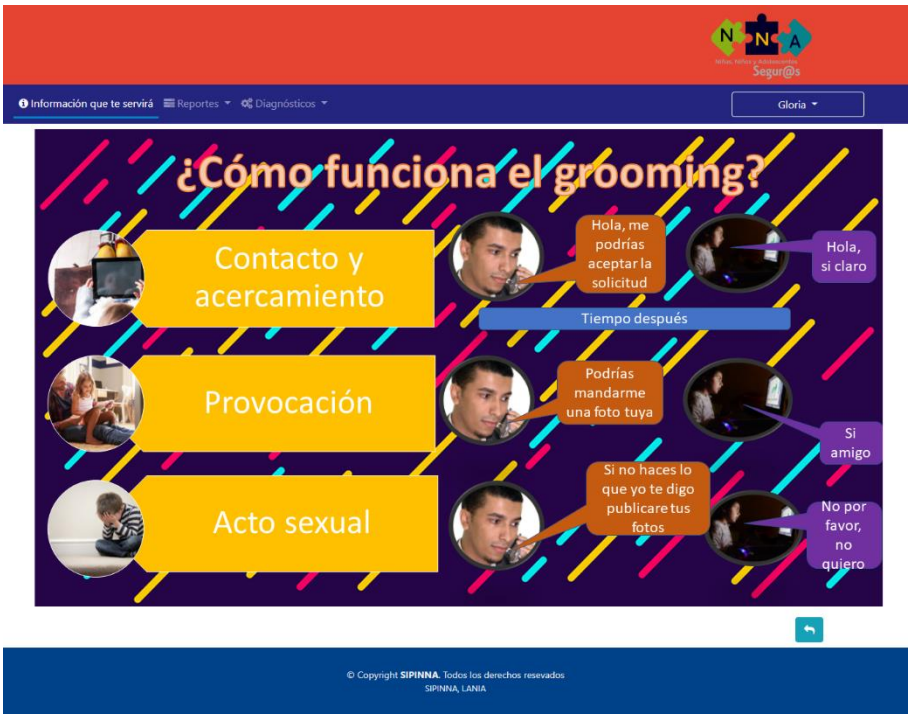

Figura 6. Pantalla ejemplo del Módulo informativo de #NNASegur@s.
Nota: Elaboración propia.

Módulo de diagnósticos

Está compuesto por una sección de diagnóstico que permite medir el nivel de vulnerabilidad de las niñas, niños y adolescentes en línea (Figura 7). Por otro lado, SIPINNA cuenta con una sección donde puedan gestionar los diagnósticos generados y un apartado de estadísticas generales en las que ellos podrán utilizar para la toma de decisiones, así como para ver la posibilidad de generar talleres en las escuelas (de nivel primaria, secundaria y bachillerato) en caso de que identifiquen alto riesgo o varios casos de ciberacoso reportados. Es decir, que el sistema, servirá a la institución para la toma de decisiones e implementación de acciones de prevención o atención.

Figura 7. Ejemplo de pantalla del módulo Diagnóstico.
Nota: Elaboración propia.

Módulo de reportes de incidentes

Este apartado, permite a las niñas, niños y adolescentes reportar casos de ciberacoso. Los reportes pueden ser anónimos o propios, dependiendo de tipo de reporte que se elija, aparecerán los campos correspondientes. Por otro lado, SIPINNA gestionará los reportes y dará de alta un seguimiento continuo para brindar la correcta atención al problema. Es importante mencionar que SIPINNA no cuenta con el suficiente personal en diferentes áreas, por ejemplo, SIPINNA solo cuenta con psicólogos y no con abogados. En todo caso y dependiendo de la gravedad del caso reportado, el SIPINNA, se encargará de canalizar la situación con la dependencia correspondiente (Figura 8).

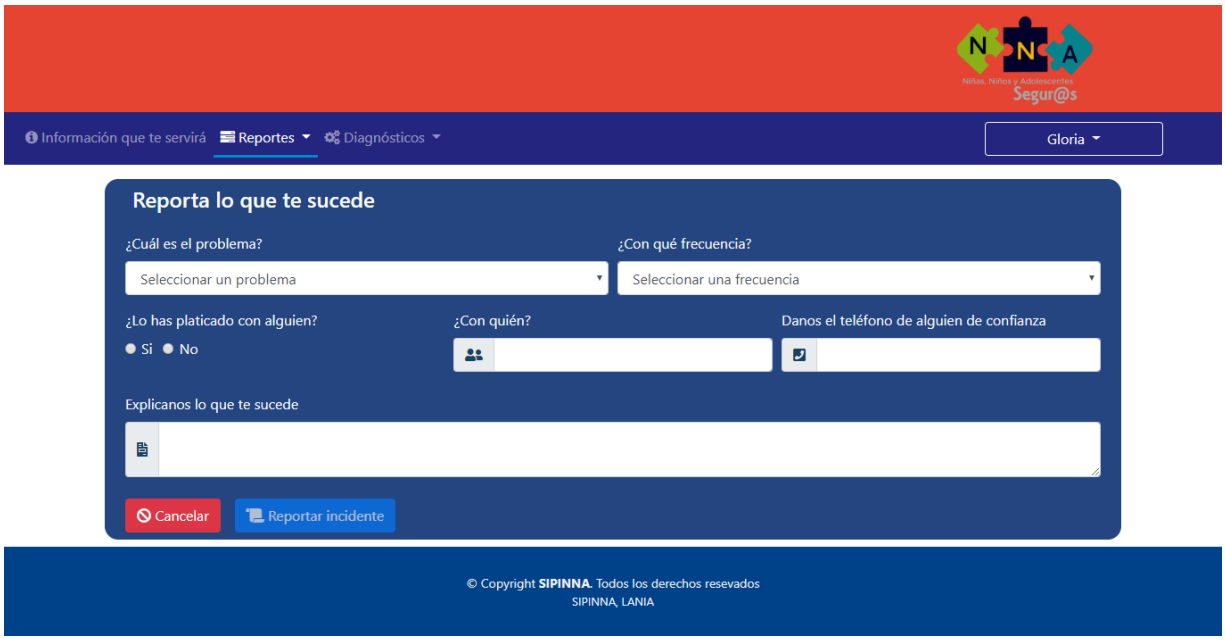

Figura 8. Ejemplo de pantalla de módulo de reporte de #NNASegur@s.
Nota: Elaboración propia.

4.2 Pruebas

Durante la fase de pruebas, se definieron tres tipos de pruebas: unitarias, integrales y Alfa. A continuación, lo encontrado en cada una.

Pruebas unitarias

Estas requieren de un conjunto de pruebas aplicadas a las funcionalidades de cada uno de los módulos. Para lograrlo, se llevó a cabo la ejecución de unos formatos denominados casos de prueba y se registraron resultados de entrada, los resultados esperados y los resultados obtenidos por el sistema. Cada caso de prueba se segmenta en una funcionalidad (un propósito), requerimiento previo, secuencia y proceso, para que al final, se puedan evaluar los datos de entrada, los datos de salida y los datos esperados y así validar que las funcionalidades arrojen los resultados correctos o si estos tienen un margen de error, aplicar correcciones a las funcionalidades.

Pruebas integrales

Las pruebas integrales, reflejan un proceso secuencial en el que intervienen varias funcionalidades, esto con la finalidad de verificar el correcto funcionamiento del sistema mediante la simulación de realización de tareas específicas. Para lograrlo se definieron flujos basados en la plantación de escenarios de prueba, con la intervención de tres niñas, niños o adolescentes y dos psicólogos: uno reflejando el rol de psicólogo y el otro el rol de administrador. Los flujos seleccionados, fueron los siguientes: a) registro y autenticación de usuario, b) registro de diagnóstico y consulta de resultados mediante indicadores estadísticos, c) generación de reporte de incidentes y registro de seguimiento y d) gestión del contenido informativo.

Pruebas Alfa

Estas pruebas fueron aplicadas a la primera versión completa del sistema y se llevaron a cabo con los clientes, testers o en su defecto el equipo de desarrolladores. En este caso, se aplicó con los

usuarios finales para poder detectar errores u opiniones de usuarios, sin conocimiento previo del sistema (desplegado en un ambiente real y contralado). En esta evaluación de laboratorio, se capacitó a cuatro miembros de SIPINNA (ambos usaron los roles de niñas, niños o adolescentes, Administrador y Psicólogo), después de la capacitación se asignó a cada integrante una serie de métricas que permiten identificar con qué características de calidad cuenta el producto de software. También se les asignó un documento con tareas específicas para ser ejecutadas después de la capacitación. Para evaluar la calidad, se utilizó la norma ISO25010, se seleccionaron tres de los ocho atributos de calidad. Los atributos seleccionados fueron: eficiencia del desempeño, usabilidad, seguridad. Una vez definidos los atributos de calidad a evaluar, se definieron con base a la "Goal, Question, Metrics" (GQM) tres objetivos operativos, uno para cada atributo de calidad, después se generaron una serie de aspectos a evaluar, mediante una calificación acorde a la escala de Likert. La escala de Likert permite definir una serie de ítems o cuestionamientos seleccionados para crear un criterio valido, fiable y preciso para realizar una medición que en este caso fue con valores de uno al cinco.

Respecto a la evaluación del sistema con las niñas, niños y adolescentes, se aplicó un conjunto de métricas adaptadas a un lenguaje intuitivo para los menores, de la misma forma se valoraron la usabilidad, seguridad y eficiencia del desempeño. En esta sesión participaron 8 NNA con edades de 12 a 17 años para probar las funcionalidades de la plataforma #NNASegur@s.

4.3 Análisis de los resultados de las funcionalidades del sistema con los usuarios de SIPINNA

Una vez realizadas las pruebas, se concluyó que el sistema se encuentra con porcentajes estables (mayores al 80% estimado) en cuanto a seguridad, usabilidad y eficiencia del desempeño.

Con respecto a la seguridad, se detectó que protege la información de usuarios ajenos al sistema y mantiene la información consistente.

En cuanto a usabilidad, el software es accesible ya que no se requiere de conocimientos avanzados de computación para ser usado, así también, cuenta con una estética favorable si se adapta a dispositivos con ciertas características definidas (dimensiones 1024 x 768, 1280 x 1024 y 1920 x 1080 pixeles), además de que cuenta con las etiquetas, alertas y descripciones para evitar la mínima cantidad de errores posibles durante la realización de las tareas.

Para evaluar algunos aspectos de la eficiencia de desempeño se requirió de la aplicación de pruebas automatizadas. Las pruebas automatizadas son aquellas que se realizan por medio de un software especializado en testear aspectos de rendimiento y/o seguridad. El software utilizado fue gtmerix y PageSpeed Insights, que son sitios web que hacen peticiones al backend para medir el rendimiento y la concurrencia. En cuanto a los resultados obtenidos en la eficiencia del desempeño, fue que el tiempo de respuesta es rápido en términos inferiores a 3 segundos. Los elementos del sistema responden de manera rápida, y puede soportar la concurrencia de varios usuarios simultáneos realizando operaciones de lectura y escritura.

Se observó que en las tareas de registro de usuario y en edición del perfil de usuario, los testers obtuvieron un tiempo mayor al estimado, sin embargo, en la edición del perfil fue más rápido de lo esperado. En las actividades de registro y de inicio de sesión, el tiempo esperado fue de 03:00 minutos y se obtuvo de promedio de 03:10 minutos superando el tiempo establecido

como mínimo; en las actividades de generar diagnósticos y consultarlos a detalle, los tiempos de ejecución de las actividades fueron inferiores (03:23, 02:26 y 03:41 minutos), salvo un caso (04:11 minutos). En las actividades de reportar incidentes y brindar un seguimiento se obtuvo de promedio 05:23 minutos por debajo del valor estimado (05:30 minutos); en las actividades para consultar información sobre los riesgos digitales se encontró que todos los usuarios ejecutan las tareas cerca de 01:00 minuto.

En la Figura 9, se muestra un porcentaje favorable superior a las espectativas (80%), lo que indica que el sitema tiene índices altos de seguridad y los porcentajes restantes en cada una de las subcaracteristicas del atributo de seguridad seran atendidos para reforzarla.

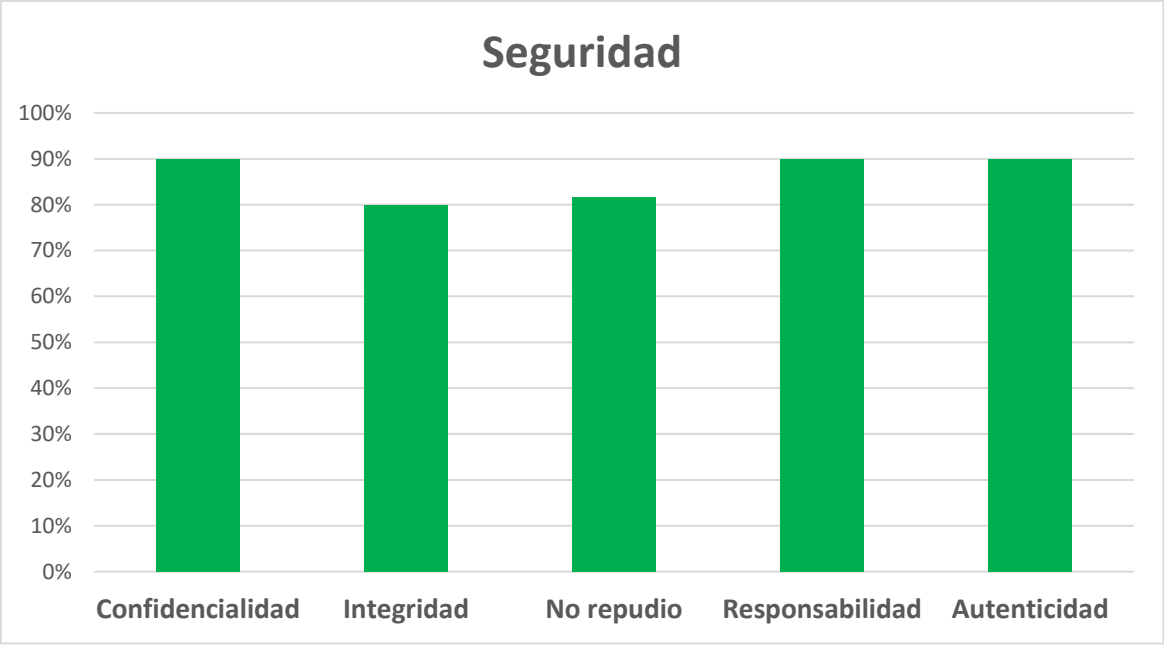

Figura 9: Gráfica sobre los resultados del atributo de seguridad.

En la Figura 10, se muestra un porcentaje favorable en la accesibilidad, estética de interfaz de usuario capacidad de aprendizaje y protección de errores, sin embargo, las validaciones de los formularios hicieron un poco complejo generar los registros de manera rápida al tiempo estimado, por lo tanto, el sistema debe de mejorarse para reducir su capacidad de ser usado en un tiempo cercano a dos horas.

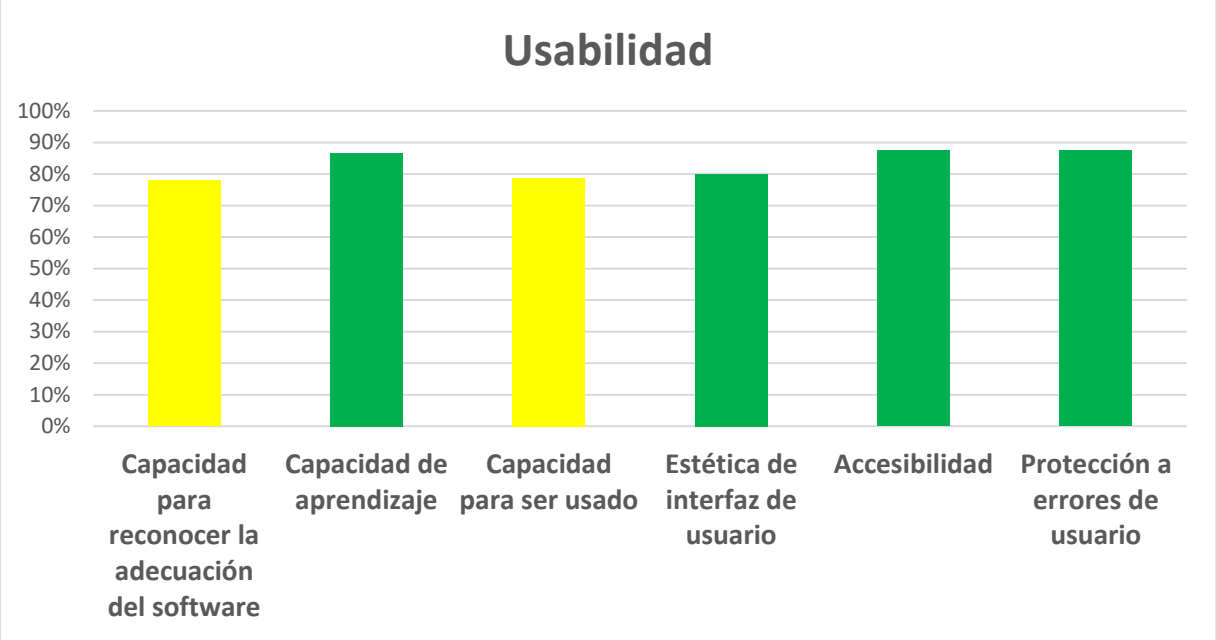

Figura 10: Gráfica sobre los resultados del atributo de usabilidad.

En la Figura 11, se muestra un porcentaje favorable en cuanto a su capacidad de responder a simultaneas operaciones de lectura y escritura, así como a tener un tiempo de respuesta rápido en las transacciones y cargas de los elementos de la página, estando entre los 3 a 5 segundos aproximados.

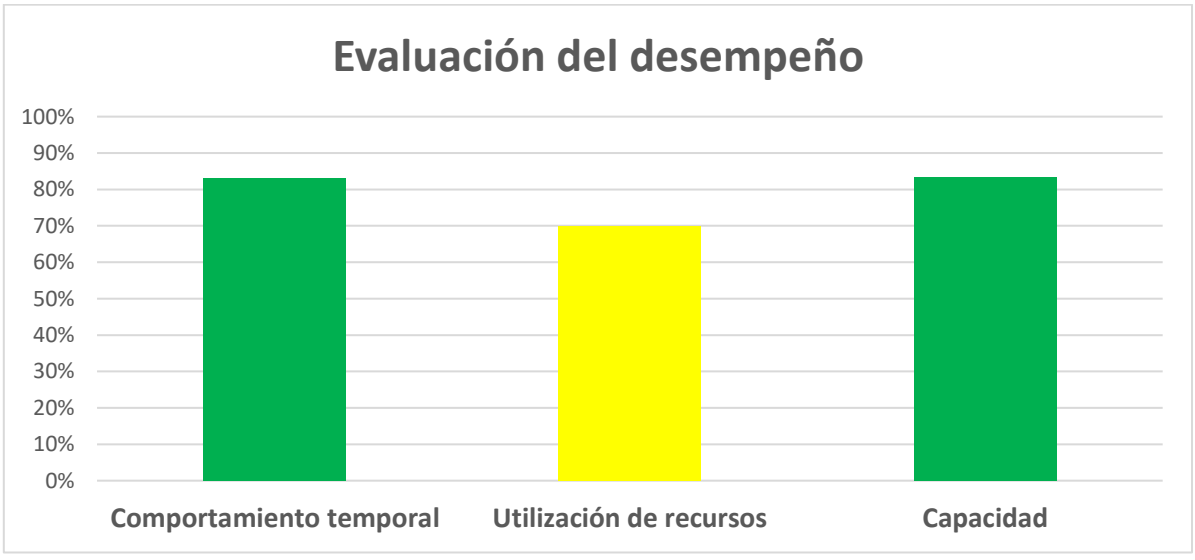

Figura 11. Gráfica sobre los resultados del atributo de evaluación del desempeño.

Evaluación de las funcionalidades del sistema con los NNA

Se llevó a cabo una reunión con las niñas, niños y adolescentes (8 personas con edades de 12 a 17 años) para probar las funcionalidades de la plataforma #NNASegur@s, para tales efectos se aplicaron un conjunto de métricas que permiten medir la calidad del producto de software e identificar el correcto funcionamiento del sistema valorando la usabilidad, seguridad y eficiencia del desempeño. El proceso se llevó a cabo dando como apertura una introducción sobre los riegos

digitales, después se les dio un contexto sobre el proyecto y se les capacitó en el sistema. Luego se les asignó un conjunto de actividades para probar el sistema y al finalizar contestaron las métricas.

En la Figura 12, se muestran los resultados de la evaluación del desempeño resaltando porcentajes favorables en el comportamiento temporal: en cuanto al tiempo de respuesta de los componentes, velocidad de carga de los elementos, de registros etc.; utilización de recursos: con respecto a la navegación del sistema, el tiempo de subida de archivos etc.; y en la capacidad: en cuanto al soporte de concurrencia en términos de escritura y lectura.

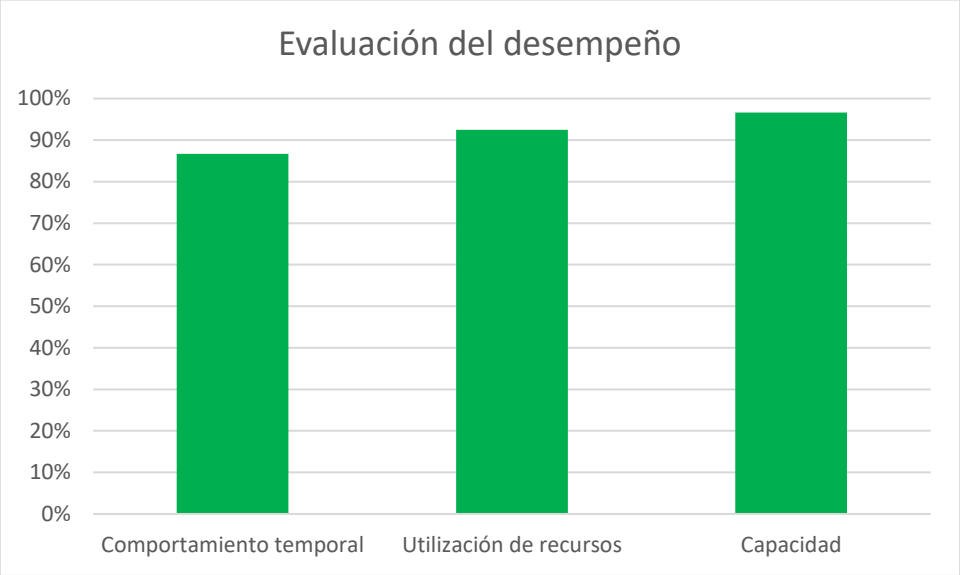

Figura 12. Resultados de la evaluación del desempeño.

En la Figura 13, se muestran índices elevados del 80% en la accesibilidad, protección de errores, capacidad de uso, de adecuación y de aprendizaje, pero desfavorece en la estética de interfaz, lo que refleja un punto que en primera instancia debe de atenderse, para garantizar una interfaz amigable para las niñas, niños y adolescentes.

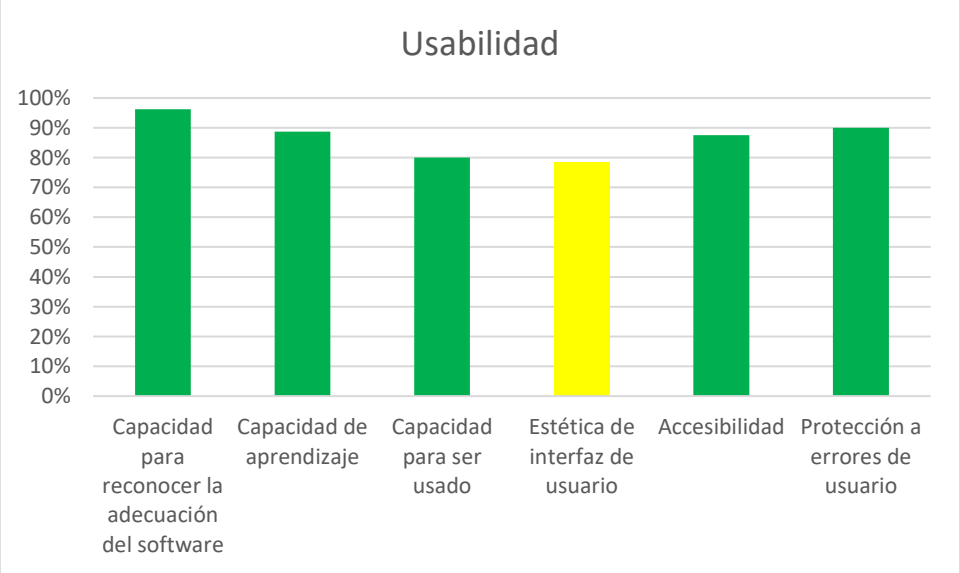

Figura 13. Resultados de la usabilidad.

En la Figura 14, se muestran los resultados de seguridad destacando principalmente la integridad de los datos que alcanzó un 100%, mientras que el resto de subcaracterísticas reflejan que el sistema cumple con la capacidad de reconocer la autenticidad de los usuarios, y es aceptable para las niñas, niños y adolescentes, así como garantizar que se proteja la información a usuarios ajenos.

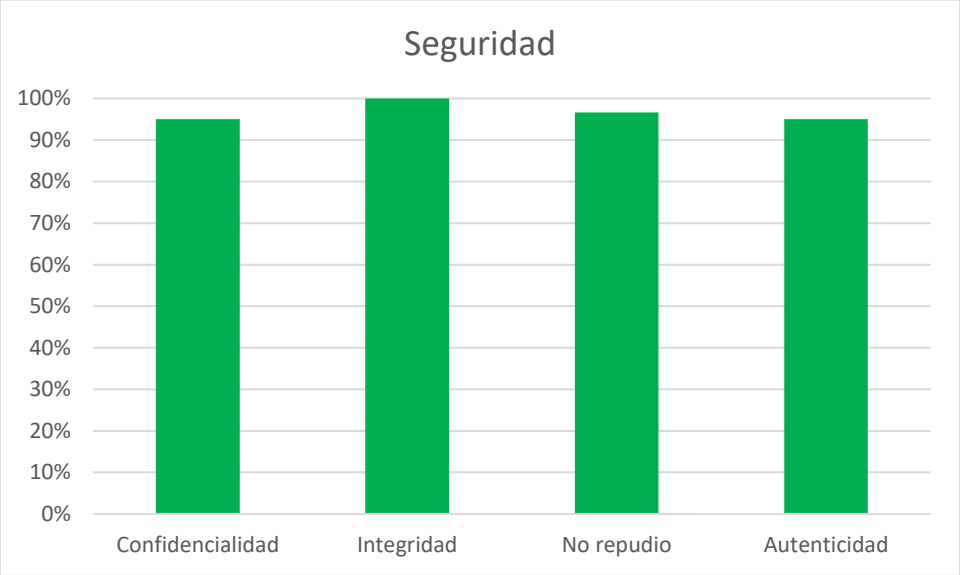

Figura 14. Resultados de la seguridad.

5 Discusión y Conclusiones

Este trabajo tuvo como objetivo desarrollar un sistema web que coadyuve a la prevención, diagnostique y brinde seguimiento de casos de ciberacoso en niñas, niños y adolescentes, sobre todo ahora que ellos se encuentran confinados, aprendiendo desde casa debido a la pandemia del COVID19 y por lo tanto el uso de medios digitales ha crecido exponencialmente (Statista, 2020). Ahora bien, para la construcción del sistema, se trabajó bajo un proceso metodológico, aplicando normas ISO, diagramas, prototipos y métricas. Con base en la metodología definida, se elaboró cada una de las actividades y al finalizar este trabajo, podemos concluir lo siguiente:

Realizar un estudio sobre los riesgos y amenazas en línea, permitió concientizar puntos específicos para poder definir la información adecuada y lograr la implementación del módulo informativo. Con esto, se observó que los riesgos en línea tienen particularidades diferentes en la forma de operar (Pereira, 2017), en el caso de cyberbullying, el acoso viene en ocasiones de origen local (generado en las escuelas, hogares o cualquier otro lugar de convivencia) y puede ser ocasionado por cualquier tipo de personas. Por lo regular, esta amenaza genera hostigamiento, provocación, denigración, violación a la intimidad y la exclusión; en el grooming, son los adultos los que observan y buscan a una víctima fácil de engañar mediante perfiles falsos (generalmente mostrándose como jóvenes) para ganarse la confianza de las niñas, niños y adolescentes; y en el phishing, la suplantación se genera usando técnicas de ingeniería social y su objetivo es con fines lucrativos, de chantaje o extorción. Es importante señalar que no existe amenaza más grave que otra, todas ellas, pueden tener en las y los NNA efectos como depresión, medio de salir a la calle, bajo rendimiento académico, suicidio u homicidio, trata de menores, prostitución, venta de órganos y pornografía infantil y juvenil, entre otros.

Al revisar las plataformas que atienden el ciberacoso y acoso escolar (Tabla 1 y 2), permitió identificar la pertinencia de desarrollar una aplicación que pudiera atender problemas de ciberacoso, y que se apegara a las necesidades requeridas por SIPINNA como: brindar contenido sobre riesgos digitales y medidas de prevención, diagnosticar a los NNA, reportar incidentes de manera anónima y personal, generar indicadores estadísticos sobre los resultados obtenidos de los diagnósticos y reportes de incidentes; y brindar seguimiento a un problema de ciberacoso determinado. En el estudio exploratorio se evaluaron aplicaciones privadas y públicas de origen extranjero y local. En el caso de México solo se encontró una y desafortunadamente está sin servicio, ya que no se puede operar debido a su falta de mantenimiento. Por otro lado, las aplicaciones extranjeras no cumplen con los requerimientos que SIPINNA solicita. En el caso de las aplicaciones privadas, tienen un costo elevado; y las públicas, consumen muchos recursos del hardware del dispositivo. En el proceso, se identificó que los NNA no tienen dispositivos móviles con características suficientes para soportar aplicaciones con consumos altos en hardware, y que no se encuentran aplicaciones web con funcionalidades específicas, ya que las que se encontraron son solo informativas o en su caso son paneles de administrador para el control parental. Por lo tanto, la solución fue desarrollar un sistema web que pudiera ser accesible en cualquier dispositivo.

En la implementación del diagnóstico para identificar si los NNA han sido víctimas de ciberacoso, se identificó que a los usuarios les parece interesante poder evaluarse mediante preguntas intuitivas que no representan un examen de escuela sino una actividad importante (Edu Kids International, 2019). Además de que podrán obtener resultados para saber si ellos pueden ser vulnerables por no tomar medidas adecuadas para protegerse sobre los riesgos digitales. También consideran importante que SIPINNA pueda detectar en que escuelas se presentan más situaciones de riesgos y de esa manera interferir mediante la aplicación de talleres y asesorías.

En cuanto a la necesidad de generar reportes de incidentes se identificó que las y los NNA consideran pertinente reportar los problemas que se presentan de manera anónima para que no identifique SIPNNA quien es el autor del reporte. Otros, prefieren que los reportes sean personales y anónimos porque consideran que es preciso que se les ayude y que no quede impune los actos que atentan contra su integridad. Además de que, anexar evidencias brinda firmeza para que SIPINNA u otras instituciones puedan encaminar investigaciones y aplicar medidas correspondientes. Para lo anterior, el sistema ofrece lo siguiente:

- Un apartado para que SIPINNA pueda gestionar la información de todas las niñas, niños y adolescentes; así como un apartado de configuración para que todos los usuarios puedan configurar su perfil de usuario y recuperar la contraseña en caso de que se requiera.
- Un módulo de contenido informativo, que cuenta con 6 submódulos y en cada uno se definió un conjunto de temas de ciudadanía digital; también se diseñó infografías y videos para integrarlas en los submódulos correspondientes.
- Un módulo de diagnóstico, que cuenta con un test que permitirá evaluar a las y los NNA para que SIPINNA pudiera identificar que tan vulnerables son en un zona o escuela y poder actuar de manera prudente y con los fundamentos necesarios para poder apoyar mediante la aplicación de talleres.
- Un módulo de reporte de incidentes: aquí se desarrollaron componentes Web que permiten reportar de manera anónima y no anónima casos de acoso y ciberacoso al SIPINNA, y así,

ésta canalice la situación y pueda atender o en su defecto pasarlo con las dependencias adecuadas llevando un control de todo el proceso para que los NNA puedan visualizar en qué etapa está su reporte.

Al concluir con el desarrollo de la aplicación se aplicó pruebas unitarias, de integración y pruebas alfa logrando verificar y validar la efectividad del sistema mediante la aplicación de métricas definidas con objetivos operacionales identificados por la Goal Question Metrics, que permitieron medir la usabilidad, seguridad y eficiencia en el desempeño, planteando un escenario real (con un conjunto de actividades) donde se presentó el sistema y se capacitó a niñas, niños, adolescentes y personal de SIPINNA.

Cabe resaltar que en la ejecución de las pruebas alfa el sistema logró los siguientes resultados favorables:

En la evaluación de la seguridad se identificó que el software puede operar correctamente ofreciendo protección de la información ante usuarios no autenticados; garantizando la privacidad de los datos para solo ser vista por el usuario que tenga las credenciales y permisos. Todo esto con base que el sistema cumplió con los estándares de confidencialidad, integridad, no repudio, responsabilidad y autenticidad en un 80% o más. Esto es importante porque a pesar de no tener información personal sobre las niñas, niños y adolescentes, el sistema debe de asegurar un ambiente seguro para establecer confianza a los menores.

En la evaluación de la usabilidad se determinó que el sistema cubre la necesidad de uso en diferentes dispositivos con dimensiones de pantallas predefinidas garantizando en todo momento una distribución de los elementos optima. También se concluyó con base a los resultados obtenidos que el sistema incluye un conjunto de elementos permitiendo facilidad de uso y de aprendizaje por el usuario.

En la evaluación de eficiencia del desempeño fue necesario complementar con pruebas automatizadas para poder simular escenarios con un exhaustivo consumo de requerimientos. Cabe resaltar que el sistema permite soportar una concurrencia de 50 peticiones y funcionar correctamente. Es importante ya que varios NNA pueden reportar y diagnosticarse sin fallos en la carga de elementos o envió de información.

Finalmente, es preciso mencionar que al cierre de este proceso de desarrollo y la generación de una versión Beta del sistema, se continúa trabajando para general la versión final, ya que de acuerdo con la literatura revisada y la falta de herramientas para prevención y atención de ciberacoso contra niñas, niños y adolescentes, #NNASegur@s servirá para prevenir, detectar, atender y dar seguimiento a este tipo de situaciones que vulneran los derechos de las niñas, niños y adolescentes.

Agradecimientos

Agradecimientos al Consejo Nacional de Ciencia y Tecnología de México por el financiamiento otorgado para el desarrollo de este trabajo de aplicación de tecnología en el ámbito educativo y social, y de forma especial al Sistema para la Protección Integral de Niñas, Niños y Adolescentes del Municipio de Xalapa, Veracruz, México.

Referencias

Balaguer, P. (2014). "Protégete", aplicación para que niños y jóvenes utilicen Internet de forma segura. Recuperado de https://blogthinkbig.com/protegete-ciberacoso

DAS Seguros de tus derechos. (2017). 10 consejos legales para evitar el ciberacoso. Recuperado de https://www.das.es/blog/10-consejos-legales-evitar-ciberacoso/

Dictionary, C. (2018). Dictionary, Cambridge. Recuperado de https://dictionary.cambridge.org/es/diccionario/ingles/grooming

Dinantia (2018). Dinantia. Recuperado de http://www.dinantia.com/es/funcionalidades/centro

Cussiánovich, V. A., Tello, G. J., y Sotelo, T. M. (2016). Violencia intrafamiliar. Recuperado de https://www.repositoriopncvfs.pe/wp-content/uploads/2016/08/Violencia-intrafamiliar.pdf

Domenech, J. (2016). Los efectos negativos del phiching. Recuperado de https://www.silicon.es/2312363-2312363

Fundación UNAM. (2018). Cómo funciona el phishing. Recuperado de http://www.fundacionunam.org.mx/unam-al-dia/sabes-como-funciona-el-phishing/

Guerrero Luque, J. M. (2015). Asociación de internautas. Recuperado de https://seguridad.internautas.org/html/451.html

Herrera, T. (2017). Sufro de bullying y ya no quiero ir a la escuela. Timon Editores, Ed. 1.

INEGI. (2017). Instituto Nacional de Estadística y Geografía. Recuperado de http://www.inegi.org.mx/saladeprensa/boletines/2017/especiales/especiales2017_03_02.pdf

Juanz, H. (2018). Sin muros. Recuperado el 18 de octubre de 2018, de https://www.sinmuros.com.mx/noticias/xalapa/29979/aumentan-casos-de-ciberacoso-en-estudiantes-ledezma.html

Llorca, Á. A. (2016). Aplicaciones para combatir el acoso escolar. Recuperado de https://www.genbeta.com/a-fondo/14-aplicaciones-para-combatir-el-acoso-escolar

López, M. E. (2012). Acoso cibernético o cyberbullying: Acoso con la tecnología electrónica. Recuperado de http://www.medigraphic.com/pdfs/conapeme/pm-2012/pm123g.pdf

López, O. L., Finalé, C. de los S. B., Villén, C. J., Mora, M. J. A., y Ortega, R. R. (2013). Acoso escolar y ciberacoso: propuestas para la acción. Recuperado de https://idus.us.es/xmlui/bitstream/handle/11441/75725/acoso_escolar_y_ciberacoso_informe_vok_-_05.14.pdf?sequence=1

Moisés, J. (2018). Web consultas revista de salud y bienestar. Recuperado de https://www.webconsultas.com/mente-y-emociones/trabajo-y-tiempo-libre/consejos-para-prevenir-el-ciberacoso-o-ciberbullying-9727

Del Peral, J. A. M., & Navarro, P. V. (2015). Bullying, ciberbullying y sexting. Ediciones Pirámide.

Pereira, M. (2017). Instituto Superior de Estudios Psicológicos. Recuperado de https://www.isep.es/actualidad/caracteristicas-comunes-de-las-victimas-de-grooming/

Sánchez, E. I. (2014). Protección de niños en la red: sexting, cyberbullying, y pornografía infantil.

SIPINNA Ciudad de México. (2016). Recuperado de http://sipinna.cdmx.gob.mx/sipinna/_pages/que_es.php

Smith, P. K., & Shu, S. (2000). What good schools can do about bullying: Findings from a survey in English schools after a decade of research and action. Childhood, 7(2), 193-212. [GS Search]

Statista (2020). Redes sociales con mayor porcentaje de usuarios en México. Recuperado de https://es.statista.com/estadisticas/1035031/mexico-porcentaje-de-usuarios-por-red-social/

UNICEF México (2018). Los derechos de la infancia y adolescencia en México. Recuperado de https://www.unicef.org/mexico/spanish/SITAN-UNICEF2018.pdf

Zapata, B. R. M., Soriano, A. E., González, J. A., Márquez, H. V., y López, R. M. del M. (2015). Educación y salud en una sociedad globalizada. (U. de Almería, Ed.). Universidad de Alemania.