

Portal Web con sistema clasificador de noticias para apoyo al fomento de la ciberseguridad.

Hilda-Díaz Rincón, José Antonio-Navarrete Prieto, Iliana Gabriela-Laguna López de Nava.

^a Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesora de tiempo completo, Maestra en Planeación Estratégica y Dirección de Tecnología, Perfil Deseable, Jefa de Proyectos de Vinculación del Depto. de Sistemas y Computación, c_computo_sic@hotmail.com, Tlalnepantla de Baz, Edo. México, México

^b Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesor de tiempo completo, Perfil Deseable, Responsable Cuerpo Académico "Ciencia, Tecnología Innovación y Sociedad", Doctor en Planeación Estratégica y Dirección de Tecnología, posgrado_ittla@yahoo.com.mx, Tlalnepantla de Baz, Edo. México, México

^c Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesora de tiempo completo, Perfil Deseable, Coordinadora de Tutorías del Depto. De Sistemas y Computación, ilianaxim@hotmail.com, Tlalnepantla de Baz, Edo. México, México

Resumen

De acuerdo al estudio Hábitos de los usuarios en ciberseguridad en México, 2019 realizado por la SCT, OEA donde reveló que la mayoría de los participantes no tienen una conciencia clara acerca de la privacidad en el uso de redes sociales e Internet, se desarrolla en el Instituto Tecnológico de Tlalnepantla (ITTTLA) el portal de ciberseguridad para apoyar el fomento a la ciberseguridad el cual incluye como parte innovadora un sistema para el control de noticias de ciberseguridad que administrara el cuerpo académico "Ciencia, Tecnología Innovación y Sociedad", quien realizara una clasificación de las noticias de mayor importancia de acuerdo a el impacto del mismo, además se incluyen herramientas básicas de ciberseguridad, e incluye información importante para los usuarios llevando un control de artículos, herramientas, visitas y usuarios, integrando secciones para niños, adolescentes y adultos.

Palabras clave—ciberseguridad, herramientas, noticias, portal

Abstract

According to the study Habitos de los usuarios en ciberseguridad en México, 2019 carried out by the SCT, OAS, which revealed that most of the participants do not have a clear conscience about privacy in the use of social networks and the Internet, the cybersecurity portal is developed at the Instituto Tecnológico de Tlalnepantla (ITTTLA) to support the promotion of cybersecurity which includes as an innovative part a system for the control of cybersecurity news administered by the academic body "Ciencia, Technology, Innovation and Society", who will classify the most important news according to its impact, also includes basic cybersecurity tools, and includes important information for users, keeping track of articles, tools, visits and users, integrating sections for children, adolescents and adults.

Keywords— cybersecurity, tools, news, portal

1. INTRODUCCIÓN

Las Tecnologías de Información y Comunicaciones actualmente están involucradas en todos los aspectos de la vida de las personas por lo que es importante fomentar la ciberseguridad a todos los niveles de usuarios.

En México son pocas las organizaciones e Instituciones que se preocupan por fomentar la cultura de la ciberseguridad, como es el caso de la Universidad Nacional Autónoma de México (UNAM), la Policía Federal y la Secretaría de Educación Pública (SEP) pero las personas desconocen los sitios a donde pueden obtener información al respecto por lo que se deben integrar sitios especializados para ello.

De acuerdo al informe que presenta la Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) indica que, en el primer semestre de 2019, las quejas por fraudes cibernéticos crecieron 35% respecto de 2018 y representan cada año una mayor proporción además de que el monto reclamado de los fraudes cibernéticos ascendió a \$5,908 mdp; se bonificó sólo el 42% y 87 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario.

La Secretaría de Seguridad y Protección Ciudadana (SSPC), a través de la División Científica de la Policía Federal, puso en marcha la campaña Ciberseguridad México 2019, que tiene como objetivo concientizar a los niños y las niñas de México sobre los riesgos que existen en el uso de las Tecnologías de la Información y Comunicaciones y fomentar la sana convivencia en el entorno digital.

En [5] Infochannel de marzo del 2019, publica que, de acuerdo con Alfonso Durazo Montaña, titular de la Secretaría de Seguridad y Protección Ciudadana (SSPC), el catálogo de delitos que ocurren en la red va de los fraudes, la extorsión y amenazas, hasta el bullying o acoso en redes sociales, la pornografía infantil, la trata de personas, intrusión no autorizada en sistemas, robo de identidad y los ataques cibernéticos dirigidos contra bases de datos relevantes para nuestro país. Además, indicó que 80% de los delitos cibernéticos se pueden evitar con medidas de concientización y que en este año, Ciberseguridad México 2019 contempla la colaboración de aliados estratégicos como la Secretaría de Educación Pública, la Asociación de Internet.MX y la Fundación Responsabilidad Social Infantil, quienes llevarán a cabo acciones de concientización sobre las modalidades de delitos cibernéticos que más afectan a la ciudadanía, recomendaciones para prevenirlas, así como las unidades de apoyo y medios de contacto y orientación técnica y legal, incluyendo los mecanismos de denuncia.

Con la realización de un sistema web de control de noticias y portal de ciberseguridad permitirán obtener información acerca la ciberseguridad que apoyara al cuerpo académico a realizar la actividad de fomento de ciberseguridad a la sociedad.

La ventaja de automatizar esta información es que permitirá tener un mejor control, ya que se van a registrar las noticias que se consideren importantes en el sistema para integrar la información en tiempo real y que esté disponible a cualquier persona la información respecto a la ciberseguridad.

Es así como la falta de portales académicos donde se involucre la ciberseguridad da la pauta principal para la

creación de un portal de apoyo a la ciberseguridad, donde se integren en el mismo contenido de:

Servicios de Ciberseguridad

Información referente a sugerencias de ciberseguridad

Información de herramientas de apoyo a la ciberseguridad

Dentro del planteamiento se involucró la investigación de portales existentes semejantes al que se está desarrollando, siendo el resultado de esta el siguiente:

El portal del Club de la Investigación Tecnológica (<https://www.clubdeinvestigacion.com>) que contiene dentro de su menú noticias, publicaciones, informes de investigación, eventos, el cual muestra las noticias en un orden jerárquico-secuencial. El objetivo primordial es crear una red de conocimiento para sus afiliados y mantenerlos al día respecto de las innovaciones tecnológicas y su aplicación en el desarrollo organizacional. Esto se logra a través de la publicación de informes de investigación, desayunos-conferencia mensuales, foros, charlas y otras actividades que promueven el entendimiento de las nuevas tecnologías. Todo esto distinguiendo el ruido mercadológico de las verdaderas tendencias en nuestro medio.

Otras series de portales son los que corresponden a los CERT (Computer Emergency Response Team) y que se maneja como Equipo de Respuesta a Emergencias Informáticas el cual actualmente es la Universidad Nacional Autónoma de México (UNAM) que está localizado en la Coordinación de Seguridad de la Información (CSI) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, de la UNAM (<https://www.seguridad.unam.mx/>).

El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios, el cual comprende dentro de su portal elementos tales como son: Estadísticas, Notas, Boletines, Incidentes, Vulnerabilidades y como parte del menú principal se accede a la Coordinación de Seguridad de la Información (CSI), UNAM_CERT, Usuario casero, becarios, Seguridad TV (videos), .Seguridad en donde en esta pestaña se promueve la cultura de prevención para TI. Cuando se accede a la noticia, muestra el título de la noticia en orden cronológico solo con fecha y texto. Cuando presenta la noticia, indica recomendaciones, fuentes recomendadas en algunos casos, en otra muestra solo la noticia y artículos recomendados

Existen diversidad de portales de organizaciones en los cuales muestran noticias de ciberseguridad las cuales dependen del interés personal de la misma como son en su caso ESET, Karpersky los cuales muestran las noticias con la fecha y un texto breve para interesar al usuario en la noticia visualizándola en forma cronológica, secuencial.

En España existe Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital y consolidada

como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Su actividad está basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional (<https://www.incibe.es/que-es-incibe>). Incibe, es un portal muy completo el cual contiene blog, avisos, kit de concienciación, hackend, políticas de seguridad, riesgos, formación, guía, sellos de confianza y en su menú principal superior contiene información de protección a empresas, eventos, otras actividades, contacto, línea de ayuda, boletines, agenda, sala de prensa, encuestas y un mapa web, este fue el portal que se tomo como base para la primera etapa de desarrollo del que se propone en esta investigación.

Al realizar la comparación de portales permitió el considerar establecer primeramente un sistema integrador estándar de noticias, para interesar al usuario en las mismas y llevar un estadístico de estas, ya que los otros portales que se mencionan no llevan un control del número de noticias, de herramientas que de primera intención el usuario puede darse cuenta de la información que le mostrara el portal y este es uno de los elementos clave que se integró al mismo. Además de que, si se optó por mostrar las noticias en orden cronológico, pero además se estableció que el control de las noticias debería de considerar los siguientes elementos, verificación de la fuente, validar si existe probable impacto de esta con base en lo que indica la misma, incluyendo ligas a herramientas para disminuir el riesgo del impacto, integrando enlaces de apoyo con respecto a la noticia, integrar las que tengan mayor impacto en México y posteriormente a nivel internacional.

En donde la dificultad principal es la integración de la información y presentarla en un formato estándar debido a la diversidad de formas con las que aparecen, por lo que como una estrategia de innovación se establece el tamaño de texto, el número de palabras base para presentar la noticia, el tamaño de la imagen, el número de enlaces a mostrar. Dentro del portal se integró una pantalla principal que muestra los sistemas base ver la figura 5, estos conforman la parte de administración de noticias del portal el cual va a contener el artículo y las herramientas, donde para el sistema de herramientas se integra la información como son: nombre, función, tipo de herramienta: da una lista del público al que va dirigido, este es importante ya que dependiendo del que se coloque es donde se estará mostrando (defensa, ataque, informativo e infografías), autor, selección de archivo (no mayor a 15 Mb), la clasificación de las herramientas se realiza como se indica a continuación:

A Defensa. "herramientas que puedan brindar apoyo en defensa para el usuario, pueden ser manuales, ejecutables comprimidos, archivos no mayores a 15 Mb"

B Ataque. "herramientas que puedan brindar apoyo forma de ataque para el usuario, pueden ser manuales, ejecutables comprimidos, archivos no mayores a 15 Mb"

C Informativo. "herramientas que puedan brindar apoyo al usuario en información general"

D Infografía. “se muestran elementos gráficos con respecto a los temas de las herramientas, ataques, recomendaciones”

En lo que respecta al “sistema de noticias”, este contiene información de los artículos que están dirigidos hacia el público en general, estudiantes y empresas, en el cual se incluyen botones para manejar las altas, modificaciones y eliminaciones, para el manejo de la información se consideran los siguientes elementos: título, subtítulo, dirigido a (el cual realiza una subclasificación para el público al que va dirigido, ya que dependiendo de la misma se muestra al usuario (público en general, estudiantes y empresarios), siguiendo con la categoría en donde esta se clasifica con base en una lista de categorías para el artículo (noticias, defensas, ataques, historias, visitas y normas) autor de artículo, fecha de artículo, url de artículo (donde se encuentra el artículo original), imagen de artículo (no mayor a 2 kb), reseña a mostrar (no mayor a 700 caracteres contando los espacios).

Como parte de la innovación se incluye una clasificación de los mismos con base en lo siguiente:

A Noticias. “artículos recientes noticias en general”

B Defensas. “artículos de actualizaciones en sistemas o para consejos de seguridad”

C Ataques. “muestra artículos donde se han mostrado los ataques a sistemas”

D Historia. “artículos de historia de ataques de cibernéticos, los primeros ataques, historia de avances científicos en el área de informática”

E Visitas. “lugares donde se han tenido participación de información sobre la ciberseguridad”

F Normas. “empresario – artículos para informes de las normativas para la seguridad informática tanto para manejo de equipamiento como la seguridad que se debe de manejar y procesos”

Y debido a la diversidad de información que se tiene para realizar las clasificaciones, se vuelve complejo realizar un algoritmo de forma inmediata para integrarlas dentro del sistema, por lo que la selección de noticias se está realizando forma manual a efectos de realizar la comprobación y validación de la misma, apoyándose en un equipo de estudiantes residentes e interesados en la seguridad para realizar las pruebas, cabe mencionar que si se consideró establecer el orden cronológico será descendente par su clasificación.

Otra de las ventajas de incluir un sistema de noticias es que se elimina la dependencia del webmaster para la actualización de las mismas, ya que la mayoría de los portales tienen que estar dependiendo de un webmaster para estar modificando y actualizando sus portales por lo que al contar con un sistema se optimizan los recursos designados para el mantenimiento del portal.

Como parte de la selección de las noticias se utilizan fuentes como son: Gartner Inc. quien es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos, Forbes, Secretaría de Seguridad y Protección Ciudadana, Revistas arbitradas e indexadas, Portales y Periódicos especializados

(Computerworld), Asociaciones y Organizaciones expertas en Seguridad Informática y Ciberseguridad, Academias /CISCO,ESET), Tesis, Trabajos de Investigación y finalmente las noticias comerciales

Al analizar las ventajas que se obtendrían con el sistema clasificador de noticias para los usuarios y visitantes es el de localizar en su solo sitio información ya organizada con base en las subclasificaciones, la amplitud de estas será la fortaleza principal para los visitantes ya que este aspecto les permite en un solo espacio ubicar información de apoyo para resolver la necesidad que tienen. La habilidad de los clasificados consiste en otorgar un espacio digital a las visitantes para mostrar información más completa sobre la ciberseguridad en un solo sitio. Como parte del posicionamiento, se podrán lograr posteriormente acuerdo con las diversas marcas para integrarlas dentro de la parte principal del portal y además de retribuirles con indicadores de las visitas realizadas con respecto a la competencia.

La forma en que se va a organizar las noticias permite acompañar a empresas, estudiantes y público en general en su búsqueda de información respecto a la ciberseguridad.

También [6] considera que la ciberseguridad es esencial en las universidades es esencial, ya que los ciberataques son una constante insoslayable en el mundo actual. Si bien los hackers tienen múltiples vías de acceso para atacar las redes informáticas, en términos cibernéticos la mayor vulnerabilidad de cualquier organización reside en acciones del personal (como abrir correos electrónicos con phishing o navegar por sitios web infectados, por ejemplo). Por ende, su capacitación constante para hacer frente a los ataques es también una de las mejores maneras de mejorar la ciberseguridad de cualquier organización.

Dentro del portal se están considerando elementos que permitan que este sea localizado más rápidamente por palabras clave que se establecerán dentro del mismo para que a la hora que un visitante realice la búsqueda de información referente a ciberseguridad este pueda ser presentado dentro las primeras búsquedas.

En conclusión la facilidad dará al visitante de contener información clasificada es una gran ventaja para el mismo ya que no tendrá que estar realizando búsquedas de temas específicos al considerar para este una clasificación como la que se menciona en los apartados anteriores, además surge la propuesta de colocar espacios específicos para protección al usuario en donde pueda encontrar mecanismos avanzados de autenticación para asegurar el acceso, monitorear y filtrar mensajes de correo y *visitas a sitios web*, escanear con antivirus archivos, herramientas de protección de ataques y amenazas y finalmente está el que con el registro de los usuarios se le esté enviando información de acuerdo a sus intereses al enviarle una encuesta al usuario para conocer sus intereses y así poder estar actualizándole de información de las nuevas herramientas que le ayuden de acuerdo a sus interés.

Para el desarrollo del portal se utilizó el modelo en espiral propuesto por Boehm. En [1] las autoras indican que para el Modelo de desarrollo evolutivo (espiral). Propuesto por Barry Boehm en 1986, en su artículo “A Spiral Model of

Software Development and Enhancement” se conjuga una naturaleza iterativa en la construcción de prototipos con aspectos controlados y sistemáticos del modelo en cascada. [2]. Cuando se aplica este modelo en espiral, el software se desarrolla en una serie de entregas evolutivas. Cada una de las actividades del marco de trabajo representan un segmento de la ruta de la espiral. En cada ciclo repetitivo va ganando madurez el producto final.

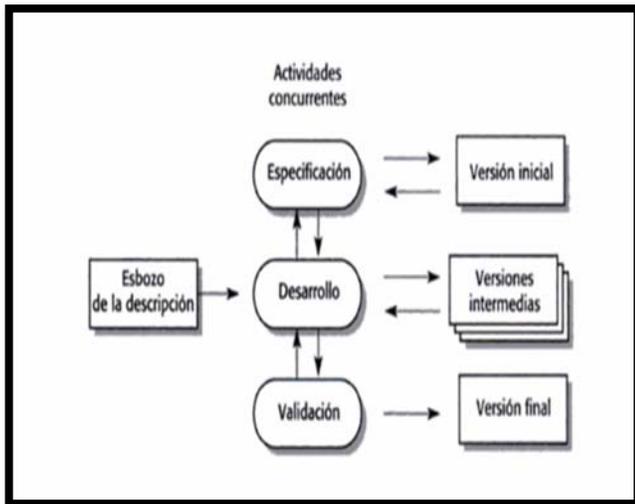
2. CONTENIDO

El desarrollo evolutivo se basa en la idea de desarrollar una implementación inicial, exponiéndola a los comentarios del usuario y refinándola a través de las diferentes versiones hasta que se desarrolla un sistema adecuado

Es evidente que todo software evoluciona con el tiempo, por lo que los requisitos del usuario y del producto suelen cambiar conforme se desarrolla el mismo. Una característica de los evolutivos es que son modelos iterativos, lo cual permite desarrollar nuevas versiones cada vez más consistentes y complejas, hasta llegar al objetivo final deseado; incluso evolucionar más allá, durante la fase de operación.

De acuerdo con [3], el modelo incremental mantiene la función anterior y aumenta otra, ya que puede ser que el primer incremento no hubiera tenido todos los requerimientos que necesitaba el proyecto.

Fig. 1 Modelo Evolutivo



Fuente: Tomando como base a Pressman [4]

En donde las actividades de especificación, desarrollo y validación se entrelazan en vez de separarse, con una rápida retroalimentación. Según [4] entre estas existen dos tipos de desarrollo evolutivo:

1. Desarrollo exploratorio, donde el objetivo del proceso es trabar con el cliente para explorar sus requerimientos y entregar un sistema final. El desarrollo empieza con las partes del sistema que se comprenden mejor. El sistema evoluciona agregando nuevos atributos propuestos al cliente.
2. Prototipos desechables, donde el objetivo del proceso de desarrollo evolutivo es comprender los requerimientos del cliente y entonces desarrollar una definición mejorada de los requerimientos para el sistema. El prototipo se centra en

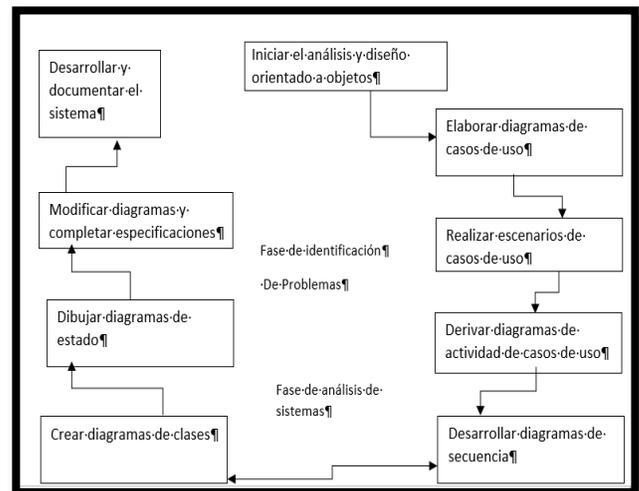
experimentar con los requerimientos del cliente que no se comprenden del todo

Con base en lo anterior el desarrollo del Portal involucrando las siguientes fases:

Identificación de Requerimientos, donde se establece un análisis sobre el estado actual, utilizando para ello la observación, la investigación documental las cuales permiten investigar aspectos generales sobre el área, para que posteriormente pueda ser especificado con mayor detalle, por ello se establece comunicación directa con el cliente para conocer su forma de trabajo y necesidades técnicas y tecnológicas, con base en el análisis de los datos obtenidos de la investigación documental se detecto que existe información de noticias de ciberseguridad pero todas tienen formatos diferentes para presentarlas, por lo que utilizando el brainstorming con los integrantes del cuerpo académico e invitando a personal especializado en el área de seguridad, se determinó el estándar para integrar en el sistema de noticias, en lo que respecta al contenido este fue definido por el usuario a través de una entrevista semiestructurada con los integrantes del cuerpo académico.

Se continuo con el Análisis del Sistema, a partir de los requerimientos obtenidos como resultado de la fase anterior, utilizando las bases de lo que indica el Lenguaje Unificado de Modelado (UML) con la finalidad de poder realizar los casos de uso y tener la oportunidad para regresar y revisar los casos, replantearlos y modificarlos cuando sea necesario, desarrollando para el proceso que se muestra en la figura 2.

Fig. 2. Proceso para el Modelado con UML



Fuente: Diseño Propio

Se considero además los actores principales que utilizaran el portal los cuales se muestran en la tabla 1.

En el análisis se determinaron los softwares a utilizar para el desarrollo como fueron: Ubuntu/Linux Server 12.4, PhpMyAdmin que es una herramienta escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando un navegador web, se utilizó Adobe Dreamweaver CS6 el cual es un potente y profesional editor web que incluye una gran cantidad de nuevas funciones de diseño y desarrollo y para realizar las pruebas se determinó utilizar el hosting que tiene el cuerpo académico para pruebas de sus desarrollos.

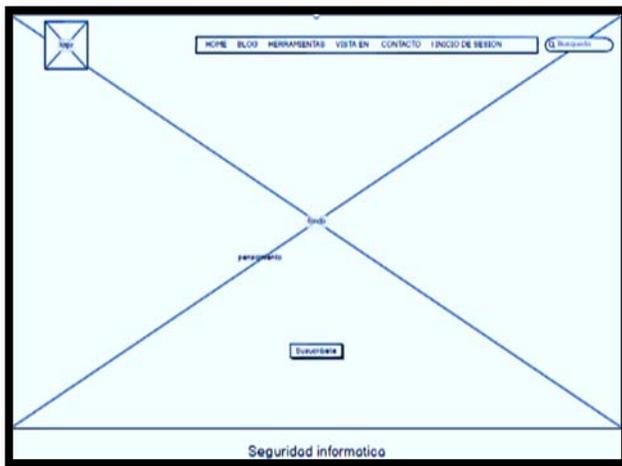
Tabla 1. Modelo de Actores identificados.

Actores	Descripción	Usuarios
Administrador	Representa final autorización de levantamiento de la información a mostrar en el portal web. Es quien se encarga de dar mantenimiento al portal por medio del sistema o inclusive por medio del hosting de almacenamiento.	Encargado de sistema
Subadministrador	Es la encargada de levantamiento de la información búsqueda de la misma y propuestas de herramientas en apoyo a la comunidad.	Encargado de recopilación de información y levantamiento de la misma
Usuario	Comunidad que puede aportar información, ideas y puntos de vista sobre la temas a tocar en el portal web.	

Fuente: Diseño Propio

Dentro del Diseño del Portal se diseña la maquetación correspondiente quedando como se muestra en la figura 3, donde como una primera parte integran los elementos a presentar en la parte principal del Portal, además de que se diseña un logotipo para identificar el mismo y que lo diferencie como tal.

Fig.3. Maquetación del Menú General del Portal



Fuente: Diseño Propio

La primera maquetación contiene se indica el contenido de los elementos de la Página Principal del portal, el cual integra lo siguiente: Menú General el cual permite el acceso a cada una de las áreas del sitio con las cuales se cuentan, Inicio del portal, Blog, Herramientas, Enfocado a (teniendo este un submenú dando a direccionar a los apartados de KIDS, Adolescentes, Empresas), Contáctanos, Inicio de sesión. El encabezado contiene imagen de fondo con un eslogan teniendo en la parte inferior un botón en direccionamiento a la parte de suscripción de usuario

En la segunda maquetación se define el contenido del sistema de control de noticias la cual se puede ver en la figura 4.

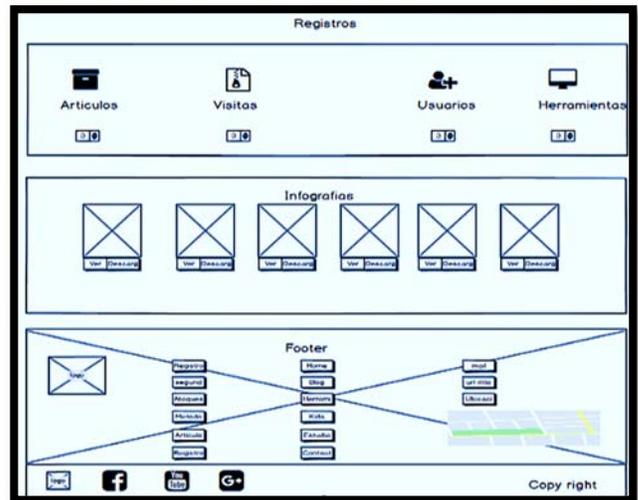


Figura 4. Maquetación del Menú del Sistema de control de Noticias. Diseño Propio.

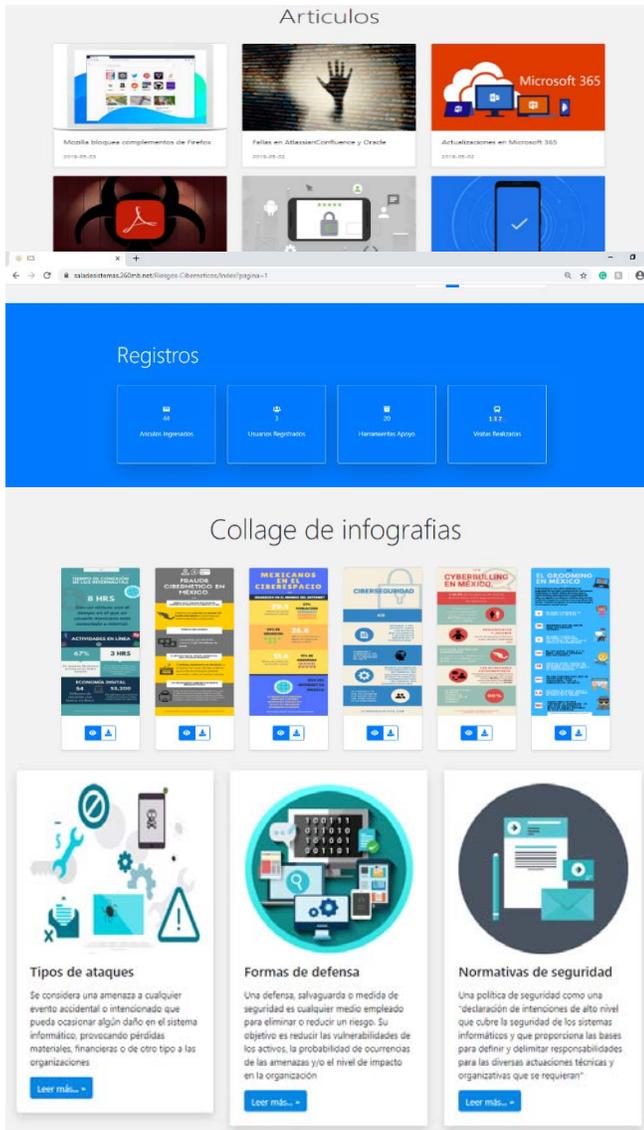
Para la construcción del portal considerando el análisis y diseño con base en las maquetaciones, casos de uso, actores involucrados se obtienen los siguientes resultados del portal el cual se encuentra actualmente en la fase de pruebas para que se pueda colocar dentro del Portal Institucional teniendo así ya un dominio que lo identifique con el ITTLA.

Una vez definida la estrategia, el desarrollo del sistema se realizan las siguientes etapas: Planeación del proyecto, Entrevistas con el cliente, Recopilación de información, Identificación de necesidades y requerimientos, Identificar alcances y limitaciones, Análisis de información, Desarrollo de casos de uso, Maquetación, Diseño de las interfaces

- Configurar servidor
- Crear base de datos
- Programación y configuración de BD con interfaz
- Realización de la documentación
- Implementación y pruebas.

Finalmente se muestran los contenidos del portal haciendo énfasis en el sistema de noticias el cual se encuentra en su fase de pruebas para iniciar con la implementación en la figura 5 puede verse la pantalla de inicio del portal, la cual incluye los elementos indicados en la maquetación correspondiente al menú principal.

En la siguiente figura 6, se muestran los apartados de: administrador de usuarios, altas de noticias y altas de herramientas. el inicio, muestra el usuario logeado y maneja un submenú (cerrar sesión, chat (dirige al portal de inicio de sesión del administrador del chat en línea, para lo cual igual debe de contar con el usuario y contraseña para los accesos), barra de búsqueda.



Fuente: Elaboración propia

3. CONCLUSIONES Y RECOMENDACIONES

Como resultado de la investigación y elaboración del portal web el cual está dirigido a difundir información acerca de revistas, páginas web, libros y noticias sobre la ciberseguridad, es posible concluir que hoy en día la cantidad de personas que utilizan el internet va en ascenso al igual que los riesgos que esto conlleva al tener que proporcionar en algunos casos información personal o al encontrarse involucrados niños o personas que no tienen el conocimiento para desarrollar este tipo de operaciones de una manera segura.

Las personas necesitan tener el conocimiento de los riesgos siendo esta la función de la página la cual es brindar ayuda e información de una forma sencilla y didáctica para las personas de todas las edades cuenten con información acerca de la ciberseguridad y su importancia ya que se les brinda información, consejos donde pueden consultar un apartado en

el cual los usuarios pueden pedir ayuda a un asesor este será un residente y/o experto del área de Ciberseguridad ya que dentro del Departamento de Sistemas y Computación se ofrecen talleres de Ciberseguridad además de que se les está preparando dentro de la especialidad en materia de seguridad, además de que cuentan en todo momento con el apoyo de los docentes especializados en el área de Ciberseguridad.

La importancia de establecer el estándar para presentar las noticias apoyara en la forma en que los usuarios pueden ver la información ya que en ocasiones no se presenta la información a todo tipo de usuarios debido a que necesitan para obtenerla un correo institucional o de una organización, el mantener el portal contrae un compromiso institucional de permanencia de actualización de la ciberseguridad además de la selección de materiales por lo que en este momento se esta probando el manejo y selección de noticias además de que se esta estableciendo el contacto con la Policía Federal ahora Guardia Nacional, para poder realizar convenios institucionales para proporcionar talleres de ciberseguridad con el apoyo de residentes y docentes del plantel.

En lo que respecta a la selección de noticias se va a considerar los indicadores siguientes de acuerdo con lo que indica [9]: quienes de entre un listado inicial de 37, de medios participantes en The Trust Project han seleccionado ocho indicadores de confianza que son los siguientes:

1. Mejores prácticas. ¿Cuáles son los principios del medio? ¿quién lo financia? ¿cuál es su misión? Implica, además, la inclusión del código ético, el compromiso por la diversidad, el rigor, las correcciones y otros estándares.
2. Experiencia del periodista: ¿Quién escribió este artículo? Información sobre el autor, incluyendo su trayectoria y los artículos publicados.
3. Tipo de trabajo: ¿A qué género periodístico pertenece el artículo? Etiquetas que distinguen los textos de opinión, de análisis o publicitarios de las noticias.
4. Citas y referencias: ¿Cuál es la fuente? Para historias de investigación o en profundidad, acceso a las fuentes detrás de los hechos y las afirmaciones.
5. Métodos de trabajo: ¿Cómo se construyó? También para historias en profundidad, información sobre por qué los reporteros decidieron seguir una historia y cómo abordaron el proceso.
6. ¿De origen local? Identificar cuándo la historia surgió en un lugar sobre el que el medio cuenta con un profundo conocimiento sobre el contexto local o de la comunidad a la que se dirige.
7. Diversidad: ¿Cuál es el compromiso de la redacción por aportar perspectivas diversas?
8. Comentarios de los lectores: Verificar las opiniones de los lectores y generadores del artículo

Para el desarrollo de este se investigó en la parte del marketing digital como una estrategia para integrar información al usuario buscando orientar la información hacia este y que se familiarizara con la estructura mediante la usabilidad, funcionalidad, sin ser complejo. Ofreciendo al usuario un ambiente agradable mediante los recursos en ese momento se tienen en el ITTLA.

Finalmente es importante indicar que el portal aun esta en pruebas por lo cual solo se dio a conocer a los estudiantes del Instituto quienes apoyaron con sus observaciones y pruebas de funcionalidad e incluso desarrollaron simuladores de ransomware con el lenguaje Python, con la realización de las pruebas se están considerando lo que indican [7] y [8], al integrar a estás los siguientes cuestionamientos: ¿El Sitio web es responsive?, ¿Cuál es la frecuencia de publicaciones?, ¿Hay un calendario editorial?, ¿Rankeamos en la primera página de Google?, ¿Qué palabras nos posicionan? ¿Se actualizan diariamente?, ¿Cuál es el índice de participación? ¿Cuántos suscriptores se tienen?, ¿Cuánto es el tráfico de visitas?, ¿Qué tipo de artículos son los más visitados? ¿Cuál es el tiempo de permanencia del visitante?

Al responder a preguntas anteriores, se pudo observar que aun faltan elementos dentro del portal para que este se de a conocer a todo tipo de usuarios por lo que se están realizando las modificaciones necesarias para ello y se espera que para el cuarto mes del 2020 se hayan completado las observaciones y las propuestas que se dieron para el mismo.

Se utilizaron los dispositivos móviles (Tabletas, Celulares) para realizar las revisiones de funcionalidad en dichos dispositivos móviles en distintos navegadores, los principales fueron Safari, Chrome, Firefox, lo que permitió ampliar la revisión para realizar observaciones y establecer un registro de errores o anomalías y realizar los cambios en las menús y submenús correspondientes si tener que estar buscando o localizando la falla por sí mismo, ya que como mencionaba esta metodología permite apoyarse entre sí y aumenta la productividad de una forma más dinámica.

4. REFERENCIAS

- [1] J.P. Zumba, C. A. León A., “Evolución de las Metodologías y Modelos utilizados en el Desarrollo de Software”, INNOVA Research Journal, Vol 3, No. 10, 20-33. ISSN 2477-9024, Universidad de Guayaquil, 2018.
- [2] J. Cendejas, “Implementación del modelo integral colaborativo (MDSIC) como fuente de innovación para el desarrollo ágil de software en las empresas de la zona centro - occidente en México” (Tesis doctoral). Universidad Popular Autónoma del Estado de Puebla, México. (2014).
- [3] Pressman, J.,” Ingeniería de Software: Un enfoque práctico”, 5a. Edición, Mc Graw Hill, México, 2005
- [4] R. Enriquez G.,”Administración informática de las organizaciones”, Polilibros (UPIICSA), recuperado de: http://www.sites.upiicsa.ipn.mx/polilibros/portal/Polilibros/P_externos/Administracion_informatica_de_las_organizaciones/Ramon_E_Enriquez_Gonzalez/AIO2_Mod_ESPIRAL.html, 2017
- [5] Staff High Tech Editores, Inicia campaña nacional Ciberseguridad México 2019, recuperado de: <https://www.infochannel.info/inicia-campana-nacional-ciberseguridad-mexico-2019,2019>
- [6] Vinculo TIC, Ciberseguridad en las universidades: cómo lograrla, recuperado de: <https://vinculotic.com/educacion/ciberseguridad-universidades-como-lograrla/>, 2019
- [7] Guerra, C. Cómo hacer un plan de marketing digital paso

a paso en 2020, <https://carlosguerraterol.com/como-hacer-un-plan-de-marketing-digital/>, 2019

[8]Chávez, A. ¿Qué tan accesible es tu sitio web? Si la respuesta es “no tanto”, dejas ir estas oportunidades, <https://www.merca20.com/que-tan-accesible-es-tu-sitio-web-si-la-respuesta-es-no-tanto-dejas-ir-estas-oportunidades/>, 2019

[9] Pino García, Gabriela, Aguilar Barajas, Ismael, & Ayala Gaytán, Edgardo Arturo. (2018). El papel de la confianza en proyectos de innovación colaborativa. Propuesta teórico-metodológica. Economía, sociedad y territorio, 18(58), 629-655. <https://dx.doi.org/10.22136/est20181219>

[10] Ediciones el País, ¿Qué es The Trust Project?, <https://elpais.com/estaticos/que-es-the-trust-project/>,