Desarrollo de un Juego Formativo para Aportar a la Concienciación en Ciberseguridad al Personal de la Escuela Militar de Aviación (Emavi) "Marco Fidel Suárez" de la Fuerza Aérea Colombiana en la ciudad de Cali[1]

Desenvolvimento de um jogo de treinamento para contribuir com a conscientização da segurança cibernética do pessoal da Escola de Aviação Militar "Marco Fidel Suárez" da Força Aérea Colombiana na cidade de Cali.[2]

Development of a Training Game to Provide Awareness in Cybersecurity to the Staff of the Aviation Military School "Marco Fidel Suárez" of the Colombian Air Force in the city of Cali[3]

Jair Abadía Correa[a], Ludwing Ortiz Páez[b] y Nicolás Peña Castiblanco[c]
Escuela Militar de Aviación Marco Fidel Suárez. Cali, Colombia

CIENCIA Y PODER AÉREO
ISSN 1909-7050 / E- ISSN 2389-9468 / Volumen 12/ Enero-Diciembre de 2017/ Colombia/ Pp. 264-275
Recibido: 23/08/2017
Aprobado: 15/09/2017
Doi: http://dx.doi.org/10.18667/cienciaypoderaereo.577

Para citar este artículo:
Correa, J. A., Ortíz, P. & Peña, N. (2017). Desarrollo de un Juego Formativo para Aportar a la Concienciación en Ciberseguridad al Personal de la Escuela Militar de Aviación (Emavi) "Marco Fidel Suárez" de la Fuerza Aérea Colombiana en la ciudad de Cali. *Ciencia y Poder Aéreo, 12*, 264-275. Doi: http://dx.doi.org/10.18667/cienciaypoderaereo.577

---

[1] Artículo científico producto de una investigación realizada para optar el título de Ingeniero Informático en la Escuela Militar de Aviación Marco Fidel Suárez.

[2] Artigo científico produto de uma investigação realizada para escolher o título de Engenheiro de Informática na Escola Militar de Aviação Marco Fidel Suárez.

[3] Scientific paper product of an investigation conducted to qualify the Computer Engineering degree at the Military Aviation School Marco Fidel Suárez.

[a] Ingeniero Electrónico y Telecomunicaciones. MSc. Gestión en Informática y Telecomunicaciones. Fuerza Aérea Colombiana - Escuela Militar de Aviación "Marco Fidel Suárez", Programa de Ingeniería Informática, Cra 8 No 58-67. Cali, Colombia. Correo electrónico: jabadia@emavirtual.edu.co

[b] Ingeniero Informático. Fuerza Aérea Colombiana - Escuela Militar de Aviación "Marco Fidel Suárez", Programa de Ingeniería Informática, Cra 8 No 58-67. Cali, Colombia. Correo electrónico: jlortiz@emavirtual.edu.co

[b] Ingeniero Informático. Fuerza Aérea Colombiana - Escuela Militar de Aviación "Marco Fidel Suárez", Programa de Ingeniería Informática, Cra 8 No 58-67. Cali, Colombia. Correo electrónico: npena@emavirtual.edu.co

Resumen: en este artículo se presenta el resultado de un trabajo de grado de Ingeniería Informática de la Escuela Militar de Aviación (Emavi). Este trabajo tiene tres finalidades: la primera, el desarrollo de un programa aplicando mejores prácticas por estudiantes de último grado de Ingeniera Informática; la segunda, usar soluciones TIC para la enseñanza en ciberseguridad o seguridad cibernética; tercera, aplicar una estrategia de capacitación motivadora en la temática de ciberseguridad (gamificación): juego formativo (*serious game*) como programa desarrollado para lograr sensibilizar al personal de Escuela Militar de Aviación (EMAVI) Marco Fidel Suárez - Fuerza Aérea Colombiana en la ciudad de Cali.
Para elaborar el juego formativo se usaron diferentes lenguajes de programación web (HTML5, JavaScript, css y php), y se le integró una base de datos en mysql para que el juego fuese interactivo. El juego formativo fue diseñado para educar a diferentes usuarios. Se divide en varias interfaces: la primera, la entrada al juego, en la cual el sistema pide un usuario y una contraseña; la segunda, en la cual se explica la seguridad de la información, con lo cual se logra que el usuario construya conocimiento del objeto virtual de aprendizaje (Ova). La tercera interfaz es del juego tipo *Quien quiere ser millonario*, desde el cual se evaluará lo aprendido mediante unas preguntas aleatorias que arrojarán una calificación. La cuarta y final interfaz muestra los puntajes obtenidos.
En el corto plazo, el grado de conocimiento de ciberseguridad del personal de Emavi será evaluado para saber si es posible aplicar un plan piloto de mediano plazo, en el cual se implemente dicha estrategia en CACOM 7, teniendo en cuenta los resultados arrojados en la primera fase de interacción. El aplicativo se cargó en la plataforma virtual de la institución, con lo cual se logró que el 60 % del personal lo usara y conociera tanto sus avances en conocimientos en ciberseguridad como consejos para minimizar los riesgos en seguridad de la información al usar tecnología.

Palabras clave: juego formativo, ciberseguridad, seguridad cibernética, gamificación, ISO27000.

Resumo: Este artigo apresenta o resultado de um diploma de engenharia informática da Escola Militar de Aviação. Este trabalho tem três propósitos: primeiro, o desenvolvimento de um programa de aplicação das melhores práticas por estudantes do último grau de Ciência da Computação; o segundo, usar as soluções de TIC para o ensino na segurança cibernética ou na cibersegurança; Em terceiro lugar, aplique uma estratégia de motivação de treinamento no tema da segurança cibernética (gamification): jogo de treinamento (jogo sério) como um programa desenvolvido para conscientizar o pessoal da Escola Militar de Aviação, Marco Fidel Suarez - Força Aérea Colombiana na cidade de Cali.
Para desenvolver o jogo de treinamento, utilizaram-se diferentes linguagens de programação web (HTML5, JavaScript, css e php), e um banco de dados mysql foi integrado para tornar o jogo interativo. O jogo de treinamento foi projetado para educar diferentes usuários. É dividido em várias interfaces: a primeira, a entrada ao jogo, no qual o sistema solicita um usuário e uma senha; o segundo, no qual a segurança da informação é explicada, com a qual o usuário é capaz de construir conhecimento do objeto de aprendizagem virtual (Ova). A terceira interface é do tipo jogo Quem quer ser um milionário, do qual a aprendizagem será avaliada por meio de algumas questões aleatórias que produzirão uma nota. A quarta e última interface mostra os escores obtidos.
A curto prazo, o grau de conhecimento da segurança cibernética do pessoal da Escola de Aviação Militar será avaliado para saber se é possível aplicar um plano piloto de médio prazo, no qual a referida estratégia é implementada no CACOM 7, levando em consideração os resultados jogado na primeira fase de interação.
O aplicativo foi carregado na plataforma virtual da instituição, o que permitiu que 60% da equipe usasse e conhecesse seus avanços no conhecimento da segurança cibernética e dicas para minimizar os riscos na segurança da informação ao usar a tecnologia.

Palavras-chave: Jogo de treinamento, Cibersegurança, Segurança cibernética, Gamificação, ISO27000.

Abstract: This article presents the results of a final research work from the Systems Engineering program at Aviation Military School "Marco Fidel Suárez. This work aims at three objectives: first, to develop a program by applying better practices by last year students at the program; second, to use ICT for teaching cybersecurity; third, applying a motivational teaching strategy related to cybersecurity (gamification): a serious game as a program developed for sensitizing the staff from Escuela Militar de Aviación Marco Fidel Suárez – Fuerza Aérea Colombiana in Cali (Colombia).
In order to develop the game, different web programming languages were used (HTML5, JavaScript, CSS, and PHP), to which a mysql database was integrated to make the game interactive.
The game was designed to educate different users. It is divided into several interfaces: first, the game presentation, in which the system requests a username and a password; second, an interface in which information security is explained, which helps the user build knowledge from the learning virtual object. The third interface is a game in a Who wants to be a millionaire format, which will evaluate what was learned by using random questions that will display a grade when answered. The final interface shows the user's score.
In the short term, the degree of knowledge in cybersecurity of Emavi's staff will be evaluated to know if it is possible to perform a medium term pilot plan to apply such an strategy to CACOM 7, taking into account the results displayed in the first stage of interaction.
The application was uploaded to the institution's virtual platform, which helped 60 % of the staff use it and know both their advances in cybersecurity knowledge and tips to minimize risks in information security when using technology.

Key Words: Serious Game, Cybersecurity, Gamification, ISO27000

Introducción

Este artículo integra seguridad cibernética con soluciones de TIC para la enseñanza a través de la aplicación de una estrategia de educación como gamificación, juego formativo y el desarrollo de software. Con este juego se logra concienciar al personal de la Emavi en el tema de ciberseguridad, con lo cual se busca minimizar los riesgos para la seguridad de la información cuando se usa conexión a Internet, tales como robo de información, robos de claves de tarjetas bancarias, bullying, y secuestro de información. Si los ataques se dan, es necesario que los usuarios conozcan los planes de recuperación de desastres y resiliencia.

El propósito de la concienciación a los empleados es aconsejar sobre seguridad de la información a través de la divulgación de las mejores prácticas en materia de seguridad (ISO 27000) para que adopten pautas de comportamiento seguro en los diversos contextos en los que desempeñan su actividad profesional, extendiéndolas a su ámbito personal. Al común de las personas le interesa usar la tecnología para comunicarse, pero desconoce de los riesgos y considera que éste es un tema muy complejo; por ello se tiene la necesidad de usar estrategias que motiven a estudiar sobre la ciberseguridad. En este proyecto se desarrolló un juego que se implementó en la plataforma virtual de la institución.

Para estar preparados y mitigar los ataques, las mejores estrategias preventivas son la educación y la conciencia de seguridad cibernética. Por ello, instituciones como el Instituto Nacional de Ciberseguridad de España desarrollo un kit de concienciación con el objetivo de facilitar a los empresarios y directores la tarea de fomentar buenos hábitos de seguridad entre sus empleados y colaboradores. (Cisco Systems, 2016)

En la figura 1 se presenta el resultado de una encuesta del Centro de Investigaciones Pew (Accounting Information Systems). En general, los entrevistados respondieron correctamente a menos de la mitad de las preguntas en una prueba de conocimiento sobre temas y conceptos de seguridad cibernética.

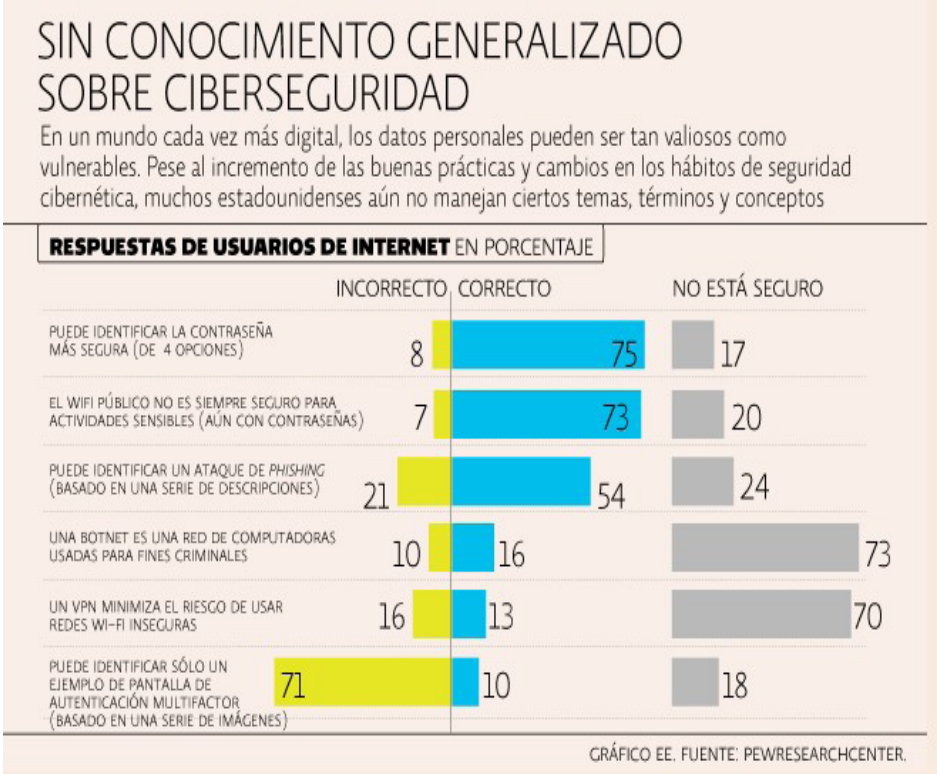

Figura 1. Resultados de prueba de conocimiento sobre temas y conceptos de seguridad cibernética realizada por el centro de investigaciones Pew en diciembre del 2016.

Fuente: tomado de http://eleconomista.com.mx/tecnociencia/2017/03/27/que-tanto-sabes-ciberseguridad

De acuerdo a los estudios reportados en CONPES, el 42 % de las organizaciones calificó a la seguridad informática como su principal prioridad, teniendo en cuenta que el 75 % de ellas sufrió algún tipo de quiebre en su seguridad durante los 12 meses anteriores a la realización del estudio (Alonso, 2017). Si bien lo anterior muestra un aumento de fraude electrónico, desafortunadamente no existe una conciencia situacional. Las personas no están exentas de caer en dicho crimen, por lo cual es importante tener conocimientos previos de la situación. Todos los integrantes de la organización deben ser conscientes de las amenazas a las que están expuestos cuando ingresan a internet, pues éste es un escenario de múltiple interacción, lo cual crea riesgos informáticos. La ingeniería, entonces, genera acciones que permitan relacionar el ciberespacio y personas, con lo cual hace que los espacios sean más seguros. Daniela Álvarez de Lugo (Braude, 2003); gerente de la firma de ciberseguridad Kaspersky Lab para el Territorio Andino, asegura que "Vivimos tiempos muy intranquilos, ya que los diversos grupos de ciberdelincuentes han estado manteniendo sus operaciones de una forma muy activa".

Según el Ministerio de Defensa Colombiano, los servicios en la nube se están desplegando de forma masiva, igual que el uso de nuevas tecnologías, lo que permite laborar desde cualquier parte y en cualquier momento. No obstante, ello provoca grandes riesgos ante la vulnerabilidad que aporta un dispositivo no normalizado dentro de las políticas de seguridad de la información. Esta forma de trabajar ha hecho que, desde el punto de vista de la seguridad de la información, el perímetro de seguridad de la organización se desvanezca.

Los ciberataques son ejecutados por sus beneficios económicos para quien los ejecuta. Por ese motivo, en la estrategia de cualquier empresa que se conecta a la red de redes es prioritario contar con el hecho de que el ciberespacio se ha convertido en el quinto dominio de las operaciones militares tras la tierra, los mares, el aire y el espacio (Caparroso, 2017). A diferencia del resto de los entornos donde se combate, el ciberespacio tiene una dimensión física y virtual; de esa manera, cualquier suceso que ocurra en el ciberespacio tiene efectos en el mundo físico y viceversa. Cuanto más se extienda el uso de internet en nuestro país y se aumente la dependencia a las infraestructuras y tecnologías informáticas, el nivel de vulnerabilidad se incrementará.

La ciberseguridad es protagonista estos últimos tiempos en la agenda del Pentágono, el cual anunció que el

Ejército de EEUU ha desplegado nuevas armas digitales en internet para atacar al Estado Islamico (EI) y acabar con sus comunicaciones, la coordinación de sus militantes y sus fuentes de financiación en Siria e Irak. Actualmente, ya existe una política de ciberseguridad que empieza a dar frutos en Colombia, pero los CEO y, en general, todos los involucrados con el sector TI del país –tanto de entidades públicas como de la empresa privada– deben trabajar en estas áreas para consolidar los progresos y aumentar la protección de las organizaciones.

Por su parte, la multinacional Cisco realizó un estudio de Seguridad basado en encuestas a más de mil empleados de organizaciones españolas. El resultado de esta encuesta presenta que la falta de conciencia y el desconocimiento ponen en riesgo los datos corporativos de las organizaciones. Además, muestra que el comportamiento de los trabajadores constituye un débil eslabón en la cadena de ciberseguridad, lo cual se convierte en una creciente fuente de riesgos que se debe más a la falta de conciencia y al desconocimiento que a la malevolencia, pues los empleados esperan que los mecanismos de seguridad implementados por la empresa se ocupen de todo. (Varios, 2010)

Por otro lado, se viene desarrollando un programa de ciberseguridad y ciberdefensa con el fin de proteger cibernéticamente las infraestructuras críticas nacionales y a la ciudadanía en el ciberespacio. En esta materia, se logró la firma y la aprobación del CONPES sobre ***Lineamientos de Política para Ciberseguridad y Ciberdefensa***, mediante el cual se crea el Centro de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), el Comando Conjunto Cibernético (CCOC) y el Centro Cibernético Policial (CCP) (Alonso, 2017). Sin embargo, el problema central radica en que el conocimiento en el área de ciberseguridad es deficiente por la falta de personal capacitado. Es por ello que deben diseñarse e implementarse estrategias para promover, mejorar y mantener un nivel de cultura en ciberseguridad –así como para lograr la concienciación de todos los funcionarios y terceros que interactúan en el sector defensa– para minimizar la ocurrencia de incidentes de seguridad de la información y para que hagan un uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

Las organizaciones deben apostar por desarrollar la capacidad para enfrentarse a la creciente amenaza cibertnética, de forma que puedan atender a clientes, consumidores, accionistas y organismos reguladores. La Sociedad de la Información se caracteriza por el empleo masivo de las nuevas tecnologías para el acceso, transacción y difusión de la información, lo cual juega un papel clave en la mejora de la eficiencia, siendo la causa de importantes mejoras de la productividad, un poderoso motor para el crecimiento, la competitividad y el empleo. Este desarrollo tecnológico en particular supone cambios en el concepto de la seguridad tecnológica sobre los que se deben establecer tecnologías, procesos, procedimientos y servicios encaminados a proteger los activos (físicos, lógicos, o de servicios) que garanticen la protección de las infraestructuras y redes de comunicación tanto nacionales como a nivel de empresa u organismo.

Según la IEEE [6], la ciberseguridad aparece hoy en la mayoría de estrategias de seguridad nacionales como uno de los factores clave en la protección de las infraestructuras críticas esenciales para el bienestar económico y social, desde donde debe reforzarse la confianza y la protección de la información y privacidad en los servicios de la sociedad de la información, aportando valor a ciudadanos, empresas, administración, redes académicas, de investigación y sectores estratégicos en general. Resulta evidente la importancia que para el buen desarrollo de las organizaciones supone un apropiado conocimiento de su ciberseguridad: una concienciación adecuada de su situación en el ciberespacio y de las amenazas que éste conlleva para su normal desarrollo en este nuevo medio. Para desarrollar una conciencia de ciberseguridad, es necesario conocer las amenazas y los riesgos, y asumirlos en el sentido de aceptarlos y enfrentarlos: comunicar las incidencias, formar en materias de ciberseguridad y la necesaria adaptabilidad de usuarios de la institución y las circunstancias cambiantes del ciberespacio. (CONPES, 2016).

Desarrollo de software, juego formativo, ciberseguridad

La ciberseguridad es un tema complejo, técnico, extenso y especializado. Para hacer el tema más manejable, organizaciones como la OSI, Isaca, IBM, HP, Cisco, Symantec y Sans han definido 10 dominios de ciberseguridad : dominio legal; dominio de gestión de riesgos y seguridad de información; dominio de diseño y arquitectura de seguridad; dominio de seguridad en internet, redes y telecomunicaciones; dominio de control de acceso; dominio de operaciones de seguridad; dominio de seguridad ambiental y física; dominio de seguridad de la aplicación; dominio de recuperación de desastre y continuidad del negocio; dominio de criptografía (CONPES, 2011).

En la investigación sobre gamificación se identificaron varios referentes. ***SecuKid*** (Instituto Nacional de Ciberseguridad de España, 2015), por ejemplo, es un juego para móviles dirigido a todos los públicos, el cual está concebido para conocer mejor algunos riesgos de internet, sus efectos y cómo prevenirlos. Este juego formativo (creado

en 2009) nace como una innovadora iniciativa de ***Pantallas Amigas*** e ***Inteco*** (Instituto de Tecnologías de la Comunicación, promovido por el Ministerio de Industria, Turismo y Comercio del Gobierno de España) que aprovecha la capacidad de los videojuegos como fuente de aprendizaje informal. Se trata de un juego de estrategia e inteligencia que permite al usuario desarrollar capacidades como la orientación espacial, el pensamiento creativo y la planificación de recursos. SecuKid dispone de 5 áreas temáticas: las tres primeras abordan los aspectos del software malicioso o malware (virus, troyanos/gusanos y software espía), mientras que las dos últimas entran de lleno en cuestiones relacionadas con el ciberbullying y el grooming.

Otro juego formativo es ***Need to Know***, un simulador de espionaje que pone a prueba la ética. La privacidad, la seguridad en las redes y en las telecomunicaciones, así como la libertad individual y otros controversiales se dan cita en un simulador de espionaje en el que el jugador debe encargarse de buscar el equilibrio entre privacidad y seguridad. En este juego, desarrollo de ***Monomyth Games***, los jugadores son agentes del Departamento de Libertad, encargados de monitorear toda clase de actividad sospechosa, y de ser necesario, emitir órdenes adicionales. Al principio, el jugador sólo puede investigar elementos como metadatos o el historial de navegación, pero a medida que su nivel mejore, podrá obtener patrones de compras, geolocalización, y hasta vigilancia vía drones. Avanzar dentro del Departamento de Libertad también implica saber más sobre sus actividades. En este punto es cuando se abre la posibilidad de asistir en la formación de un verdadero estado policial, comenzar a ayudar a ciertas personas, o lograr el mayor beneficio personal posible.

Por otro lado, el Centro de Ciberseguridad Industrial (MINDEFENSA, sf) ha creado el primer juego de mesa español de ciberseguridad, ***CiberSospecha***, herramienta de concienciación para niños, profesionales y alta dirección, donde cada jugador asumirá el papel de un investigador de ciberseguridad que debe utilizar sus facultades de deducción para descubrir dónde, cómo, por qué y quién ha provocado el incidente de ciberseguridad que ha paralizado una planta industrial. Este juego pretende servir como una herramienta profesional de concienciación y formación en Ciberseguridad para proveedores, administradores y usuarios de los sistemas de operación industrial y los sistemas de información corporativos, pero ha sido especialmente diseñado para sensibilizar a los directivos de las organizaciones. El juego contiene un tablero de 60x60 cm, un manual de usuario, notas de investigación, tarjetas, las piezas de juego, dados, y un sobre confidencial. El juego tiene una duración entre 30 y 60 minutos por partida. El número mínimo de jugadores es 3, y el máximo es 6. Es un juego fácil y divertido que requiere de estrategia y también de un poco de suerte.

La firma de seguridad cibernética estadounidense ***Norse*** (MINTIC, 2017). ideó un software que detecta y genera un mapa interactivo que muestra ataques cibernéticos en tiempo real, lo cual evidencia detalles de los ataques como lugares de origen, los objetivos más buscados y las regiones más atractivas para los ***hackers***, direcciones IP que deben bloquearse, entre otros. La guerra de rayos que se visualiza en su mapa es en realidad ataques registrados a la infraestructura de Norse, atraídos mediante 8 millones de sensores repartidos en 50 países. Unos sensores simulan blancos favoritos de los ciberataques como PCs, smartphones o cajeros automáticos. Norse solo muestra uno de cada mil ataques para evitar bloquear el navegador.

El juego es un mediador en el proceso de aprendizaje y los contenidos educativos están inmersos dentro del propio juego. Uno de los factores que contribuyen al éxito del juego formativo es su componente de diversión, el cual mantiene la motivación de las personas que, convertidos en jugadores, afrontan los retos educativos sin ser conscientes de ello.

La ingeniería de software implica un trabajo integral: se produce un análisis del contexto, se diseña el proyecto, se desarrolla el correspondiente software, se efectúan las pruebas para asegurar su correcto funcionamiento y, finalmente, se implementa el sistema (Pressman, 2006).

Los lenguajes de programación usados para este proyecto de desarrollo de software (HTML5, JavaScript, CSS3, php y base de datos en mysql) cumplen con una misión importante para el desarrollo del juego. Por ejemplo, el HTML5 hace que la página web sea compatible con todos los servidores web; por ejemplo, el layout para mejorar la presentación del contenido del juego tiene inserción de multimedia en la página web del juego formativo con etiquetas diseñadas para el audio y video, con lo cual se ahorra un plug-in de flash y además se utiliza en la creación del OVA.

Por su parte, el CSS3 sirve para la presentación de la página web, es decir, a tener la posibilidad de poner las reglas y estilos para la presentación de la página web. Se usó en este proyecto ya que ofrece compatibilidad con muchos navegadores web además de las opciones que ofrece para sombrear, redondear, hacer transformaciones. El JQuery es una librería de JavaScript, la cual sirve para optimizar el trabajo de programación; en el juego formativo apoya el uso de Jtable que también es una librería de JavaScript que ayuda a crear la tabla que guardara las preguntas, respues-

tas, opciones, nivel de la pregunta, retroalimentación de respuesta, puntajes, usuario y contraseña. Esta tabla esta enlazada con una base de datos en MySQL donde se almacenan todas estas opciones.

El lenguaje de programación de PHP sirve para el enlace de la página web con la base de datos. Los códigos de estos lenguajes de programación se ponen en DreamWeaver. Sin embargo, dado que éste no sirve para leer el lenguaje de programación de PHP, se utilizó el programa XAMP para ayudar a conectar todos los códigos y la base de datos. Este programa permite leer el lenguaje de programación de PHP, crear un ***host*** y enlazar el juego con la base de datos.

El juego formativo se puso a disposición del personal de Emavi en el sistema de gestión de aprendizaje ***Blackboard*** de la Fuerza Aérea Colombiana. El modelo que se utilizó para el proyecto de desarrollo del software fue el modelo en cascada. Se siguió una secuencia de fases ejecutando las actividades correspondientes para cumplir con las metas definidas en cada de ellas. En este modelo no se puede avanzar hasta terminar la fase anterior dejando bien desde el principio todo el proyecto; de igual manera, se debe tener control sobre el tiempo de realización del mismo y sus etapas para así entregar en el tiempo establecido y no tener que devolverse a corregir cualquier error.

Entre las ventajas del modelo, se cuentan que permite la departamentalización y control de gestión y que el horario se establece con los plazos normalmente adecuados para cada etapa de desarrollo, lo cualconduce a entregar el proyecto a tiempo. Es sencillo, facilita la gestión de proyectos, permite tener bajo control el proyecto y limita la cantidad de interacción entre equipos que se produce durante el desarrollo. Sin embargo, también tiene varias desventajas: no refleja realmente el proceso de desarrollo del software ya que la mayoría de los que desarrollan proyectos no cumple con este lineamiento; se tarda mucho tiempo en pasar por todo el ciclo; la aplicación de la metodología en cascada se orienta mejor al desarrollo de proyectos de corto plazo, de poca innovación y proyectos definitivos y detallados; la metodología puede confundir al equipo profesional en las etapas tempranas del proyecto, y no es frecuente que el cliente o usuario final explicite clara y completamente los requisitos.

Para el diseño del programa se definieron los requisitos funcionales (ver tabla 1).

Tabla 1.

Requisitos funcionales. Fuente: elaboración propia.

Código Requerimiento	Descripción	Clasificación
RQ O1	El software debe permitir el registro de los siguientes perfiles de usuario. Usuario Administrador: Ingresa preguntas, modifica preguntas, da resultados e ingresa contenido informativo del juego Usuario Final: Accede al juego, recibe información acumulada de puntos.	Funcional
RQ 02	El software debe permitir la autenticación de usuario.	Funcional
RQ 03	El usuario administrador ingresara las preguntas generadas en el juego.	Funcional
RQ 04	El usuario administrador ingresara el contenido temario para el juego	Funcional
RQ 05	El sistema debe generar un juego de preguntas relacionadas con ciberseguridad.	Funcional
RQ 06	El usuario seleccionara la pregunta que crea correcta.	Funcional
RQ 07	El sistema evaluara la respuesta y la calificara.	Funcional
RQ 08	El sistema avanzara de nivel dependiendo de la respuesta acertada seleccionada por el usuario.	Funcional
RQ 09	El sistema generara 3 ayudas únicas y disponibles por juego iniciado. La primera será ayuda del publico donde el sistema mostrara la pregunta correcta como nivel más alto de probabilidad, la segunda es 50 y 50 mostrara las dos preguntas opcionales como correctas y la tercera ayuda es llamada a un amigo	Funcional

RQ10	El sistema tendrá una interfaz intuitiva y amigable	Funcional
RQ11	El sistema proporcionara claridad y correcta organización de la información	Funcional

A continuación se presentan los diagramas de casos de uso, en los cuales se evidencia la forma como los actores operan con el sistema en desarrollo. En la figura 2 se muestra el diagrama de caso de uso principal. Esta interacción propone que el usuario realice diferentes procesos simulando el escenario ideal en que se desarrollara el software.

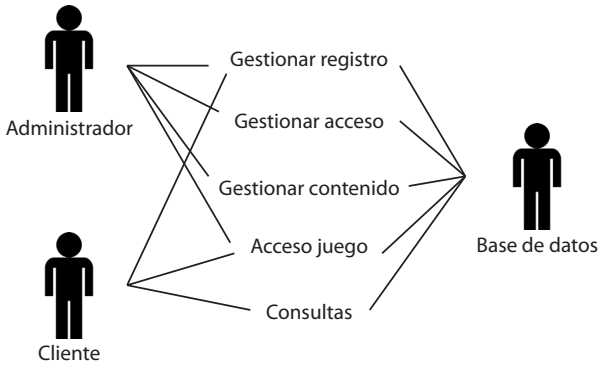

Figura 2. Diagrama caso de uso principal.

Fuente: elaboración propia.

En la figura 3 se muestra el caso de uso ***gestionar registro***, la fase inicial en la cual se determinan los procesos para ingresar a la plataforma.

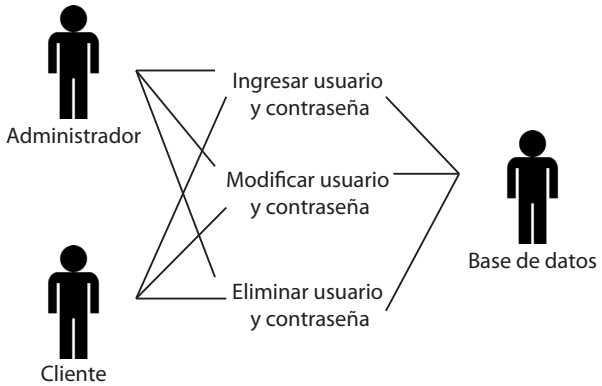

Figura 3. Diagrama caso de uso registro.

Fuente: elaboración propia.

En la figura 4 se muestra el caso de uso ***gestionar acceso***. Esta define el acceso de cada usuario previamente registrado teniendo asignado y garantizado su ingreso al juego.

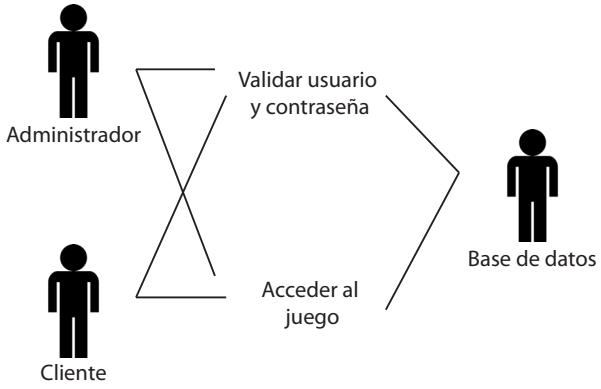

Figura 4. Diagrama caso de uso acceso.

Fuente: elaboración propia.

La figura 5 muestra el caso de uso ***gestionar contenido***. Siempre que se deba contestar una pregunta, el que se encarga de resolver es el programa, con lo cual se logra tener el control total del mismo.

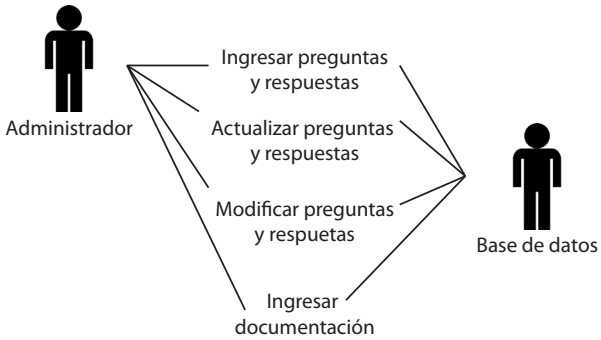

Figura 5. Diagrama caso de uso contenido.

Fuente: elaboración propia.

En la figura 6 se presenta el caso de uso ***gestionar juego***. Plantea cada uno de los parámetros de inicio de nivel e instructivo del mismo.

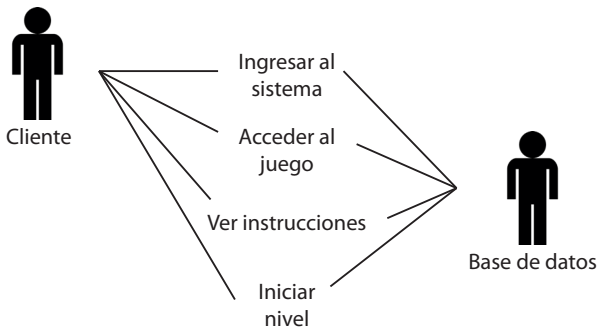

Figura 6. Diagrama caso de uso juego.

Fuente: elaboración propia.

La figura 7 muestra el caso de uso ***consultas***. Este plantea cada una de las consultas o resultado obtenidos durante el juego.

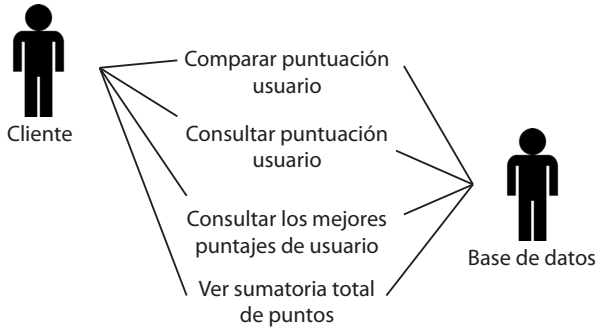

Figura 7. Diagrama caso de uso consulta.

Fuente: elaboración propia

En la figura 8 se presenta el diagrama de actividades definido, en el cual se muestra el proceso del programa a través de una serie de acciones.

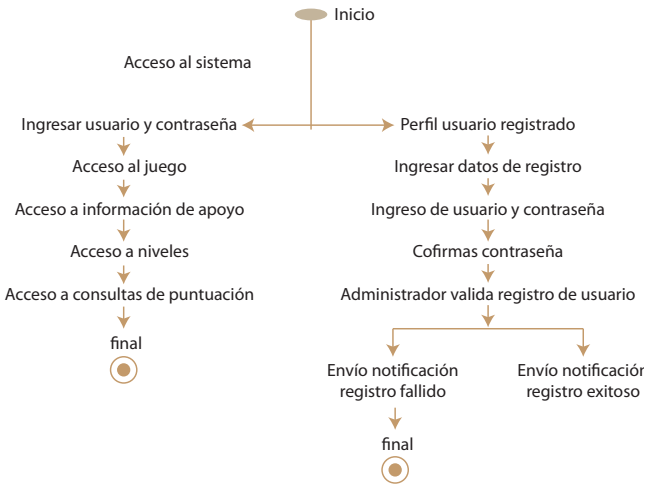

Figura 8. Diagrama de actividades.

Fuente: elaboración propia.

En la figura 9 está el diagrama ***entidad-relación***, en el cual se representan las entidades relevantes del sistema de información y sus interrelaciones y propiedades.

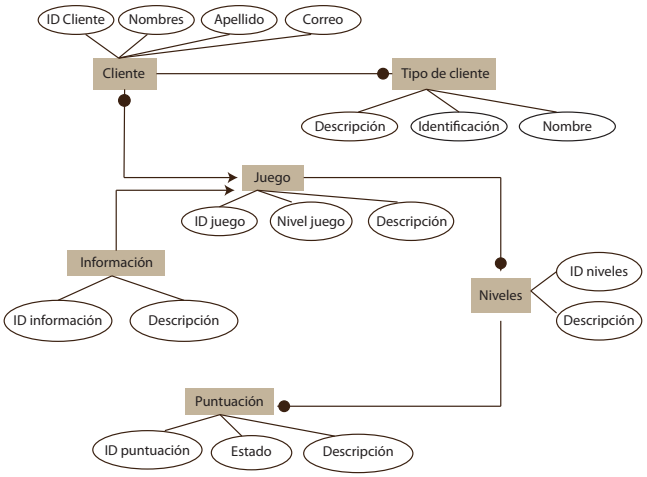

Figura 9. Diagrama entidad-relación.

Fuente: elaboración propia.

A continuación, en la figura 10, se presenta el diagrama relacional, en el cual puede verse la interacción de cada uno de los componentes del software, representado por las entidades reales que ofrecen la interfaz para realizar las operaciones planteadas por la misma.

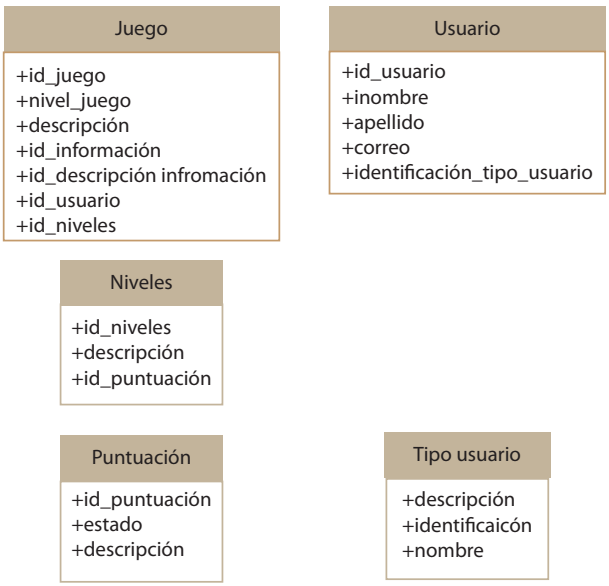

Figura 10. Diagrama relacional.

Fuente: elaboración propia.

En la figura 11, ***diagrama de clases***, se evidencia la estructura planteada y la realización del código fuente.

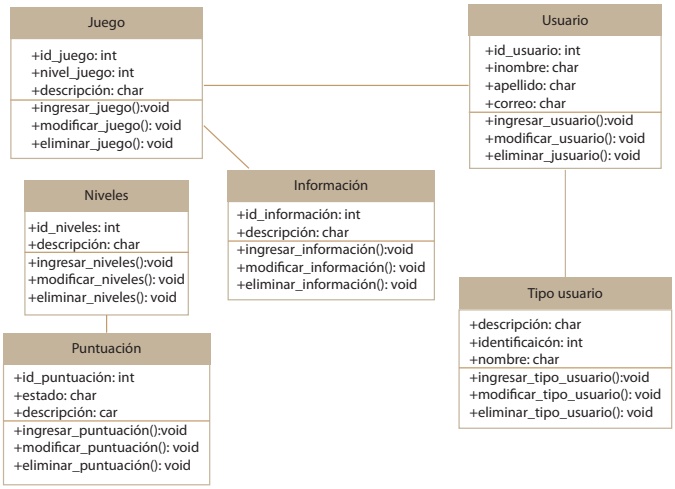

Figura 11. Diagrama de clases.

Fuente: elaboración propia.

En la figura 12 se muestra la interfaz de entrada al juego.

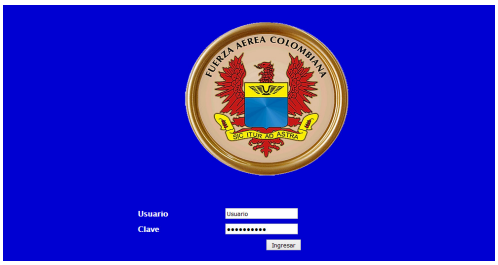

Figura 12. Interfaz de entrada.

Fuente: elaboración propia.

En la figura 13 se muestra la interfaz de selección de opciones para el usuario. Desde allí puede escogerse ir al contenido, ingresar al juego, ver historial de resultados en el juego y cerrar sesión.

Figura 13. Interfaz de selección de opciones.

Fuente: elaboración propia.

El juego formativo desarrollado incluyó actividades, como llamar a un amigo para ayudar a dar respuesta o solicitar la ayuda del público para encontrar ayuda a la respuesta en el juego.

A continuación, se muestra parte del código fuente:

```
/* Las siguientes funciones plantean el sistema de ayuda del juego, con un peso diferente entre ellas de acertar con la respuesta correcta con un único uso */
    var np=0;
    var puntaje=0; var sel=0;
    var ayuda1=0; var
    ayuda2=0; var ayuda3=0;
    var gameover=0;

/* Esta función es la ayuda telefónica utiliza random para presentar el chance de dar una respuesta con la pregunta correcta */

    function cancelar3(){ document.getElementById('llamada').style="opacity:0.4; max- width: 5%; top:10%; left: 65%; position: absolute;" if(ayuda1==0)
        {ayuda1=1;
          //Tasa de acierto al 70%
          var prob=Math.random();
          if(prob<=0.70)
              {//dar la respuesta correcta
              alert('Hola gracias por creer en mi ayuda creo que la respuesta es la '+correcta[np]);
              }
          else
          {//dar la respuesta incorrecta

              varz=Math.random();
              while(Math.floor(4*z)==correcta[np])
              {z=Math.random();
              }
              alert('Hola gracias por creer en mi ayuda creo que la respuesta es la'+Math.floor(4*z));
              }
              //Fin de tasa de acierto
              }
              }
/*Esta función es la ayuda del 50/50. Como la anterior, usa random para determinar el chance de escoger. La pregunta correcta tiene una tasa 50% para acertar. Al final de usarla, se a desactiva la ayuda */

    function cancelar2(){ document.getElementById('5050').style="opacity:0.4; max-width: 5%; top:10%; left: 59.5%; position: absolute;"
    var a1=0;
```

```
var b1=0;
var c1=0;
var d1=0;
if(ayuda2==0)
        {ayuda2=1; cuenta=0;
        while(cuenta<2)
            {varz=Math.random();while(Math.
             floor(4*z)==(correcta[np]-1))
                {z=Math.random();
                }
            if((Math.floor(4*z))==0&&a1==0)
                {document.getElementById('d1').in-
                nerHTML=''; cuenta++;
                a1=1;
                }
            if((Math.floor(4*z))==1&&b1==0)
                {document.getElementById('d2').in-
                nerHTML=''; cuenta++;
                b1=1;
                }
            if((Math.floor(4*z))==2&&c1==0)
                {document.getElementById('d3').in-
                nerHTML=''; cuenta++;
                c1=1;
                }
            if((Math.floor(4*z))==3&&d1==0)
                {document.getElementById('d4').in-
                nerHTML=''; cuenta++;
                d1=1;
                }
            }
            }
    }
```

Conclusiones

Con este trabajo se determina la importancia de invitar al personal vinculado a conocer los peligros cibernéticos a los que se enfrenta por navegar o hacer uso de medios interactivos. En la encuesta de parametrización, un 70,5 % valida la importancia de conocer sobre la ciberseguridad por acciones como robos, fraudes y ataques a usuarios de los que han sido víctimas; sin embargo, existe la necesidad de capacitar sobre nuevas prácticas de ataque en el ciberespacio.

Recopilar e integrar el diseño de requisitos del modelo cascada permitió crear los parámetros en los que se basa el juego con el fin de reducir el nivel de riesgo, aumentar las medidas de seguridad y hacerlo atractivo al usuario, con lo cual se posiciona como una estrategia de conocimiento que enseña ciberseguridad.

Se construyó un juego formativo con el cual el usuario aprenderá de ciberseguridad, diseñado para facilitar la lectura de los textos y la comprensión de los códigos fuente, por si llegase a necesitar modificar alguna fase al momento de implementarlo en la plataforma ***Blackboard***, desarrollado con lenguajes de programación de fácil usabilidad que permiten que el software tenga aceptación.

El software implementado en la plataforma ***Blackboard*** integra el diseño de características del modelo cascada y permite reducir el nivel de riesgo. Se sugiere acatar las medidas de seguridad, como colocar una clave de seguridad a las redes inalámbricas, no dejar puertos abiertos; no realizar descargas indiscriminadas de páginas de dudosa procedencia y menos sin tener un antivirus totalmente funcional y actualizado. Tales son herramientas que se enseñan en el juego formativo a medida que se avanza con las preguntas.

Agradecimientos

Este trabajo ha sido financiado parcialmente por la Fuerza Aérea Colombiana, Escuela Militar de Aviación "Marco Fidel Suarez", grupo de investigación del Programa de Ingeniería Informática Sigintel. Forma parte del trabajo de grado ***Desarrollo de un juego formativo para generar concienciación de la ciberseguridad en la Emavi.***

Los autores desean expresar su agradecimiento a los directivos de la institución.

Referencias

Accounting Information Systems. http://media.pearsoncmg.com/ph/bp/bp_harrison_BP/Kay/

Alonso, R. (2017) ¿Qué tanto sabes de ciberseguridad? ***Diario El Economista***. Disponible en: http://eleconomista.com.mx/tecnociencia/2017/03/27/que- tanto-sabes-ciberseguridad

Braude, E. J. (2003). ***Ingeniería de software. Una perspectiva orientada a objetos.*** Lerez, España: RA-Ma

Caparroso, J. (2017). Colombia vive un 'boom' de empleos en seguridad digital. ***El Tiempo***, 8 de marzo 2017. Recuperado de http://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-vive-un-boom-de-empleos-en-seguridad-digital-71092

Cisco Systems. ***La falta de conciencia y el desconocimiento ponen en riesgo los datos corporativos de las organizaciones españolas***. Recuperado de http://globalnewsroom.cisco.com/es/es/release/La-falta-de-conciencia-y-el- desconocimiento-ponen-en-riesgo-los-datos-corporativos-de-2047151

CONPES. (2016). Política nacional de seguridad digital 11 de abril de 2016. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

CONPES. (2011). Lineamientos de política para ciberseguridad y ciberdefensa,14 de julio de 2011. Recuperado de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Instituto Nacional de Ciberseguridad de España. (2015). Ciberseguridad en el comercio electrónico. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad_0.pdf

MINDEFENSA, Colombia presenta estrategia de Ciberseguridad y ciberdefensa. Recuperado de https://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml

MINTIC. (2017). Ciberseguridad. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-6120.html

Pressman, R. (2006). ***Ingeniería del software Un enfoque práctico: Modelo de análisis y diseño.*** México: McGraw Hill Interamericana.

Varios. (2010). Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. ***Cuadernos de Estrategia***, 149, 1-368. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf