UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computaciones

DESARROLLO DE UN SIMULADOR WEB APLICANDO LA NORMA ISO/IEC 27002 ENFOCADO A INGENIERÍA SOCIAL

Trabajo de grado presentado ante la ilustre Universidad Técnica del Norte previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Franklin Wladimir Vallejo Rodríguez

Director:

MSc. Alexander Guevara

Ibarra-Ecuador

Julio-2020

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información.

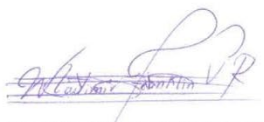
DATOS DEL CONTACTO	
CÉDULA DE IDENTIDAD:	040154321-0
APELLIDOS Y NOMBRES:	VALLEJO RODRÍGUEZ FRANKLIN WLADIMIR
DIRECCIÓN:	CHORLAVY 8-15
EMAIL:	flakovallejo12@gmail.com, fwvallejor@utn.edu.ec
TELÉFONO MOVIL	0988600170

DATOS DE LA OBRA				
TÍTULO:	DESARROLLO DE UN SIMULADOR WEB APLICANDO LA NORMA ISO/IEC 27002 ENFOCADO A INGENIERÍA SOCIAL			
AUTOR (ES):	VALLEJO RODRÍGUEZ FRANKLIN WLADIMIR			
FECHA:	2 de Julio de 2020			
PROGRAMA:	x	**PREGRADO**		**POSGRADO**
TÍTULO POR EL QUE OPTA:	INGENIERÍA EN SISTEMAS COMPUTACIONALES			
DIRECTOR:	MSc. ALEXANDER GUEVARA			

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, a los 2 días del mes de julio de 2020



Franklin Wladimir Vallejo Rodríguez
040154321-0

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Ibarra, 2 de julio de 2020

CERTIFICACIÓN DEL DIRECTOR

El Sr. Franklin Wladimir Vallejo Rodríguez, portador de la cédula de ciudadanía número: 0401543210, ha trabajado en el desarrollo del proyecto de grado **"DESARROLLO DE UN SIMULADOR WEB APLICANDO LA NORMA ISO/IEC 27002 ENFOCADO A INGENIERÍA SOCIAL."**, previo a la obtención del Título de Ingeniero en Sistemas Computacionales, realizando con interés profesional y responsabilidad, que certifico en honor a la verdad.

Es todo en cuanto puedo certificar a la verdad.
Atentamente.

.....

MSc. ALEXANDER GUEVARA
DIRECTOR DE TRABAJO DE GRADO

AUTORÍA

Yo, FRANKLIN WLADIMIR VALLEJO RODRÍGUEZ, portador de la cédula de ciudadanía número 0401543210, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, **"DESARROLLO DE UN SIMULADOR WEB APLICANDO LA NORMA ISO/IEC 27002 ENFOCADO A INGENIERÍA SOCIAL."**, que no ha sido previamente presentada para ningún grado, ni calificación profesional, y que se ha respectado las diferentes fuentes y referencias.

Franklin Wladimir Vallejo Rodríguez
040154321-0

DEDICATORIA

Dedico el presente trabajo de grado, mi carrera de Ingeniería y mi vida entera, a Dios principalmente por darme la oportunidad de llegar hasta esta etapa tan importante de mi vida.

A los héroes que me dieron la vida, Antonio y Liliana por ser el apoyo incondicional en todo este arduo proceso, por esta siempre allí y nunca dejarme solo, por sus sabias palabras y únicos consejos, por su paciencia, amor, dedicación, confianza, gracias por ser el pilar más importante de mi vida… ***Los amo mis héroes.!***

A mis hermanos, la preciosa Marjorie el inquieto e inteligente Josué y el más hermoso de todos los niños Jersael, por ser una de las motivaciones más grandes para culminar mi carrera universitaria… ***son los mejores.!***

A ti pelitos (Josselin E.), por todo, absolutamente todo el apoyo incondicional, conocerte fue lo mejor que me pudo pasar en mi vida y le agradezco a Dios por ese regalo tan maravilloso que me ha regalado, espero seguir contigo hasta el final de mis días… ***Muchas gracias****.!*

Franklin Wladimir Vallejo Rodríguez

AGRADECIMIENTOS

A Dios por su amor incondicional, por ser la esencia de mi mida, por regalarme estos años de mucha alegría, salud, mi familia, y todo lo que me rodea, guiándome siempre por el camino correcto.

A mis amados padres ***Antonio y Liliana***, por todo el amor que me han dado desde el primer día que nací, hasta el día de hoy, por ser la base y la inspiración para culminar esta etapa de mi vida.

A mis hermanos, ***Marjorie***, ***Josué*** y ***Jersael***, ustedes han demostrado valor al asumir este reto conmigo, muchas veces con lágrimas de despedida y otras veces con lágrimas de reencuentro, videollamadas, viajes sorpresas, pero siempre mostrándome su apoyo e inspiración.

A ***Josselin***, por ser una de las personas que más apoyo me ha dado en todo este proceso, ayudándome muchas veces, y por ***nunca irte***… muchas gracias.!

A ***Nelson C***. y ***Kevin E***. por ser los mejores amigos durante mi vida universitaria, muchas gracias por su gran colaboración y apoyo en los diferentes proyectos que llevamos a cabo, también a ***Brayan C***, ***Cristoper T*** y ***Michelle*** por ser los mejores amigos, siempre los llevaré en mi corazón.

Un agradecimiento enorme a mi director de tesis al Ingeniero ***Alexander Guevara***, por su significativa ayuda para llevar a cabo este proyecto, y que aparte de ser uno de los mejores docentes que he conocido, es un gran amigo, ***gracias por todo inge***.!

A todo el cuerpo docente de la carrera de Ingeniería en Sistemas Computacionales encabezado por el ingeniero ***Pedro Granda***, por haber transmitido sus sabios conocimientos durante estos años.

Finalmente, un agradecimiento al ***Club Ethical hacking UTN*** y la ***Rama Estudiantil IEEE UTN***, junto a su capítulo técnico ***CS***, me llevo hermosos recuerdos.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación se fundamentó en el desarrollo de un simulador web, aplicando las características del control accesos del estándar ISO/IEC 27002, las cuales permitieron obtener información sobre lineamientos y normas a implementar en el desarrollo de aplicaciones web seguras ante ataques de ciberdelincuentes, mismas que se deben aplicar de manera ideal para obtener aplicaciones estandarizadas y seguras.

Este simulador web permitirá brindar información a toda la comunidad universitaria UTN, sobre las principales amenazas, vulnerabilidades y riesgos que coexisten en el internet y a las cuales está expuesto, ya que permitirá al usuario simular y conocer las técnicas más comunes de extorsión aplicando Ingeniería social, dentro de escenarios controlados.

La Ingeniería social es el arte de obtener acceso a infraestructura e información mediante el engaño y fraude psicológico, específicamente está encaminada a explotar y vulnerar debilidades en seres humanos, con el fin de traspasar su tecnología aprovechando el descuido, dando como resultado accesos no autorizados, robo de información y extorción.

En la Introducción, se detalló el problema, la situación actual, prospectiva, problema, objetivos, alcance y justificación para el inicio del proyecto de tesis.

En el capítulo I, Es definido el marco teórico referente al internet, Seguridad Informática, Seguridad de la Información, introducción al hacking ético, Ingeniería Social y sus técnicas más usadas, simuladores y su impacto en el mundo actual, definición de la ISO 27002 y el marco de trabajo para el proceso del desarrollo.

En el capítulo II, el desarrollo del simulador web es evidenciado, aplicando Scrum como marco de trabajo, siguiendo los lineamientos y métricas del estándar ISO/IEC 27002 basada en las características del control de accesos para asegurar la aplicación.

En el capítulo III, el impacto obtenido por medio de un análisis estadístico es validado y evaluado, además de los resultados que se generen, finalizando con algunas conclusiones y recomendaciones de la presente tesis.

ABSTRACT

This research was based on the development of a web simulator, applying the access control features of the ISO/IEC 27002 standard, which allowed obtaining information on guidelines and standards to be implemented in the development of secure web applications against attacks by cybercriminals, which should be applied ideally to obtain standardized and safe applications.

This web simulator will provide information to the entire UTN university community about main threats, vulnerabilities and risks that coexist on the internet and to which it is exposed, since it will allow the user to simulate and learn about the most common extortion techniques by applying social engineering, inside of controlled scenarios.

Social Engineering is the art of obtaining access to infrastructure and information through cheat and psychological fraud. Specifically, it is aimed at exploiting and violating weaknesses in human beings, in order to transfer their technology taking advantage of carelessness, resulting in unauthorized access, information theft and extortion.

In the Introduction, the problem, the current situation, prospective, problem, objectives, scope, and justification for starting the thesis project were detailed.

In Chapter I, is defined the theoretical framework referring to the Internet, Computer Security, Information Security, introduction to ethical hacking, Social Engineering and its most used techniques, simulators and their impact in today's world, definition of ISO 27002 and the framework for the development process.

In Chapter II, the development of the web simulator is evidenced, applying Scrum as a framework, following the guidelines and metrics of the ISO / IEC 27002 standard based on the characteristics of access control to ensure the application.

In Chapter III, the impact obtained by means of a statistical analysis is validated and evaluated, in addition to the results generated, ending with some conclusions and recommendations of this thesis.

INTRODUCCIÓN

Tema

Desarrollo de un simulador web aplicando la norma ISO/IEC 27002 enfocado a ingeniería social.

Antecedentes

Según el portal ESET Latinoamérica se han suscitado diversos incidentes de seguridad en Ecuador, y entre los más relevantes se destaca: “Falsa alerta de terremoto en Ecuador propaga malware”, este ataque es una clara evidencia de las técnica que utilizaron los creadores de software malicioso para propagar amenazas, virus y falsa información aprovechando la poca o nula formación en seguridad de los usuarios digitales (Eset Latinoamérica, 2014).

Dentro del ámbito de la Seguridad Informática enfocada a seguridad y privacidad digital, una de las herramientas más explotadas por los llamados “hackers” o “cibercriminales” que, aprovechando factores psicológicos y tecnológicos, es sustraer información de vital importancia para los individuos, con el fin lucrarse o extorsionar a la víctima por la venta o devolución de esta información secuestrada, a través de técnicas de Ingeniería Social (Barbero et al., 2015).

La Ingeniería Social o el arte del engaño es una herramienta que permite “hackear seres humanos”(HADNAGY, 2017), ya sea mediante interacción social humana o utilizando recursos computacionales, El eslabón más débil de un sistema informático son los usuarios(Mitnick, 2017), esta célebre frase hace referencia a cuán importante es la cibereducación para poder mitigar este tipo de ataques y evitar ser víctimas de cibercriminales.

Los estudiantes de la UTN, al no poseer ni adquirir formación necesaria relacionada con Seguridad Informática se evidencia que las competencias sobre esta temática son muy limitadas. Se encuentran vulnerables a ataques de Ingeniería Social debido a que infravaloran su información personal y suponen que solo aquellas organizaciones que manejan grandes sumas de dinero o información pueden ser blancos potenciales, e ignoran que pueden ser víctimas de interés para un cibercriminal al desconocer el gran valor que tiene su información.

Situación actual

La Universidad Técnica del Norte cuenta con equipos de trabajo de investigación estudiantil, entre los cuales se destaca el Club Ethical Hacking-UTN (CEH-UTN) cuyos objetivos son investigar, formar y capacitar a la comunidad Universitaria en temas relacionados a seguridad informática enfocada en Hacking Ético.

El CEH-UTN por medio de la realización de cursos, comparte investigaciones en un marco teórico-práctico, con un especial enfoque en las técnicas de ingeniería social y la automatización de ataques mediante herramientas libres y gratuitos, y por consecuente, se ha evidenciado el alto índice de desconocimiento con respecto a vectores de ataques enfocadas a ingeniería social, llevando siempre como lema y nada de unirse al lado del mal.(Astudillo, 2016)

En una investigación realizada aplicando técnicas de ingeniería social por el CEH-UTN, a partir de una muestra de 276 personas, arrojó resultados de que el 10% de la población es vulnerable a ataques de ingeniería social.(PROYECTO DE CREACIÓN DEL CLUB ETHICAL HACKING, 2017)

Existen en la UTN carreras con materias especializadas en Seguridad Informática como lo son la carrera de Ingeniería en Sistemas Computacionales y la carrera de Electrónica y redes, las cuales en sus mallas curriculares contemplan temática referente a Ingeniería Social y como evitar ser víctimas, pero también en todas las carreras existentes en el campus universitario está presente la materia de TIC´s, asignatura en la cual se mira a simples rasgos la Ingeniería Social, pero no se pone énfasis en todo lo que esta técnica puede generar si alguien es víctima y debido a diversos factores el proceso de enseñanza-aprendizaje de adquisición de competencias en seguridad y privacidad digital es incompleta, ya que no se tratan temas de vital importancia como la cibereducación referente a la navegación segura, ciberbullying, sexting, scamming, entre otros.

Tales falencias no permiten que estudiante reconozca el peligro y el alto porcentaje que tiene de ser víctima de cualquier ciberataque, ya que al desconocer o tener poco conocimiento referente a Seguridad Informática puede ser presa fácil de un ataque de Ingeniería Social, lo cual permitiría que el estudiante entregue datos sensibles a hackers y ponga en riesgo datos personales sensible voluntaria e inconscientemente sin darse cuenta.

Prospectiva

La presente investigación pretende desarrollar un simulador web aplicando la norma ISO/IEC 27002:2013 enfocado a Ingeniería Social, que permita adquirir buenas prácticas, habilidades y destrezas para lograr la ciberresiliencia de los involucrados y mitigar los riesgos de las amenazas informáticas que coexisten en la Internet.

Planteamiento del problema

Alto índice de analfabetismo en el área de Ingeniería Social en los estudiantes de la UTN.

Los ataques informáticos dirigidos hacia la seguridad y privacidad digital de los estudiantes y ejecutados exitosamente puede generar consecuencias catastróficas como fuga o brecha de datos, lo cual generará repercusiones económicas, sociales, e implicaciones legales para las partes afectadas.

La ausencia de recursos para los estudiantes tales como, mallas curriculares sencillas, la falta de expertos en el área y la confianza de los involucrados y la falta de herramientas tecnológicas tales como, un simulador web que permita el acceso libre y gratuito a contenidos de calidad, solo aumenta la dificultad hacia la parte formativa de los estudiantes. Cabe señalar que este simulador web pretende fortalecer el conocimiento en seguridad y privacidad digital enfocado a ingeniería social, dirigido a estudiantes de la UTN.

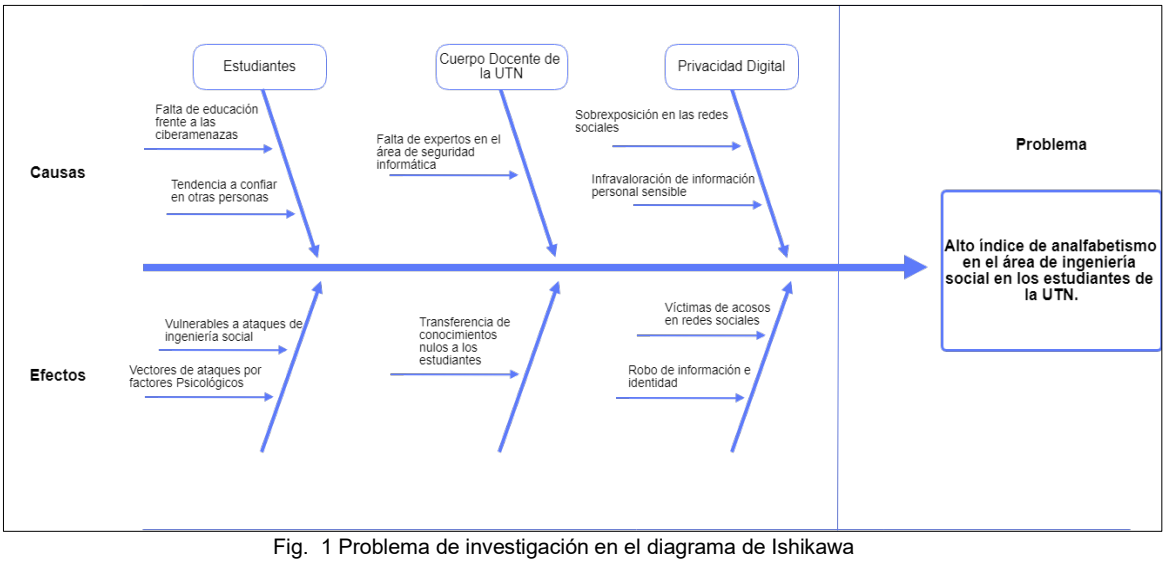


Fig. 1 Problema de investigación en el diagrama de Ishikawa

Objetivos

Objetivo general

Desarrollar un simulador web aplicando la norma ISO/IEC 27002:2013 enfocado a Ingeniería Social.

Objetivos específicos

1. Elaborar un marco teórico sobre simuladores web orientados al área de Seguridad Informática
2. Desarrollar un simulador web enfocado a Ingeniería Social.
3. Aplicar técnicas, métodos y herramientas de Seguridad Informática enfocado a Ingeniería Social.
4. Validar los resultados de la presente investigación.

Alcance

La presente propuesta busca concientizar sobre las amenazas informáticas que proliferan en la internet y que afecta a los usuarios digitales, mediante una instrucción y formación en un entorno controlado que pretenderá confrontar al estudiante frente a amenazas informáticas en un escenario controlado referente a Ingeniería Social.

Aplicando la característica de control de accesos de la norma ISO/IEC 27002 se implementará un inicio de sesión para acceder al simulador web, seguido de una serie de ejercicios prácticos desde un nivel básico, hasta llegar a un nivel avanzado, posterior al entrenamiento se proveerá un puntaje de acuerdo a la capacidad de solución-respuesta, y se brindará una retroalimentación sobre las amenazas y soluciones respectivas que permitan fortalecer las competencias en seguridad y privacidad digital en los estudiantes de la UTN.

Las herramientas que se utilizarán son las siguientes:

- Lenguaje de programación Java EE
- JSF + PrimeFaces
- RDBMS PostgreSQL
- IDE Eclipse
- Servidor de aplicaciones local UTN
- ISO/IEC 27002
- Modelo Curricular TIC´s

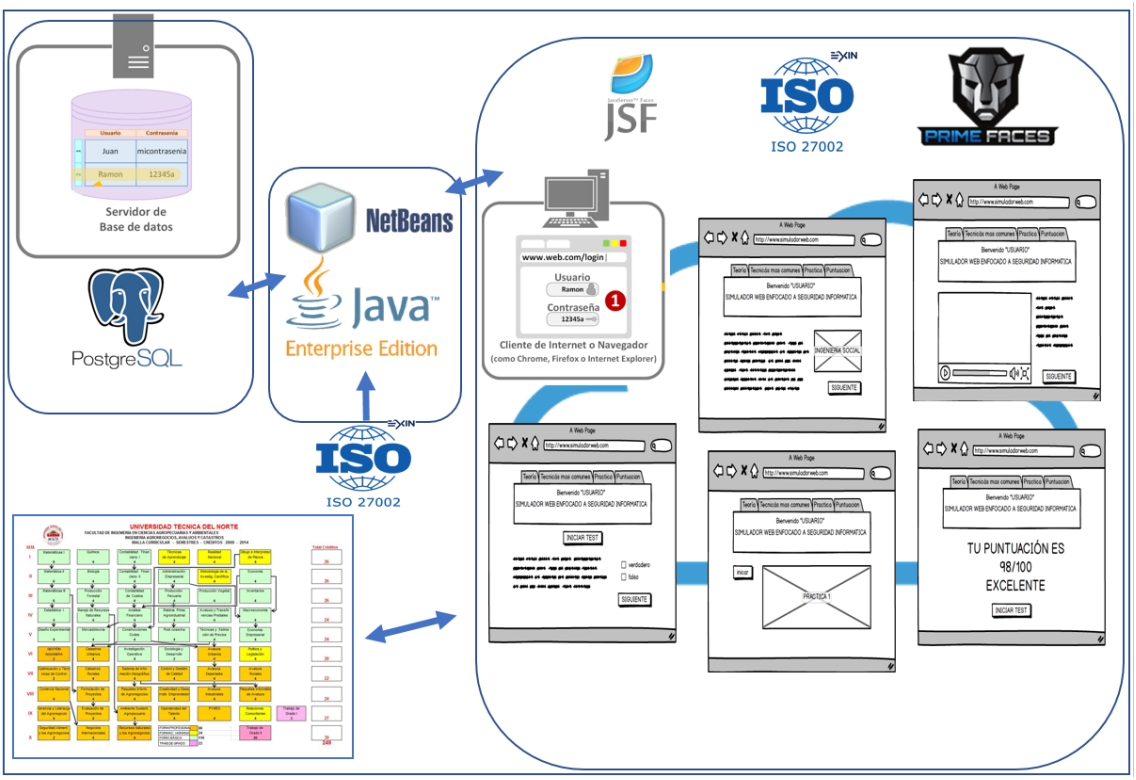


Fig. 2 Diagrama de solución propuesta

Justificación

El presente proyecto fomentará la adopción de cibercultura en los estudiantes y permitirá afrontar y mitigar los riesgos que pueden generar los ataques a Ingeniería Social.

Además, se contribuirá a los Objetivos de Desarrollo Sostenible, en especial con el objetivo N°9 Industria, Innovación e Infraestructura. Este objetivo hace énfasis en la inversión en infraestructura e innovación ya que son motores fundamentales para el crecimiento y el desarrollo económico del país.

Contexto

Las referencias más similares al proyecto como un simulador web y que cumplen con los parámetros de gestión de campañas e informes, se muestran a continuación.

El framework Gophish es opensource y una potente herramienta de phishing, el cual facilita la realización de pruebas a las organizaciones expuestas a ataques de phishing. Gophish permite definir los objetivos, lanzar la campaña y hacer seguimiento de los resultados (Gophish, 2018).

Phishing Frenzy es una aplicación Ruby on Rails opensource y diseñado como una herramienta de pentesting, posee características que permite ver de manera detallada el estado de las campañas y generar informes en archivos en formato pdf o xml (Phishing Frenzy, 2018).

Lucy permite poner a prueba la seguridad de la organización mediante una simulación de ciberataques realistas, a través de fases como probar, entrenar y lograr el compromiso del empleado para detectar e informar a los encargados del departamento de TI (Lucy Security, 2019).

La suite The Social-Engineer Toolkit (SET), fue creada y escrita por David Kennedy fundador de TrustedSec, SET es un framework opensource para pruebas de penetración diseñado para ataques de Ingeniería Social, posee la particularidad que es una herramienta directamente enfocado a la comunidad de Seguridad Informática enfocado en hacking ético (trustedsec, 2019).

La presente investigación en contraste con las herramientas antes mencionadas pretende que el estudiante tenga acceso a contenido gratuito y actualizado referente a Ingeniería Social, adquiriendo conocimientos en el área de Seguridad Informática mediante la retroalimentación de las prácticas realizadas.

CAPÍTULO I
Marco teórico

1 Internet

1.1 Introducción a Internet

1.1.1 ¿Qué es Internet?

Las redes de computadoras han creciendo de manera exponencial, desde la década de los 70', la comunicación e interacción de los equipos computacionales ha pasado de ser un tema de investigación avanzado y accesible solo para algunas organizaciones gubernamentales, a formar una parte esencial de la vida diaria de todos los seres humanos, ya que estas redes se usan en todos los ámbitos sea, empresarial, publicidad, producción audiovisual, planificación, facturación, comercialización, contabilidad, entre otras áreas más. (Comer, 2015)

Actualmente desde pequeñas microempresas hasta empresas multinacionales cuentan con una red de computadoras interconectadas, encargadas de proporcionar al recurso humano, acceso en línea a información que se encuentre disponible en la red.

(Comer, 2015) afirma que el crecimiento y uso de Internet global se encuentran entre los fenómenos más interesantes y emocionantes de las comunicaciones, en los 80', Internet era un proyecto de investigación que involucraba pequeñas redes de equipos computacionales con el fin de compartir información; Al presente, Internet ha crecido exponencialmente en tiempo y amplitud, convirtiéndose en un sistema de comunicación que llega prácticamente a cualquier lugar del mundo, con características muy particulares como acceso a una conexión de alta velocidad mediante módems de cable, tecnologías ópticas o inalámbricas.

Todo está en Internet, desde el conocimiento, comunicación, ciencia, ocio, arte, historia, música, negocios, educación hasta trabajo, los antes mencionados son a penas pocos ejemplos de lo que se encuentra en esta extensa red, así como existen grandes beneficios, también podemos encontrar fraude, acceso a material pornográfico, drogas, violencia, extorción hasta contratación de asesinos, porque, Internet no es más que un mundo paralelo al mundo real que vivimos, que se refleja como un espejo, debido a esto, es importante conocerlo, manejarlo, disfrutarlo y estar preparados para protegernos de su lado oscuro (Martos, 2015).

1.2 Seguridad de la Información

Existen conceptos erróneos y frecuentemente se especula sobre si la Seguridad de la Información y la Seguridad Informática son lo mismo, no obstante, son nociones disímiles debido a su área de aplicación en la protección de información, organismos, instituciones y empresas indistintamente de la actividad que desempeñen, fundan su crecimiento en la información la cual posee un valor especial, siendo uno de los activos más costosos dentro de una organización, debiendo ser protegida apropiadamente ya que por su gran valor está bajo vulnerabilidades y amenazas, manejadas por delincuentes informáticos cuyo objetivo es poner en riesgo los pilares de la Seguridad de la Información.

Dada la gran cantidad de información, esta tiene diversas maneras de reproducirse como papel, e-mails, digitalizada, transmitida mediante voz, video, audio, entre otros, existen así mismo diferentes maneras por la que la información puede ser adulterada, robada, falsificada o eliminada dado el incremento de los sistemas informáticos.

La Seguridad de Información, (ISO 27000:2013, 2019), consiste en la preservación de sus tres pilares fundamentales confidencialidad, integridad y disponibilidad, así como de los sistemas informáticos existentes conectados en red, dentro de una organización; Es decir, garantizar a como dé lugar la continuidad de acciones de la organización ante un riesgo, previniendo la pérdida de información, posibles fallos de sistemas, pérdidas económicas, entre otras.

Las bases sobre los cuales funciona la Seguridad de la Información son:

1.2.1 Confidencialidad

Principio básico de la Seguridad de la Información la cual garantiza o segura que la información solo sea accedida o interpretada por usuarios, sistemas o procesos autorizados quienes poseen los privilegios necesarios para acceder a dicha información y únicamente por medios autorizados.

1.2.2 Integridad

Otro de los principios de la Seguridad de la Información la cual garantiza o asegura que la información solo pueda ser alterada por usuarios, sistemas o procesos autorizados quienes cuenten con privilegios necesarios puedan realizar dichas modificaciones, asegurando que la información sea la misma en todo momento, es decir no ser alterada por algún ente no autorizado durante su almacenamiento o transmisión.

1.2.3 Disponibilidad

El tercer pilar fundamental de la Seguridad de la Información es la disponibilidad, que como su nombre lo indica es asegurar o garantizar que en todo momento la información sea accesible para los usuarios, sistemas o procesos autorizados.

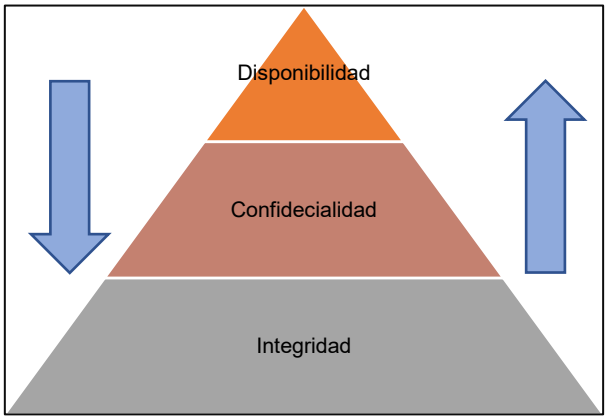


Fig. 3 Principios de la seguridad de la Información

1.2.4 Autenticidad

A estos tres pilares se le añade también la autenticidad, que garantiza o asegura que una entidad es quien dice ser, en otras palabras, es asegurar que la fuente es legítima, que no exista una suplantación u extorción, lastimosamente los ataques enfocados suplantar la identidad mayormente son a dispositivos de la capa de red, de transporte de datos como son routers, switchs encargados de origen y destino.

1.3 Seguridad Informática

La Seguridad Informática actualmente forma parte de los grandes negocios en materia de tecnología y seguridad en empresas, se reflejan distintos tipos de ataques, vulnerabilidades y amenazas al acceso de información de organizaciones, es necesario crear, aplicar y actualizar medidas, estándares y procesos que contrarresten estos riesgos que afectan los recursos informáticos de las organizaciones. (Suárez & Fontalvo, 2017).

Una de las ramas de la Seguridad de la Información es la Seguridad Informática la cual como principal objetivo es la protección tanto física como lógica, y ésta se define como: *"la disciplina que, fundamentada en políticas, reglamentos y normas internas y externas de las organizaciones, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas o vulnerabilidades minimizando los riesgos tanto físicos como lógicos, a los que está expuesta"* (Baca, 2016).

Tabla 1 Tipos de seguridad informática

USO	TIPOS
Dependiendo lo que se requiera proteger	**Seguridad Física** Relacionado totalmente la protección física de los sistemas ante vulnerabilidades, amenazas o la unión de estos como lo es un riesgo, y pueden ir desde desastres naturales hasta robos muy bien estructurados por delincuentes o ciberdelincuentes, con el fin de adquirir información valiosa. **Seguridad Lógica** Enfocado netamente a garantizar la seguridad la parte lógica en el uso de los sistemas informáticos, el software, las bases de datos, los sistemas operativos, propuestos a administrar los datos y los procesos.
Dependiendo del momento en el que se hace uso de la protección	**Seguridad Activa** Proceso de invocación a una sucesión de medidas preventivas las cuales están enfocadas en impedir y detener diferentes tipos de riesgos en un sistema con el fin de proteger y resguardar la información. **Seguridad Pasiva** Proceso de invocación a una sucesión de medidas correctivas que ponen en uso al instante para minimizar o contrarrestar las derivaciones ocasionadas por un riesgo en la seguridad tales como un ataque a un servidor.

Fuente Propia

1.4 Introducción al Hacking Ético

Cuando se menciona el término hacking ético, específicamente se describe a la operación de realizar pruebas de intrusión o intromisión en sistemas o instalaciones informáticas; concretamente se refiere a que el pentester o hacker ético, tomará el rol de un hacker, con el fin de que a través de una serie de pruebas encontrar vulnerabilidades o brechas de seguridad en los equipos o sistemas informáticos, obteniendo algunas veces el acceso total a un sistema o centro de datos, obviamente trabajando en un entorno vigilado, donde no ponga en riesgo los pilares de la seguridad de información, tampoco de la Seguridad Informática de la organización.

Es importante enfatizar que, aunque es indudable que el experto en Seguridad Informática debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una intrusión de este tipo. Se requiere además seguir una metodología que nos permita llevar un orden en nuestro trabajo para optimizar nuestro tiempo en la fase de explotación, además de aplicar nuestro sentido común y experiencia (Astudillo, 2016).

1.4.1 Fases del Hacking

Un tema bastante controversial y que ha estado en auge en los últimos años es el hacking, algunos expertos han determinado fases específicas o metodologías con las cuales seguir este proceso, tanto el hacker ético como el hacker siguen un orden lógico establecido de pasos, los cuales tanto profesionales como entes especializados en

Seguridad Informática han llegado a un beneplácito de que las fases más prominentes en un procedimiento de hacking son cinco establecidas de la siguiente manera.

a) Hacker ético.

Su función es encontrar vulnerabilidades, amenazas o riesgos para posteriormente tomar las medidas necesarias para evitar cualquier pérdida de información o fallos de servicio de la organización. Comúnmente se estable un ciclo para las fases del hacking (ver figura 1) con el fin de exponer que, después de que el hacker ético obtiene acceso realiza dos fases diferentes a lo que comúnmente un hacker haría en la misma situación.

b) Hacker.

La manera de operar de un hacker es que mientras el hacker ético realiza informes y los presenta para que esos riesgos se mitiguen, el hacker luego de mantener el acceso borra sus huellas sin dejar rastro de haber vulnerado sean un sistema informático o un centro de datos, para luego continuar en un ciclo que si no es detectable podría causar grandes pérdidas tanto económicas como tecnológicas (pérdida de información).

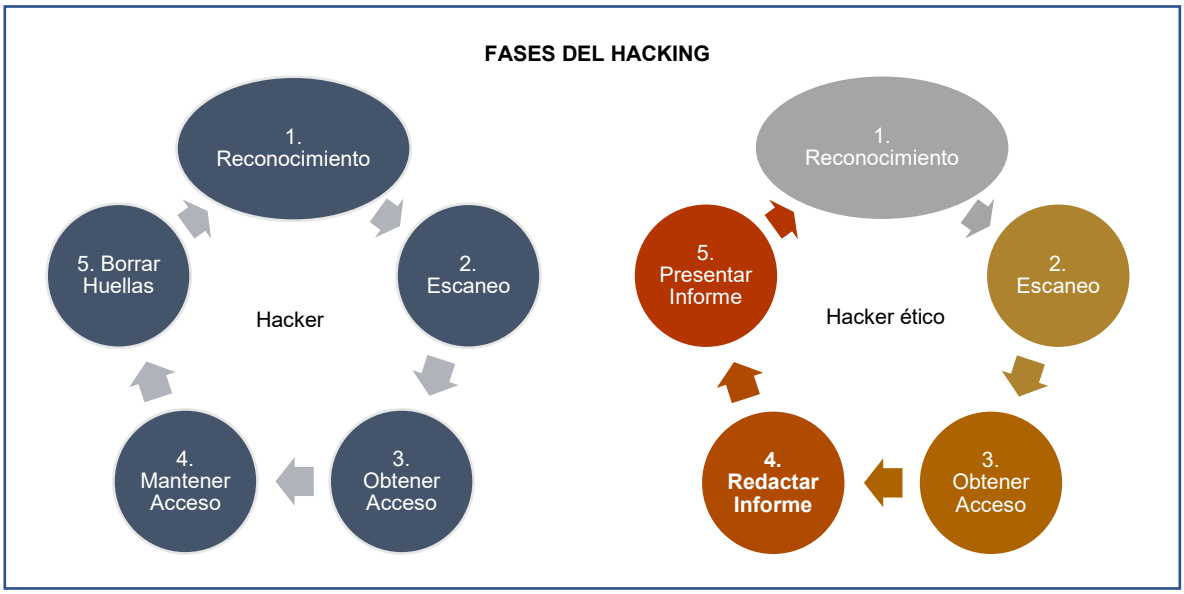


Fig. 4 Fases del hacking - Fuente propia

1.4.2 Tipos de Hacking

Depende desde donde se realice, aplique o efectúe los sondeos necesarios por parte del hacker ético, el hacking es externo o interno.

Tabla 2 Tipos de hacking

Tipo	Definición
Hacking ético externo	Se realiza a equipos o infraestructura desde internet expuestos públicamente o que estén brindando un servicio a la comunidad. Ejemplo de estos se podrían listar: servidor web, página o portal web, firewall, servidor de correo, etc.
Hacking ético interno	Aquí el experto en seguridad encargado del hacking interactúa solamente con la red interna de la organización, tomando diferentes roles ya sea desde hacerse pasar por un simple empleado recién contratado, hasta un empelado de alta jerarquía que constantemente está accediendo a la red interna de la institución.

Fuente Propia

1.4.3 Modalidades del Hacking

Existen modalidades que dependiendo del costo que la empresa u organización requiera invertir en su seguridad provee al hacker ético cierta información para proceder con un análisis y determinar posibles riesgos.

a) White box hacking.

Este es el denominado hacking de caja blanca, aunque en ocasiones también se le llama hacking transparente. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma porque la empresa auditada le da al consultor información completa de las redes y los sistemas a atacar o probar. (Astudillo, 2016)

Es decir, que además de brindarle un punto de red e información de configuración para la estación de auditoría, como en el hacking de caja gris, el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información de subredes remotas, etc. *"Debido a que el consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también; sin embargo, esto es relativo, porque en un hacking de caja blanca es usual que se le pida al consultor probar varios escenarios*" (ej..: sin credenciales, con credenciales de un perfil de usuario X o Y, etc.) (Astudillo, 2016).

b) Gray box hacking.

En esta modalidad el cliente provee información finita al hacker ético como un documento con listas de direcciones IP de los equipos en su red interna. Se conoce

más comúnmente a esta fase como hacking de caja gris ya que el hacker ético debe de realizar pruebas tanto internas como externas para obtener más información, simple y sencillamente ya que hasta ahora la información entregada por el cliente solo le permite actuar como un empleado sin ningún tipo de privilegios.

c) **Black box hacking.**

En países donde el idioma predominante es el español como en el caso de Ecuador se conoce más comúnmente a esta modalidad como hacking de caja negra, en esta modalidad las pruebas son netamente externas, aquí el cliente provee al hacker ético de poca o nula información sobre su organización como por ejemplo solo se provee el nombre de la empresa por lo que para el hacker ético el ambiente a trabajar es a ciegas.

1.5 Ingeniería Social

Según estudios realizados por diversas empresas y consultores de Seguridad Informática y en seguridad de Internet, el 50% de las empresas son y han sido víctimas de la Ingeniería Social. Los delincuentes han utilizado phishing y redes sociales para obtener información de personas y/o empresas. Empleados nuevos, y aquellos que no tienen aún la pertinencia de estar en una empresa, con frecuencia son los objetivos más atacados por ciberdelincuentes (Domínguez, 2014).

Empero, aunque exista una excelente estructuración de proyectos de seguridad que la organización pudiera equipar, existen medios de ataques que se fundamentan en el engaño y fraude psicológicos, específicamente están encaminados a explotar y vulnerar debilidades en seres humanos, los hackers conocen muy bien que estrategia usar para llevar exitosamente un ataque aplicando la denominada Ingeniería Social.

Esta es esencialmente el arte de obtener acceso a edificios, a sistemas o a datos (archivos, programas y fotografías) mediante la explotación de la psicología humana, en lugar de romper o quebrar su tecnología. Por ejemplo, en lugar de tratar de encontrar una vulnerabilidad de software, un ingeniero social puede llamar a un empleado y hacerse pasar por una persona de soporte de Tecnología de Información o un amigo o un cliente, tratando de engañar al empleado para que divulgue su contraseña (Domínguez, 2014).

Características humanas como la negligencia, ignorancia, descuido, son de vital importancia para un hacker otorgándole acceso no autorizado a sistemas informáticos o centro de datos evadiendo las costosas inversiones por parte de la organización en equipos sofisticados especializados en Seguridad Informática. En relación con las

debilidades humanas, las más explotadas para obtener datos conexos a un sistema son la divulgación y la confianza.

La mejor implementación de tecnología de punta hoy en día referente a Seguridad Informática, firewalls, antivirus, sistemas de detección de hackers, o complejos sistemas de autenticación no garantiza al cien por ciento el robo de información o accesos no autorizados, ya que lo único que se necesitan son cinco a diez segundos de un empleado desprevenido de su computador interconectado a la red interna de la organización y ya se obtiene el acceso al sistema

1.5.1 Técnicas de Ingeniería Social más usadas

A continuación, se enlistan tres tipos de técnicas en relación con el nivel de injerencia del hacker

Tabla 3 Tipos de técnicas de Ingeniería Social

Técnicas	Tipo	Definición
Técnicas presenciales	Observación	Esta técnica es el medio para conseguir una gran cantidad de información en diferentes escenarios para el ingeniero social, ya sea en un lugar específico, un individuo o un grupo de individuos en lapsos de tiempos extremadamente cortos. Aparentemente es un ataque simple, pero es muy efectivo ya que con esta técnica se realiza un análisis sobre el exterior e interior en busca conversaciones, diálogos, que puedan proveer de información valiosa. Ejemplo, cuando las contraseñas son puestas en papeles que se adhieren a la pantalla del ordenador, conversaciones descuidadas del personal, entrevistas falsas, etc.
	Mirando por encima del hombro	Básicamente es mirar por encima del hombro de un individuo para lograr obtener su contraseña de acceso o pin mientras lo digita. Existen variaciones de esta técnica una de ellas es la del uso de binoculares o miras de alta potencia para apreciar lo que digita, otra es el uso de cámaras o videograbadoras de alta resolución para grabar o fotografiar para de alguna manera descifrar los códigos de acceso.
Técnicas no presenciales	Contraseña perdida	Esta técnica se especializa en operaciones hábiles que fuercen al individuo voluntariamente a realizar recuperación de contraseña, sin importar ningún nivel de seguridad.
	Correo electrónico	Los correos electrónicos o e-mails son una herramienta de comunicación muy usada hoy en día en todo el mundo, y por tal razón uno de los puntos clave para que un atacante obtenga información, el simple hecho de poder enviar una cantidad enorme de correos electrónicos a la vez, esto facilita la atacante llegar a más posibles víctimas y engañarles, disfrazando su identidad, llegando a robar información de la organización, infecciones al equipo por virus contenidos en documentos adjuntos, descarga de malware, entre otros.
	Teléfonos	Una de técnicas más emocionantes y eficaces para los atacantes es el uso de celulares para la obtención de información, en la mayoría de los casos información personal. Los atacantes menos experimentados hacen uso de su propia línea telefónica para realizar estas fechorías, obviamente existen atacantes muy bien preparados los cuales a través de ciertos aparatos electrónicos convierten a una línea pública en una línea casi imposible de rastrear, aparte con aplicaciones informáticas cambian el timbre de su voz haciendo así más difícil su localización y más efectivo su ataque.
	Chats	Actualmente uno de los medios de comunicación más usados es la mensajería instantánea y los chats en grupo para enviar

		y recibir información, esto es algo aprovechado por los atacantes, ya que a través de estos medios convencen a las víctimas de descargar música, videos, fotografías, software, apps, entre otros, sin saber que podría ser un poderoso keylogger.
Técnicas presenciales no agresivas	Husmeando en la basura	Por su nombre en inglés trashing, es un método no muy usado por todos los atacantes, pero suficiente efectivo a la hora de conseguir información de alguna organización, ya que sin previa autorización el atacante procede a revisar la información que los empleados de las organizaciones desechan al bote de basura, encontrándose con datos personales, claves de acceso, números telefónicos, direcciones IP, papeles membretados y con formatos vacíos, hardware dado de baja, entre otros, comprometiendo la seguridad de la organización.
	Seguimiento de individuos o medios de trasporte	Consiste básicamente en vigilar a un individuo para conocer su rutina diaria y ver de alguna u otra manera momentos específicos vulnerables, donde el atacante pudiera obtener información que el individuo posee. Ejemplo: la seguridad en los estacionamientos, vidrios del vehículo inseguros, entre otros. Una de las desventajas de esta técnica es que lleva mucho tiempo la investigación de un solo individuo.
	Vigilancia de instalaciones	Al igual que la vigilancia de individuos, esta técnica consiste en un profundo análisis de vigilancia a un edificio o instalación en el cual se requiera obtener el acceso o ingreso no autorizado. Esta técnica pone al atacante en observación de muchos de los dispositivos de detención en el inmueble como puertas, ventanas, cerraduras, rejas, puertas subterráneas, infrarrojos de detección de movimientos, conductos, luces de techo, puntos ciegos de cámaras de videovigilancia, y sistemas de control de acceso biométrico u ocular.

Fuente Propia

1.5.2 Perfil psicológico de un hacker e ingeniero social

Los ingenieros sociales utilizan una serie de tácticas psicológicas en las víctimas inocentes. Como Bushwood Consultores manifiesta, los ingenieros sociales exitosos están seguros y tienen control de la conversación. Simplemente actúan como si pertenecieran a una asociación, a una empresa, universidad, grupo de amistades, colegas, etc., ya que su confianza y postura corporal pone a los demás a gusto (Domínguez, 2014).

Los ingenieros sociales confunden a la gente según cuatro principios básicos:

- **Proyectan confianza.** En lugar de a escondidas, de manera proactiva se acercan y llaman la atención sobre sí mismos.
- **Dan algo.** Incluso un pequeño favor crea confianza y la percepción de estar en deuda.
- **Usan el humor.** Es entrañable y desarmado.
- **Hacen una petición y ofrecen una razón.** La psicología demuestra que las personas tienden a responder a cualquier solicitud motivada (Domínguez, 2014).

1.5.3 Fases de la Ingeniería Social

Como bien lo dice en su nombre, básicamente el atacante busca socializar con sus víctimas, confundirlas y en niveles más agresivos de Ingeniería Social inclusive intimidarlos para conseguir de esta manera resultados más rápidos, pero ¿Cómo realiza esto el atacante?, a continuación, se mostrará una serie de fases de como un ingeniero social lleva acabo un efectivo ataque.

a) Fase de acercamiento.

Proceso de mantener una buena relación con las posibles víctimas, ganándose su confianza a través de distintos métodos como, entrega de presentes o favores, haciéndose pasar como nuevo en la oficina, o es un nuevo proveedor, o simplemente un compañero más de trabajo con el fin de sacar información a la víctima, inclusive en algunos casos llegar a tocar los sentimientos de las víctimas con el único fin de obtener la información.

b) Fase de Alerta.

Permite asegurarse de que la víctima no sospeche del acercamiento previo el cual puede ser un riesgo para atacante y su posible caída, si no realizar una serie de pruebas para asegurarse como, proponerle pequeños retos en chiste y ver hasta donde realmente llega.

c) Borrado de huellas.

Al igual que en las fases del hacking, este paso es fundamental ya que al eliminar toda la evidencia que el atacante tenga en posesión, claro luego de haber hecho uso de esta, puede seguir teniendo acceso al sistema en cualquier momento sin ser detectado por los administradores o el experto encargado de la seguridad de la red interna de una organización.

1.5.4 Caso de Ingeniería Social

La Universidad Técnica del Norte una prestigiosa Institución de Educación Superior de carácter pública ubicada al norte del Ecuador en la ciudad de Ibarra, cuenta con algunos clubs académicos y de investigación, uno de ellos el club de Ethical Hacking-UTN, fundado en el año 2017 encargado de generar, desarrollar, asimilar y aplicar el conocimiento científico y tecnológico, a través de la investigación en el área de Seguridad Informática (PROYECTO DE CREACIÓN DEL CLUB ETHICAL HACKING, 2017).

En agosto de 2017 el club inicia sus actividades con un primer evento de carácter educativo bajo el tema “Ethical Hacking Day´s 1.0”, donde se dictaron una serie de charlas enfocadas a fortalecer el conocimiento en Seguridad Informática a la comunidad

universitaria. En la charla titulada “Ingeniería Social” se realizó un experimento social donde el conferencista realizó una llamada telefónica a un número aleatorio que dio el púbico, el conferencista, experto se hizo pasar por un empleado de la dirección de desarrollo tecnológico e informático UTN, pidiendo información a una estudiante, la cual entregó toda su información personal e inclusive otorgó ciertas credenciales de acceso a su portafolio estudiantil y también de su correo institucional en menos de cinco minutos de llamada, mostrando así el expositor cuan fácil es manipular a una persona para conseguir información personal sensible.

1.6 Simuladores

(Mañeru, 2015) afirma que “Las legiones romanas utilizaban tablas de arena y piezas en miniatura de batalla alrededor del 30 a.C., un concepto que ha sobrevenido la prueba del tiempo como una herramienta para el entrenamiento de soldados en las academias militares.

Actualmente con la basta información que está disponible en línea, no parece arriesgado afirmar que en las civilizaciones antiguas probablemente se simulaban las acciones militares y entrenaban para mejorar la preparación técnica de sus soldados en el manejo de armas, así como la estrategia y la táctica a emplear por medio de simulacros. También es razonable pensar que, en los diferentes oficios artesanos, al igual que ocurre hoy, los aprendices pasaban por una etapa de aprendizaje en la que se evitaban los riesgos tanto sobre la integridad física del aprendiz, como en los procedimientos que pudieran daños los productos y materiales que se empleaban. De este modo se simulaban situaciones de la realidad en las que el aprendiz tutorizado por el maestro, comprueba hasta qué punto puede ejercitarse en el contexto real de un modo autónomo y seguro (Mañeru, 2015).

En el ámbito deportivo lo que hace un atleta o un equipo bien conformado, es utilizar recursos o estrategias para simular escenarios de posibles retos que pongan al deportista ante posibles circunstancias de la vida real y de cierta manera entrenarlo y ejercitarlo para que esté preparado ante el hecho, obviamente ante un proceso de simulación controlado de inicio a fin.

Entre las muchas definiciones que se han ofrecido sobre la simulación, conviene tener presente que un simulador es un dispositivo de formación que representa la realidad, pero en el que la complejidad de los acontecimientos puede ser controlado (Mañeru, 2015).

1.6.1 La simulación como metodología de enseñanza

El uso de simuladores en la educación no pretende remplazar el contacto del estudiante con la amenaza, sino prepararlo adecuadamente para el encuentro con la realidad, dándole mayor seguridad y habilidad en un área específica. Desde esta perspectiva se puede valorar a un simulador como aquel medio con el que se procura recrear y reproducir un fenómeno que se pretende explicar, facilitando el aprendizaje al estudiante (Mañeru, 2015).

De esta manera lo que se pretende es que el estudiante o aprendiz, tenga la oportunidad de estar en un ambiente interactivo expuesto ante una situación de ataque real, adquiriendo el conocimiento y destrezas necesarias para su formación.

La simulación como metodología de enseñanza no es algo nuevo hoy en día, es más que nada un recurso didáctico de enseñanza, que a través de los años se ha venido involucrando en diferentes campos educativos, ya que el aprendizaje por simulación en gran manera facilita a los estudiantes estar más seguros y desarrollar destrezas necesarias para aplicarlas en ambientes reales cuando sea necesario aplicar los conocimientos adquiridos.

En la enseñanza por simulación adquiere una particular importancia que el alumno asuma el protagonismo en su formación, es decir, que tome la iniciativa, de modo que el profesor pase a ser guía y ayuda cuando lo requiera. Es decir el estudiante, debe saber que hay que hacer, para ser capaz de saber cómo hacerlo y, aquí aparece la nota distintiva y diferenciadora del aprendizaje por simulación, debe tomar la decisión de realizar aquel procedimiento con los indicadores, los tiempos y los medios disponibles en un momento dado (Mañeru, 2015).

1.7 Simuladores web

La importancia de dinamizar el proceso de enseñanza-aprendizaje basado en tecnologías web en el marco en la Web 2.0, permite a los usuarios participar y colaborar en la construcción del conocimiento, dando origen a un aprendizaje colaborativo y a la vez la utilización de herramientas educacionales para interacción social e intercambio libre y legal de información. La sucesora de la Web 2.0 es la web semántica o Web 3.0 que involucra el uso de la inteligencia artificial para la categorización de la información basado en el perfil e interés del usuario y fomenta una formación integral e interdisciplinaria (Contreras Espinosa, 2014, p. 2).

1.7.1 Tipos de simuladores web

a) Simuladores web académicos

La utilización de simuladores basado en aplicaciones web permite el aprovechamiento de recursos computacionales para el proceso de enseñanza-aprendizaje en un marco de e-learning, es así, que el proyecto PHET de la Universidad de Colorado brinda un laboratorio online que permite una gran variedad de simulaciones interactivas en el área de física, química, biología, ciencias de la tierra y matemáticas, esta herramienta tecnológica tiene modalidad tanto para docentes como para estudiantes en los niveles de formación primaria, intermedia, secundaria y universitaria. Cabe señalar que todas las simulaciones de PHET se basan en investigación educativa extensiva, es decir, los estudiantes dentro de un ambiente intuitivo aprenden mediante la interacción, exploración y descubrimiento (PhET, 2019).

b) Simuladores de ciberseguridad

En un esfuerzo sinérgico de las universidades Carlos III de Madrid (UC3M), la de Málaga (UMA) y la compañía de consultoría y tecnología Indra, se creó un simulador avanzado de entrenamiento para la formación de profesionales en el ámbito de la ciberseguridad, el cual integra cuatro áreas: ciberataques, ciberseguridad, ciberdefensa e informática forense. Cabe indicar que esta solución forma parte del proyecto “Simulador Avanzado para la Ciberseguridad Organizada” (SACO) del programa INNPACTO coordinado por Indra (Uc3m, 2014).

c) Simuladores de hacking ético

En un trabajo de masterado de la Universidad Internacional de la Rioja, se plantea el “Diseño e implementación de sistema informático para entrenamiento en test de intrusión”, el cual contempla realizar una prueba de penetración o pentesting a un laboratorio virtualizado mediante una interfaz de aplicación web que permite la ejecución de los procesos basado en los roles de los usuarios registrados del sistema informático (Fonseca, 2017).

d) Simuladores tributarios

La Agencia Tributaria del gobierno de España tiene un sitio web dedicado para procedimientos y trámites de tipo declaración de la renta mediante un simulador denominado Renta Web Open, entre las funcionalidades de la herramienta permite la recopilación de datos identificativos del declarante y finaliza el proceso con la generación de un reporte con el valor de declaración individual del involucrado.

e) Simuladores web enfocados a Ingeniería Social

En el ámbito de los ataques cibernéticos orientado a las técnicas de Ingeniería Social, el phishing es la estafa digital más común y es utilizado para la suplantación digital, es decir, mediante el uso de correos proveniente de remitentes con dudosa reputación, logran persuadir a la potencial víctima a dar clic sobre enlaces que redirigen a sitios web que solicitan credenciales e información personal, y su vez abrir archivos adjuntos que en segundo plano realiza la instalación de software malicioso tipo troyano bancario o keylogger capaz de atrapar, guardar y enviar remotamente todas las pulsaciones de teclado que la víctima realiza recopilando información financiera para el atacante. La técnica de spearphishing involucra un previo estudio muy cuidadoso de la víctima, con el fin de garantizar el éxito del ataque y obtención de la información personal sensible (Eset Latinoamérica, 2019).

Una plataforma similar que permite realizar pruebas (entorno interactivo con 8 preguntas) de Ingeniería Social tipo phishing, cuyo lanzamiento lo realizó Jigsaw (incubadora tecnológica de Google) permite la experimentación con varias muestras de técnicas de phishing, como URL de dominios que suplantan a direcciones reales o reconocidas y archivos adjuntos maliciosos.(Jigsaw, 2019).

1.8 Estándar ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 forma parte de la familia de las normas ISO/IEC 27000. Es una guía de buenas prácticas que describe los dominios, objetivos de control y controles recomendables en cuanto a Seguridad de la Información (ISO 27000:2013, 2019), es un estándar en el ámbito de la Tecnología de la Información (TI) y proporciona una serie de instrumentos para la selección de controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información apoyado en la norma ISO/IEC 27001 o como una guía de ayuda para desarrollar directrices en la gestión de la seguridad de la información de la organización.

1.8.1 Características

Una característica de la norma ISO/IEC 27002:2013 es el control de accesos la cual tiene como objetivo controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema informático (ISO 27000:2013, 2019).

Para el presente proyecto en base a las limitaciones de tiempo e infraestructura, se ha considerado la característica 9 de Control de Acceso y la subcaracterística 9.4 Sistemas y Control de Acceso a Aplicaciones, y de manera específica la 9.4.2 Procedimiento de

Inicio de Sesión Seguros, debido a que el proyecto involucrado posee un mecanismo de inicio de sesión para los usuarios que deseen utilizar la plataforma bajo un previo registro.

La aplicación de la 9.4.2 Procedimiento de Inicio de Sesión Seguros contempla algunos de los siguientes parámetros:

- Desplegar una notificación general de advertencia que el ordenador debería ser accedido por usuarios autorizados.
- No proveer mensajes de ayuda durante el proceso de inicio de sesión que podría cooperar a un usuario no autorizado.
- Validar la información del inicio de sesión únicamente al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar que parte de los datos es correcta o incorrecta.
- No desplegar la contraseña que se ingresa.
- No transmitir contraseñas en texto claro sobre la red.
- Terminar sesiones inactivas después de un periodo de inactividad.

1.9 Scrum como marco de trabajo

Scrum es un marco de trabajo sencillo y de fácil adaptación en diferentes entornos, su aplicación puede darse en áreas como: arquitectura, comercial, marketing, finanzas, gestión de proyectos, electrónica, mecatrónico, industrial, biológico, procesos, sistemas, ingeniería de software entre otras, que tiene por objetivo manejar equipos de trabajo colaborativo donde se aplican de manera frecuente un conjunto de buenas prácticas para lograr el desarrollo de productos tanto simples como complejos.

Scrum realiza entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos, donde la innovación, la competitividad, la flexibilidad y la productividad son fundamentales (proyectosagiles, 2018).

Este marco de trabajo consiste en organizar equipos con sus respectivos roles, eventos, artefactos y reglas asociadas. Cada componente dentro del marco de trabajo sirve a un propósito específico y es esencial para el éxito de la aplicación de Scrum. (Schwaber & Sutherland, 2016).

Scrum prescribe cuatro eventos formales, contenidos dentro del Sprint, para la inspección y adaptación, tal y como se describen en la sección Eventos de Scrum del presente documento.

- Planificación del Sprint (Sprint Planning)
- Scrum Diario (Daily Scrum)
- Revisión del Sprint (Sprint Review)
- Retrospectiva del Sprint (Sprint Retrospective)(Schwaber & Sutherland, 2016)

Uno de los pilares fundamentales durante el ciclo de vida del software es la metodología Scrum, la cual se aplica durante todo proceso y desarrollo de aplicaciones informáticas, esta metodología consta de fases, una de ellas es la planificación donde se procede con la creación de las historias de usuario y el "Product Backlog" , posteriormente se establecen los distintos roles que existirán para el desarrollo del proyecto y sus respectivas tareas, y se nombran los miembros que conformarán el equipo de trabajo y sus respectivas funciones.

Una fase de la aplicación de la metodología Scrum es la toma de requerimientos, donde se registran todas las tareas que el usuario busca automatizar y la manera como se lo hará basado en las reglas del negocio, las historias de usuario registrarán todo lo antes mencionado y es en la primera reunión donde se definirán todos los requerimientos tanto funcionales como no funcionales a los cuales estará sujeta la aplicación. El dueño del producto (product owner) será único responsable encargado de gestionar la lista del producto (Product Backlog) que se realizará luego de tener todas las historias de usuario, ésta se la puede representar en una tabla donde se registrarán las tareas que incluyen: (Schwaber & Sutherland, 2016)

- Expresar claramente los elementos de la lista del producto;
- Ordenar los elementos en la Lista del Producto para alcanzar los objetivos y misiones de la mejor manera posible;
- Optimizar el valor del trabajo que el Equipo de Desarrollo realiza;
- Hay que asegurar que la Lista del Producto es visible, transparente y clara para todos y que muestra aquello en lo que el equipo trabajará a continuación; y,
- Hay que asegurar que el Equipo de Desarrollo entiende los elementos de la Lista del Producto al nivel requerido. (Schwaber & Sutherland, 2016)

1.9.1 Roles de Scrum

- Dueño del producto (Product Owner)
- Equipo de desarrollo (Development Team)
- Líder del proyecto (Scrum Master)

1.9.2 ¿Qué es un Sprint?

El corazón de Scrum es el Sprint, es un bloque de tiempo (time-box) de un mes o menos durante el cual se crea un incremento de producto “Terminado” utilizable y potencialmente desplegable. Es más conveniente si la duración de los Sprints es consistente a lo largo del esfuerzo de desarrollo. Cada nuevo Sprint comienza inmediatamente después de la finalización del Sprint anterior (Schwaber & Sutherland, 2016).

1.9.3 Planificación del Sprint

Aquí se realiza un listado de las actividades que se van a desarrollar en el tiempo definido en el Sprint.

1.9.4 Scrum diario

Es una pequeña reunión diaria que no sobrepasa los quince minutos, donde se reúne el Scrum máster y el equipo de desarrollo y se discuten tres preguntas que determinan el avance del proyecto.

- “¿Qué hice ayer que ayudó al Equipo de Desarrollo a lograr el Objetivo del Sprint?” (Schwaber & Sutherland, 2016)
- “¿Qué haré hoy para ayudar al Equipo de Desarrollo a lograr el Objetivo del Sprint?”(Schwaber & Sutherland, 2016)
- “¿Veo algún impedimento que evite que el Equipo de Desarrollo o yo logremos el Objetivo del Sprint?”(Schwaber & Sutherland, 2016)

1.9.5 Revisión del Sprint

A diferencia de un Scrum diario, esta es una reunión que lleva más tiempo y donde se reúnen todos los miembros del equipo de trabajo aquí se analizan los avances que se han realizado en el tiempo planificado y si por algún inconveniente hay errores, corregirlos a tiempo.

1.9.6 Retrospectiva del Sprint

Es la oportunidad para realizar una inspección e identificar los elementos más importantes que salieron bien con sus posibles mejoras y crear un plan para implementar las mejoras a la forma en la que el Equipo Scrum desempeña su trabajo, en cuanto a personas, relaciones, procesos y herramientas (Schwaber & Sutherland, 2016).

CAPÍTULO II

CICLO DE VIDA DE LA APLICACIÓN

2 Desarrollo

2.1 Planificación

La planificación es una de las partes más fundamentales en el proceso de llevar a cabo un proyecto de forma exitosa; la planificación consiste en organizar y racionalizar aquello que se quiere hacer, con el propósito de alcanzar determinados objetivos (Consejo Estatal de Estudiantes de Medicina, 2019). Para el presente proyecto se ha definido el siguiente mapa de procesos (Fig. 5), el cual servirá de base para de la planificación y también en el desarrollo del ciclo de vida de la aplicación.

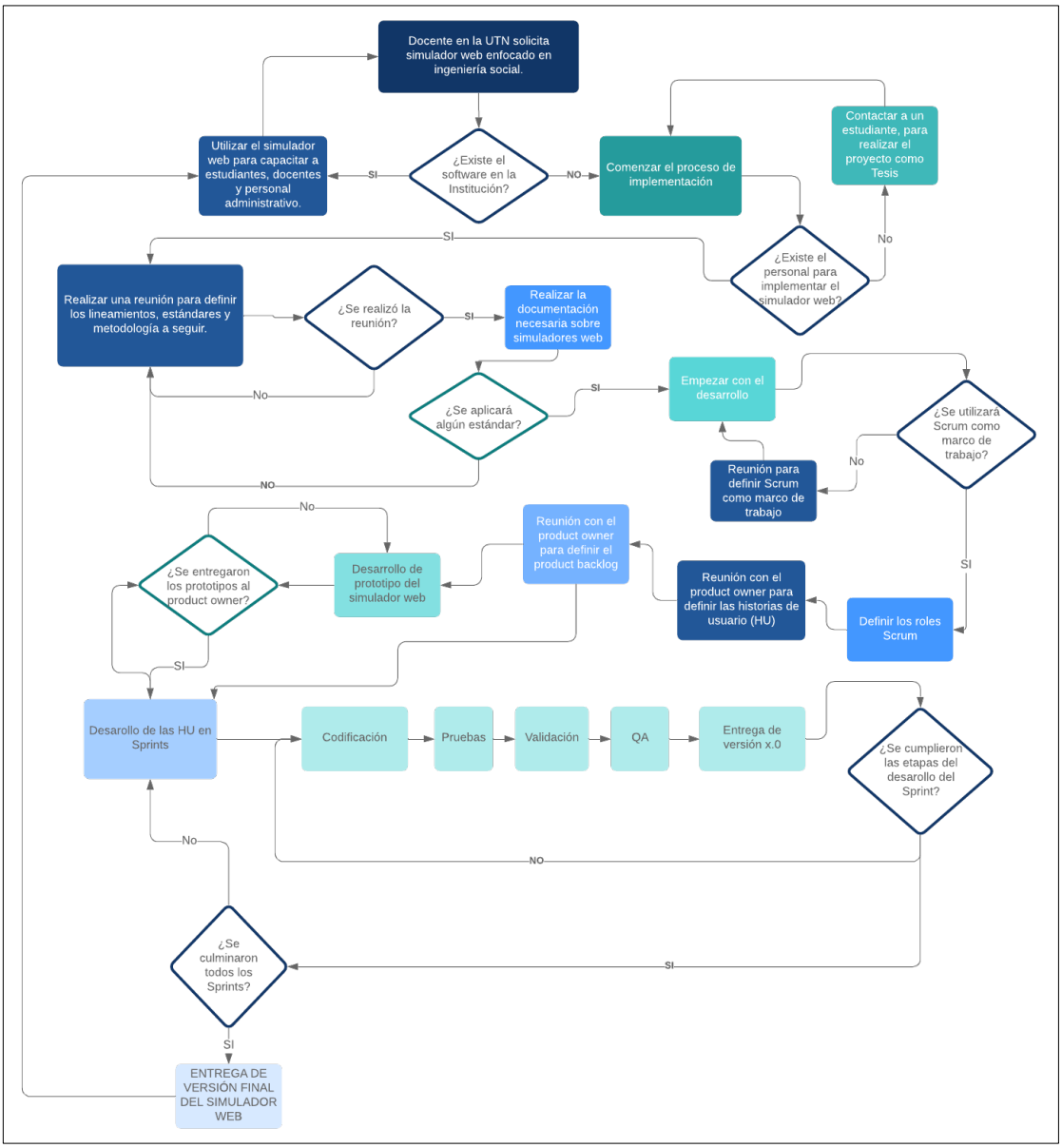


Fig. 5 Mapa del proceso

2.2 Implementación del simulador web enfocado a ingeniería social

Para la implementación del simulador web en la Universidad Técnica del Norte, se desarrolló una aplicación web, la cual servirá como ayuda pedagógica en la materia de Seguridad Informática en la carrera de Ingeniería en Sistemas Computacionales.

2.3 Definición de requisitos

Las historias de usuario son el resultado de levantar requisitos donde se encuentran descripciones provistas por el product owner y permiten realizar la respectiva documentación de los requisitos que tendrá el presente proyecto.

Tabla 4 Historia de usuario n°1

HISTORIA DE USUARIO	
Número: 1	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Levantamiento de requisitos	
Prioridad en negocio: Alta	
Estimación (horas): 8	
Descripción: Levantamiento de requisitos mediante una reunión con el product owner	
Pruebas de aceptación:	
Levantamiento de requisitos aprobados y firmados por el product owner.	

Fuente: Propia

Tabla 5 Historia de usuario n°2

HISTORIA DE USUARIO	
Número: 2	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Base de datos, arquitectura	
Prioridad en negocio: Alta	
Estimación (horas): 8	
Descripción: Como dueño de producto requiero un modelo entendible base de datos de la información de los usuarios, también necesito que los usuarios se registren para ingresar al sistema y tener el control de su información y sus registros.	
Pruebas de aceptación:	
La base de datos debe estar bajo un software libre. La base de datos debe ser administrable	

Fuente: Propia

Tabla 6 Historia de usuario n°3

HISTORIA DE USUARIO	
Número: 3	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Gestión de usuarios	
Prioridad en negocio: Alta	
Estimación (horas): 12	
Descripción: Como dueño de producto necesito gestionar la información, para registrar nuevos usuarios en el simulador ingresando su información (cédula, nombre, apellido, correo y contraseña), para después asignarle un rol al usuario como: administrador o estudiante, también poder leer, editar y activar usuarios y consultar sus puntajes.	
Pruebas de aceptación:	
Verificar que todos los campos del formulario de registro estén correctamente validados según sea el tipo de dato. Indicar donde están los errores en caso de que un registro de información esté incompleto.	

Fuente: Propia

Tabla 7 Historia de usuario n°4

HISTORIA DE USUARIO	
Número: 4	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Módulo de acceso	
Prioridad en negocio: Alta	
Estimación (horas): 12	
Descripción: Como dueño de producto necesito dos páginas de ingreso al sistema, una para ingreso a los usuarios con rol estudiante y otra para para la parte administrativa, en las dos páginas deben constar dos campos de ingreso, uno de identificación de usuario y otro para la contraseña.	
Pruebas de aceptación:	
Validar que todos los campos del formulario de registro estén correctamente validados según sea el tipo de dato. No mostrar donde están los errores en caso de que un registro de información esté incompleto. La contraseña debe tener un mínimo de 8 caracteres y letras y números	

Fuente: Propia

Tabla 8 Historia de usuario n°5

HISTORIA DE USUARIO	
Número: 5	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Módulo de registro	
Prioridad en negocio: Alta	
Estimación (horas): 12	
Descripción: Como dueño de producto necesito una página de registro de usuarios con rol estudiante en el sistema, en la página debe constar los siguientes campos obligatorios para el registro (cédula, nombre, apellido, correo y contraseña), además se deberá realizar obligatoriamente la validación del correo electrónico del usuario con rol estudiante a registrarse para posteriormente hacer uso del simulador.	
Pruebas de aceptación:	
Validar que todos los campos del formulario de registro estén correctamente validados según sea el tipo de dato.	

No mostrar donde están los errores en caso de que un registro de información esté incompleto.
La identificación del usuario será el número de cédula.
Validar correo electrónico mediante envío de correo de confirmación

Fuente: Propia

Tabla 9 Historia de usuario n°6

HISTORIA DE USUARIO	
Número: 6	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Plantilla de interfaz de usuario

Prioridad en negocio: Alta

Estimación (horas): 12

Descripción: Como dueño de producto necesito que la interfaz del simulador sea amigable con el usuario, que exista un menú desplegable en la parte izquierda de forma vertical y se muestre las diferentes páginas web en cascada y de forma jerárquica y que al pasar el ratón sobre este se oculte automáticamente, y a su vez tenga la opción de dejar estático el menú.

Pruebas de aceptación:

Validar que al momento de desplegar un menú con su respectivo submenú los otros menús abiertos se contraigan y solo se muestre el menú seleccionado.

Fuente: Propia

Tabla 10 Historia de usuario n°7

HISTORIA DE USUARIO	
Número: 7	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Módulo de bienvenida

Prioridad en negocio: Alta

Estimación (horas): 10

Descripción: Como dueño de producto necesito una página de inicio del simulador donde se muestre información relevante del simulador, debe contener un logotipo del simulador y tener 5 apartados en el siguiente orden.

Inicio: Se mostrará el nombre del Simulador (SEmulator) y en dos líneas o menos se mostrará una descripción y el área de aplicación
Características: Se mostrará 4 de las características más relevantes del simulador
Niveles: Se explicará que el simulador constará de tres niveles de dificultad un Básico (para principiantes de 0% hasta 30%) – Intermedio (de 31% hasta 70%) - Avanzado (para expertos de 71% hasta 100%)
Descripción: Se mostrarán 3 apartados con la información referente a lo que contiene cada nivel.
Básico: Consta de 5 preguntas sencillas, área de aplicación phishing, porcentaje de avance en el simulador 30%.
Intermedio: Consta de 5 preguntas de conocimiento intermedio, área de aplicación clonación de páginas web y malware, porcentaje de avance en el simulador 70%.
Avanzado: Consta 4 preguntas de conocimiento avanzado, área de aplicación psicológica, porcentaje de avance en el simulador 100%.
Contacto: Se mostrará los datos de la Universidad Técnica del Norte (Nombre, dirección, sitio web, teléfono, mapa de localización, Facultad y carrera). También los datos del desarrollador (opcional).

Pruebas de aceptación:

La página web debe ser amigable al usuario

Fuente: Propia

Tabla 11 Historia de usuario n°8

HISTORIA DE USUARIO	
Número: 8	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Módulo de simulación de nivel básico.

Prioridad en negocio: Alta

Estimación (horas): 12

Descripción: Como dueño de producto necesito que se despliegue un menú general de simulación donde uno de los tres niveles sea el nivel de simulación básica el cual encabezará la lista con sus respectivos submenús el cual constará de una página con información y otras 5 con escenarios predefinidos enfocados al área de phishing, escenarios que serán gestionados únicamente por el programador.

La página de información contendrá una breve introducción referente a phishing, luego de la cual podrá iniciar la simulación. El programador es el encargado de preparar los diferentes escenarios con las siguientes temáticas:

Escenario 1: Premiación de boletos
Escenario 2: Actualización de sistema empresarial
Escenario 3: Email ANT
Escenario 4: ¿Recuerdas este video?
Escenario 5: Alguien accedió a tu cuenta

Cada escenario debe contener botones de elección si es phishing o es legítimo e independientemente de la elección del usuario se debe presentar una página con retroalimentación detallada referente al escenario propuesto.

Pruebas de aceptación:

Cada escenario debe ser entendible al usuario (nivel básico).
En la página de retroalimentación de cada escenario presentar imágenes.
Al terminar la simulación básica se debe presentar una página de información, mostrando el progreso (30%) y regresar al menú o continuar con el nivel intermedio de simulación

Fuente: Propia

Tabla 12 Historia de usuario n°9

HISTORIA DE USUARIO	
Número: 9	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Módulo de simulación de nivel intermedio.

Prioridad en negocio: Alta

Estimación (horas): 12

Descripción: Como dueño de producto necesito que se despliegue un menú general de simulación donde uno de los tres niveles principales sea el nivel de simulación intermedia y sus respectivos submenús bajo el menú de simulación básica, que constará de una página con información y otras 5 con escenarios predefinidos enfocados al área de clonación de sitios web y malware, escenarios que serán gestionados únicamente por el programador.

La página de información contendrá una breve introducción referente a clonación de sitios web y malware, luego de la cual podrá continuar la simulación. El programador es el encargado de preparar los diferentes escenarios con las siguientes temáticas:

Escenario 6: Clonación Facebook
Escenario 7: Inicio de sesión del simulador repentino
Escenario 8: Tarea por expirar aula virtual
Escenario 9: Generar PDF
Escenario 10: Descarga de malware

Cada escenario debe contener botones de elección si es clonación o es extorsión e independientemente de la elección del usuario se debe presentar una página con retroalimentación detallada referente al escenario propuesto.

Pruebas de aceptación:

Subir de dificultad respecto al nivel básico.
En la página de retroalimentación de cada escenario presentar imágenes.
A través de archivos inofensivos intentar poner en riesgo a privacidad del usuario
Al terminar la simulación intermedia se debe presentar una página de información, mostrando el progreso avanzado (70%) y permitir regresar al menú o continuar con el nivel avanzado de simulación

Fuente: Propia

Tabla 13 Historia de usuario n°10

HISTORIA DE USUARIO	
Número: 10	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Módulo de simulación de nivel avanzada.

Prioridad en negocio: Alta

Estimación (horas): 12

Descripción: Como dueño de producto necesito que se despliegue un menú general de simulación donde uno de los tres niveles principales sea el nivel de simulación avanzada y sus respectivos submenús bajo el menú de simulación intermedio, que constará de una página con información y otras 4 con escenarios predefinidos enfocados al área psicológica, escenarios que serán gestionados únicamente por el programador, este es el encargado de preparar los diferentes escenarios con las siguientes temáticas:

Escenario 11: Mensajes de voz (Pago retrasado)
Escenario 12: Generación de certificado (Usar cámara)
Escenario 13: Obtener datos (Formulario)
Escenario 14: Mejor estudiante

Cada escenario debe contener botones de elección si es extorsión o el escenario es legítimo e independientemente de la elección del usuario se debe presentar una página con retroalimentación detallada referente al escenario propuesto.

Pruebas de aceptación:

Subir de dificultad respecto al nivel intermedio.
En la página de retroalimentación de cada escenario presentar imágenes.
A través de archivos inofensivos intentar poner en riesgo a privacidad del usuario
Al terminar la simulación avanzada se debe presentar una página de información, mostrando el progreso avanzado (100%) y permitir regresar al menú.
No existirá una página de información inicial en este nivel.

Fuente: Propia

Tabla 14 Historia de usuario n°11

HISTORIA DE USUARIO	
Número: 11	**Usuario:** Ing. Daysi Imbaquingo

Nombre de Historia: Subida del aplicativo al servidor local de la UTN.

Prioridad en negocio: Alta

Estimación (horas): 12

Descripción: Como dueño de producto necesito que la aplicación esté disponible en la red interna de la UTN, para lo cual se proveerá un servidor local al desarrollador.

Pruebas de aceptación:

La aplicación debe estar disponible para acceder desde el campus universitario UTN.

Fuente: Propia

Tabla 15 Historia de usuario n°12

HISTORIA DE USUARIO	
Número: 12	**Usuario:** Ing. Daysi Imbaquingo
Nombre de Historia: Prototipo del simulador web	
Prioridad en negocio: Alta	
Estimación (horas): 10	
Descripción: Como dueño de producto necesito tener un prototipo del simulador web antes de empezar con el desarrollo.	
Pruebas de aceptación:	
El prototipo debe estar desarrollado bajo software libre. El prototipo solamente indicará los escenarios del simulador web.	

Fuente: Propia

2.4 Definición del product backlog

Tabla 16 Definición del product backlog

Prioridad	ID	Historia de Usuario	Tiempo estimado (h)
1	HU1	Levantamiento de requisitos	12
2	HU2	Base de datos, arquitectura	24
8	HU3	Gestión de usuarios	10
7	HU4	Módulo de acceso	18
6	HU5	Módulo de registro	15
4	HU6	Plantilla de interfaz de usuario	16
5	HU7	Módulo de bienvenida	6
9	HU8	Módulo de simulación de nivel básico	18
10	HU9	Módulo de simulación de nivel intermedio	21
11	HU10	Módulo de simulación de nivel avanzado	23
12	HU11	Subida del aplicativo al servidor local de la UTN	15
3	HU12	Prototipo del simulador	10

Fuente: Propia

2.5 Conformación del equipo de trabajo

La conformación del equipo de trabajo es parte fundamental dentro de la metodología Scrum, en este apartado se documenta las respetivas funciones y responsabilidades de cada uno de los miembros, para el desarrollo de este proyecto el equipo se conformó como se detalla a continuación.

Tabla 17 Conformación del equipo de trabajo

Nombre	Rol	Descripción	Responsabilidad
Ing. Daysi Imbaquingo	Product owner	Encargada de informar los procesos que estarán presentes en el simulador web.	Facilitar todos los requerimientos principales que estarán presentes en el simulador web Solicitar revisión de los avances Verificar que todos los requisitos sean cumplidos.
Ing. Alex Guevara	Scrum master	Responsable de asegurar que la metodología Scrum sea entendible, adaptable y aplicable.	Líder del equipo de trabajo Convocar e reuniones periódicas para verificar que todos los requisitos sean cumplidos.
Sr. Franklin Vallejo	Equipo de desarrollo	Su función es desarrollar y entregar el simulador web al usuario final.	Programador

Fuente: Propia

2.6 Desarrollo del aplicativo

El desarrollo del simulador web se realizó implementando Scrum como marco de trabajo, la característica principal de esta metodología es que trabaja bajo lapsos de tiempo denominados Sprints, en los cuales se definen las tareas a realizar enfocados a cumplir los requerimientos de desarrollo de software, los cuales son visibles en las historias de usuarios.

Cada Sprint tuvo la duración de cuatro semanas y se realizó el siguiente proceso:

Tabla 18 Proceso general de los Sprints

Id	Nombre reunión	Descripción
1	Reunión de planificación	En esta reunión se planificó las actividades a desarrollarse en el lapso del Sprint, del cual se obtiene el product backlog y la planificación del Sprint.

2	Reunión de revisión	Al finalizar el Sprint, el product owner, scrum master y el equipo de desarrollo se reunieron con la finalidad de hacer un análisis acerca de todo lo que se llevó a cabo durante el sprint como el cumplimiento del objetivo, aquí los involucrados colaboraron para determinar las siguientes cosas que se pudo hacer para optimizar ya sean recursos o tiempo en el siguiente Sprint y se mostró la lista de producto en el estado actual para observar las tareas de los siguientes Sprints.
3	Reunión de retrospectiva	Esta reunión definió la etapa final del sprint donde se reunieron el scrum master y el equipo de desarrollo con la finalidad de inspeccionarse a sí mismos y crear un plan de mejoras que ayudaron a superar dificultades del Sprint.

Fuente: Propia

Estas reuniones fueron mucha importancia en el presente proyecto ya que a medida que avanzó el desarrollo se presentaron dificultades, las cuales fueron superadas a tiempo para no retrasar el proyecto, basándose en los lineamientos del marco de trabajo Scrum, con el fin de entregar u ofrecer un producto terminado al product owner.

2.6.1 Desarrollo de los Sprints

Para el desarrollo de los Sprints a continuación se muestra las iteraciones que se realizó hasta la entrega del simulador web terminado. En la tabla 19 se puede apreciar el cumplimiento y ejecución de los Sprints.

Tabla 19 Fechas de cumplimiento y ejecución de los Sprints

Sprint	Inicio	Finalización	Horas
0	lunes, 9 de diciembre de 2019	viernes, 13 de diciembre de 2019	40
1	lunes, 16 de diciembre de 2019	viernes, 20 de diciembre de 2019	39
2	lunes, 23 de diciembre de 2019	viernes, 27 de diciembre de 2019	40
3	lunes, 30 de diciembre de 2019	viernes, 3 de enero de 2020	40
4	lunes, 6 de enero de 2020	viernes, 10 de enero de 2020	40
5	lunes, 13 de enero de 2020	viernes, 17 de enero de 2020	40

Fuente: Propia

Sprint 0

a. Reunión planificación

Fecha de la reunión: viernes, 6 de diciembre de 2019

Asistentes a la reunión: Scrum master, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 9 de diciembre de 2019

Fechas de finalización Sprint: viernes, 13 de diciembre de 2019

Objetivo de Sprint: Levantamiento de requisitos y arquitectura tecnológica

- **Historias de Usuario involucradas en el Sprint 0**

Tabla 20 Historias de usuarios involucradas sprint 0

ID	HISTORIA DE USUARIO
HU1	Levantamiento de requisitos
HU2	Base de datos, arquitectura

Fuente: Propia

Como inicio de las fases del proyecto, se realizó un análisis de la arquitectura a ser seleccionada para el desarrollo del simulador web, siguiendo las especificaciones del dueño del producto establecidas en la figura 5 como diagrama del proceso.

- **Planificación de tareas**

Tabla 21 Planificación tareas sprint 0

PLANIFICACIÓN DE TAREAS SPRINT 0			
HISTORIA DE USUARIO	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
HU1	Análisis	Realizar los diagramas de proceso	2
	Análisis	Historias de Usuario	8
HU2	Análisis	Definir la base de datos	2
	Análisis	Realizar el modelo entidad-relación, utilizando software para modelamiento de la base de datos	5
	Análisis	Normalizar la base de datos para una mejor administración de la información	5
	Análisis	Implementar el modelo en la RDBMS seleccionada	8
Reuniones	Planificación	Planificación	4
	Revisión	Revisión	3
	Revisión	Retrospectiva	3
		TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos planteados en el product backlog.

Tabla 22 Reunión revisión sprint 0

HISTORIA DE USUARIO	DESARROLLADOR	TAREA	TIEMPO ESTIMADO (HORAS)	HORAS REALES
HU1	Franklin Vallejo	Reunión para definición de requerimientos	3	2
	Franklin Vallejo	Realizar e diagrama de proceso	2	4
	Franklin Vallejo	Historias de Usuario	5	3
HU2	Franklin Vallejo	Definir la base de datos	2	2
	Franklin Vallejo	Modelarla base de datos	5	8
	Franklin Vallejo	Normalizar la base de datos	5	3
	Franklin Vallejo	Implementar el modelo en la RDBMS seleccionada	8	8
Reuniones	Scrum Team	Planificación	4	4
	Scrum Team	Revisión	3	3
	Scrum Team	Retrospectiva	3	3
		TOTAL	**40**	**40**

Fuente: Propia

- **Diagrama de la base de datos**

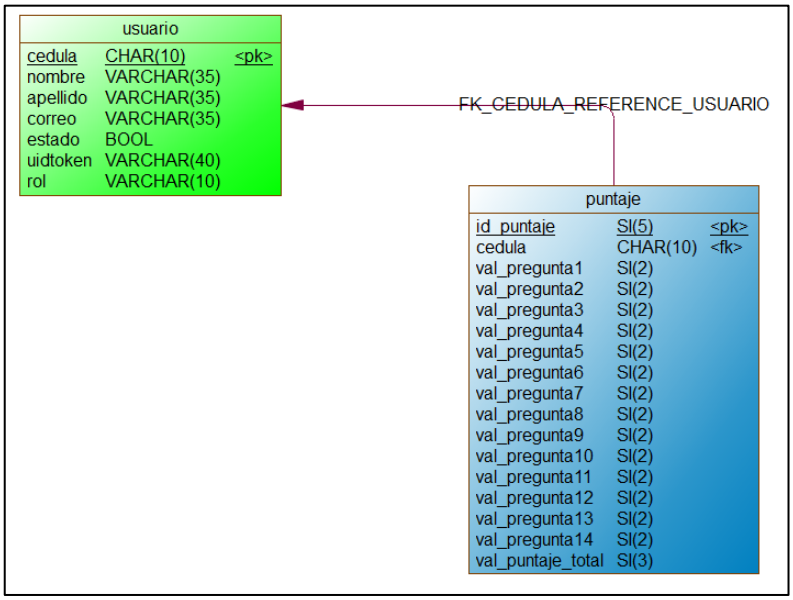


Fig. 6 Diagrama base de datos SEmulator

c. Arquitectura

La arquitectura se definió en una reunión con la tutora en la figura 2.

d. Reunión retrospectiva

Tabla 23 Reunión retrospectiva sprint 0

RETROSPECTIVA		
Fecha: viernes, 13 de diciembre de 2019		
Asistentes a la reunión: Daysi Imbaquingo (Scrum Master), Franklin Vallejo (Equipo de desarrollo)		
¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
El equipo de desarrollo culminó su tarea en el tiempo establecido	No hubo buena comunicación entre los integrantes del Scrum Team	Mejorar la comunicación entre los miembros del equipo

Fuente: Propia

Sprint 1

a. Reunión planificación

Fecha de la reunión: sábado, 14 de diciembre de 2019

Asistentes a la reunión: Scrum master, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 16 de diciembre de 2019

Fechas de finalización Sprint: viernes, 20 de diciembre de 2019

Objetivo de Sprint: Desarrollo CRUDS de tabla usuario de la base de datos, entrega de prototipo simulador web

- **Historias de Usuario involucradas en el Sprint 1**

Tabla 24 Historias de usuarios involucradas sprint 1

ID	HISTORIA DE USUARIO
HU12	Prototipo del simulador web
HU3	Gestión de usuarios

Fuente: Propia

- **Planificación de tareas**

Tabla 25 Planificación tareas sprint 1

PLANIFICACIÓN DE TAREAS SPRINT 1				
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
HU12	Franklin Vallejo	Investigación	Capacitación e instalación del software para prototipado	5
	Franklin Vallejo	Diseño	Modelado del prototipo	5
HU3	Franklin Vallejo	Diseño	Modelado del prototipo	10
	Franklin Vallejo	Codificación	Listar usuarios	4
	Franklin Vallejo	Codificación	Editar usuario	5
	Franklin Vallejo	Codificación	Activar usuario y consulta de puntajes	2
Reuniones	Scrum Team	Planificación	Planificación	4
	Scrum Team	Revisión	Revisión	3
	Scrum Team	Revisión	Retrospectiva	2
			TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos planteados en el product backlog.

Tabla 26 Reunión revisión sprint 1

HISTORIA DE USUARIO	DESARROLLADOR	FASE DESARROLLO	TAREA	TIEMPO ESTIMADO (HORAS)	TIEMPO REAL (HORAS)
HU12	Franklin Vallejo	Investigación	Capacitación e instalación del software para prototipado	5	4
	Franklin Vallejo	Diseño	Modelado del prototipo	5	5
HU3	Franklin Vallejo	Diseño	Modelado del prototipo	10	8
	Franklin Vallejo	Codificación	Listar usuarios	4	5
	Franklin Vallejo	Codificación	Editar usuario	5	4
	Franklin Vallejo	Codificación	Activar usuario y consulta de puntajes	2	3
Reuniones	Scrum Team	Planificación	Planificación	4	4
	Scrum Team	Revisión	Revisión	3	4
	Scrum Team	Retrospectiva	Retrospectiva	2	2
			TOTAL	**40**	**39**

Fuente: Propia

- **Construcción y entrega del prototipo**

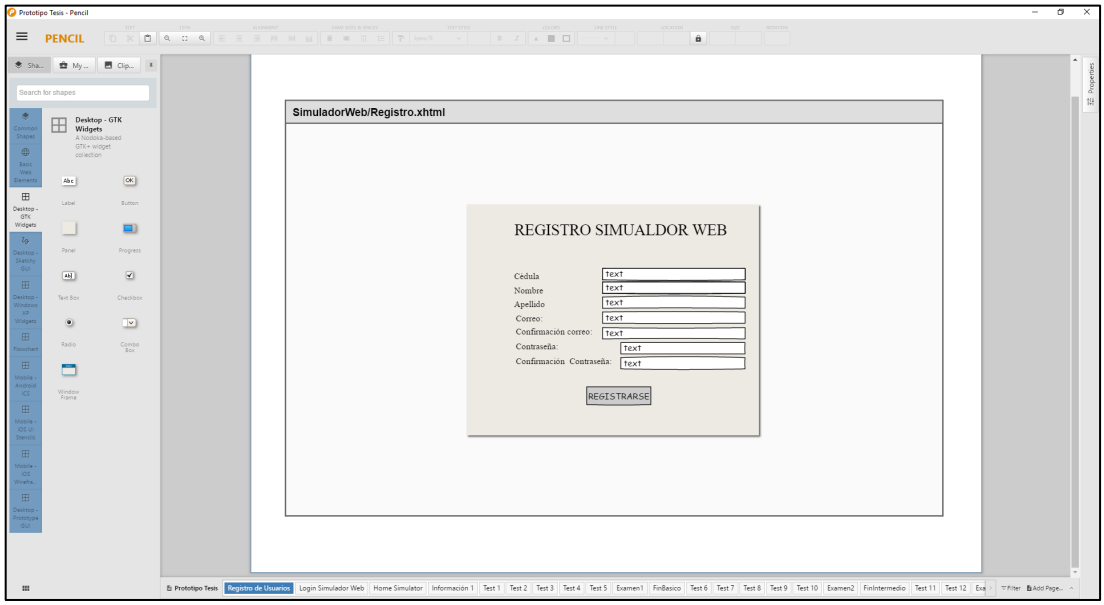


Fig. 7 Construcción del prototipo registro en Pencil

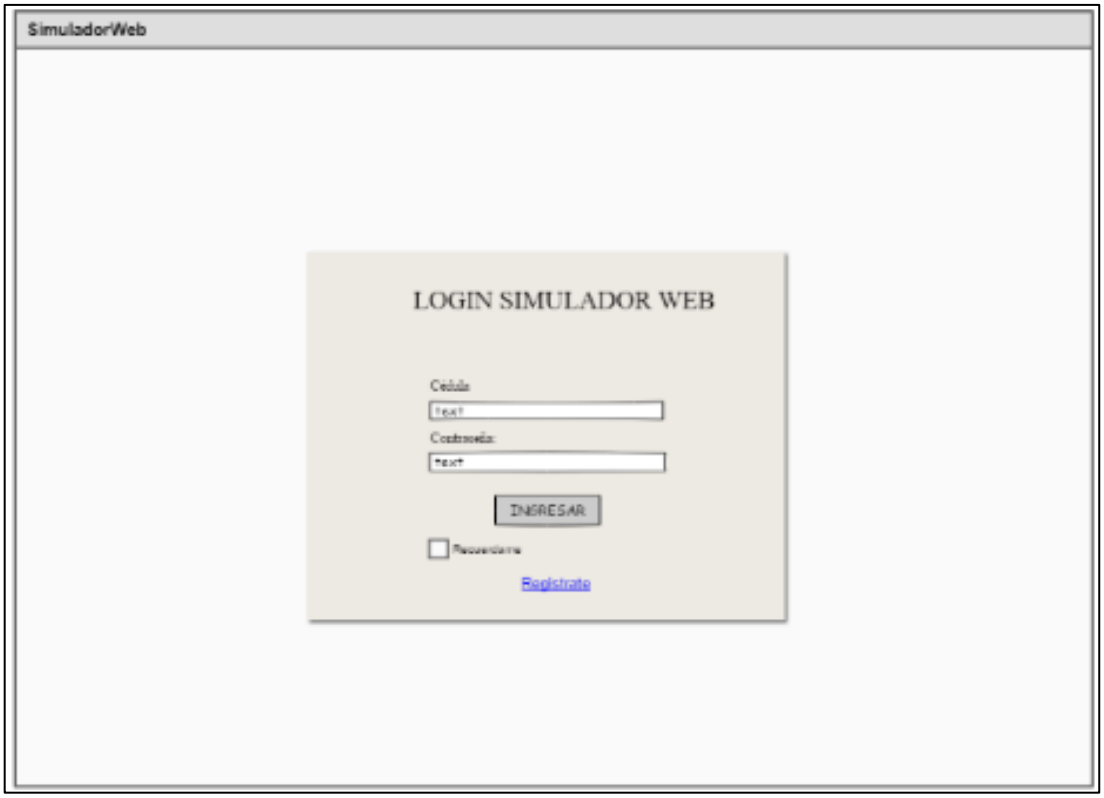


Fig. 8 Entrega del prototipo SEmulator en Pencil

- **Imágenes del sistema o código**

```
public String actionAddUserStudent() {
    String ptoken = "";
    try {
        System.out.println("controller init");
        UUID = managerUsuario.randomCodeGenerator();
        boolean estadotemp = false;
        String roltemp = "ESTUD";
        managerUsuario.createUserStudent(cedula, nombre, apellido, correo, contrasenia, UUID, estadotemp, roltemp);
        System.out.println("controller passed");
        System.out.println("controller email init");
        this.actionEnvioMailVerification();
        System.out.println("controller email passed");
        JSFUtil.crearMensajeInfo("Se ha registrado un nuevo usuario");
        ptoken = "token_student";

    } catch (Exception e) {
        JSFUtil.crearMensajeError(e.getMessage());
    }
    return ptoken;
}
```

Fig. 9 Código java en eclipse creación usuario

```
public void actionListenerCargarDatosUsuario(Usuario usuario) {
    cedulaEditar = usuario.getCedula();
    nombre = usuario.getNombre();
    apellido = usuario.getApellido();
    correo = usuario.getCorreo();
    contraseniaEditar = usuario.getContrasenia();
    estado = usuario.getEstado();
    UUID = usuario.getUuidtoken();
    roleditar = usuario.getRol();
}
```

Fig. 10 Código java en eclipse listar usuario

```
public void actionListenerActualizarUsuario() {
    try {
        managerUsuario.editUser(cedulaEditar, nombre, apellido, correo, contrasenia, estado, UUID, roleditar);
        list_usersest = managerUsuario.findAllUsersEstudiante();
        list_users = managerUsuario.findAllUsersAdmin();
        JSFUtil.crearMensajeInfo("Actualización correcta");
    } catch (Exception e) {
        JSFUtil.crearMensajeError(e.getMessage());
    }
}
```

Fig. 11 Código java en eclipse editar usuario

```
public void actionListenerActivar(String cedula) {
    try {
        managerUsuario.actualizarEstado(cedula);
        list_usersest = managerUsuario.findAllUsersEstudiante();
        JSFUtil.crearMensajeInfo("El estudiante con cédula " + cedula + " ha cambiado su estado.");
    } catch (Exception e) {
        JSFUtil.crearMensajeError(e.getMessage());
        e.printStackTrace();
    }
}
```

Fig. 12 Código java en eclipse activar usuario

c. Reunión retrospectiva

Tabla 27 Reunión retrospectiva Sprint 1

RETROSPECTIVA		
Fecha: viernes, 20 de diciembre de 2019 **Asistentes a la reunión:** Daysi Imbaquingo (Scrum Master), Franklin Vallejo (Equipo de desarrollo)		
¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
El equipo de desarrollo culminó su tarea en menos del tiempo establecido	Ya existió mejor comunicación entre los integrantes del Scrum Team	Mejorar aún más la comunicación entre los miembros del equipo

Fuente: Propia

Sprint 2

a. Reunión planificación

Fecha de la reunión: sábado, 21 de diciembre de 2019

Asistentes a la reunión: Scrum master, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 23 de diciembre de 2019

Fechas de finalización Sprint: viernes, 27 de diciembre de 2019

Objetivo de Sprint: Desarrollar la plantilla de interfaz de usuario y el módulo de bienvenida tanto para el usuario estudiante como para el usuario administrador.

- **Historias de Usuario involucradas en el Sprint 2**

Tabla 28 Historias de usuarios involucradas sprint 2

ID	HISTORIA DE USUARIO
HU6	Plantilla de interfaz de usuario
HU7	Módulo de bienvenida

Fuente: Propia

- **Planificación de tareas**

Tabla 29 Planificación tareas sprint 2

PLANIFICACIÓN DE TAREAS SPRINT 2				
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
HU6	Franklin Vallejo	Codificación	Creación y edición de plantilla	8
	Franklin Vallejo	Codificación	Menú estático	4
	Franklin Vallejo	Codificación	Jerarquía desplegable	4
HU7	Franklin Vallejo	Codificación	Creación de secciones del cuerpo de la página de bienvenida	9
	Franklin Vallejo	Codificación	Alimentación de información a la página de bienvenida	6
Reuniones	Scrum Team	Planificación	Planificación	4
	Scrum Team	Revisión	Revisión	3
	Scrum Team	Revisión	Retrospectiva	2
			TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos planteados en el product backlog.

Tabla 30 Reunión revisión sprint 2

HISTORIA DE USUARIO	DESARROLLADOR	FASE DESARROLLO	TAREA	TIEMPO ESTIMADO (HORAS)	TIEMPO REAL (HORAS)
HU6	Franklin Vallejo	Codificación	Creación y edición de plantilla	8	8

	Franklin Vallejo	Codificación	Menú estático	4	4
	Franklin Vallejo	Codificación	Jerarquía desplegable	4	4
HU7	Franklin Vallejo	Codificación	Creación de secciones del cuerpo de la página de bienvenida	9	8
	Franklin Vallejo	Codificación	Alimentación de información a la página de bienvenida	6	6
Reuniones	Scrum Team	Planificación	Planificación	4	4
	Scrum Team	Revisión	Revisión	3	4
	Scrum Team	Retrospectiva	Retrospectiva	2	2
			TOTAL	**40**	**39**

Fuente: Propia

- **Imágenes del sistema o código**

Fig. 13 Creación y edición de plantilla en eclipse

Fig. 14 Menú estático en eclipse

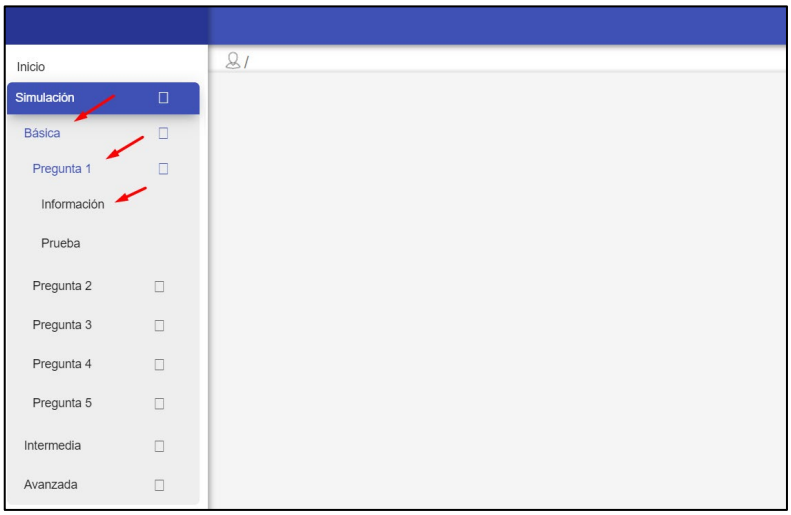


Fig. 15 Jerarquía desplegable en eclipse

Fig. 16 Creación de secciones del cuerpo de la página de bienvenida en eclipse

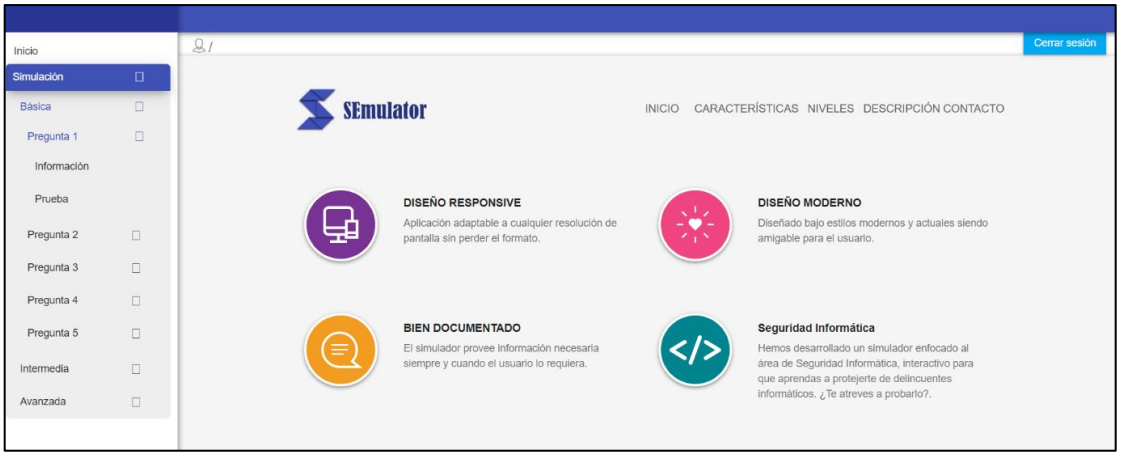


Fig. 17 Alimentación de información a la página de bienvenida en eclipse

c. Reunión retrospectiva

Tabla 31 Reunión retrospectiva sprint 2

RETROSPECTIVA		
Fecha: viernes, 27 de diciembre de 2019 **Asistentes a la reunión:** Daysi Imbaquingo (Scrum Master), Franklin Vallejo (Equipo de desarrollo)		
¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
El equipo de desarrollo culminó su tarea en menos del tiempo establecido	Al no haber mucha comunicación entre el equipo de trabajo, se puso información desactualizada en la página de bienvenida.	Mejorar aún más la comunicación entre los miembros del equipo. Proveer información clara y actualizada entre los miembros del equipo de trabajo.

Fuente: Propia

Sprint 3

a. Reunión planificación

Fecha de la reunión: sábado, 28 de diciembre de 2019

Asistentes a la reunión: Scrum master, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 30 de diciembre de 2019

Fechas de finalización Sprint: viernes, 3 de enero de 2019

Objetivo de Sprint: Desarrollar los módulos de registro para el rol estudiante y acceso al simulador ya sea con el rol estudiante (simulador) o rol administrador (panel de administración).

- **Historias de Usuario involucradas en el Sprint 3**

Tabla 32 Historias de usuarios involucradas sprint 3

ID	HISTORIA DE USUARIO
HU5	Módulo de registro
HU4	Módulo de acceso

Fuente: Propia

- **Planificación de tareas**

Tabla 33 Planificación tareas sprint 3

PLANIFICACIÓN DE TAREAS SPRINT 3				
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
HU4	Franklin Vallejo	Codificación	Codificación de nuevo usuario	5
	Franklin Vallejo	Codificación	Codificación de la lista de usuarios	8
	Franklin Vallejo	Codificación	Codificación de editar usuarios	5
	Franklin Vallejo	Codificación	Codificación de activar usuario	2
HU5	Franklin Vallejo	Codificación	Codificación de Login de usuario	6
	Franklin Vallejo	Codificación	Codificación de Login de administradores	5
Reuniones	Scrum Team	Planificación	Planificación	4
	Scrum Team	Revisión	Revisión	3
	Scrum Team	Revisión	Retrospectiva	2
			TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos plateados en el product backlog.

Tabla 34 Reunión revisión sprint 3

HISTORIA DE USUARIO	DESARROLLADOR	FASE DESARROLLO	TAREA	TIEMPO ESTIMADO (HORAS)	Tiempo REAL (HORAS)
HU4	Franklin Vallejo	Codificación	Codificación de nuevo usuario	5	6

	Franklin Vallejo	Codificación	Codificación de la lista de usuarios	8	8
	Franklin Vallejo	Codificación	Codificación de editar usuarios	5	5
	Franklin Vallejo	Codificación	Codificación de activar usuario	2	3
HU5	Franklin Vallejo	Codificación	Codificación de Login de usuarios	6	6
	Franklin Vallejo	Codificación	Codificación de Login de administradores	5	4
Reuniones	Scrum Team	Planificación	Planificación	4	3
	Scrum Team	Revisión	Revisión	3	3
	Scrum Team	Revisión	Retrospectiva	2	2
			TOTAL	**40**	**40**

Fuente: Propia

- **Imágenes del sistema**

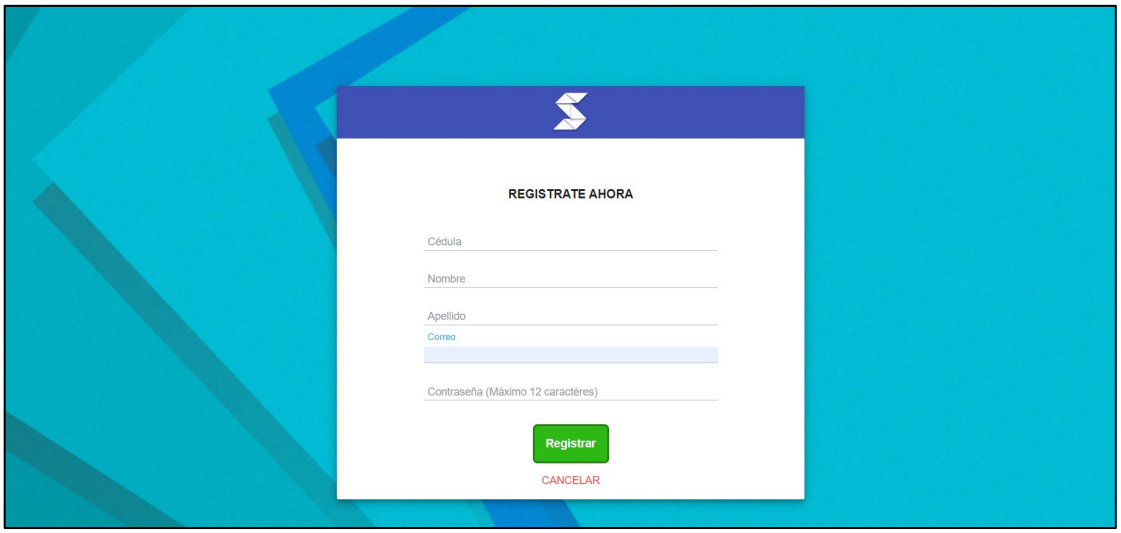


Fig. 18 Codificación de nuevo usuario en eclipse

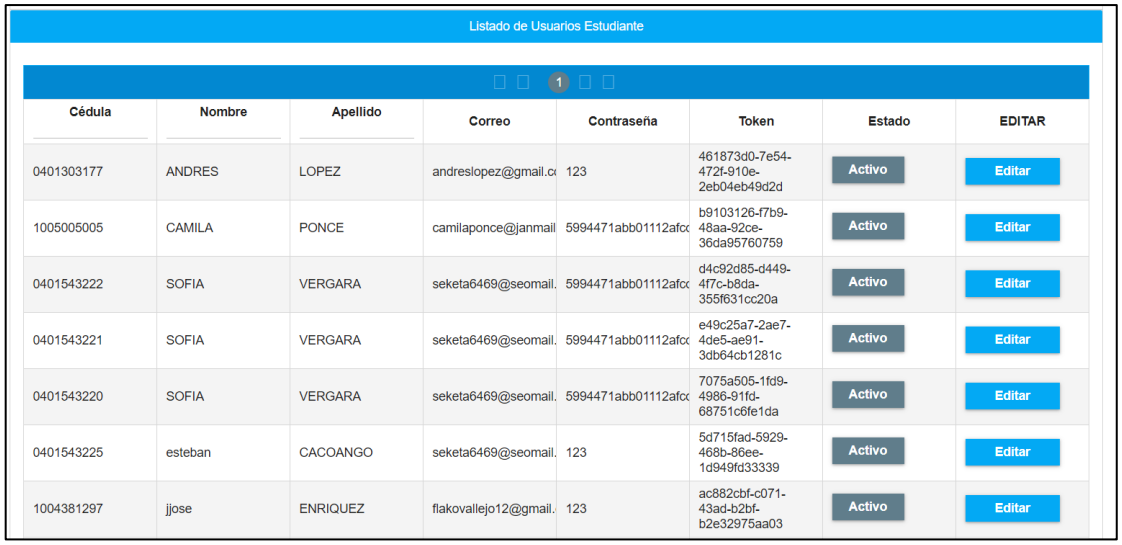


Fig. 19 Codificación de la lista de usuarios en eclipse

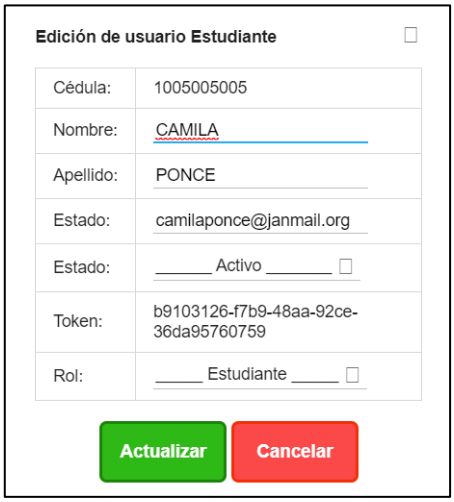


Fig. 20 Codificación de editar usuarios en eclipse

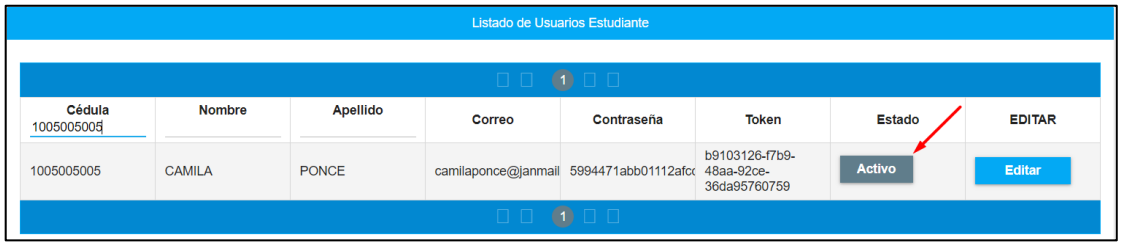
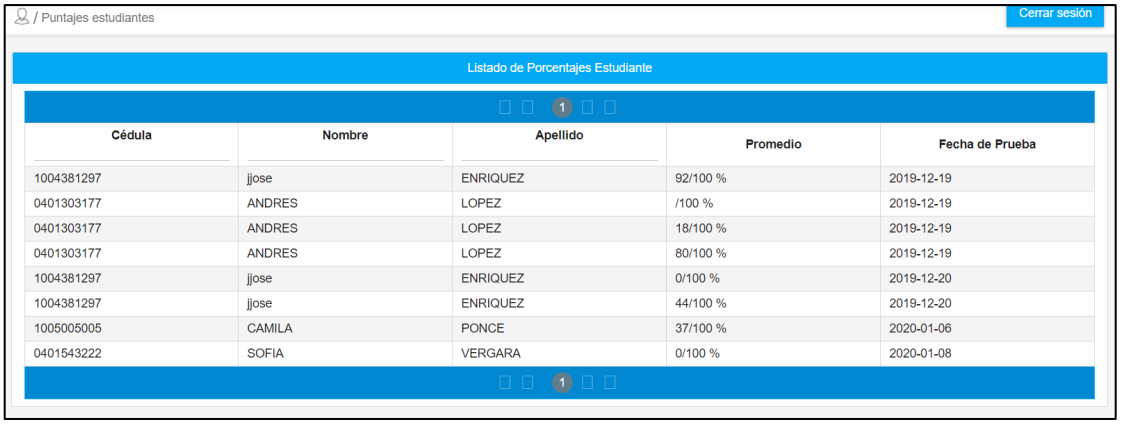


Fig. 21 Codificación de activar usuario en eclipse



Cédula	Nombre	Apellido	Promedio	Fecha de Prueba
1004381297	jjose	ENRIQUEZ	92/100 %	2019-12-19
0401303177	ANDRES	LOPEZ	/100 %	2019-12-19
0401303177	ANDRES	LOPEZ	18/100 %	2019-12-19
0401303177	ANDRES	LOPEZ	80/100 %	2019-12-19
1004381297	jjose	ENRIQUEZ	0/100 %	2019-12-20
1004381297	jjose	ENRIQUEZ	44/100 %	2019-12-20
1005005005	CAMILA	PONCE	37/100 %	2020-01-06
0401543222	SOFIA	VERGARA	0/100 %	2020-01-08

Fig. 22 Consulta de puntajes en eclipse

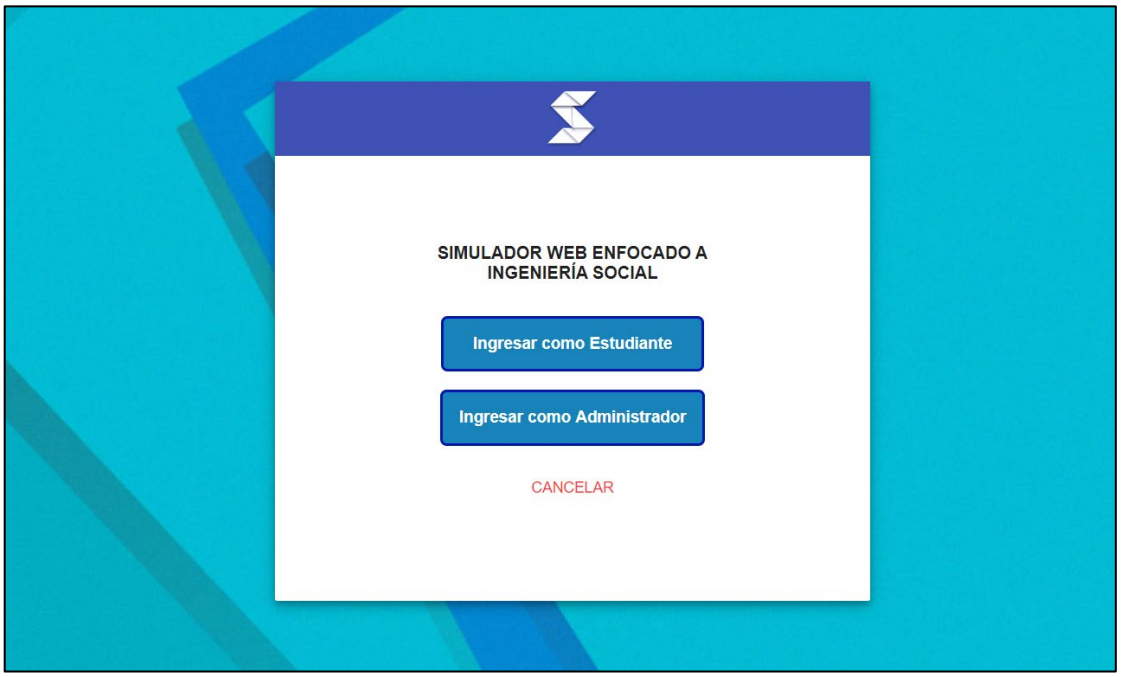


Fig. 23 Codificación de login usuario estudiante y usuario administrador en eclipse

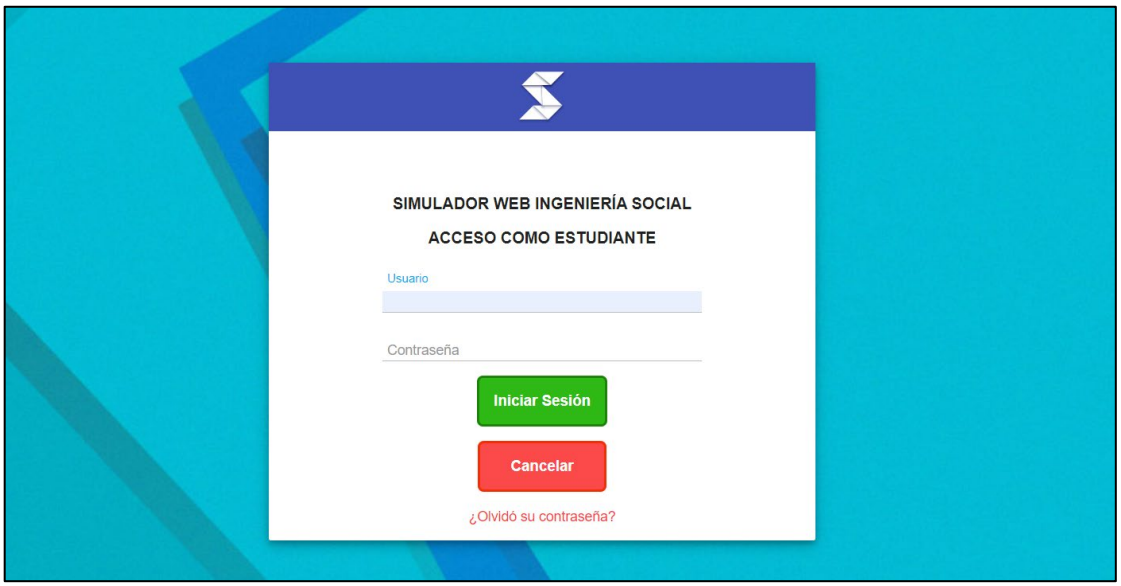


Fig. 24 Codificación de login de usuarios estudiantes en eclipse

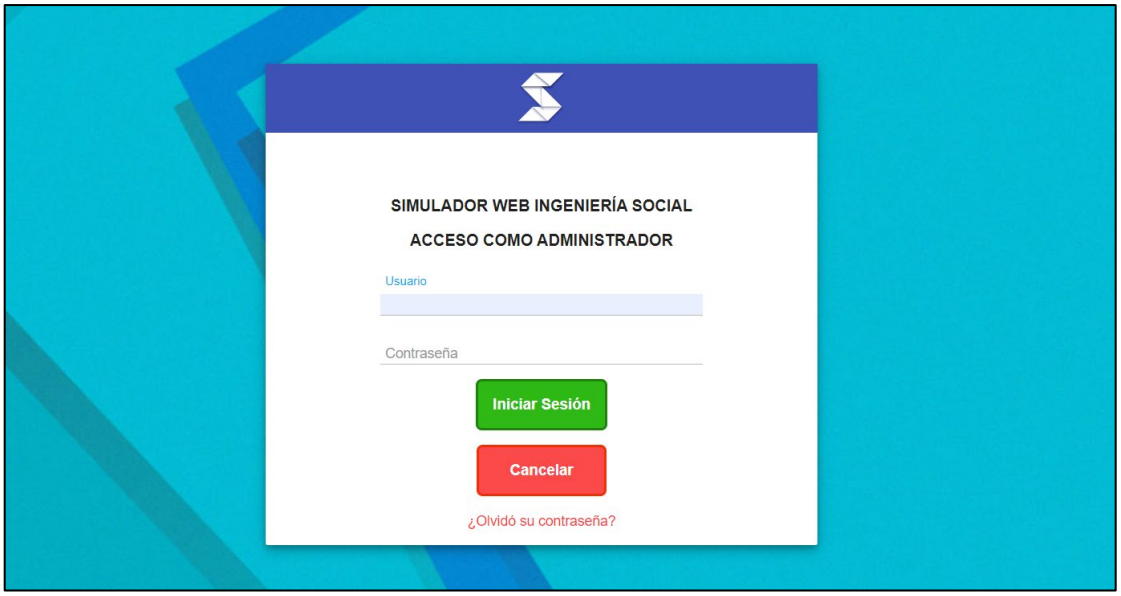


Fig. 25 Codificación de login de administradores en eclipse

c. Reunión retrospectiva

Tabla 35 Reunión retrospectiva sprint 3

RETROSPECTIVA		
Fecha: viernes, 3 de enero de 2019		
Asistentes a la reunión: Daysi Imbaquingo (Scrum master), Franklin Vallejo (Equipo de desarrollo)		
¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
Todo el scrum team estuvo informado de todos los cambios realizados en el simulador	Los programadores tomaron un curso aparte de programación para nivelar conocimientos	Realizar primero la documentación antes que el desarrollo.

Fuente: Propia

Sprint 4

a. Reunión planificación

Fecha de la reunión: sábado, 4 de enero de 2019

Asistentes a la reunión: Scrum master, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 6 de enero de 2020

Fechas de finalización Sprint: viernes, 10 de enero de 2020

Objetivo de Sprint: Desarrollo de los módulos de simulación básica, intermedia y avanzada

- **Historias de Usuario involucradas en el Sprint 4**

Tabla 36 Historias de usuarios involucradas sprint 4

ID	HISTORIA DE USUARIO
HU8	Módulo de simulación básica
HU9	Módulo de simulación intermedia

Fuente: Propia

- **Planificación de tareas**

Tabla 37 Planificación tareas sprint 4

PLANIFICACIÓN DE TAREAS SPRINT 4				
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
HU8	Franklin Vallejo	Codificación	Codificación de la página de información del simulador básico	2
	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación básica y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación básica y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación básica y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación básica y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del quinto y último escenario de simulación básica y su respectiva retroalimentación	3
HU9	Franklin Vallejo	Codificación	Codificación de la página de información del simulador intermedio	2
	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación intermedia y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación intermedia y su respectiva retroalimentación	2
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación intermedia y su respectiva retroalimentación	2
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación intermedia y su respectiva retroalimentación	3
	Franklin Vallejo	Codificación	Codificación del quinto escenario de simulación intermedia y su respectiva retroalimentación	3
Reuniones	Scrum Team	Planificación	Planificación	4
	Scrum Team	Revisión	Revisión	2
	Scrum Team	Revisión	Retrospectiva	2
			TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos plateados en el product backlog.

Tabla 38 Reunión revisión sprint 4

PLANIFICACIÓN DE TAREAS SPRINT 3					
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**	**TIEMPO REAL (HORAS)**
HU8	Franklin Vallejo	Codificación	Codificación de la página de información del simulador básico	2	2
	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación básica y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación básica y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación básica y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación básica y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del quinto y último escenario de simulación básica y su respectiva retroalimentación	3	3
HU9	Franklin Vallejo	Codificación	Codificación de la página de información del simulador intermedio	2	2
	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación intermedia y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación intermedia y su respectiva retroalimentación	2	2
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación intermedia y su respectiva retroalimentación	2	2
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación intermedia y su respectiva retroalimentación	3	3
	Franklin Vallejo	Codificación	Codificación del quinto escenario de simulación intermedia y su respectiva retroalimentación	3	3
Reuniones	Scrum Team	Planificación	Planificación	4	4
	Scrum Team	Revisión	Revisión	2	2
	Scrum Team	Revisión	Retrospectiva	2	2
			TOTAL	**40**	**40**

Fuente: Propia

- **Imágenes del sistema**

Fig. 26 Codificación de la página de información del simulador básico en eclipse

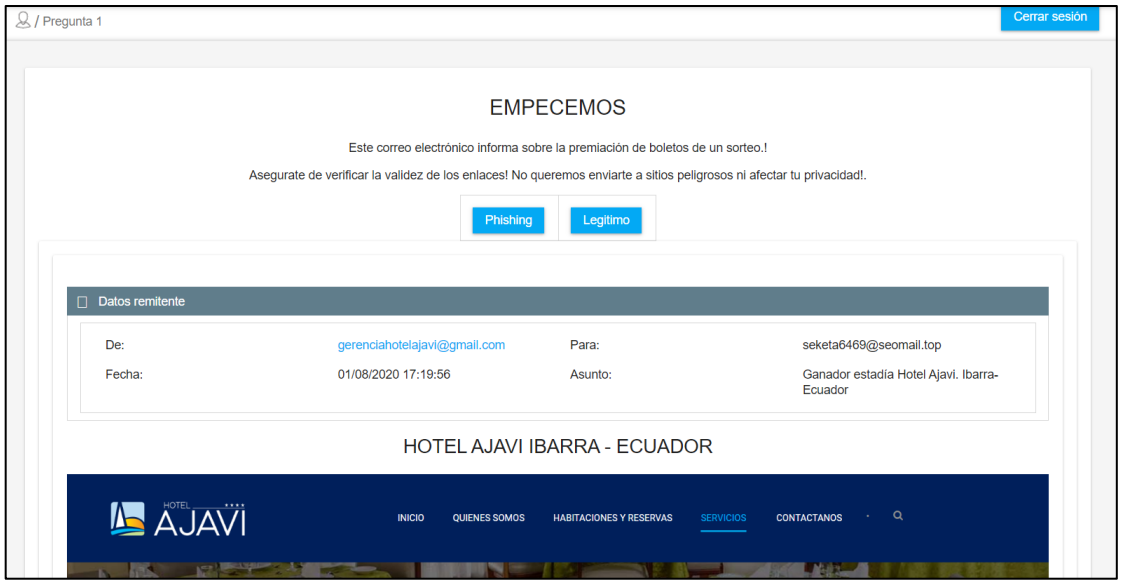


Fig. 27 Codificación del primer escenario de simulación básica y su respectiva retroalimentación en eclipse

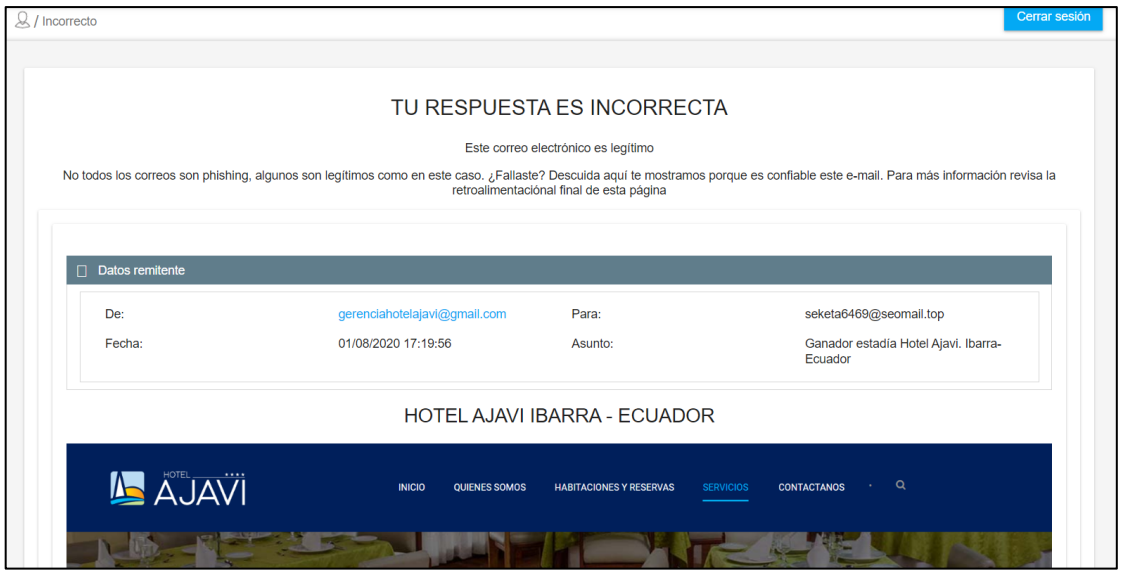


Fig. 28 Calificación pregunta 1 realizada en eclipse

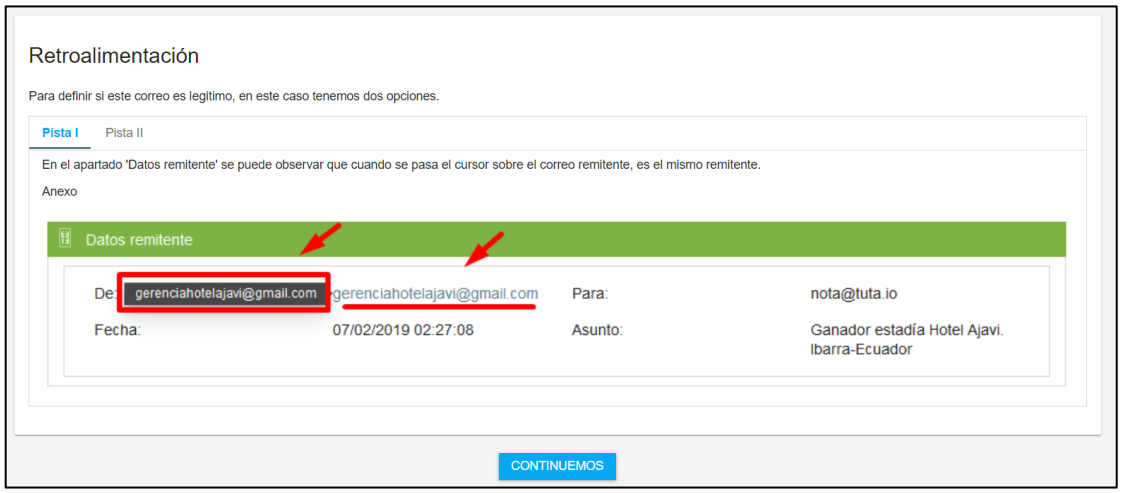


Fig. 29 Retroalimentación pregunta 1 respondida en eclipse parte 1

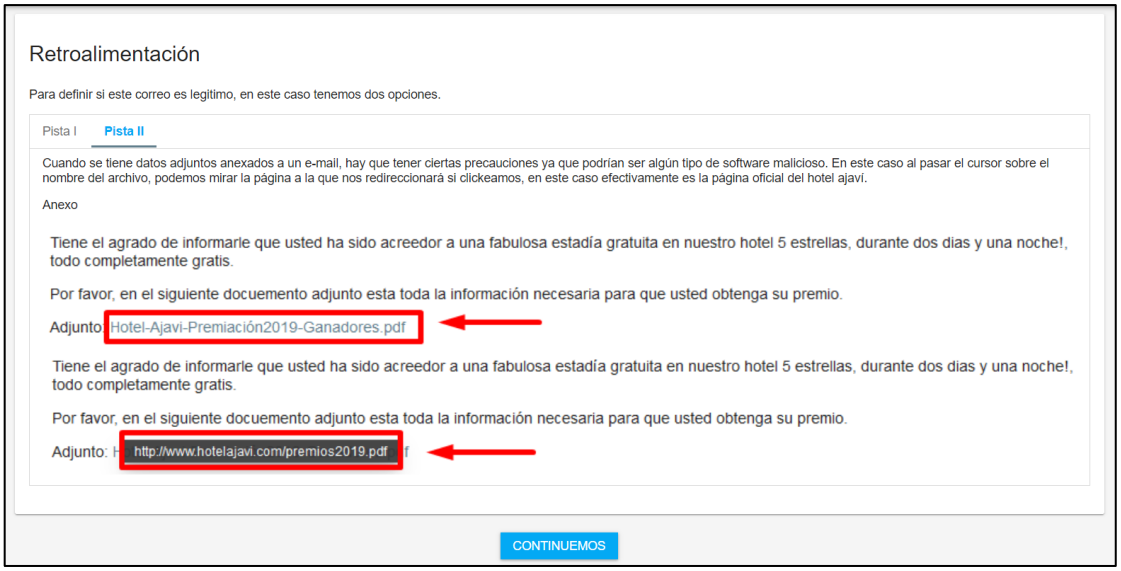


Fig. 30 Retroalimentación pregunta 1 respondida en eclipse parte 2

Fig. 31 Codificación del primer escenario de simulación intermedia y su respectiva retroalimentación en eclipse parte 1

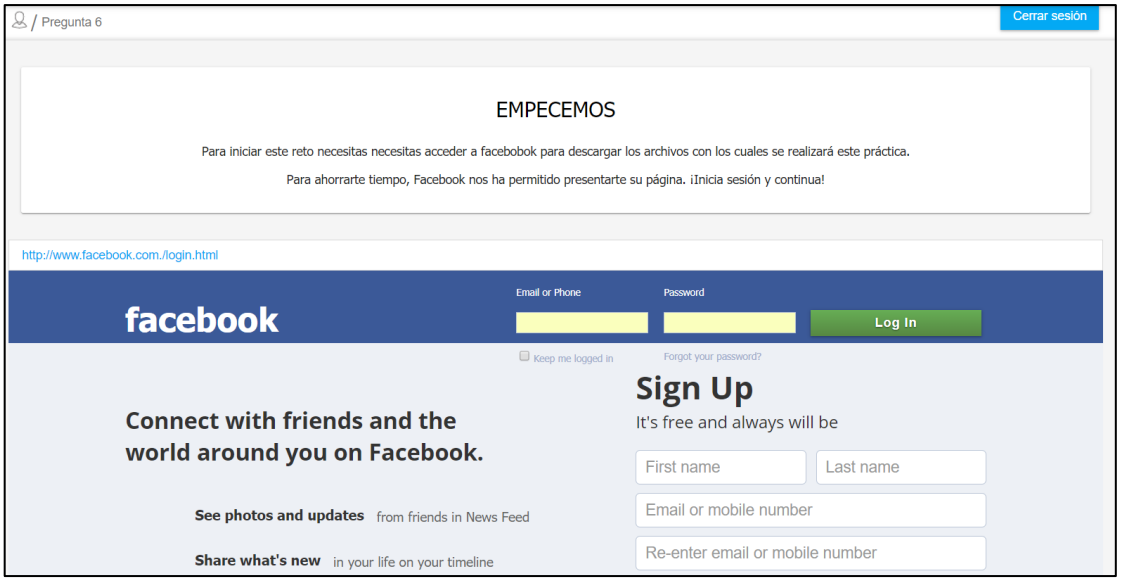


Fig. 32 Codificación del primer escenario de simulación intermedia y su respectiva retroalimentación en eclipse parte 2

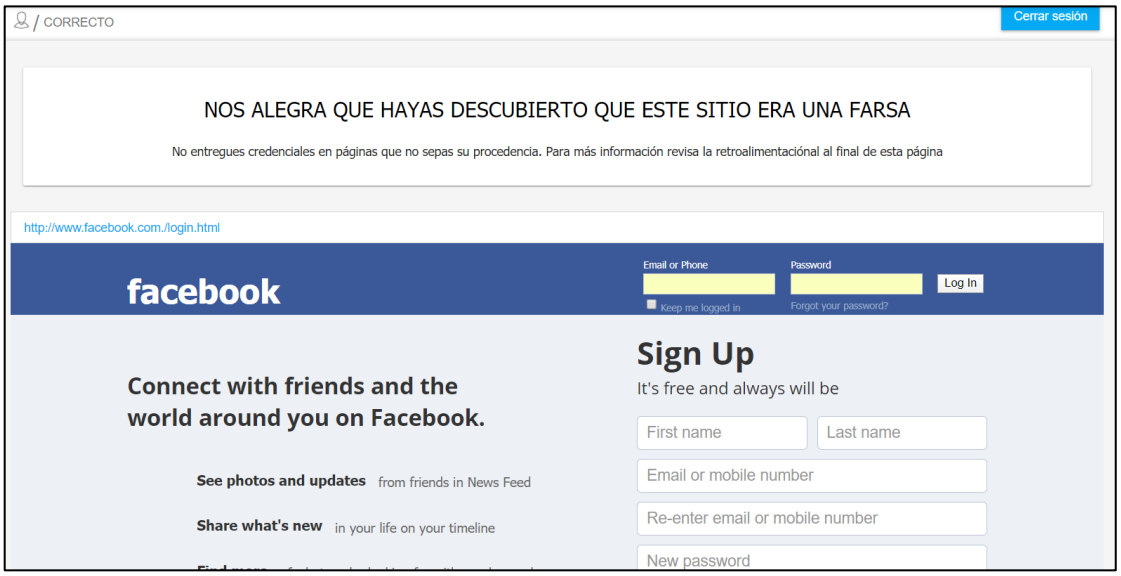


Fig. 33 Calificación pregunta 6 realizada en eclipse

Fig. 34 Retroalimentación pregunta 6 respondida en eclipse parte 1

Fig. 35 Retroalimentación pregunta 6 respondida en eclipse parte 2

c. Reunión retrospectiva

Tabla 39 Reunión retrospectiva sprint 4

RETROSPECTIVA		
Fecha: viernes, 10 de enero de 2020 **Asistentes a la reunión:** Daysi Imbaquingo (Scrum master), Franklin Vallejo (Equipo de desarrollo)		
¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
Se culminó el desarrollo en el tiempo establecido y se logró una comunicación exitosa entre los integrantes del grupo	El equipo de desarrollo tuvo que realizar un curso pagado sobre el uso de primefaces para front-end del simulador.	Regularizar a un solo color el front-end.

Fuente: Propia

Sprint 5

a. Reunión planificación

Fecha de la reunión: sábado, 11 de enero de 2019

Asistentes a la reunión: Scrum máster, Product Owner, Team Development

Fechas de inicio Sprint: lunes, 13 de enero de 2020

Fechas de finalización Sprint: viernes, 17 de enero de 2020

Objetivo de Sprint: Desarrollo de los módulos de simulación básica, intermedia y avanzada

- **Historias de Usuario involucradas en el Sprint 5**

Tabla 40 Historias de usuarios involucradas sprint 5

ID	HISTORIA DE USUARIO
HU10	Módulo de simulación avanzada
HU11	Subida del aplicativo al servidor local de la UTN

Fuente: Propia

- **Planificación de tareas**

Tabla 41 Planificación tareas sprint 6

PLANIFICACIÓN DE TAREAS SPRINT 5				
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**
H10	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación avanzada y su respectiva retroalimentación	5
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación avanzada y su respectiva retroalimentación	5
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación avanzada y su respectiva retroalimentación	5
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación avanzada y su respectiva retroalimentación	6
H11	Franklin Vallejo	Codificación	Subida del aplicativo a la nube	11
Reuniones	Scrum Team	Planificación	Planificación	4
	Scrum Team	Revisión	Revisión	2
	Scrum Team	Revisión	Retrospectiva	2
			TOTAL	**40**

Fuente: Propia

b. Reunión revisión

Tras haber finalizado las tareas que previamente se planificaron en el tiempo definido, se concluyó que efectivamente se cumplieron los requerimientos plateados en el product backlog.

Tabla 42 Reunión revisión sprint 5

PLANIFICACIÓN DE TAREAS SPRINT 3					
HISTORIA DE USUARIO	**DESARROLLADOR**	**FASE DESARROLLO**	**TAREA**	**TIEMPO ESTIMADO (HORAS)**	**TIEMPO REAL (HORAS)**
H10	Franklin Vallejo	Codificación	Codificación del primer escenario de simulación avanzada y su respectiva retroalimentación	5	5
	Franklin Vallejo	Codificación	Codificación del segundo escenario de simulación avanzada y su respectiva retroalimentación	5	5
	Franklin Vallejo	Codificación	Codificación del tercer escenario de simulación avanzada y su respectiva retroalimentación	5	6
	Franklin Vallejo	Codificación	Codificación del cuarto escenario de simulación avanzada y su respectiva retroalimentación	6	6
H11	Franklin Vallejo	Codificación	Subida del aplicativo a la nube	11	10
Reuniones	Scrum Team	Planificación	Planificación	4	4
	Scrum Team	Revisión	Revisión	2	3
	Scrum Team	Revisión	Retrospectiva	2	1
			TOTAL	**40**	**40**

Fuente: Propia

- **Imágenes del sistema**

Fig. 36 Codificación del primer escenario de simulación avanzada y su respectiva retroalimentación en eclipse

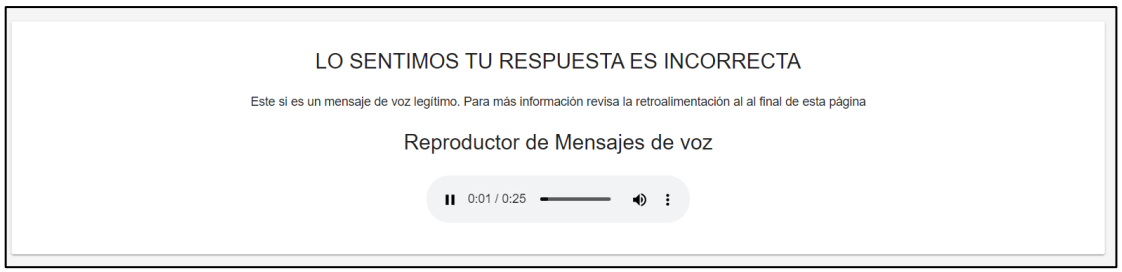


Fig. 37 Calificación pregunta 11 realizada en eclipse

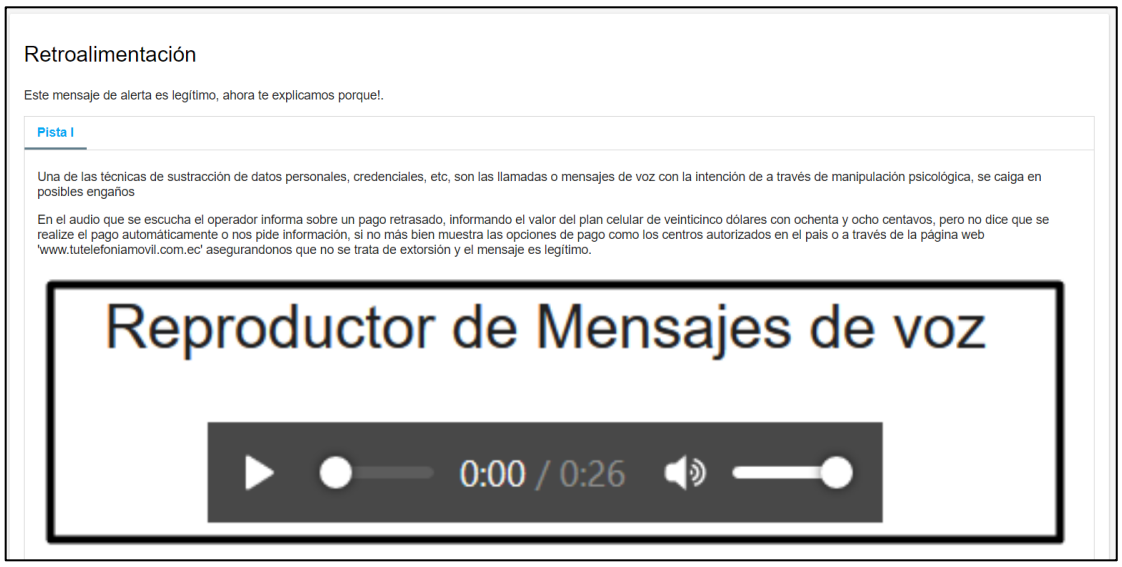


Fig. 38 Retroalimentación pregunta 11 respondida en eclipse

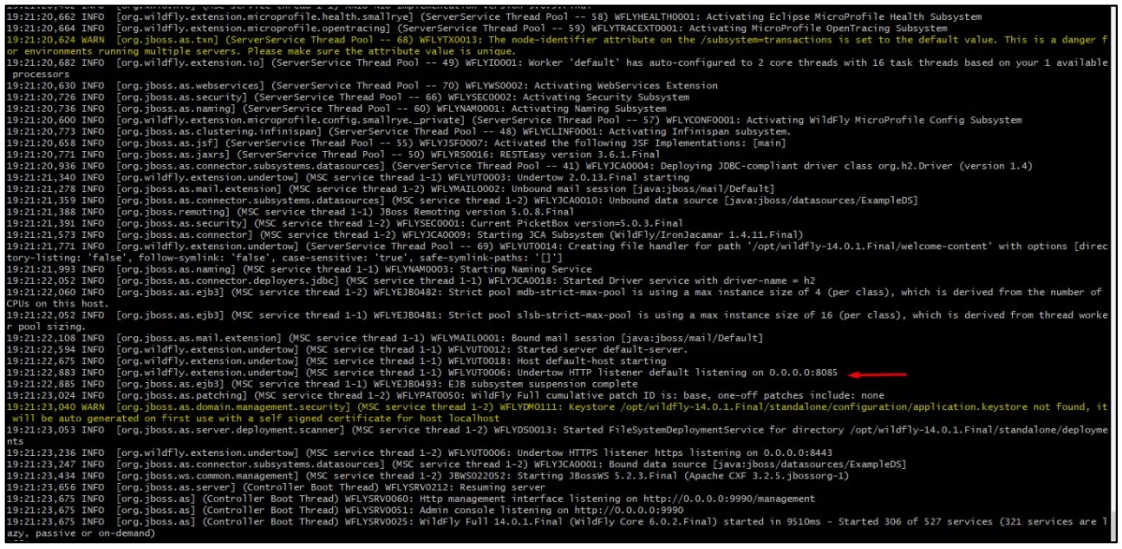


Fig. 39 Subida del simulador web al servidor local de la UTN

c. Reunión retrospectiva

Tabla 43 Reunión retrospectiva sprint 5

RETROSPECTIVA			
	Fecha: viernes, 17 de enero de 2020 **Asistentes a la reunión:** Daysi Imbaquingo (Scrum Máster), Franklin Vallejo (Equipo de desarrollo)		
	¿Qué salió bien en la iteración? (aciertos)	**¿Qué no salió bien en la iteración? (errores)**	**¿Qué se podría implementar en la siguiente iteración? (Recomendaciones)**
➢	Se culminó el desarrollo en el tiempo establecido y se logró una comunicación exitosa entre los integrantes del grupo	Ninguno	Nada

Fuente: Propia

CAPÍTULO III
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En el presente capítulo se llevó a cabo fases de procesamiento, clasificación y representación de los resultados sobre la investigación en indicadores gráficos, desarrollados sistemáticamente en base a métodos estadísticos, de forma entendible y comprensible.

3 Desarrollo

3.1 Obtención de datos

La obtención de datos se realizó a través de una encuesta compuesta de 13 preguntas, que se diseñó considerado la subcaracterística 9.4.2 denominada "Procedimiento de Inicio de Sesión Seguros", en base a la normativa ISO/IEC 27002, para valorar las puntuaciones que los usuarios del simulador web otorgaron a los diferentes componentes del inicio de sesión por roles (rol administrador y rol estudiante).

Una vez que se ejecutó el instrumento de investigación se obtuvo 138 resultados, mismos que fueron tratados y ejecutados mediante pruebas estadísticas empleando el lenguaje de programación R, mediante la herramienta de RStudio, lo que permitió verificar que no existan valores perdidos mediante la librería ***mise***[1], además permitió obtener las distancias para cada variable donde se detectó y eliminó 13 observaciones atípicas, por lo que los resultados con los que se trabajó fueron 125 encuestas.

Mode	FALSE	TRUE
logical	13	125

Fig. 40 Eliminación de observaciones atípicas en espacio de trabajo de Espacio imagen de Rstudio

3.2 Método estadístico

El Análisis Factorial Exploratorio (AFE) y el Análisis factorial Confirmatorio (AFC) son técnicas estadísticas paramétricas, con las cuales se verificó los supuestos de los datos, inicialmente para el supuesto de aditividad, se obtuvo la matriz de correlación para todas posibles combinaciones de preguntas, donde se observó que todas las preguntas superan el supuesto de aditividad, ya que ninguna está en el rango de 0,95 a 1 para considerarse no superada, permitiendo trabajar con todas las preguntas sin excluir ninguna.

[11] La librería Mise es útil para los inicios de los scripts R, para evitar problemas potenciales con el uso accidental de información de variables o funciones de evaluaciones de scripts anteriores.(Rstudio, 2016)

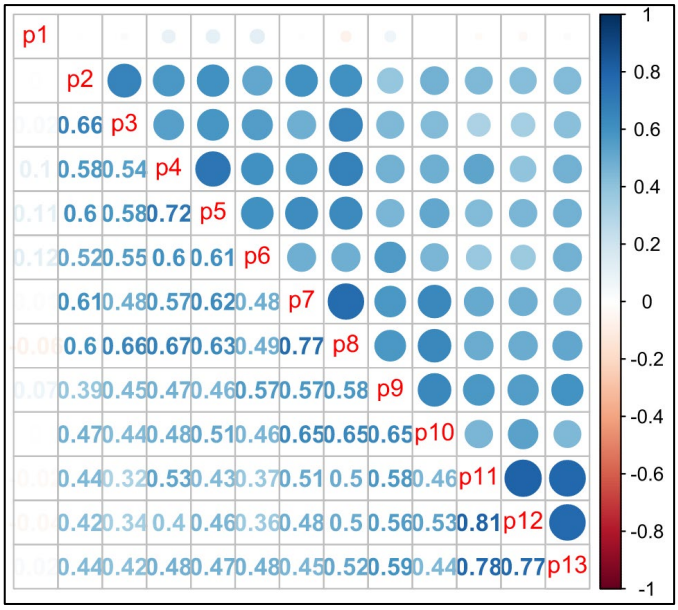


Fig. 41 Matriz de correlación histograma dispersión de las 125 encuestas – Espacio imagen de Rstudio

3.3 Verificación de supuestos de los datos.

Posteriormente se procedió a verificar los supuestos de linealidad y normalidad, para ello se ejecutó un análisis de falsa regresión basado en los resultados estandarizados de la matriz de correlación. Los resultados obtenidos se resumen a continuación.

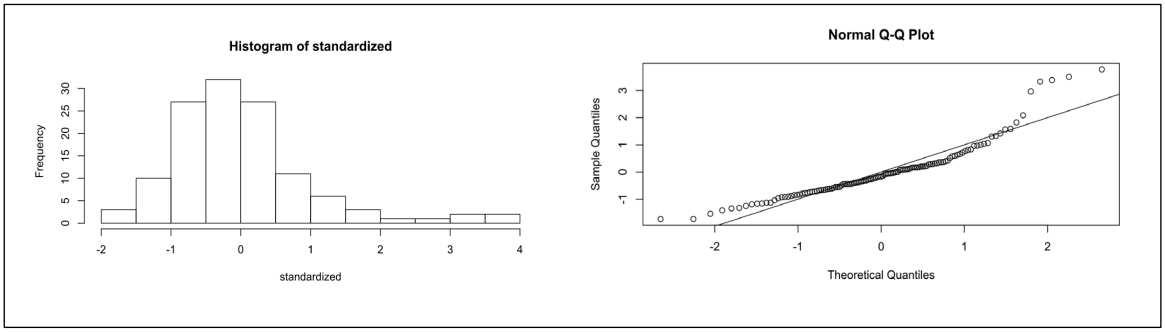


Fig. 42 Histograma y QQ Plot de los valores estandarizados obtenidos - Espacio imagen de Rstudio

El supuesto de normalidad permitió verificar la regresión hecha a partir de los cuantiles mediante la visualización del histograma, donde las frecuencias se distribuyeron con una tendencia normal entre **-2 a 2**. De la misma manera el **supuesto de linealidad** se verifica ya que los cuantiles cumplen con una tendencia lineal creciente en el intervalo de **-2 a 2**, **obteniendo resultados efectivos** para realizar posteriormente el AFE y AFC.

3.4 Análisis factorial Exploratorio

El AFE es un método utilizado para descubrir la estructura potencial de un grupo de variables. Principalmente se extrae y obtiene variables explícitas observables para variables factoriales no observables. (Coldman, 2019).

Para el AFE se tomó en cuenta 6 factores los cuales coinciden con los 13 ítems deseados para la estructura factorial.

```
Factor Analysis using method =  ml
Call: fa(r = noout, nfactors = 6, rotate = "oblimin", fm = "ml")
Standardized loadings (pattern matrix) based upon correlation matrix
      ML4   ML5   ML3   ML2   ML1   ML6    h2    u2 com
p1  -0.12  0.23  0.05 -0.02 -0.11 -0.07 0.037 0.963 2.4
p2   0.04  0.00 -0.01  0.99 -0.01 -0.04 0.995 0.005 1.0
p3  -0.05  0.11  0.09  0.54  0.20  0.28 0.756 0.244 2.0
p4  -0.03  0.89 -0.02  0.04  0.08 -0.18 0.927 0.073 1.1
p5   0.11  0.78  0.00  0.01  0.08  0.22 0.869 0.131 1.2
p6   0.05  0.72  0.18  0.06 -0.09  0.08 0.715 0.285 1.2
p7   0.04  0.10  0.22  0.18  0.47 -0.12 0.750 0.250 2.0
p8   0.04  0.03  0.02  0.02  0.93  0.01 0.995 0.005 1.0
p9   0.01  0.01  0.99  0.01 -0.02  0.03 0.995 0.005 1.0
p10  0.08  0.04  0.64 -0.01  0.20 -0.12 0.741 0.259 1.3
p11  0.89  0.06  0.01  0.05 -0.04 -0.16 0.879 0.121 1.1
p12  0.95 -0.03 -0.04  0.00  0.04  0.10 0.897 0.103 1.0
p13  0.81  0.01  0.10  0.00  0.04  0.03 0.822 0.178 1.0

                       ML4  ML5  ML3  ML2  ML1  ML6
SS loadings           2.62 2.37 1.88 1.63 1.64 0.24
Proportion Var        0.20 0.18 0.14 0.13 0.13 0.02
Cumulative Var        0.20 0.38 0.53 0.65 0.78 0.80
Proportion Explained  0.25 0.23 0.18 0.16 0.16 0.02
Cumulative Proportion 0.25 0.48 0.66 0.82 0.98 1.00
```

Fig. 43 Pruebas efectuadas para el diseño de la estructura factorial - Espacio imagen de Rstudio

Luego del AFE se evidenció que de la pregunta 1 a la 13 pasaron exitosamente la prueba de hipótesis considerándose suficiente.

```
 With factor correlations of
     ML4  ML5  ML3  ML2  ML1  ML6
ML4 1.00 0.48 0.64 0.50 0.50 0.06
ML5 0.48 1.00 0.59 0.66 0.67 0.03
ML3 0.64 0.59 1.00 0.47 0.65 0.06
ML2 0.50 0.66 0.47 1.00 0.64 0.05
ML1 0.50 0.67 0.65 0.64 1.00 0.09
ML6 0.06 0.03 0.06 0.05 0.09 1.00
Mean item complexity =  1.3
Test of the hypothesis that 6 factors are sufficient.
```

Fig. 44 Prueba de hipótesis para seis factores - Espacio imagen de Rstudio

3.5 Análisis factorial Confirmatorio

Finalmente, mediante el AFC se validó la estructura factorial, donde se **obtuvo** saturaciones por **encima de 0,5** para cada pregunta. De esta manera la estructura final y su estructura para el AFC se muestran en la figura 45.

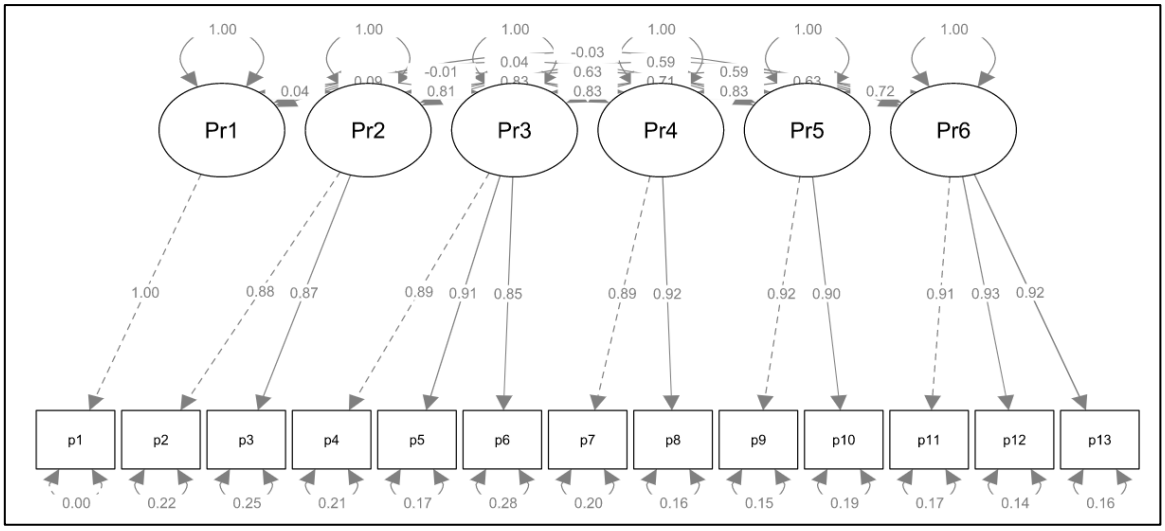


Fig. 45 Diagrama de la estructura factorial resultante para el AFC - Espacio imagen de Rstudio

Finalmente las saturaciones **superan en todos los casos a 0,5** y ningún factor está correlacionado, por otra parte el índice de Tucker y Lewin y el NNFI (Non Normed Fit Index) obtenidos son de **0,952** el cual entra en la categoría de **excelente > 0,95**, además el CFI (Comparative Fit Index), **fue de 0,969 ubicándose en la categoría de excelente** y los índices RMSEA.PVALUE (Root Mean Square Error of Approximation) y SRMR (Standardized Root Mean Residual) alcanzaron valores de **0,019 y 0,026** lo cual **demuestra la validez** al aplicar el presente método estadístico.

npar	fmin	chisq	df	pvalue
40.000	0.384	96.060	51.000	0.000
baseline.chisq	baseline.df	baseline.pvalue	cfi	tli
1508.523	78.000	0.000	0.969	0.952
nnfi	rfi	nfi	pnfi	ifi
0.952	0.903	0.936	0.612	0.969
rni	logl	unrestricted.logl	aic	bic
0.969	-604.456	-556.426	1288.912	1402.045
ntotal	bic2	rmsea	rmsea.ci.lower	rmsea.ci.upper
125.000	1275.557	0.084	0.058	0.110
rmsea.pvalue	rmr	rmr_nomean	srmr	srmr_bentler
0.019	0.008	0.008	0.026	0.026
srmr_bentler_nomean	crmr	crmr_nomean	srmr_mplus	srmr_mplus_nomean
0.026	0.028	0.028	0.026	0.026
cn_05	cn_01	gfi	agfi	pgfi
90.357	101.700	0.895	0.813	0.502
mfi	ecvi			
0.835	1.408			

Fig. 46 Índices de bondad de ajuste en - Espacio imagen de Rstudio

CONCLUSIONES

- El uso de los instrumentos tecnológicos como el IDE de programación de Java Enterprise Edition (Eclipse), permitió facilitar el desarrollo del software, logrando eficiencia en el desarrollo e integración de módulos y librerías, entregando un producto de calidad empresarial.
- La Aplicación de Scrum como marco de trabajo en el proceso de desarrollo de software, permitió llevar a cabo exitosamente cada fase del proyecto, engranando desde el levantamiento de requisitos, proceso de prototipado, desarrollo, hasta la entrega del producto final al cliente, generando una aplicación web tipo simulador, validado para el cumplimiento de los objetivos.
- La integración de la norma ISO/IEC 27002, permitió asegurar el simulador web frente a ataques cibernéticos y mediante diferentes pruebas de intrusión se calificó al sistema, obteniendo una puntuación de **0,952** la cual está en la categoría de **excelente** aplicando el índice de Tucker y Lewin, cumpliendo así la aplicación de la normativa.

RECOMENDACIONES

- Se recomienda actualizar de forma permanente los escenarios del simulador, en relación con la aparición de nuevos ataques informáticos en el área de ingeniería social.
- Se recomienda seguir usando las herramientas de JAVA EE, Eclipse y PostgreSQL, para la integración de nuevos escenarios y funcionalidades al simulador web.
- Se recomienda publicar el simulador a una plataforma institucional, y que sea libre de acceso para todos los usuarios dentro de la comunidad universitaria.
- Se recomienda aplicar instrumentos tipo encuestas, para recolectar datos de retroalimentación de los usuarios, los cuales ayudan a validar el cumplimento de los objetivos de la investigación.
- Se recomienda aplicar técnicas estadísticas que permitan validar la integridad y efectividad de los resultados obtenidos, al realizar un trabajo de investigación.
- Se recomienda un plan de mantenimiento y monitoreo constante al simulador web para mejorar sus funcionabilidades.
- Se recomienda aplicar la metodología Scrum como marco de trabajo para el desarrollo de aplicaciones web, logrando obtener eficacia y eficiencia en los proyectos.
- Se recomienda aplacar el estándar ISO/IEC 27002 para asegurar aplicaciones web, centro de datos, acceso a información frente ataques de ciberdelincuentes.

REFERENCIAS BIBLIOGRAFÍCAS

Astudillo, K. (2016). *Hacking ético 101 ¿Cómo hackear profesionalmente en 21 días o menos?*

Baca, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria.

Barbero, C., Ramos, A., & Marugán, D. (2015). *HACKING CON INGENIERÍA SOCIAL. TÉCNICAS PARA HACKEAR HUMANOS. MUNDO HACKER* (2015.ª ed.). RA-MA EDITORIAL.

PROYECTO DE CREACIÓN DEL CLUB ETHICAL HACKING, 33 (2017). https://utneduec-my.sharepoint.com/personal/fwvallejor_utn_edu_ec/Documents/UTN/CLUB%20ETHICAL%20HACKING%20UTN/CREACION%20CEH%20UTN/CEH%20UTN%20FINAL%20PREMIUM/Proyecto%20de%20Creaci%c3%b3n%20del%20Club%20Ethical%20Hacking%20UTN%20FINAL.pdf

Coldman. (2019, enero 19). *Data Modeling-Factor Analysis*. Data Modeling-Factor Analysis. https://programmer.group/data-modeling-factor-analysis.html

Comer, D. E. (2015). *Redes de computadoras e Internet* (Sexta). Litográfica Ingramex, S.A.

Consejo Estatal de Estudiantes de Medicina. (2019). *Planificación y elaboración de proyectos*. *1*(1), 17.

Contreras Espinosa, R. (2014). *Web 2.0+ educación: Colaboración y recursos abiertos*.

Domínguez, C. J. (2014). *Aspectos interesantes sobre la Ingeniería Social*. *1*(1), 7.

Eset Latinoamérica. (2014, septiembre 1). *Falsa alerta de terremoto en Ecuador propaga malware*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2010/09/01/falsa-alerta-de-terremoto-en-ecuador-propaga-malware/

Eset Latinoamérica. (2019, enero 24). *Google publicó test de phishing para que usuarios aprendan a reconocer correos fraudulentos*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2019/01/24/google-publico-test-phishing-reconocer-correos-fraudulentos/

Fonseca, J. C. (2017). *Diseño e implementación de sistema informático para entrenamiento en test de intrusión* [Universidad Internacional de La Rioja]. https://reunir.unir.net/bitstream/handle/123456789/5870/FONSECA%20ROMERO%2C%20JULIAN%20CAMILO.pdf?sequence=1&isAllowed=y

Gophish. (2018). *Gophish—Open Source Phishing Framework*. https://getgophish.com/

HADNAGY, C. (2017). *INGENIERIA SOCIAL: EL ARTE DEL HACKING PERSONAL*. ANAYA MULTIMEDIA.

ISO 27000:2013. (2019). *ISO27000.es—El portal de ISO 27001 en español. Gestión de Seguridad de la Información*. http://www.iso27000.es/

Jigsaw, G. (2019). *Take Jigsaw's Phishing Quiz*. https://g.co/phishingquiz

Lucy Security. (2019). *Homepage | Lucy Security | Awareness Training*. Lucy Security. https://lucysecurity.com/

Mañeru, G. Z. (2015). *FUNDAMENTOS PEDAGÓGICOS DE LA SIMULACIÓN EDUCATIVA EN EL ÁREA SANITARIA: COMPETENCIAS DOCENTES* (2015.ª ed.). Ediciones Eunate.

Martos, A. R. (2015). *Internet* (2015.ª ed.). Anaya Multimedia.

Mitnick, K. D. (2017). *The Art of Invisibility*.

PhET. (2019). *PhET: Simulaciones gratuitas en línea de física, química, biología, ciencias de la tierra y matemáticas.* https://phet.colorado.edu/es/

Phishing Frenzy. (2018). *Home—Phishing Frenzy—Manage Email Phishing Campaigns—Penetration Testing*. https://www.phishingfrenzy.com/

proyectosagiles. (2018). Qué es SCRUM. *Proyectos Ágiles*. https://proyectosagiles.org/que-es-scrum/

Rstudio. (2016, junio 30). *Mise function | R Documentation*. Package 'mise'. https://www.rdocumentation.org/packages/mise/versions/0.1.0/topics/mise

Schwaber, K., & Sutherland, J. (2016). *La Guía de Scrum*.

Suárez, D., & Fontalvo, A. Á. (2017). Una forma de interpretar la seguridad informática. *Journal of Engineering and Technology*, *4*(2).

http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015

trustedsec. (2019). The Social-Engineer Toolkit (SET). *TrustedSec*. https://www.trustedsec.com/social-engineer-toolkit-set/

Uc3m. (2014). *Universidad Carlos III de Madrid—La UC3M participa en un nuevo simulador de entrenamiento en ciberseguridad*. http://portal.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/simu_ciberseguridad

ANEXOS

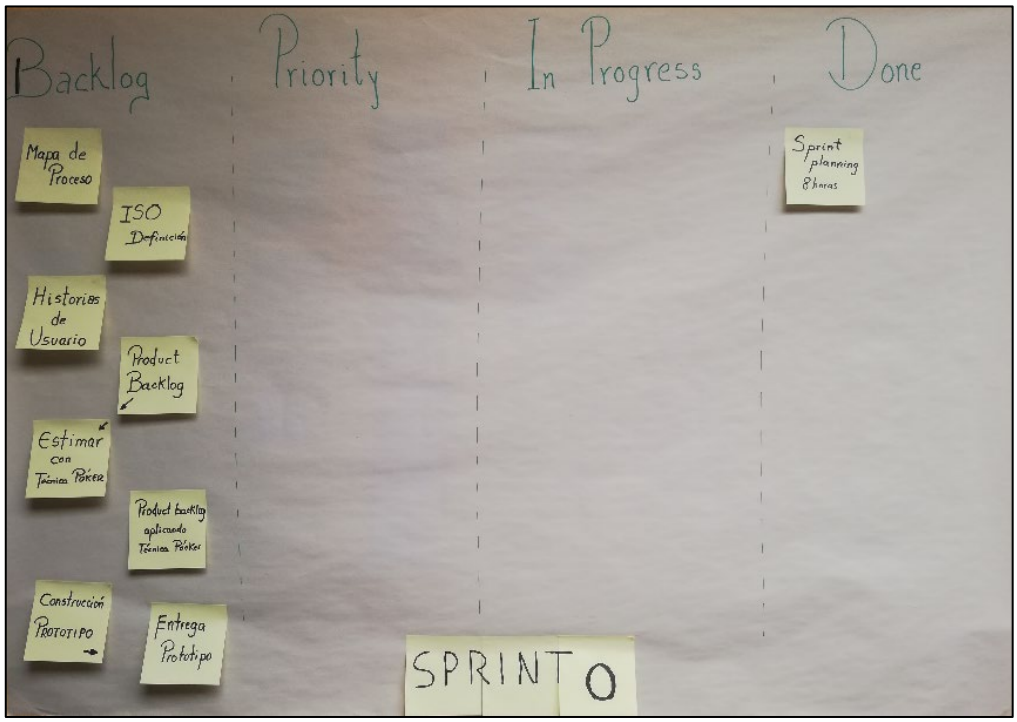


Fig. 47 Evidencia tablero cambam Sprint 0

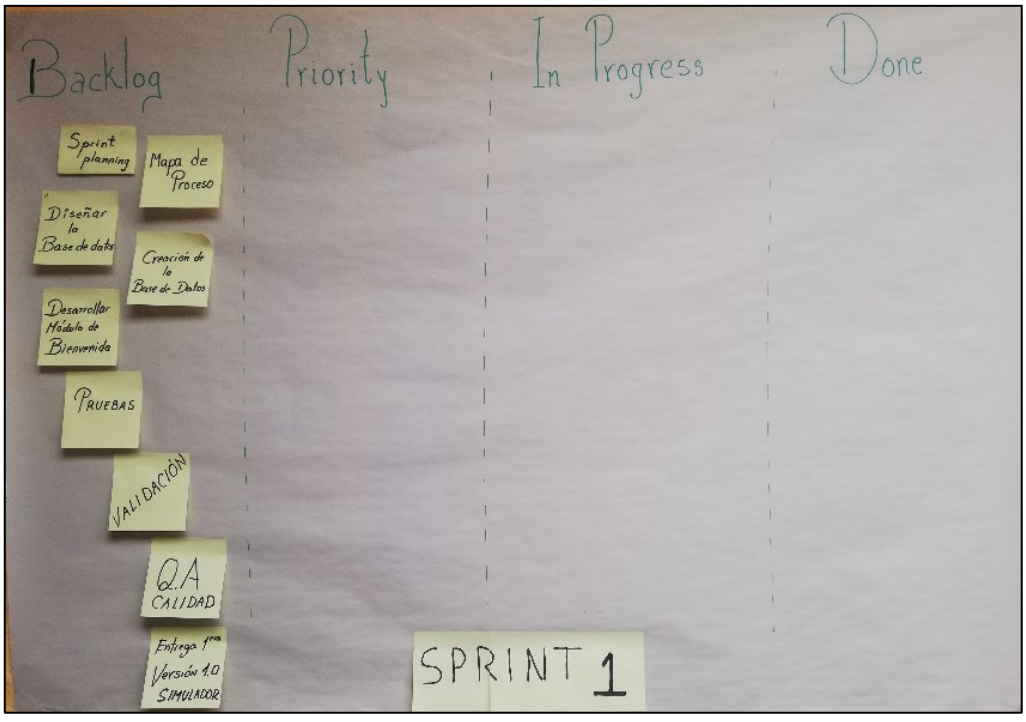


Fig. 48 Evidencia tablero cambam Sprint 1

Encuesta

SEmulator

Simulador enfocado a Ingeniería Social

El siguiente instrumento tiene como fin recabar datos sobre la aplicación de la característica 9.4.2 referente al procedimiento de inicio de sesión seguro de la ISO/IEC 27002 en el simulador web enfocado a Ingeniería Social (SEmulator).

Instrucciones:
*Siga en orden los pasos que se muestran en los diferentes protocolos.
*Observe detenidamente el comportamiento del sistema al seguir los pasos establecidos en los diferentes protocolos.
*Al final marque la casilla de acuerdo con su opinión.

Sección 1 ...

PROTOCOLO #1

"Desplegar una notificación general de advertencia que el ordenador debería ser accedido por usuarios autorizados".

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: Lea detenidamente el mensaje que se muestra en la página.

Instrucciones: Marque la casilla de acuerdo con su opinión.

1. Pregunta *

	Nunca	Casi nunca	Regularmente	Casi siempre	Siempre
PROTOCOLO #1 - P.1.1: Al acceder al sistema se puede visualizar una notificación que advierte que el ordenador debe ser accedido solamente por usuarios autorizados	○	○	○	○	○

Sección 2

PROTOCOLO #2

"No proveer mensajes de ayuda durante el proceso de inicio de sesión que podría cooperar a un usuario no autorizado".

PROTOCOLO #2.1
Acceso como estudiante.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Estudiante".
Instrucción #4: Sin llenar los campos del formulario que se le presenta, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #5: Complete el formulario con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #6: Complete solamente el primero de los campos correspondiente a la identificación del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #7: Complete solamente el segundo de los campos correspondiente a la contraseña del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.

PROTOCOLO #2.2
Acceso como administrador

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Administrador".
Instrucción #4: Sin llenar los campos del formulario que se le presenta, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #5: Complete el formulario con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #6: Complete solamente el primero de los campos correspondiente a la identificación del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #7: Complete solamente el segundo de los campos correspondiente a la contraseña del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.

Instrucciones: Marque la casilla de acuerdo con su opinión.

2. Pregunta *

	Nunca	Casi nunca	Regularmente	Casi siempre	Siempre
PROTOCOLO #2 - P.2.1: Los mensajes de alerta o ayuda, no proveen información a usuarios no autorizados que le ayudar a cooperar un acceso no autorizado.	○	○	○	○	○
PROTOCOLO #2 - P.2.2: Considera usted que el acceso al sistema es seguro, ya que no entrega información alguna en caso de ser un usuario no autorizado.	○	○	○	○	○

Sección 3

PROTOCOLO #3

"Validar la información del inicio de sesión únicamente al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar que parte de los datos es correcta o incorrecta".

PROTOCOLO #3.1
Acceso como estudiante.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Estudiante".
Instrucción #4: Sin llenar los campos del formulario que se le presenta, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #5: Complete el formulario con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #6: Complete solamente el primero de los campos correspondiente a la identificación del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #7: Complete solamente el segundo de los campos correspondiente a la contraseña del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #8: Complete el formulario con la siguiente información sin comillas (Usuario: '1003454647'; Contraseña: ' 123*H ')
Instrucción #9: De clic en el botón iniciar sesión y observe el comportamiento del sistema.
Instrucción #10: De clic en el botón "Cerrar sesión" ubicado en la parte superior derecha.

PROTOCOLO #3.2
Acceso como administrador.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Administrador".
Instrucción #4: Sin llenar los campos del formulario que se le presenta, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #5: Complete el formulario con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #6: Complete solamente el primero de los campos correspondiente a la identificación del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #7: Complete solamente el segundo de los campos correspondiente a la contraseña del usuario estudiante con datos ficticios, de clic sobre el botón "Iniciar Sesión". A continuación, observe los mensajes emergentes y su alerta.
Instrucción #8: Complete el formulario con la siguiente información sin comillas (Usuario: '1001001001'; Contraseña: '123')
Instrucción #9: De clic en el botón iniciar sesión y observe el comportamiento del sistema.
Instrucción #10: De clic en el botón "Cerrar sesión" ubicado en la parte superior derecha.

Instrucciones: Marque la casilla de acuerdo con su opinión.

3. Pregunta *

	Nunca	Casi nunca	Regularmente	Casi siempre	Siempre
PROTOCOLO #3 - P.3.1: Al iniciar sesión únicamente con datos válidos el sistema funciona perfectamente y sin errores.	○	○	○	○	○
PROTOCOLO #3 - P.3.2: Al iniciar sesión con datos inválidos el sistema muestra alertas de error, pero no proporciona información referente a cuál de los campos del formulario está incorrecto.	○	○	○	○	○
PROTOCOLO #3 - P.3.3: El sistema valida la información siempre y cuando ésta sea correcta.	○	○	○	○	○

Sección 4

PROTOCOLO #4

"No desplegar la contraseña que se ingresa".

PROTOCOLO #4.1 Acceso como estudiante.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Estudiante".
Instrucción #4: Complete el formulario con la siguiente información sin comillas (Usuario: '1003454647'; Contraseña: '123*H')
Instrucción #5: Sin dar clic en el botón iniciar sesión, observe el comportamiento del sistema.

PROTOCOLO #4.2 Acceso como administrador.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Administrador".
Instrucción #4: Complete el formulario con la siguiente información sin comillas (Usuario: '1001001001'; Contraseña: '123')
Instrucción #5: Sin dar clic en el botón iniciar sesión, observe el comportamiento del sistema.

Instrucciones: Marque la casilla de acuerdo con su opinión.

4. Pregunta *

	Nunca	Casi nunca	Regularmente	Casi siempre	Siempre
PROTOCOLO #4 - P.4.1: Cuando se ingresa la contraseña en el formulario de inicio de sesión, esta es ilegible a los usuarios.	○	○	○	○	○
PROTOCOLO #4 - P.4.2: El sistema oculta su contraseña mientras ésta es digitada	○	○	○	○	○

Sección 5

PROTOCOLO #5

"No transmitir contraseñas en texto claro sobre la red".

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button

El sistema al cual se accede con la URL de la instrucción #1 cuenta con un sistema de cifrado de contraseña, que es un sistema de seguridad informática, el cual permite a la contraseña ingresada, convertirse en una cadena de texto diferente a la que ingresó y así viajar en la red, asegurando que si algún usuario no autorizado desea interceptar la contraseña fracasará ya que, si logra obtener el dato 'contraseña', éste será el valor convertido, más no la contraseña que el usuario digitó inicialmente.

Instrucciones: Marque la casilla de acuerdo con su opinión.

5. Pregunta *

	Nunca	Casi nunca	Regularmente	Casi siempre	Siempre
PROTOCOLO #5 - P.5.1: Aplicando cifrado de contraseña, considera usted que, la contraseña digitada está segura mientras viaja por la red y es imposible capturarla en texto claro.	○	○	○	○	○
PROTOCOLO #5 - P.5.2: Como usuario, siente seguridad al acceder al sistema, confiando que sus datos de inicio de sesión no pueden ser interceptados por un usuario no autorizado.	○	○	○	○	○

Sección 6

PROTOCOLO #6

"Terminar sesiones inactivas después de un periodo de inactividad".

La finalización de la sesión es una parte importante del ciclo de vida de la sesión. La reducción al mínimo de la vida útil de los tokens de sesión disminuye la probabilidad de un ataque de secuestro de sesión exitoso. Esto puede verse como un control contra la prevención de otros ataques como Cross Site Scripting y Cross Site Request Forgery. Se sabe que tales ataques dependen de que un usuario tenga una sesión autenticada presente. No tener una finalización de sesión segura solo aumenta la superficie de ataque para cualquiera de estos ataques.

PROTOCOLO #6.1 Acceso como estudiante.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Estudiante".
Instrucción #4: Complete el formulario con la siguiente información sin comillas (Usuario: '1003454647'; Contraseña: '123*H')
Instrucción #5: De clic en el botón Iniciar sesión.
Instrucción #6: Haga uso del sistema y observe el comportamiento de este.

PROTOCOLO #6.1 Acceso como administrador.

Instrucción #1: Acceda a la siguiente URL http://localhost:8080/simuladorWeb/advertenciaAccesoSistema.xhtml#no-back-button
Instrucción #2: De clic sobre el botón "Soy Usuario Autorizado".
Instrucción #3: De clic sobre el botón "Ingresar como Administrador".
Instrucción #4: Complete el formulario con la siguiente información sin comillas (Usuario: '1001001001'; Contraseña: '123')
Instrucción #5: De clic en el botón Iniciar sesión.
Instrucción #6: Haga uso del sistema y observe el comportamiento de este.

Instrucciones: Marque la casilla de acuerdo con su opinión.

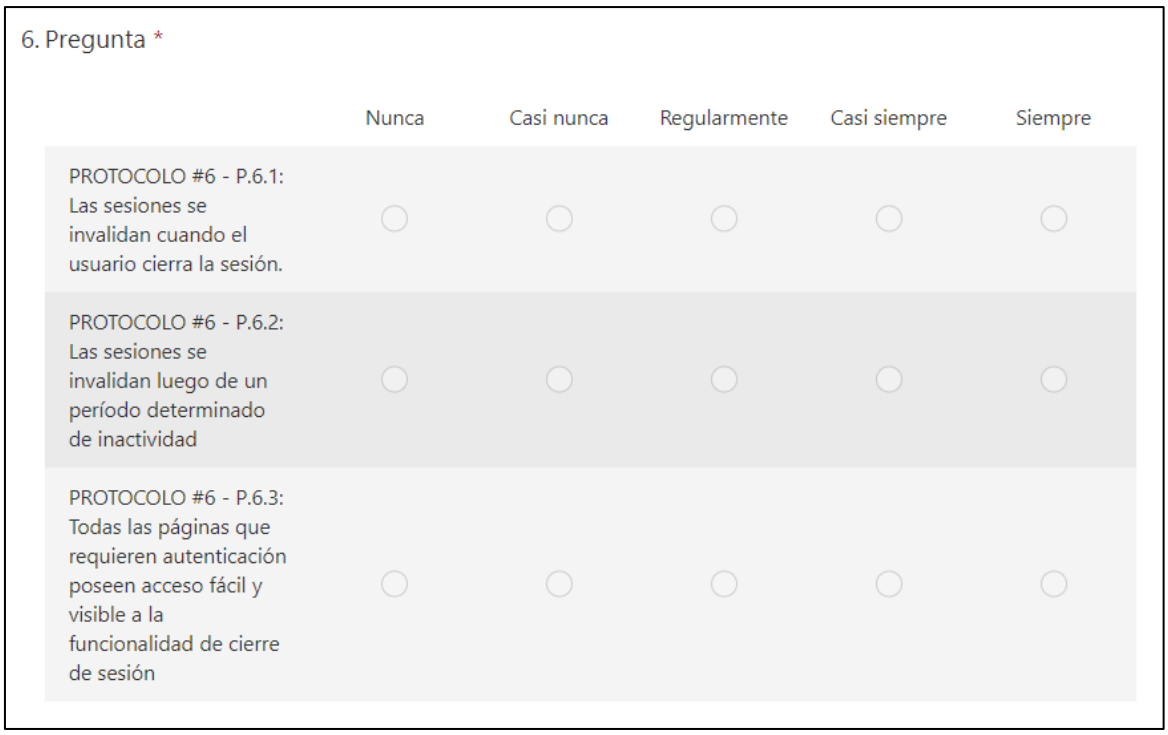


Fig. 49 Encuesta de la presente investigación