UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO Y DESARROLLO DEL SITIO WEB "CIBERCULTURA EN CIBERSEGURIDAD: AHORA Y SIEMPRE"

TESIS

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

P R E S E N T A N

MENDOZA RODRÍGUEZ LUIS ALBERTO

TREJO LUNA EVA MARION SHANIK

DIRECTORA DE TESIS

ING.MAGDALENA REYES GRANADOS

Ciudad Universitaria, Cd. Mx., 2022

Agradecimientos

Trejo Luna Eva Marion Shanik

A mi profesora y directora de tesis.
Ingeniera Magdalena Reyes Granados por ser una docente dedicada, que sabe transmitir el conocimiento y el gusto por aprender, por su paciencia y consejos en la realización de este proyecto.

A mis docentes.
Ingeniero Héctor Hernández López, que me ayudó a tener confianza en mí misma en las materias de Ciencias Básicas puesto que hubo materias que no lograba entender y me motivó a no rendirme, pero sobre todo a persistir. A la M.C. Jaquelina López Barrientos por el amor y entusiasmo con el que imparte clases, que además forma parte de diversos proyectos en favor de la Comunidad de la Facultad de Ingeniería, gracias por su ayuda en el desarrollo de esta tesis, a la M.C Cintia Quezada Reyes y al Ingeniero Edgar Martínez Meza por ayudarnos en el alojamiento web, por los comentarios, sugerencias y correcciones de los manuales desarrollados, a los docentes de las materias de Ingeniería en Computación, puesto que gracias a sus conocimientos y consejos fuimos capaces de dar lo mejor de nosotros mismos para entregar a la Comunidad de la Facultad de Ingeniería el presente trabajo y sitio web.

A mi madre y familia.
Mamá eres el pilar de mi vida, siempre estás ahí para apoyarme y motivarme todos los días de la vida a ser una mejor versión de mi misma, sabemos que la vida nunca ha sido fácil para nosotras, pero sin importar el reto o la adversidad siempre caminamos juntas al futuro. Gracias por acompañarme en este sueño, a Malo que siempre se quedó conmigo largas horas cuando tenía que hacer tarea, proyectos y estudiar para los exámenes, por ser mi apoyo emocional. A Gerardo Alberto Esparza Ramírez por ser un hombre asombroso que siempre está presente en nuestras vidas de una u otra forma, gracias por tu calidez humana, por hacer reír a mi mamá y ser nuestro apoyo.

A mis amigos.
Estoy sumamente agradecida de haber realizado este recorrido por la Facultad de Ingeniería con ustedes, logramos hacer equipos de trabajo fantásticos, nos apoyamos mutuamente dándonos consejos, explicando temas que no lográbamos entender en clase, por las risas y la motivación.

Mendoza Rodríguez Luis Alberto

A mi profesora y directora de tesis.
Ingeniera Magdalena Reyes Granados, gracias por brindarme la oportunidad de crecer personal y académicamente dentro del área de redes y ciberseguridad. Sin su ayuda, su conocimiento y consejos este proyecto no hubiera sido posible. Estoy muy agradecido por haber sido su alumno durante mi estancia en la Facultad de Ingeniería.

A mis docentes.
Ingeniero Marco Antonio Guerra Arce gracias a sus clases, conocimientos transmitidos en el aula de clases, a su paciencia y a su manera de incitar a sus alumnos a ser mejores, a investigar y a darle soluciones a los problemas, eso me ayudó mucho a mejorar en el área en la que me estoy especializando. A la M.I. Elizabeth Fonseca Chávez, por enseñarme a nunca rendirme ante las situaciones complicadas, a dar el mejor esfuerzo a pesar de las circunstancias y también a ser autodidacta. A la M.C. María Jaquelina López Barrientos, quien me brindó la posibilidad de poder cursar mi Diplomado en Ciberseguridad. Y, por último, pero no menos importante, a todos los docentes que tuve a lo largo de mi licenciatura, les agradezco por su esfuerzo y conocimiento.

A mis padres.
Mamá, papá, les doy las gracias por su enorme amor y apoyo incondicional hacia mí, les agradezco por siempre estar conmigo, por estar a mi lado y apoyarme siempre que lo necesitaba. Doy gracias por tener a unos padres como ustedes, gracias a ustedes soy quien soy ahora, con su amor he logrado alcanzar muchas metas. Ustedes son mi motor para seguir adelante, son mi ejemplo por seguir y siempre me motivan a ser una mejor persona, a esforzarme y dar lo mejor de mí, a conseguir mis metas, a ser una persona humilde y respetuosa. Gracias, mamá y papá.

A mis amigos.
Amigas y amigos, muchas gracias por estar conmigo durante toda la licenciatura. Gracias por todos los momentos inolvidables que pasamos, por todas las risas, bromas, momentos de estudio juntos, salidas y buenas convivencias. Les agradezco por hacer que el tiempo que pasamos en la facultad haya valido mucho la pena, espero verlos en el futuro como los exitosos ingenieros e ingenieras que seremos.

Prólogo

Internet en términos técnicos es una red de redes, es decir, es el conjunto de computadoras y dispositivos que se interconectan entre sí intercambiando información de manera global, en términos culturales es un lugar en el ciberespacio en donde surgen diferentes tipos de comunicaciones y relaciones, ambos son el resultado de la unión de esfuerzos de personas capacitadas que desde 1960 han generado un nuevo paradigma tecnológico que ha ido evolucionando y ha adaptado la vida de las personas creando una hiperconectividad de individuos, empresas, computadoras y dispositivos electrónicos que constantemente están generando información.

En el ciberespacio surgen diferentes tipos de sociedades o comunidades de personas que se dedican a generar, desarrollar y difundir conocimiento a través de las tecnologías de la información, cabe destacar que el desarrollo de dichas tecnologías es impulsado por los contextos sociales, institucionales, económicos, culturales, políticos, religiosos entre otros.

A nivel cultural las principales capas que dieron paso creación, desarrollo e innovación de Internet, es la universitaria ya que la cultura de la investigación de la conmutación de paquetes y de ARPANET, la siguiente capa cultural es la de los hackers, personas que vieron el potencial de la innovación tecnológica y se especializaron en el manejo de las tecnologías de la información en el Laboratorio de Inteligencia Artificial del MIT.

Muchos de los desarrollos que han hecho de Internet un proyecto global inicialmente creado por académicos e investigadores es que todos los protocolos en los que éste se basa son realizados en código libre, la razón de que muchos programas se mantengan vigentes es porque existen personas que en una cooperativa global desarrollan, mantienen y perfeccionan diseños (ya sean protocolos, softwares o sistemas operativos) de personas como Linus Torvalds, quien creó el kernel de Linux en 1991 siendo aún un estudiante universitario que publicó su desarrollo de forma gratuita con la condición de que las personas que lo mejoren mantengan el programa como distribución libre.

Retomando las capas culturales, la tercera es la que formó la historia del Internet, en esta se encuentran las personas a las que la vida en la sociedad no les satisfacía y encontraron en Internet otras formas de vivir con mayor libertad, históricamente

esta capa surge entre los años sesenta y setenta con los movimientos contraculturales, generando así comunidades virtuales que aplican los desarrollos de las capas anteriores con una inclinación cultural, política y personal. Ejemplo de esto son las personas que poseen múltiples talentos que los aplican para mejorar la calidad de vida de las personas.

En la última capa se puede apreciar que toda la investigación, desarrollo y aplicación han alcanzado niveles de madurez tecnológica y es aquí cuando los empresarios con una visión de innovación y sabiendo los riesgos que corrían apostaron por implementar estos desarrollos en el plano empresarial para generar recursos económicos basados en la capacidad de innovar de manera: tecnológica, el modelo de negocio y el producto que ofertan, por ejemplo para aumentar la productividad en las empresas hicieron la transición de máquinas de escribir a computadoras y a estas les fueron incrementando sus capacidades tanto de hardware como de software.

Estas capas culturales que generaron Internet lo hicieron con el propósito de liberar sus conocimientos, donde la gran mayoría de ellos los podemos encontrar de manera libre y gratuita, en un inicio Internet estaba pensado para ser una tecnología abierta a todos, controlada por todos, evitando a toda costa la privatización de éste por parte de los gobiernos, en cuanto a la economía, se crearon nuevas condiciones de organización e innovación empresarial que fundaron la base de la nueva economía de las empresas capaces de reorganizarse en redes e innovación en la capacidad de generar nuevas formas de riqueza gracias a la tecnología en la red, es decir, Internet fue el gran impulsor de la industria, la cual en la actualidad es conocida como la Industria 4.0.

Internet permite la interacción y participación creando diversas plataformas que impulsan la innovación, creación expresada a través de las tecnologías de la información y comunicación, ampliando el intercambio artístico, cultural, social e incluso generando una evolución de las expresiones de arte y cultura explotando la creatividad y talento de las personas [1].

El rezago digital en México se debe a factores económicos, empresariales, sociales, culturales ya que el desarrollo tecnológico no ha tenido una mayor inversión e implementación en las principales esferas culturales: académica, social, sobre todo la empresarial puesto que son pocas las medianas, pequeñas y microempresas que han implementado las tecnologías de la información y comunicación en pro del desarrollo tecnológico.

En un esfuerzo que llevó décadas de política para impulsar el acceso y uso de las tecnologías de la información y comunicación, los países de América latina y el Caribe lograron en 2016 la implementación de estas tecnologías en actividades comunes en la sociedad, como son el acceso a servicios de telecomunicaciones, uso de dispositivos móviles con acceso a diferentes aplicaciones, incluyendo las redes sociales, otras políticas relevantes en temas como la educación, salud y gobierno electrónico.

Gran parte de la sociedad mexicana ha podido adaptarse y generado las nociones de la cibercultura, no obstante, existe una brecha tecnológica digital por zonas geográficas, en donde la zona mayormente beneficiada es el centro del país, lo que significa que en la zona suroeste y la región norte tienen un fuerte rezago en el uso de las tecnologías de la información y comunicación.

La implementación de estas tecnologías en sectores estratégicos como la educación, salud e industria ha tenido ciertos roces puesto que las personas no se adaptan a ellas o no se encuentran lo suficientemente motivadas para utilizar estas tecnologías, esto es conocido como una interferencia natural entre el comportamiento de las personas y el objetivo que desean lograr, lo que significa que: "La intención de aceptar o rechazar una tecnología en particular se basa en una serie de compensaciones entre los beneficios percibidos del sistema para el usuario y la complejidad de aprender o usar el sistema. (Haryaka, Agus, Kridalaksana, 2017, pág. 375)", la cita anterior es apreciable en nuestra sociedad, pues existen personas que por diversas situaciones no logran incorporar estas tecnologías debido a el grado de dificultad en cuanto a comprensión o de efectuar ciertas operaciones, por lo que las personas optan por seguir haciendo uso de métodos o herramientas que saben que obtendrán el resultado esperado, por lo que es evidente el poco aprovechamiento del Internet en nuestro país, reflejo de diversos factores socioeconómicos, que evitan que las personas de escasos recursos accedan a la sociedad de la información al no contar con los recursos necesarios para poseerlos, por ende no todas las personas gozan de los beneficios que ofrece la cibercultura, mientras que otras personas utilizan las tecnologías de la información de forma cotidiana, puesto que poseen los medios para acceder a ellas pero eso no significa que todas las personas las usen correctamente.

La educación en México ha sido uno de los sectores más favorecidos por estas tecnologías, pero también ha sido uno de los más descuidados, puesto que la educación digital está entorpecida por la desigualdad de condiciones de los estudiantes, puesto que muchos tienen acceso a una computadora o dispositivo con Internet para enriquecer su educación, por otro lado existen estudiantes que no

poseen los recursos necesarios, o no poseen los conocimientos necesarios para utilizar dichas herramientas digitales, lo que a largo plazo tiene un efecto negativo en el desempeño de dichas personas en su entorno social y laboral, perdiendo oportunidades laborales contra personas capacitadas en el uso de las Tecnologías de la Información y Comunicación (TIC) [2].

En la Facultad de Ingeniería de la UNAM se buscó el apoyo de los alumnos de todas las carreras y semestres para conocer su nivel de cibercultura de acuerdo con la encuesta titulada como "Cibercultura en la Facultad de Ingeniería (UNAM)" que tuvo como objetivo analizar las Fortalezas, Oportunidades, Debilidades y Amenazas a los que nuestra comunidad está expuesta al hacer uso de las Tecnologías de la información, tanto en su vida académica como personal, cabe destacar que en el "Anexo 1. Cuestionario", se muestra la estructura general de dicha encuesta realizada en el 2020, por lo que se optó por diseñar y desarrollar un sitio web exclusivo que aborde los temas anteriores por parte del Área de Redes y Seguridad de la Facultad de Ingeniería, el cual contendrá materiales y recursos propios que ayuden a la comunidad de la Facultad e incluso a la sociedad, a desarrollar una cibercultura con procedimientos, metodologías, herramientas y tips que los protejan dentro de Internet.

Índice

Capítulo 1. Internet como fenómeno cultural y tecnológico 11
1.1 Conceptos básicos 12
1.2 Vulnerabilidades, amenazas y ataques en Internet 15
1.2.1 Principales vulnerabilidades y sus clasificaciones 16
1.2.2 Amenazas 20
1.2.3 Ataques 23
1.2.4 Principales fraudes con la identidad digital 27
1.2.5 Clasificación de víctimas digitales 29
1.2.6 Riesgos de ser una víctima digital 37
1.2.7 Retos de la cibercultura 37
Capítulo 2. Análisis y diseño del sitio web 39
2.1 Metodología de diseño web 40
2.1.1 Paleta de colores 41
2.1.2 Estilos de tipografía 45
2.1.3 Imágenes 46
2.1.4 Iconos 48
2.1.5 Menús y submenús 49
2.2 Boceto del diseño del sitio web 52
Capítulo 3. Propuesta y desarrollo del sitio web 74
3.1 Consideraciones de las amenazas presentes 2020-2021 75
3.2 Herramientas de desarrollo web 79
3.2.1 Lenguajes de programación 80
3.2.2 Herramientas de programación (Editores e IDES, Frameworks, Arquitectura, NuGet, API y plugins) 82
3.3 Tipos de Hosting 91
3.4 Migración del sitio web al servidor Linux 94
3.4.1 Servidores web (IIS Express, Kestrel, Apache y Apache como proxy reverso) 94
3.4.2 La importancia de MariaDB en el desarrollo del sitio web 96
3.4.3 Elementos adicionales al sitio web para su correcto funcionamiento en el servidor 97
3.4.3.1 Archivo de configuración de VirtualHost 98
3.4.3.2 Certificado de autenticación 98

3.4.3.3 Archivo de servicio 100
Capítulo 4. Resultados y Mantenimiento 103
4.1 Pruebas del sitio web 104
4.2 Resultados 115
4.3 Respuesta a la hipótesis 117
4.4 Liberación del sitio web 118
Conclusiones 119
Anexos 121
Glosario de términos 122
Cuestionario 131
Boceto del diseño del sitio web 135
Manual de creación del sitio web “Cibercultura en la Ciberseguridad: Ahora y Siempre” 162
Manual del usuario final 210
Fuentes de información 232

Capítulo 1. Internet como fenómeno cultural y tecnológico

1.1 Conceptos básicos

A lo largo de este trabajo de investigación, se utilizarán diversos conceptos relacionados al tema de la ciberseguridad, los cuales sirven para explicar el trabajo que realizan los usuarios a través de las aplicaciones integradas en los diferentes dispositivos que están conectados a Internet. Es posible que las personas los utilicen de forma cotidiana sin aprovechar por completo su potencial e incluso que desconocen la existencia de las múltiples clasificaciones que comprenden el mundo de la ciberseguridad, las cuales se describen a continuación.

Ciber

Componente inicial de la mayoría de las siguientes definiciones, proviene del griego Kybernetes, que significa timonel, es decir, la persona que gobierna una nave. El término Cibernética del cual proviene este prefijo fue utilizado por primera vez en una novela, por el escritor Norbert Wiener, en 1948, dicha novela hablaba del papel que tendrían las máquinas en un futuro en cuanto control de procesos, es por ello por lo que el prefijo indica que algunos conceptos tienen una relación con Internet [3].

Cibernética

Ciencia que estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos [4].

Ciberacoso (ciberacosador y ciber acosado)

El ciberacoso es la acción que realiza una persona (ciberacosador) a otra (ciber acosado) de hostigar mediante el uso de las tecnologías de la información y comunicación [5].

> Existe otro tipo de acoso denominado **grooming** que es el ciberacoso sexual a menores de edad.

Ciberactivista (Hacktivista)

Persona que utiliza las tecnologías de la información y comunicación para participar activamente en la difusión de medidas y acciones enfocadas a lograr cambios en el área de su interés personal [6].

Ciberactivismo

Es el conjunto de técnicas de comunicación que emplean personas (ciber activistas), mediadas por el ciberespacio y su tecnología, permitiendo la dedicación intensa a

una determinada línea de acción en la vida pública, en el área social, política o religiosa, mediante el logro de una comunicación más rápida, mayor difusión y una gran audiencia [7].

Ciberarma

Es la implementación de medidas, técnicas, procedimientos e instrumentos o dispositivos con el objetivo de realizar funciones ofensivas o defensivas (según sea el caso) que se materialicen en un ataque con la finalidad de causar un daño intencional, generando la destrucción de bienes, violencia hacia un grupo específico de personas, disfuncionalidad o disrupción, temporal o permanente, de redes, sistemas, equipos, funciones, servicios o instalaciones, o que atente contra intereses, derechos o libertades.

Ciberataque

Ofensiva, agresión o acción realizada en perjuicio de valores, personas, bienes, sistemas o servicios, mediados por el ciberespacio y su tecnología.

Ciberespacio

El Ciberespacio es un entorno virtual de interacción siendo un espacio-sistema relacional, se dice que es relacional porque existe siempre y cuando se dé un intercambio de información a través de dispositivos tales como computadoras de escritorio, laptops, teléfonos inteligentes, entre otros, creando enlaces de comunicación mediante las aplicaciones que utilizan dentro de dichos dispositivos para entablar una comunicación.

Es claro que en este espacio virtual se llevan diversos tipos de comunicaciones (intercambio de información), las cuales son de tres tipos diferentes: la primera se da entre dispositivos, la segunda es intercambio de información entre seres humanos y dispositivos, por último, se encuentra el intercambio de información de seres humanos con seres humanos a través de aplicaciones.

Ciberespacio e identidad

Las personas tienden a asumir personalidades distintas dependiendo de la situación en la realidad como en el mundo virtual, lo cierto es que en este ciberespacio cada usuario asume una nueva identidad en donde se realiza una transformación de una persona a un ser informacional en donde la esencia, presencia y existencia unifica a la representación informática siendo un conjunto de datos que interactúan con otros datos [8].

Cibercultura

El término Cibercultura representa a diferentes movimientos culturales que se han ido gestando con la evolución de las tecnologías de la información y comunicación sobre el espacio, la realidad, las relaciones humanas y sociales [9].

Según Lévy el Ciberespacio se entiende como la red, Internet es una red conformada por otras redes, estas emergen de la conexión global de las computadoras y dispositivos conectados a la red, la cultura es el resultado de las creaciones de los seres humanos basados en diversas técnicas materiales e intelectuales, prácticas, actitudes, modos de pensar para hacer crecer el ciberespacio mediante conexiones y dispositivos.

Es por ello que Internet de acuerdo con Lévy es la esencia de la Cibercultura puesto que es el ciberespacio propicio para la creación de una "inteligencia colectiva", donde una comunidad de usuarios no solamente recopila información sino que, de manera innovadora, construye, crea, comparte, opina, debate, sugiere, donde sus miembros se interconectan formando así el universo cibercultural que conforma la actual sociedad digital, a pesar de que Internet representa infinidad de soluciones proactivas en favor de la humanidad también hay conflictos de interés dentro de la sociedad digital, en donde los puntos de vista, críticas y contra críticas se hacen presentes [10].

Ciberdelincuencia

Conjunto de actos ejecutados mediante el uso de Internet y su tecnología con el fin de realizar actividades delictivas que atentan contra confidencialidad, integridad y disponibilidad de los sistemas informáticos, las redes y los datos.

Ciberdiplomacia y diplomacia digital

La Ciberdiplomacia es el conjunto de medidas diplomáticas realizadas a través del ciberespacio y mediadas por las tecnologías de la información y comunicación mientras que la diplomacia digital son las medidas diplomáticas que realiza el Estado orientadas a la protección de sus intereses en el ciberespacio.

Cibergeopolítica

Rama de la geopolítica (estudio del territorio y el poder de los países) que toma en cuenta que el ciberespacio constituye un mundo donde la tecnología informática debe ser explotada únicamente por el gobierno local dentro del territorio propio, es decir, que los países que gocen de determinados desarrollos que hagan uso de

Internet vinculados a otra nación (potencia económica rival) posean restricciones al considerarse una violación de la Seguridad Nacional.

Ciberguerra

Lucha con medios, organización y doctrina cibernética, realizada a través de actos cibernéticos de guerra, llevada a cabo entre Estados enemigos con fines políticos irreconciliables o incompatibles, que comporta siempre la posibilidad de una escalada al extremo, una intervención sin límites para alcanzar la victoria y la destrucción del adversario, por medios cibernéticos. Adopta una forma organizada y representa el instrumento último de la política en el ámbito cibernético.

Ciberinteligencia

Es la actividad de obtener y analizar información con el objetivo de identificar, rastrear y predecir las capacidades, intenciones y actividades de los actores hostiles en el ciberespacio [11].

Ciberterrorismo

Son las acciones que ejerce un estado, nación o grupo de personas para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o alteraciones físicas en infraestructuras críticas como son las plantas eléctricas, el sistema de agua potable, sistemas de telecomunicaciones.

Ciberseguridad

La ITU define a la ciberseguridad como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".

1.2 Vulnerabilidades, amenazas y ataques en Internet

En los últimos años los delincuentes han empleado las TIC para cometer crímenes contra países, empresas y personas que son inexpertas en Internet y estas tecnologías, por lo que es muy común que muchas amenazas se difundan a través de la red afectando a otras redes, computadoras y dispositivos con acceso a Internet.

Es común confundir los términos vulnerabilidad, amenaza y ataque puesto que están íntimamente relacionados, en los siguientes subtemas se definirán dichos conceptos, pero se debe hacer énfasis en que la vulnerabilidad es un fallo, debilidad e incluso un agujero en la seguridad de los sistemas operativos, softwares,

aplicaciones o cualquier dispositivo que esté conectado a una red y que puede ser explotado por algún tipo de amenaza que explota dicha debilidad. Un ataque que es el método por el cual la amenaza espera causar efecto en algún elemento de la tríada de la seguridad de la información -CID- (Confiabilidad, Integridad y Disponibilidad) que son los principios fundamentales de la seguridad informática.

1.2.1 Principales vulnerabilidades y sus clasificaciones

Vulnerabilidad

Debilidad o fallo de un sistema de software o de hardware que puede ser aprovechado con fines maliciosos.

Descripción de las diferentes vulnerabilidades

Desbordamiento de buffer

La vulnerabilidad se da cuando una aplicación no es capaz de controlar la cantidad de datos que se copian en el buffer, cuando este se desborda almacena los bytes sobrantes en las zonas de memoria adyacentes, sobrescribiendo su contenido original por lo que este problema puede ser aprovechado para ejecutar código que le otorga al atacante privilegios de administrador.

Condición de carrera

Para cumplir esta condición se deben estar ejecutando varios procesos a la vez sobre un recurso compartido al cual tienen acceso de forma simultánea.
Error de formato de cadena: Error de diseño producido a nivel programación en donde se acepta sin validar la entrada de datos por el usuario.

Cross Site Scripting (XSS)

Esta vulnerabilidad es aprovechada en ataques que permiten ejecutar scripts de lenguajes como JavaScript.

Inyección de SQL

Técnica que hace posible insertar código SQL permitiendo el procesamiento de datos a un código SQL previamente programado.

Denegación de servicio (DoS y DDoS)

Técnica utilizada para impedir que los usuarios no puedan acceder a cierto recurso a través de la red, debido al excesivo consumo de ancho de banda de la red o consumiendo los recursos conectados al sistema informático.

Ventanas engañosas

Técnica que le permite a un atacante mostrar ventanas con mensajes en el monitor de la computadora de la víctima haciéndola creer que ha ganado un premio.

Vulnerabilidades en los dispositivos de red

Router vulnerado

Ocurre por diferentes factores como dejar la configuración inicial, errores en la configuración, contraseñas débiles, falta de actualizaciones de seguridad hasta el secuestro del ancho de banda dando oportunidad a que los dispositivos que se conecten a la red a través de él se infecten y se conviertan en parte de una botnet.

Suplantación de identidad DNS

El ciberdelincuente introduce datos falsos en la caché de resolución de DNS produciendo que los servidores DNS redirijan el tráfico de un dominio específico a la computadora del delincuente, en lugar de redirigirlo al propietario legítimo del dominio.

Falsificación del paquete (inyección de paquetes)

La inyección de paquetes le permite a un ciberdelincuente alterar o interceptar los paquetes de información que son transmitidos entre un emisor y receptor, facilitando el secuestro de una conexión autorizada o denegar la capacidad de una persona para usar determinados servicios de red, esta actividad es conocida como un ataque de **Man In The Middle (MITM)**.

Desde el punto de vista de las redes de comunicaciones también se dan diferentes vulnerabilidades que ponen en riesgo las conexiones a Internet como son los servicios de routing, asignación de direcciones, designación

de nombres y bases de datos, entre otros. Este tipo de amenazas son efectuadas por hackers con fundamentos tecnológicos que hacen uso de herramientas de análisis de paquetes, dispositivos alterados de Access Point (AP) para conexiones inalámbricas es por ello por lo que las redes inalámbricas (WiFi) en especial las públicas representan un riesgo crítico para los usuarios.

Las vulnerabilidades pueden ser clasificadas de acuerdo con el riesgo y la función en la cual surgen, como se puede observar en las tablas 1.1-1.2.

Tabla 1.1. *Clasificación de vulnerabilidades por riesgo [12].*

Riesgo	**Definición**
Crítico	Permite la propagación de amenazas sin que sea necesaria la participación del usuario.
Importante	Es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios y los recursos de procesamiento que ellos dispongan.
Moderado	El riesgo que presenta es sencillo ya que se puede disminuir con configuraciones predeterminadas, auditorías, entre otras.
Bajo	Impacto mínimo a usuarios.

Tabla 1.2. *Vulnerabilidades por función.*

Tipo de vulnerabilidad	Descripción	Ejemplo
Diseño	Debilidad en el diseño de protocolos utilizados en redes y políticas de seguridad nulas o ineficientes.	1. Inyección de paquetes. 2. MitM. 3. Suplantación de identidad DNS. 4. XSS. 5. Inyección de SQL.
Implementación	Errores de implementación, existencia de puertas traseras en software o hardware y descuidos de los fabricantes.	1. Desbordamiento de buffer. 2. Condición de carrera.
Uso: Producidas por el usuario	Configuración inadecuada de las aplicaciones y mala asignación de permisos y privilegios. Error humano. Malas prácticas (uso de contraseñas fáciles de descifrar, desconocimiento y falta de sensibilización de los usuarios y responsables de la seguridad informática).	1. Router vulnerado. 2. Ventanas engañosas. 3. DoS. 4. DDoS.
Día cero	Se da cuando no existe una solución conocida para la vulnerabilidad.	1. WannaCry. 2. Stuxnet.

1.2.2 Amenazas

Amenaza

El Instituto Nacional de Estándares y Tecnologías (NIST) define a una amenaza como "Un evento con potencial de afectar negativamente a las operaciones de una organización o a sus activos, "a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio".

Tipos de amenazas

Adware

Software que utiliza anuncios como propaganda para financiar el programa, en algunos casos es considerado como programa maligno (malware), es común encontrarlo en las versiones gratuitas de ciertas aplicaciones [13].

Amenaza persistente avanzada (APT)

Ataque complejo y de elevado nivel con el objetivo de obtener datos confidenciales durante un largo período de tiempo.

Ataques a algoritmos

Se dan a los diseños utilizados para mejorar el consumo de energía, disminuir las fallas de sistemas críticos y optimizar las eficiencias, puesto que estos datos se pueden rastrear mediante el informe propio de un sistema, como la cantidad de energía que utiliza una computadora, y usar esa información para seleccionar los objetivos o para activar alertas falsas.

Ataque de diccionario

Técnica que consiste en la creación de un archivo que contiene una lista con palabras, frases y las contraseñas más fáciles de utilizar y recordar, probándola con el objetivo de descifrar la clave de acceso de los usuarios.

Ataque de fuerza bruta

Es el intento de descifrar un usuario y/o contraseña con el método de prueba y error utilizando diferentes combinaciones de frases, letras, palabras y números.

Botnet

Red de dispositivos infectados que tienen conexión a Internet, utilizados para cometer ciberataques coordinados y sin el conocimiento de sus dueños.

Carding

Copiado de las tarjetas de crédito de la víctima para realizar posteriormente una adquisición de bienes con estas [14].

Denegación de servicio (DoS)

Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

Denegación de servicio distribuido (DDoS)

Es un DoS que envía las peticiones desde diversos orígenes, de esta forma es más efectivo, complicado de detener y determinar su origen.

Gusano

Malware que se instala en la computadora y se copia a sí mismo en otros equipos.

Ingeniería social

Es la implementación de técnicas utilizadas por personas para manipular a empleados e incluso otras personas (víctimas estratégicas) a fin de que realice acciones específicas o se sume a la difusión de información que es útil para un atacante.

Keylogger

Hardware o software que registra el pulso de teclas del usuario para capturar en secreto información confidencial, usualmente sin su consentimiento.

Malware

Software diseñado para llevar a cabo acciones perjudiciales y no autorizadas en un sistema de información.

Phishing

Ataque en el que una persona suplanta a una entidad o servicio mediante un correo electrónico o mensaje instantáneo para conseguir información confidencial como lo es la información bancaria y contraseñas de la víctima.

Pharming

Ataque que redirige el tráfico de un sitio web legítimo a uno falso que es manipulado para permitir el robo de información confidencial.

Smishing

El ciberdelincuente intenta obtener información privada a través de un mensaje de texto o SMS.

Vishing

Método donde se le solicita al usuario marcar un número telefónico gratuito que aparenta ser una compañía financiera, la víctima logra caer en la trampa puesto que se imita el servicio bancario utilizando una grabación solicitando que la víctima verifique los datos de su tarjeta de crédito o débito, ingresando mediante el teclado telefónico los 16 dígitos de la tarjeta, fecha de vencimiento e incluso el código de verificación de la tarjeta (CVV o CVC).

Ransomware

Códigos maliciosos diseñados por ciberdelincuentes para bloquear el acceso a los dispositivos electrónicos o codificar los archivos en ellos, para después solicitar a sus víctimas un pago por el "rescate" de su información.

Spyware

Malware que controla la actividad o la información en un equipo sin el consentimiento del usuario y la envía a otra persona.

Stuxnet

Fue el primer malware descubierto apuntando a sistemas industriales y el primero en incluir un rootkit contra controladores lógicos programables, una técnica sigilosa que se basa en la falsificación de información sobre la presencia del código, con el fin de ocultarse.

Troyano

Código malicioso diseñado para ocultarse en el sistema del equipo infectado bajo la fachada de software legítimo.

Virus

Malware diseñado para propagarse automáticamente.

WannaCry

Es un tipo de ransomware, el objetivo de WannaCry es el secuestro de datos por medio de un cifrado y solicitando un pago de rescate en bitcoins con la promesa de devolver los datos, afecta principalmente a los equipos de cómputo con sistema operativo Windows.
WannaCry tiene como objetivo los ordenadores que utilizan Microsoft Windows como sistema operativo. Cifra los datos y exige el pago de un rescate en la criptomoneda bitcoin por su devolución.

Watering hole attack

Ataque basado en la creación de un sitio web falso que busca comprometer uno real, con el objetivo de explotar a los usuarios visitantes.

Zero day attack

Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

Como se puede apreciar en los conceptos previamente mencionados existen diversas amenazas y vulnerabilidades dentro de Internet que atentan contra naciones, empresas y personas, es por ello por lo que resulta de suma importancia explicarlas y clasificarlas.

Las amenazas más comunes que se propagan por Internet son: malware como virus, gusanos, troyanos y ransomware, spyware (keylogger) y adware, ataques de hackers, ataques DoS y DDoS, intercepción o robo de datos y robo de identidad.

1.2.3 Ataques

Debido a que existen infinidad de ciberdelitos que se gestan desde Internet no existe una solución única para contrarrestarlos, pero se pueden clasificar los principales ataques que se aprovechan de las vulnerabilidades e incluso se puede hacer un análisis desde la perspectiva del derecho al uso de las TIC, con dicho enfoque se pueden catalogar los delitos que cometen los ciberdelincuentes utilizando las amenazas y vulnerabilidades del software, hardware y la red.

Ataque

Intento de acceder a dispositivos informáticos o servidores ajenos y sin autorización, mediante la inserción de malware, para alterar su funcionamiento, producir daños o sustraer información sensible.

Definiciones relevantes a la infraestructura física y de red de las telecomunicaciones:

1. **Física**

   Fraude de SIM box

   Uso de las tarjetas SIM por parte de los ciberdelincuentes para enrutar el tráfico entrante a través de voz sobre IP (VoIP) cambiando los metadatos de operadores arbitrarios e incluso evitar procesos legítimos de aplicación de la ley como escuchas telefónicas y órdenes de producción.

   IRSF (Fraude internacional de ingresos compartidos)

   En este fraude intervienen dos grupos de delincuentes. El primer grupo hace el lavado de dinero y el segundo facilita el fraude real a través de acciones nefastas.

   Prepago

   Dadas las características de las tarjetas SIM de prepago se multiplican las posibilidades de movilizar los ingresos ilegales.

2. **De red**

   Hackeo de PBX

   Uso no autorizado por atacantes externos de una red telefónica privada utilizada dentro de una empresa.

   Fraude de suscripción

   Pagar por servicios prestados por terceros sin que el dueño haya realizado ninguna acción.

   Wangiri

   El usuario recibe una llamada y cuelgan. Con este método de fraude la máquina marca automáticamente a muchos números de diferentes personas, pero cuelga en los primeros sonidos.

Al perder la llamada, la víctima podría devolver la llamada, lo que genera una facturación inmediata al tratarse de números con tarifas especiales, que repercute en ganancias hacia los estafadores. Y mayor será la ganancia dependiendo del tiempo que la víctima permanezca en línea.

En la tabla 1.3 se puede observar los tipos de ataques que se aprovechan de las vulnerabilidades más conocidas.

Tabla 1.3. *Tipos de ataques.*

Tipo	Daño	Ejemplo
Interrupción	Atenta contra la disponibilidad de algún recurso de la red para los usuarios que hacen uso de él.	1. DoS. 2. DDoS. 3. Ransomware. 4. WannaCry. 5. Stuxnet
Intercepción	Acceso no autorizado a la información almacenada en el sistema o incluso de la información que se está transmitiendo por la red a otros usuarios de esta.	1. Desbordamiento de buffer 2. Inyección de paquetes.
Modificación	Intercepción y manipulación de la información sin tener un acceso autorizado.	1. Inyección de SQL 2. Inyección de paquetes. 3. Ataques a algoritmos.
Fabricación	Diseñado para suplantar ilegalmente un sitio web engañando a los usuarios para ingresar datos personales y confidenciales.	1. Watering hole attack. 2. Phishing. 3. Suplantación de identidad DNS.

Desde el punto de vista de delitos cometidos a través de Internet (ver tabla 1.4) se puede observar el tipo de delito y las aplicaciones de los ataques y amenazas con las que los cibercriminales atentan contra las personas, empresas y naciones.

Tabla 1.4. *Clasificación de delitos comunes en Internet.*

Tipo de delito	Descripción del delito	Ejemplo
Estafa informática	Consiste en realizar una actividad engañosa produciendo un desplazamiento patrimonial en perjuicio de la víctima y obteniendo así un ánimo de lucro.	1. Phishing. 2. Ingeniería social. 3. Carding.
De daño	Son delitos informáticos que consiste en borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin autorización y con un resultado gravoso para el perjudicado.	1. Virus informáticos en general. a. WannaCry. b. Ransomware.
Fraude de telecomunicaciones	Los usuarios de compañías de telecomunicaciones pagan una cuota para obtener diversos servicios como hacer una llamada, enviar un mensaje, navegar por internet, escuchar música, entre otros. El pago de dicho servicio es fácil de interceptar por los atacantes directamente del sistema para beneficio propio. Se podrían clasificar en dos estas amenazas: a través de la infraestructura física de telecomunicaciones, y aquellas que están basadas en la red [15].	1. Robo de WiFi. 2. Vishing. 3. Infraestructura física: a. SIM Box. b. IRSF. c. Prepago. 4. Infraestructura de red: a. Hackeo de PBX. b. Suscripción. c. Wangiri.
Contra la intimidad	Acceso no autorizado a dispositivos vulnerando el derecho a la intimidad a través del apoderamiento,	1. Ciberbullying. 2. Sexting. 3. Grooming. 4. Robo de identidad.

	alteración, uso o revelación de datos personales, conversaciones escritas, e-mails o fotografías de una persona.	

1.2.4 Principales fraudes con la identidad digital

Los fraudes con la identidad digital se han incrementado día a día, siendo un delito que va en ascenso en todo el mundo, de acuerdo con el Banco de México, el país ocupa el octavo lugar en el que se ha incrementado este delito.

De acuerdo a la Home Office Identity Fraud Steering del Reino Unido, se puede definir el robo de identidad como "la recopilación de información relativa a la identidad de una persona con el fin de obtener un fraude identitario, prescindiendo del hecho de que la víctima sea una persona viva o fallecida (...) por lo tanto consiste en la apropiación indebida de la identidad o de cualesquiera otros datos personales (fecha de nacimiento, domicilio, claves bancarias, contraseñas de acceso a redes, etcétera)" [16].

Los principales fraudes con la identidad digital son [17]:

1. Phishing: La estafa consiste en crear un sitio web falso extremadamente similar al de algunas empresas legítimas (Watering hole attack). A través de mensajes vía correo electrónico, WhatsApp o SMS, los delincuentes envían un enlace, solicitando la confirmación de los datos. Al hacer clic en este enlace, las víctimas son redirigidas al sitio web falso, donde terminan cayendo en la trampa y proporcionando sus datos.
2. Envío de estados de cuenta falsos: Consiste en la creación de recibos falsos en nombre de grandes empresas. Al realizar el pago, la víctima deposita el dinero en la cuenta de los estafadores.
3. Instalación de malware: Ocurre por navegar en sitios web sospechosos o dar clic en enlaces recibidos por correo electrónico y el usuario no es consciente de la descarga de malware que da acceso a terceros a la información personal, privada y financiera del usuario.
4. Robo de datos de tarjetas bancarias: Este tipo de fraude puede ocurrir físicamente, cuando a un usuario le roban su tarjeta; y virtualmente, cuando el consumidor ingrese los datos de la tarjeta en sitios web falsos, no protegidos o no seguros. En posesión de estos datos, los estafadores pueden

realizar compras hasta que el usuario se dé cuenta y bloquee la tarjeta o mediante el uso de Vishing [18].

De acuerdo con la CONDUSEF (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros) el robo de identidad se ha utilizado principalmente para la contratación de créditos o servicios de telefonía celular [19].

Cabe mencionar que existen diferentes vías por las cuales los delincuentes obtienen la información necesaria para efectuar el robo de identidad o el fraude con una identidad falsa: el robo físico de la información, el robo de identidad a través de las TIC y el engaño telefónico o presencial.

Debido a la pandemia del COVID-19 ha aumentado el número de transacciones en Internet, en donde los usuarios han realizado pagos, compras de bienes y servicios y por ende los cibercriminales han incrementado los métodos para cometer fraudes digitales que incluyen la identidad de la persona vulnerada.

A continuación, se muestra un panorama mundial de los ciberataques que han ocurrido durante la pandemia del COVID-19, iniciando con la figura 1.1, cabe destacar que el caso mencionado de ransomware del Hospital Universitario Uniklinik fue recopilado de la página web del periódico Expansión [20].

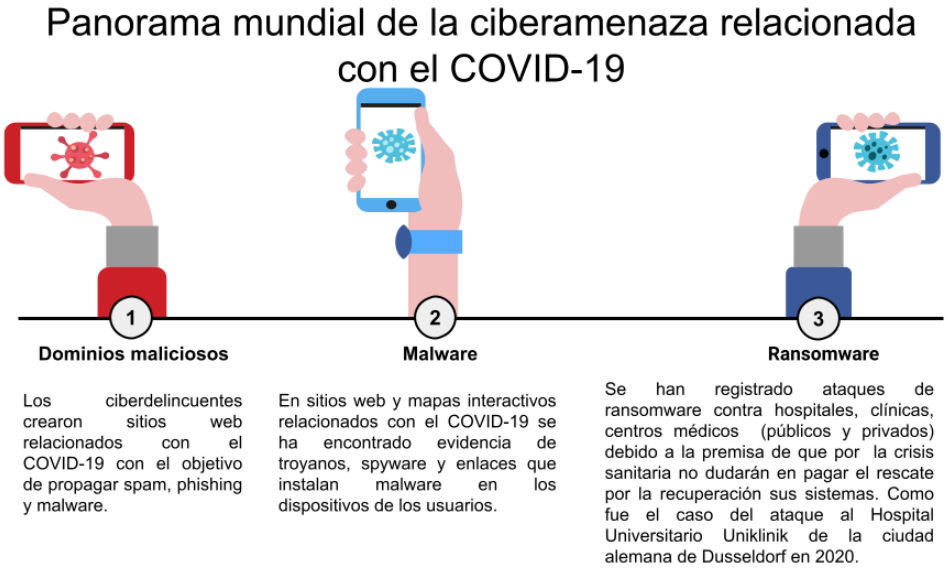


Figura 1.1 Panorama mundial de la ciberamenaza relacionada con el COVID19 [21].

La figura 2.2 muestra algunos de los casos de ciberdelincuencia a nivel mundial por el auge y consumo de ciertas tecnologías en la pandemia, en la infografía se muestran el año de la noticia y las fuentes consultadas para cada caso expuesto, Cybercrime as a Service [22], códigos QR [23], fraude realizado a través de WhatsApp [24] y robo de criptomonedas [25].

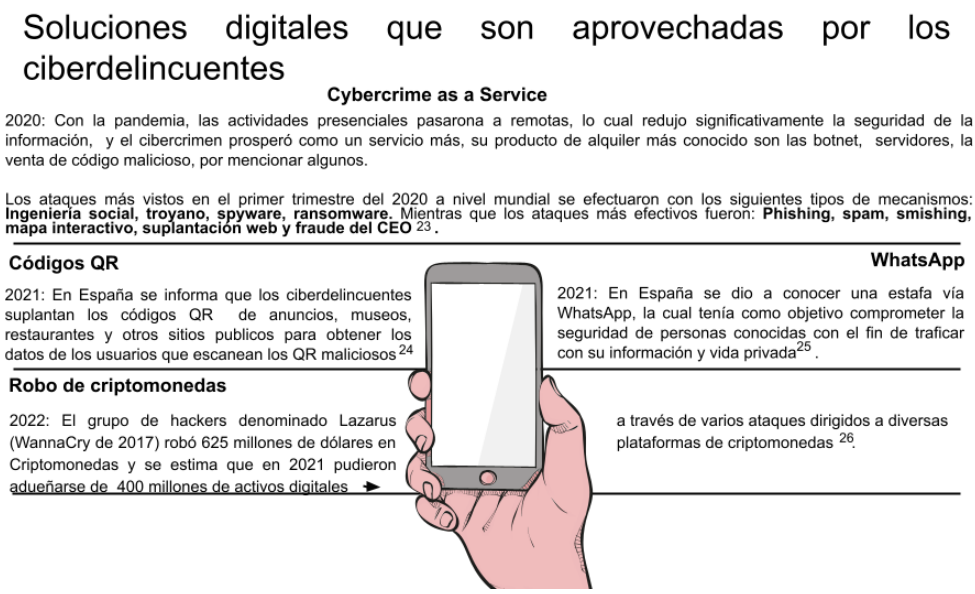


Figura 1.2 Soluciones digitales que son aprovechadas por los ciberdelincuentes.

1.2.5 Clasificación de víctimas digitales

La violencia digital ocurre de diferentes formas, afectando la vida de la víctima dentro y fuera de la red, ya que la masificación de dispositivos con conexión a Internet y uso de las TIC ayudan a la rápida propagación de la violencia contra la persona, la cual se ve afectada física y psicológicamente con daños en diferentes ejes de su vida como la social, económica, familiar, académica, entre otras.

A pesar de que cualquier persona e institución puede ser víctima digital, lo cierto es que el sector que es mayormente afectado es el de la población femenina, el rango de edad en la que sufren este tipo de violencia es entre los 12 y 59 años [26] de edad junto con un grupo de minorías, las cuales son los menores de edad, la comunidad LGBT+ y la ciudadanía en general.

Ciudadanía en general

El Instituto Nacional de Estadística y Geografía (INEGI) posee un Módulo sobre Ciberacoso (MOCIBA) [27] desde 2015, el cual operó en los primeros 3 años de

manera experimental. Cabe destacar que este reporta los casos de ciberacoso mediante un comunicado de prensa, el último fue publicado el 5 de julio de 2021 con cifras actualizadas al 2020.

Las primeras cifras reveladas en el comunicado arrojan los siguientes datos:

- "El 21% de la población de 12 años y más usuaria de Internet fueron víctimas de ciberacoso entre octubre de 2019 y noviembre de 2020".
- Los adolescentes y jóvenes son los más expuestos al ciberacoso.
    - 23.3% de hombres en un rango de edad de los 20 a los 29 años.
    - 29.2% de mujeres en un rango de edad de los 12 a los 19 años.
- Las causas de ciberacoso predominante en mujeres fueron insinuaciones o propuestas sexuales con un 35.9%.
- El ciberacoso a los hombres surgió mediante el uso de identidades falsas en un 37.1%.
- Los lugares donde fue más predominante el ciberacoso registrado fueron Colima (27.4%), Tabasco (26.9%) y Tlaxcala (26.4%).

A continuación, se muestran los porcentajes de ciberacoso sufridos por la población de acuerdo con su género.

Población femenina encuestada

1. Insinuaciones o propuestas sexuales (35.9%).
2. Contacto mediante identidades falsas (33.4%).
3. Recibir mensajes ofensivos (32.8%).

Población masculina encuestada

1. Contacto mediante identidades falsas (37.1%).
2. Recibir mensajes ofensivos (36.9%).
3. Recibir llamadas ofensivas (23.7%).

Categorías de ciberacoso

De acuerdo con los datos arrojados por MOCIBA [28] en 2020 se pueden obtener algunas categorías relevantes que reportaron mujeres y hombres que sufrieron ciberacoso como: la situación de ciberacoso, identidad del acosador y los efectos en la víctima, los cuales serán abordados en el siguiente tema.

En las situaciones más comunes se encuentran las siguientes:

1. Mensajes ofensivos.

2. Llamadas ofensivas.
3. Publicación de información personal.
4. Críticas por apariencia personal o de clase social.
5. Insinuaciones o propuestas sexuales.
6. Suplantación de identidad.
7. Contacto mediante identidades falsas.
8. Rastreo de cuentas o sitios web.
9. Provocaciones para reaccionar de forma negativa.
10. Recibir contenido sexual.

A continuación, se muestra una figura comparativa de las situaciones experimentadas durante 2020.

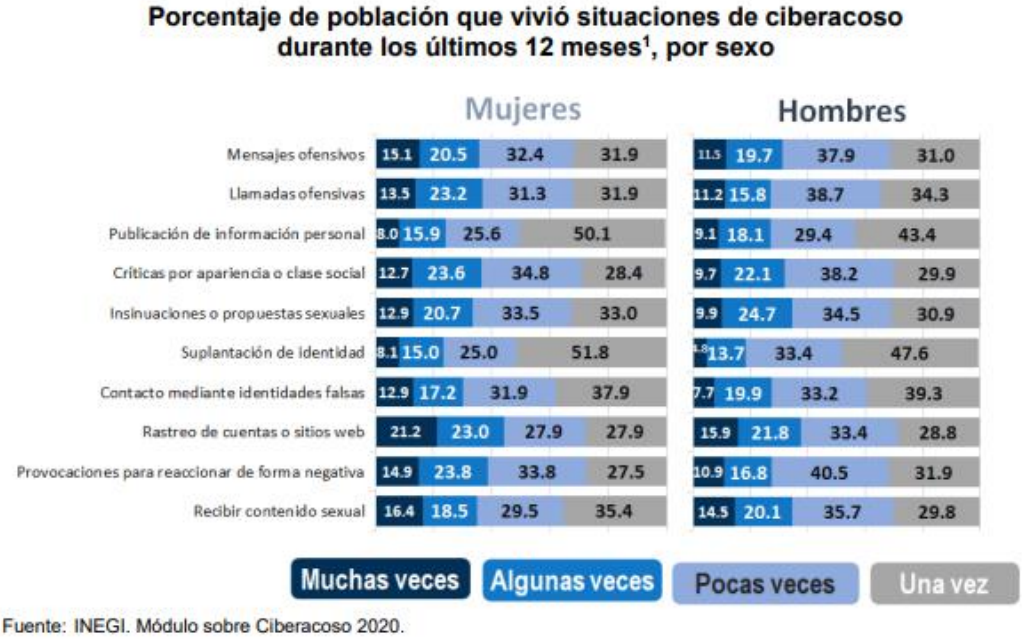


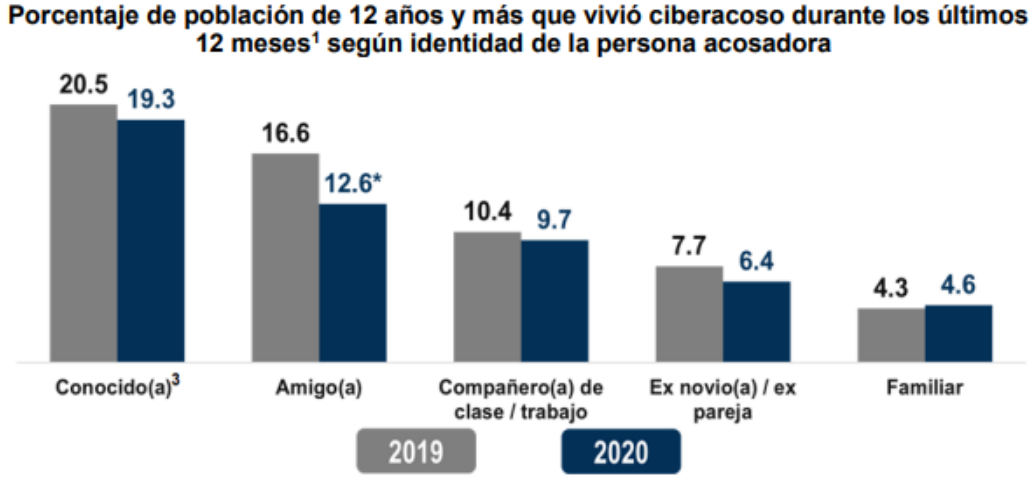
Figura 1.3 Categorías de ciberacoso en porcentaje por sexo.

La identidad del ciberacosador:

1. Exnovio(a) o expareja.
2. Familiar.
3. Amigo(a).
4. Compañero/a de clase o trabajo.
5. Conocido o conocida de:
    a. poco trato.
    b. de vista.
6. Desconocido.

7. No se logró identificar.

Esto se puede observar en la figura 1.4, en la cual se hace una comparativa del MOCIBA de 2019 con el actual de 2020.



[1] La información se refiere al periodo de octubre de 2019 a noviembre de 2020.

[2] Incluye las opciones de respuesta *Exnovio(a) / expareja*, *Familiar*, *Amigo(a)*, *Compañero(a) de clase / trabajo*, *Conocido(a) de poco trato* y *Conocido(a) solo de vista*.

[3] Incluye las opciones de respuesta *Conocido(a) de poco trato* y *Conocido(a) solo de vista*.

Figura 1.4 Identidad del ciberacosador.

Los efectos que causan el ciberacoso son los siguientes:

En mujeres es enojo (68%) y desconfianza (38.4%) mientras que en hombres son los mismos efectos con porcentajes diferentes, el enojo posee un 58.8% y la desconfianza 32.3%.

Mientras que la acción tomada con mayor frecuencia es bloquear a la persona, cuenta o página (70.1% acción tomada por mujeres y 52.9% en caso de los hombres) seguida de no contestar o ignorar llamadas o mensajes (25% mujeres y 35.4% hombres).

Cabe destacar que las mujeres que son candidatas políticas también sufren violencia digital, de acuerdo con la investigación "Violencia política a través de las tecnologías contra las mujeres en México", realizada por la organización Luchadoras, en las elecciones de 2018 hubo violencia política ejercida hacia mujeres candidatas durante las elecciones, 85 agresiones asociadas a las tecnologías, de las cuales 62 fueron hacia candidatas; en 24 estados del país. Estas

cifras sólo son las que fueron denunciadas públicamente, ya sea a través de medios de información de circulación nacional o local, o ante alguna de las instancias con competencia de atender y sancionar violencia política contra las mujeres a nivel federal o local.

De las denuncias que las mujeres levantaron referían en porcentaje las siguientes formas de violencia:

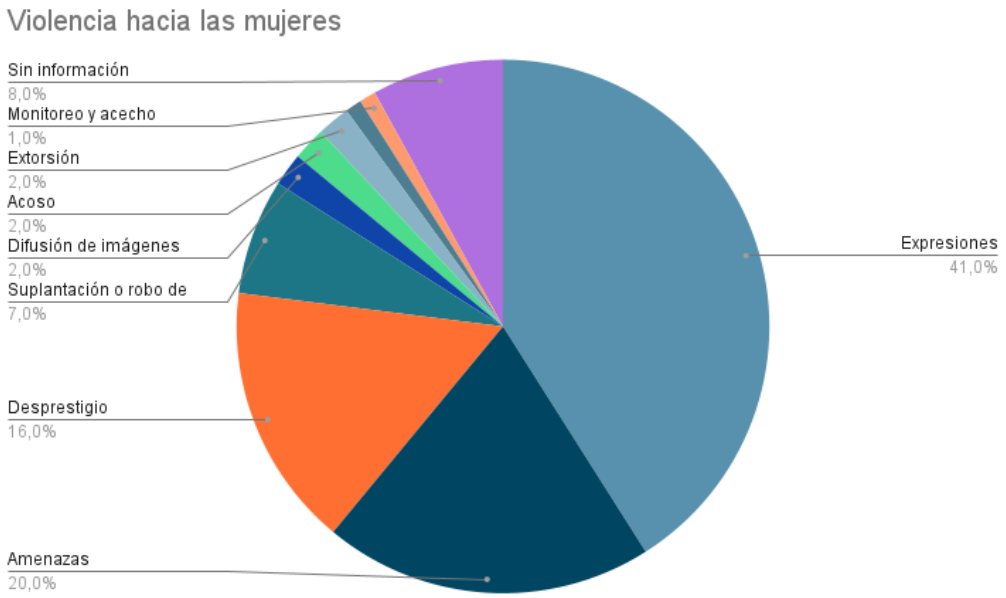


Figura 1.5 Tipos de agresiones.

Los agresores de las candidatas políticas suelen ser, en porcentaje:

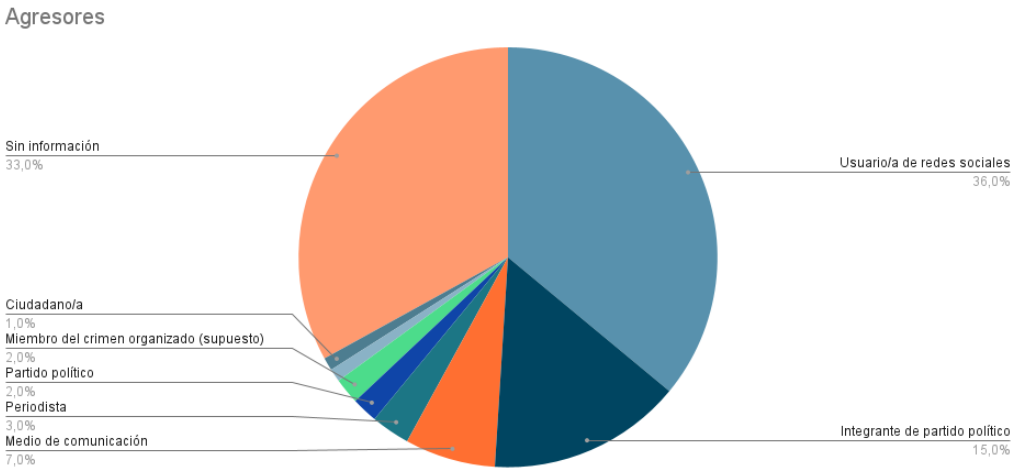


Figura 1.6 Clasificación de agresores a candidatas políticas.

De acuerdo con las elecciones llevadas a cabo en 2021 se reportan 21 feminicidios de candidatas políticas durante el proceso electoral donde en conferencia de prensa la Observatoria Ciudadana Todas MX resaltó que han sido las más violentas [29].
Los principales retos a los que se enfrenta la ciudadanía en general actualmente son:

1. Fake news (noticias falsas que provocan la desinformación de la población).
2. Suplantación de identidad: Al navegar en Internet se hace uso de la identidad digital, con ella es común que en redes sociales se publiquen datos personales que pueden ser utilizados por otra persona que se haga pasar por el usuario dueño de la información personal y realice acciones negativas como:
    a. Difamar, amenazar y acosar a otras personas.
    b. Realizar transacciones bancarias no autorizadas.
    c. Adquirir beneficios de programas de apoyo que ofrece el gobierno.
    d. Realizar compras de productos y adquisición de servicios.
    e. Solicitar créditos financieros e hipotecarios.
    f. Cometer delitos.

3. Trata de personas: Las personas buscan que las víctimas caigan en un gancho, comúnmente iniciando una relación amorosa por redes sociales o con ofertas de trabajos muy buenas para explotarlas laboral o sexualmente.
4. Sextorsión (sexo extorsión): Una persona de confianza podría solicitar fotos o vídeos de carácter sexual para que posteriormente de manera intencional, tratar de sacar provecho a través de la extorsión, inicialmente intimidando para que se le envíen más fotos o vídeos e incluso podría presionar para conseguir algún beneficio económico.
5. Ventas ilegales en Internet: La compraventa de productos y servicios a través de Internet ofrece múltiples beneficios, pero también se incrementa el riesgo de fraudes en línea e incluso se puede cometer un delito al adquirir productos que son ilegales con consecuencias legales, como son las piezas arqueológicas, arte sacro y especies en peligro de extinción.
6. Fraudes cibernéticos de carácter financiero como:
    a. Suscripciones gratuitas, que pueden contener códigos maliciosos al recibir sus boletines.
    b. Comunicados falsos, con el objetivo de confundir a los usuarios.
    c. Correos alarmantes para obtener información personal y financiera.
    d. Servicios gratuitos (smishing) en el cual ofrecen premios al entrar a un enlace fraudulento.
    e. Correos Spam de personas desconocidas con archivos maliciosos.
    f. Ofertas atractivas que suelen ser irreales y pueden derivar en robos.

g. Páginas apócrifas (phishing) donde solicitan donativos o información [30].

Otra vertiente de la violencia de género se da en la discriminación que sufren las personas pertenecientes a la comunidad LGTB+ puesto que son víctimas dentro y fuera de las TIC, sobre todo en México, que desde 2018 se plantea la falta de datos específicos sobre la homofobia en redes sociales en el país [31].

El factor común que posee la violencia de género son los discursos de odio que se esparcen por Internet, los cuales se identifican como [32]:

1. Machista y misógino.
2. Homofóbico y LGBTIQ-fóbico.
3. Antifeminista.
4. Anti-género.
5. Racista.

Figura 1.7 Espacios de discriminación y violencia.

Menores de edad

En la Convención sobre los Derechos del Niño, se reconoce en el artículo 17, que las niñas, niños y adolescentes tienen derecho al acceso a la información y material procedentes de diversas fuentes nacionales e internacionales. Es preciso cuidar de la infancia y adolescencia puesto que existe en la red y las TIC datos o medios que pueden afectarlos de diferentes formas; retomando el informe de MOCIBA perteneciente al INEGI muestra en el periodo de julio-agosto de 2018 a julio-agosto de 2019, dentro de la población entre 12-19 años, que un 32.7% de mujeres y un 28.1% de hombres reportaron haber sufrido algún tipo de ciberacoso [33].

Situaciones comunes que enfrentan los menores de edad en línea:

1. Contenido nocivo o inapropiado.
    a. Drogas.
    b. Racismo.
    c. Terrorismo.
    d. Uso ilegal de armas de fuego.
    e. Trastornos alimenticios.
    f. Pornografía.
    g. Violencia.
2. Retos en línea: Invitación a realizar un desafío o duelo de una actividad peligrosa a través de las redes sociales, que en muchas ocasiones pone en riesgo la vida de quien lo realiza.
3. Ciberbullying.
4. Sexting: Es antesala de delitos como la pornografía infantil, abuso sexual y la trata de personas.
5. Grooming: Desde un acercamiento lleno de empatía y/o engaños se pasa al chantaje más violento para obtener imágenes comprometidas del menor y, en casos extremos, pretender un encuentro en persona. El daño psicológico que sufren niños, niñas y adolescentes atrapados en estas circunstancias es enorme.
6. Pornografía infantil.

Las consecuencias de estos abusos cometidos por otras personas afectan a las mujeres, menores de edad, a miembros de la sociedad y la comunidad LGTB+ en diferentes aspectos de su vida que desencadenan diferentes impactos como son en su apariencia física, estado de ánimo, problemas psicológicos y financieros e incluso afectando su entorno social.

1.2.6 Riesgos de ser una víctima digital

La violencia en línea repercute en la vida dentro y fuera de Internet, produciendo diversos efectos sobre la persona que sufre violencia digital, las más comunes son las afectaciones físicas y psicológicas, generando daños en su vida personal, social, académica, laboral entre otras, que limitan el grado de participación de las víctimas en varios aspectos como la toma de decisiones, temas de intereses personales o comunes de la población.

Es por ello que surge la necesidad de analizar las causas y efectos que tiene la violencia digital para las personas que han sido víctimas, en la tabla 1.5 se muestran los diferentes impactos y la descripción del mismo.

Tabla 1.5. *Tipos de impacto al ser una víctima digital.*

Tipo de impacto	Descripción
Físico	Dolor en diferentes partes del cuerpo, comúnmente en cabeza, espalda y estómago, llanto, sudoración, tensión y trastorno del apetito (pérdida o exceso de este).
Emocional	Angustia, baja autoestima, cansancio, confusión, depresión, enojo, estrés, frustración, impotencia, ira, miedo y paranoia.
Financieros	Pérdida de recursos económicos destinados al hogar, familia y autoconsumo.
Otros	Abandono de uso de las TIC, autocensura, auto limitación de movilidad, sensación de un constante monitoreo y/o vigilancia o temor de salir y exponerse, suicidio.

1.2.7 Retos de la cibercultura

Como se ha podido apreciar, la cibercultura surge de las aportaciones humanas que han desarrollado a las TIC e Internet, gracias a todas las personas que utilizan y las hacen crecer mediante desarrollos tecnológicos, económicos, sociales, culturales y políticos.

Es por lo que es preciso resaltar que para cada ámbito se requiere de diferentes esfuerzos, pero el principal es el social, generando conciencia a nivel personal, para

que cada persona desde su trinchera efectúe las medidas que más le favorezcan y desarrollen buenos hábitos dentro y fuera de Internet y las TIC.

Consideraciones que los usuarios deben promover y aplicar mediante la cultura general:

1. Generar una identidad digital responsable: Tomar medidas de seguridad adecuadas para frustrar los intentos de fraude de los ciberdelincuentes. Otro punto importante por considerar es cuidar lo que se sube a las redes sociales ya que no todos son amigos, pero sobre todo se debe de cuidar el tipo de perfil que utilizan los usuarios.
2. Privacidad: Proteger la información que va a ser enviada por canales digitales mediante métodos y técnicas que garanticen que la información no ha sido modificada, alterada o visible por terceros.
3. Educación y valores dentro de la red: Se debe considerar la forma en la que se desea transmitir una idea u opinión, pues sin darse cuenta se puede afectar moralmente a otros usuarios, por lo que se debe de procurar mantener el respeto al interactuar con otros en Internet e incluso por imagen personal ya que se debe recordar que existen casos en donde las consecuencias de ciertos actos afectan en la vida real, como puede ser el daño a la reputación, integridad, pérdida de oportunidades laborales o afectar a alguien más.

De acuerdo con el desarrollo del capítulo 1 es preciso que las personas en su intimidad y en sus esferas sociales, académicas y laborales, junto con el sector empresarial, gobierno local y nacional promuevan mediante la implementación de buenas prácticas que se lleven a cabo dentro y fuera de Internet con el objetivo de proteger la identidad e integridad física y digital de los usuarios.

Capítulo 2. Análisis y diseño del sitio web

Para crear un sitio web se requiere tanto del diseño como el desarrollo web, por ello, se requiere definir estos campos para diferenciarlos. El diseño web es la parte que se encarga de lo visual del sitio web contemplando la experiencia de usuario usando herramientas enfocadas al diseño sin implementar lenguajes de programación, mientras que el desarrollo web proporciona diversas funcionalidades al sitio implementando lenguajes de programación, tales como el uso de gestores web o la conexión con una base de datos.

En el desarrollo web existen dos categorías de programación: front-end y back-end, en front-end se traslada la parte del diseño web a los lenguajes de programación y marcado que utilizan los navegadores web, tales como HTML, CSS, JavaScript, PHP y diversos frameworks, mientras que el back-end se relaciona al desarrollo de las funcionalidades en el servidor que es el encargado de alojar y ejecutar el sitio web [34].

La principal razón de explicar las diferencias de ambas ramas se debe a que las personas suelen utilizarlos como sinónimos, creyendo que el diseño web es todo el proceso de creación web unificando la parte visual y la programación, mientras que en el desarrollo web se cree que es la generación de un sitio web obviando el hecho de que para hacer el desarrollo se requiere partir del diseño web.

Es por ello que en este capítulo se explicará todo el proceso del diseño web que se realizó para iniciar el proceso de creación del sitio web de Cibercultura.

2.1 Metodología de diseño web

La metodología de desarrollo web seguro es el conjunto de procedimientos, técnicas, herramientas y soporte documental, por lo que el sitio web deberá cumplir con los siguientes objetivos de manera sistemática:

- Ser de las mejores aplicaciones en cuanto a:
    - Rendimiento web rápido y responsivo.
    - Creación de contenido.
    - Publicaciones constantes.
    - Monitoreo.
    - Escalabilidad.
- Tener un proceso de desarrollo transparente, respecto a:
    - Maquetación de los elementos de la página web: imágenes, texto, alineación, márgenes, entre otros.
    - Selección de una paleta de colores.

    - Imágenes y material gráfico (deben de tener calidad, ajuste en cuanto a tamaño).
    - Estructura y organización de:
        - Menú (es importante la ubicación del menú con pocos elementos o categorías que permitan desplegarse).
        - Contenido (categorías y subcategorías).
        - Otras variables y/o filtros.
    - Elementos clave de optimización:
        - Velocidad de carga.
        - Imágenes.
        - Caché.
        - Limpieza de la Base de Datos.
        - Posicionamiento en buscadores (SEO).
- El proceso deberá ser estándar.
- La seguridad debe ser un proceso no un producto, por lo que se deberá contemplar la seguridad por fases:
    - Seguro por diseño.
    - Seguro por defecto.
    - Seguro en la distribución.
    - Seguro en las comunicaciones.

2.1.1 Paleta de colores

Para el diseño de la página web se consideraron los colores, estilos de tipografía y logos de la Universidad Nacional Autónoma de México, Facultad de Ingeniería, Laboratorio de Redes y Seguridad y por último el logo del proyecto institucional "Cibercultura en la ciberseguridad: Ahora y siempre" puesto que es un desarrollo exclusivo de estas dependencias.

Se realizó un estudio de la psicología del color para determinar que colores son los ideales para implementar en el diseño, para reflejar el compromiso que se plantea de dar confianza y seguridad dentro de un entorno educativo institucional.

En la Figura 2.1 [35] Se muestra una infografía de los principales colores y el significado que les son atribuidos de acuerdo con la psicología, los cuales pueden ser positivos como negativos, dependiendo del contexto en el que estos se utilizan, por lo que estos significados pueden ser aprovechados por diferentes instituciones académicas y empresas, puesto que los colores son utilizados para reflejar "la personalidad", las creencias y valores de la marca que está representando.

Figura 2.1 Psicología del color.

Al ser un desarrollo institucional, se utilizarán los siguientes colores para el desarrollo general: el header será de color gris claro, para resaltar los colores de los logos de las dependencias y el proyecto, desde el punto de vista de la psicología del color se busca que los usuarios lo asocien con la modestia y la elegancia, tal como lo ejemplifica la siguiente figura.

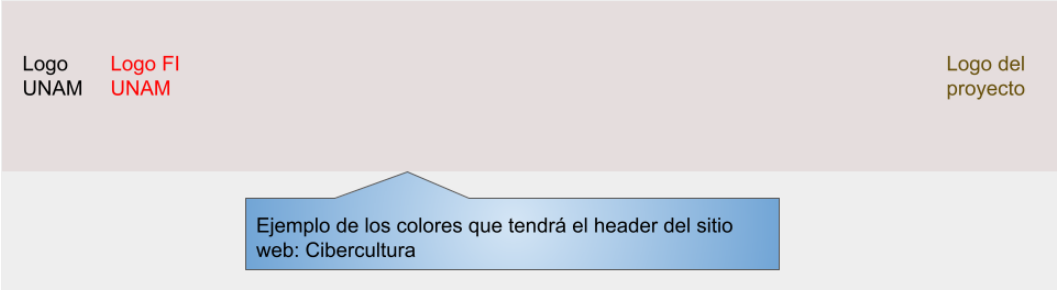


Figura 2.2 Colores del header.

El menú principal estará contenido en un rectángulo blanco con bordes rojos, el blanco se utiliza para dar claridad y simplicidad, mientras que los bordes rojos buscan dar la sensación de dinamismo, tal como se puede observar en la figura 2.3.

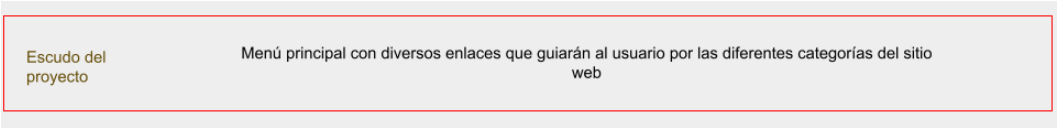


Figura 2.3 Colores del menú principal.

El fondo será blanco debido a que tendrá diferentes elementos visuales que tendrán los siguientes colores: blanco por simplicidad y ligereza, rojo en elementos visuales tales como flechas o círculos de las slides para denotar energía y dinamismo, mientras que en imágenes se utiliza para representar a las y los alumnos de la Facultad de Ingeniería junto con diferentes tonalidades de azul para denotar confianza, honestidad y armonía, principalmente azules fuertes para los marcos de los slides que representan a las diferentes secciones de la página web, gris claro y oscuro, estas tonalidades se utilizan principalmente por ser un color neutro que transmite la sensación de elegancia, modestia y sabiduría, lo que ayuda a mantener un estilo claro y sencillo para los usuarios; las imágenes del sitio web utiliza el color rosa y diferentes tonalidades de color piel, el rosa por contraste al color rojo dándole un toque de delicadeza a las imágenes, reforzando el concepto de mantener las cualidades positivas del color rojo, mientras que los diferentes tonos de color piel para los dibujos de personas se utiliza por la diversidad cultural en cuanto al tono de piel.

Los elementos antes mencionados pueden ser observados en la figura 2.4, en la cual se muestra un borrador inicial del conjunto de elementos mencionados con anterioridad.

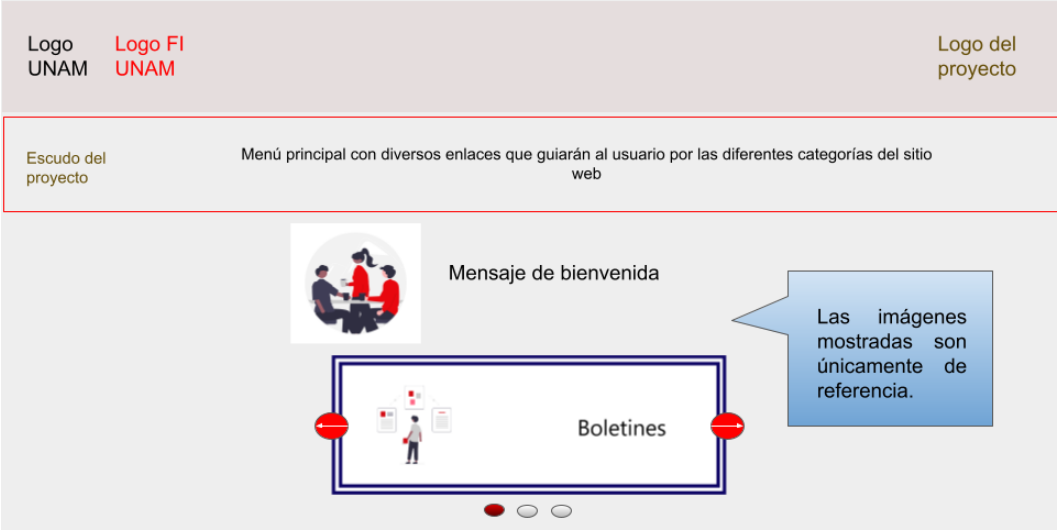


Figura 2.4 Borrador de la página de inicio del sitio web.

Los botones también utilizan la psicología del color ya que los botones azules son utilizados para realizar acciones simples, los botones verdes se utilizan para realizar operaciones permitidas, los rojos son para advertir que después de realizar un cambio no será posible volver atrás, con excepción de los botones de el carrusel y del cambio de página de los materiales, en este caso buscan resaltar las cualidades positivas de dinamismo y energía (como se puede observar en la figura 2.4), los botones amarillos se utilizan para que en caso de realizar cambios el usuario preste mayor atención al detalle. Para ilustrar este punto de la psicología del color se puede consultar la siguiente figura.

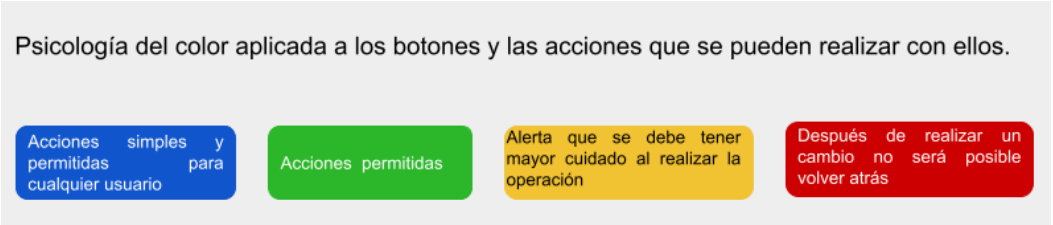


Figura 2.5 Botones y la psicología del color del sitio web.

Por último, se utilizan alertas en colores claros, tales como azul, amarillo, rojo (el rojo claro tiene un mayor parecido al rosa, pero dependiendo del tipo de tipografía y color de esta se puede observar más claramente el tipo de mensaje que se desea transmitir), transparente y verde.

Las alertas transmiten diferentes tipos de mensajes, los cuales están íntimamente relacionados con la psicología del color, por ejemplo la alerta amarilla es sinónimo de atención, la verde transmite que la operación realizada fue hecha de manera

exitosa, la roja es de advertencia, las alertas transparentes buscan resaltar el mensaje así que aunque a plena vista no son apreciadas en código se puede observar claramente, mientras que las alertas azules transmiten tranquilidad y apertura a la comunicación, tal como se muestra en la figura 2.6.

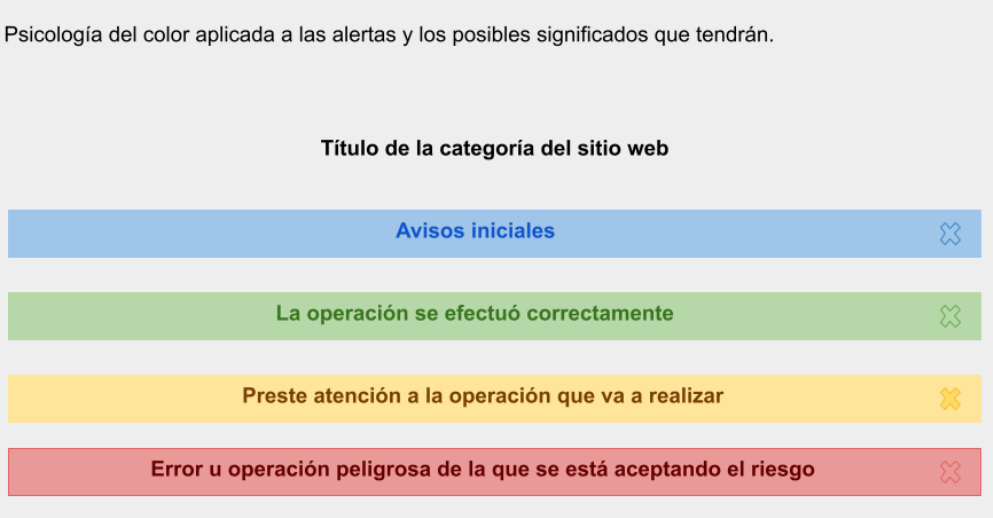


Figura 2.6 Alertas y la psicología del color del sitio web.

2.1.2 Estilos de tipografía

La tipografía es una herramienta clave de diseño, pues gracias a esta junto con la paleta de colores, logos y otros recursos visuales, se logra crear la identidad de la marca que se busca representar, todo esto con el objetivo de reforzar el mensaje que se desea transmitir a la comunidad de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México.

Se definirá a la tipografía como: "El arte de diseñar las letras, pues se denomina así a la disciplina que estudia la representación gráfica de las letras para que el lenguaje escrito sea efectivo" [36].

Como existe la psicología del color, también existe la psicología tipográfica o personalidad de la tipografía, la cual puede hacer que los lectores evoquen conceptos o emociones e incluso refuerzan la transmisión de la identidad visual de una marca, al igual que ocurre con los colores, formas e imágenes.

Variable de peso

Denominada también como variable de grosor, la cual afecta directamente al trazo de los caracteres. Un ejemplo de la variable de peso es la tipografía bold o negrita,

la cual presenta un grosor de trazo mayor, haciendo un mayor énfasis que una tipografía light que presenta un grosor del trazo menor.

Por lo que la tipografía que se utilizará será Arial light para textos del menú y del contenido, se utilizará la bold para resaltar ciertos elementos tales como el título de la sección en la que los usuarios se encuentren y dependiendo del fondo será el color de las letras, por ejemplo, en un fondo blanco, las letras serán negras, mientras que el fondo sea negro o rojo se utilizará una tipografía blanca.

Dentro de las alertas el color de la tipografía deberá ser similar al color de está con el objetivo de reforzar el mensaje, entre los colores que tendrán dichas alertas son:

- Bold: gris oscuro, negro, rojo, azul, amarillo, blanco y verde.
- Arial: amarillo, azul y negro.

Para entender un poco más la importancia de la tipografía, variable de peso y la psicología del color que van a ser parte del sitio web se puede ejemplificar en la siguiente figura.

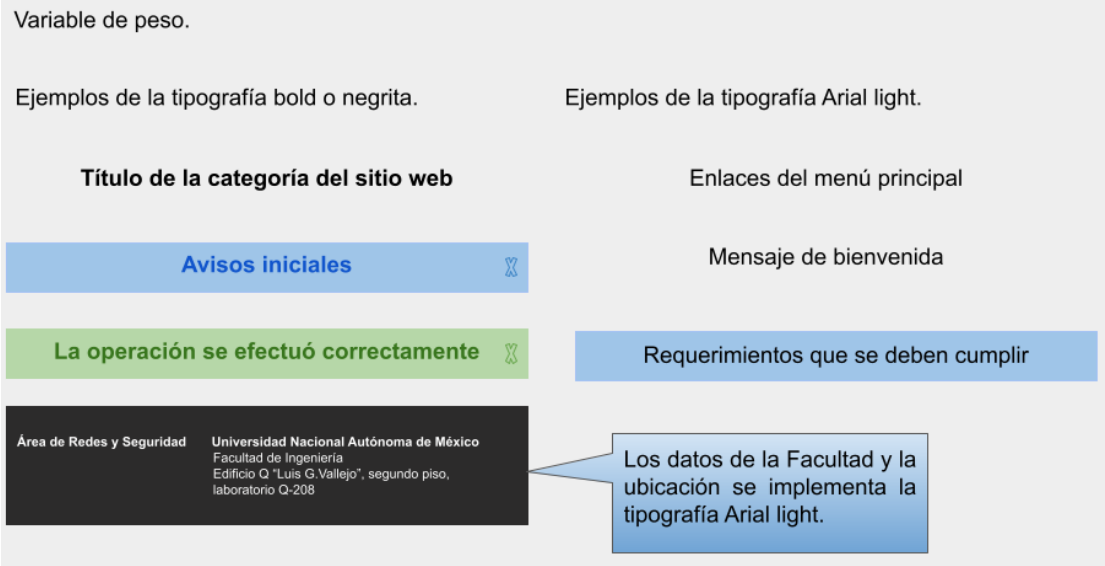


Figura 2.7 Tipografía, variable de peso y la psicología del color del sitio web.

2.1.3 Imágenes

La importancia de las imágenes en un sitio web radica en que el cerebro humano percibe antes una imagen que un texto, si la imagen inicial impacta a las personas, es probable que comience a interesarles más el contenido de la página e incluso que naveguen a través de ella buscando más contenidos interesantes, es por lo que es

necesario integrar imágenes que sean sencillas, pero llamativas en un sentido positivo, adecuadas y de una buena calidad que refuercen el contenido escrito.

De esta forma, y siguiendo la temática de la página web, se deberá contar con una galería de imágenes que muestren adecuadamente las diferentes secciones que han sido creadas.

Por lo que se utilizarán las ilustraciones de unDraw.co la cual es una biblioteca de ilustraciones libres de derechos de autor creada por Katerina Limpisouni, ilustradora que ha diseñado más de 500 ilustraciones de diversas categorías que pueden ser utilizadas sin ningún problema en cualquiera proyecto. Además, sus ilustraciones ya han sido utilizadas por instituciones como Harvard Business School, Google o Microsoft, entre otras [37].

Es importante resaltar que las ilustraciones que se utilizarán de la biblioteca de unDraw.co son sencillas, pues solo se puede seleccionar un color predominante, el cual será el rojo en representación de la Facultad de Ingeniería y los demás colores que pueda contener la ilustración son colores que son seleccionados de manera predeterminada por la diseñadora de las ilustraciones, la cual buscó el equilibrio con el color predominante, en este caso, el rojo, como son el gris claro y obscuro, negro y blanco, entre otros, con los cuales las imágenes dan un aspecto profesional, elegante e incluso minimalista, evitando que las ilustraciones se vean saturadas de elementos visuales, como se muestra en la siguiente figura.

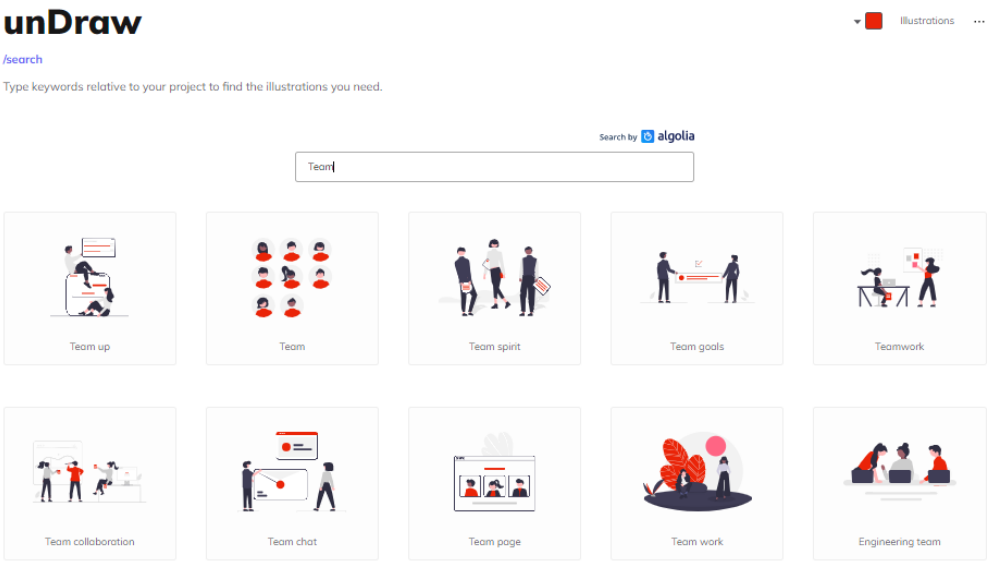


Figura 2.8 Página oficial unDraw.co.

Por otra parte se debe mencionar que de manera implícita se busca lograr mediante las ilustraciones dentro de la página web de “Cibercultura en la Ciberseguridad: Ahora y siempre” mandar un mensaje claro a la comunidad de la fomentación de la igualdad de género, es por ello que en los espacios que se requiera el uso de imágenes para reforzar los mensajes contenidos en la página se utilizarán imágenes de hombres y mujeres trabajando en conjunto, utilizando una paleta de colores en donde predomine el color rojo, pero que se encuentre en equilibrio con los diferentes elementos de las ilustraciones.

2.1.4 Iconos

La importancia de los iconos en el diseño web es comunicar a los usuarios acciones o funciones de forma clara y comprensible, al igual que las imágenes los iconos ayudan a los usuarios a tener una agradable experiencia de usuario.

Es por lo que se utilizará Fontawesome, el cual es un framework de iconos vectoriales y estilos CSS. Este framework es utilizado para sustituir imágenes de iconos comunes por gráficos vectoriales convertidos en fuentes.

De las características más relevantes de fontawesome es que posee más de 400 iconos disponibles, algunos de paga y otros gratuitos, no requiere de JavaScript para funcionar, al tratarse de iconos vectoriales estos pueden ser escalados sin perder su resolución, los estilos gráficos de los iconos se controlan mediante estilos CSS: color, size, shadow, y otras propiedades.

Fontawesome es de licencia libre para uso comercial, originalmente fue creado para ser usado con el framework de Bootstrap, pero es compatible con otros frameworks y/o librerías [38].

En la figura 2.9 se muestra la página oficial de fontawesome con su buscador de iconos disponibles.

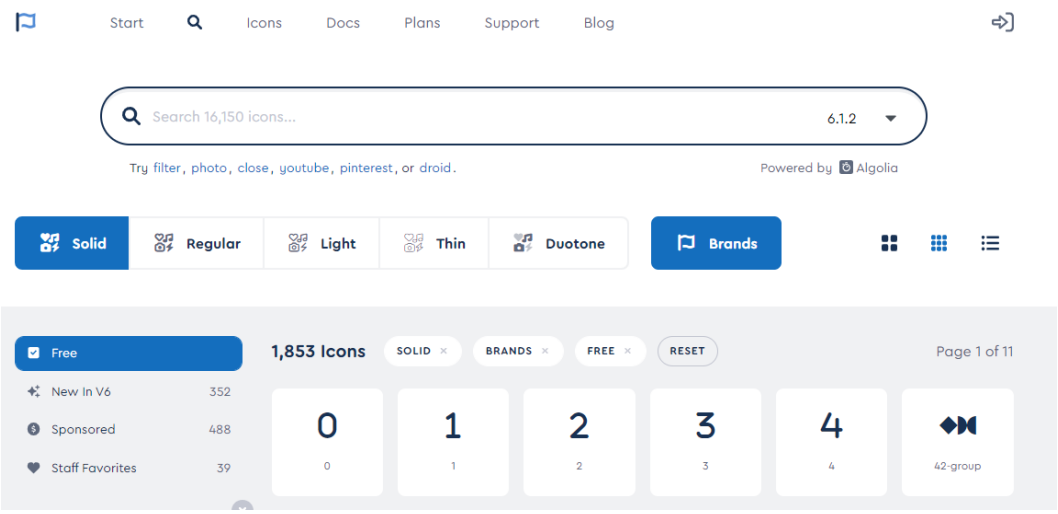


Figura 2.9 Página oficial fontawesome.

2.1.5 Menús y submenús

El objetivo de incluir un menú dentro de una página web es la distribución del contenido en diferentes páginas, para que el contenido sea fácil de encontrar por el usuario brindando una experiencia de usuario satisfactoria.

Para lograr una experiencia de usuario positiva se deben de considerar los siguientes puntos [39]:

- Crear una estructura clara y organizada.
- Categorizar los tópicos principales.
- Usar palabras clave para el título de la categoría.
- Crear submenús para las subcategorías de los tópicos principales.
- Que el usuario pueda moverse fácilmente por las diversas páginas del sitio web.

En cuanto a los submenús se debe considerar el hacer el uso de una sección desplegable dentro del mismo menú principal, dicho menú desplegable difiere en cuanto a la visualización en computadoras que en dispositivos móviles, en el caso de la visualización en computadoras es común encontrar que el menú principal se encuentra organizado en una barra horizontal, mientras que en dispositivos móviles esta barra se colapsa, un elemento común en la visualización del menú de navegación en dichos dispositivos radica que cuando un elemento principal (tópico) posee una flecha señalando hacia abajo sirve para indicar que existe un sub menú oculto y que este aparecerá hasta que el usuario interactúe con el enlace.

Para ejemplificar la importancia del menú principal y los submenús se puede observar las figuras 2.10 y 2.11 vistas desde una computadora, cabe destacar que los submenús tienen los mismos títulos en sus enlaces, pero pertenecen a categorías diferentes.

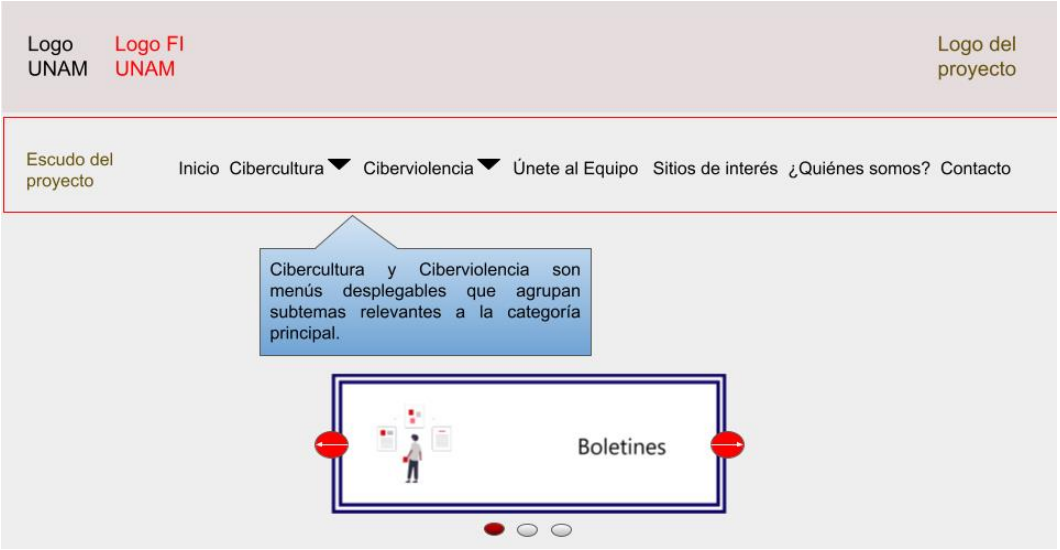


Figura 2.10 Menú principal con submenús.

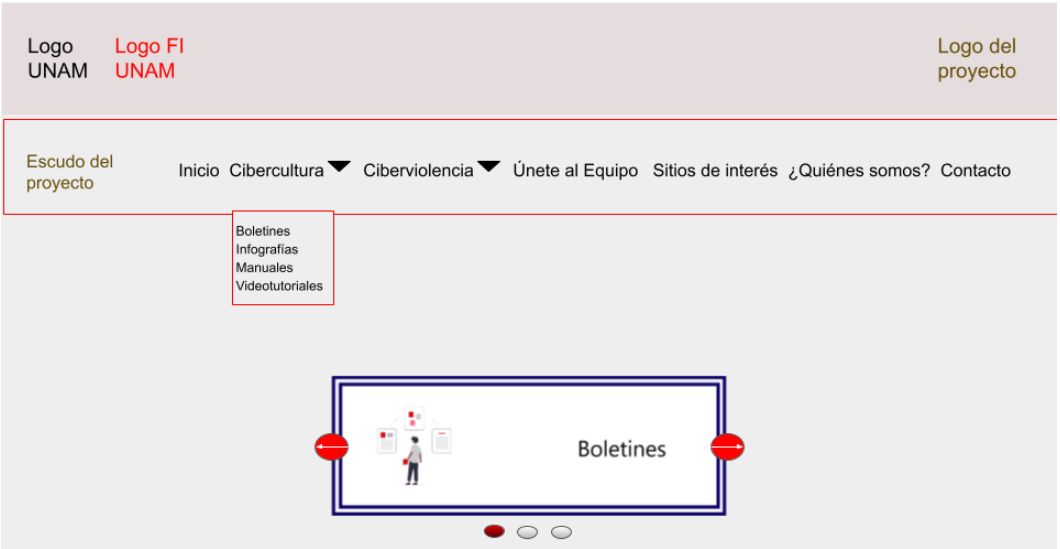


Figura 2.11 Submenú de Cibercultura.

Mientras que las figuras 2.12 a 2.14 buscan ejemplificar la visualización del menú principal y los submenús desde un dispositivo móvil.

En la figura 2.12 se puede observar que la barra del menú se contrajo y los demás elementos visuales se reajustaron a la pantalla, en este caso se pretende simular la pantalla de un smartphone.

Figura 2.12 Menú principal visto desde un smartphone.

En la figura 2.13 se puede observar que al dar clic en el botón se vuelve rojo y muestra los elementos contenidos en la barra de navegación.

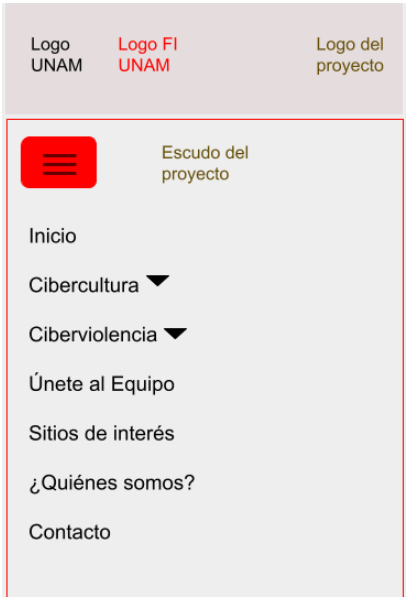


Figura 2.1 3 Menú y submenús vistos desde un smartphone.

En la figura 2.14 se pueden observar los submenús desplegados, mostrando los enlaces respectivos a cada categoría.

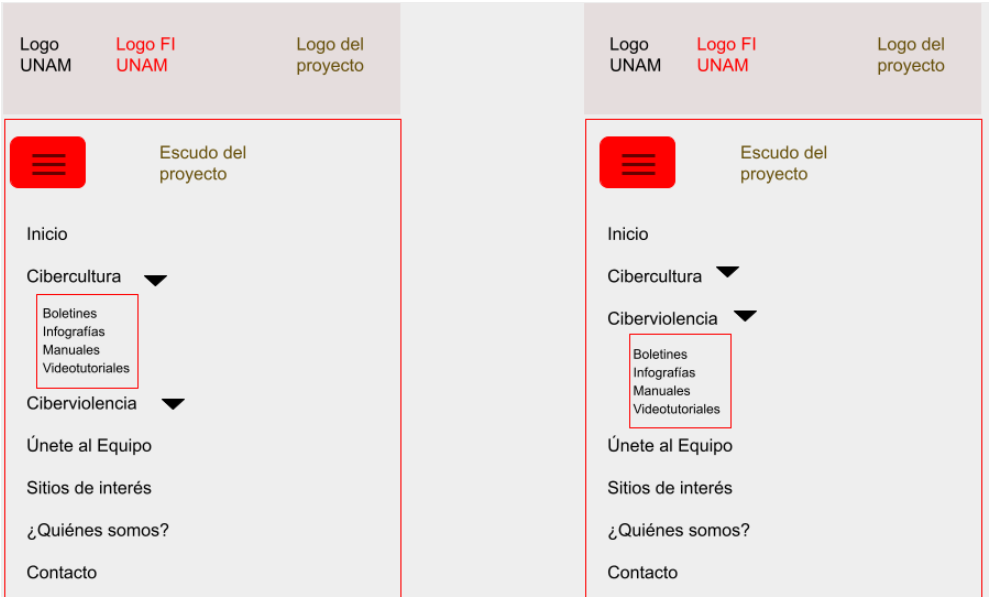


Figura 2.14 Submenús vistos desde un smartphone.

Al explicar la importancia del menú y submenús vistos desde las computadoras y dispositivos móviles se cumple el objetivo de que el sitio web que se va a crear de manera responsiva, por lo que se espera que todos los elementos que este incluya se adapten a la pantalla del usuario final, incluidos los menús y submenús, es por ello que si consulta el sitio web desde una computadora verá una barra de navegación horizontal, dicha barra contará con dos menús desplegables para los usuarios finales, mientras que para la sección administrativa tendrá un total de 4, 2 de los mismos que ve el usuario final y 2 de administración, además de que la barra de navegación no estará anclada a la parte superior de la pantalla, pues se desplazará sutilmente para que el usuario no tenga que subir de nuevo para elegir una opción diferente del menú principal, mientras que si el usuario visualiza la página web desde un dispositivo móvil, encontrará el menú colapsado del lado izquierdo de su pantalla, al hacer clic en el botón ☰ se desplegará el contenido del menú principal como se mostró con anterioridad (figuras 2.10 a 2.14).

2.2 Boceto del diseño del sitio web

A continuación, se muestran algunos bocetos del diseño web, esto debido a que la estructura es similar en varias secciones, por lo que sería muy repetitivo mostrar todos los bocetos creados, si él lector o la lectora desea revisarlos con mayor detalle,

encontrará en la sección de anexos el apartado “Boceto del diseño web” el bosquejo total del sitio web.

Se dividió el diseño en dos secciones diferentes, la primera es la sección de comunidad, en la cual las personas podrán consultar todos los materiales creados en sus respectivas vistas y la sección más importante es la administrativa, esto debido a que en dicha sección el o la administrador(a) podrá subir los materiales creados por el equipo de “Cibercultura en Ciberseguridad: Ahora y siempre” además de gestionar las solicitudes de los interesados en formar parte del equipo, los miembros del equipo y otras acciones.

Nota: Los siguientes bocetos fueron desarrollados con Google Slides y algunos de los íconos que se muestran fueron proporcionados por slidesgo, lo que hace que sean íconos ilustrativos, puesto que al momento de iniciar el desarrollo web algunos de estos íconos no serán iguales a los de fontawesome que son los que se utilizarán.

Sección comunidad: Esta puede ser vista por todos los visitantes del sitio web, en las figuras 2.15 y 2.16 se puede observar el inicio de este desarrollo.

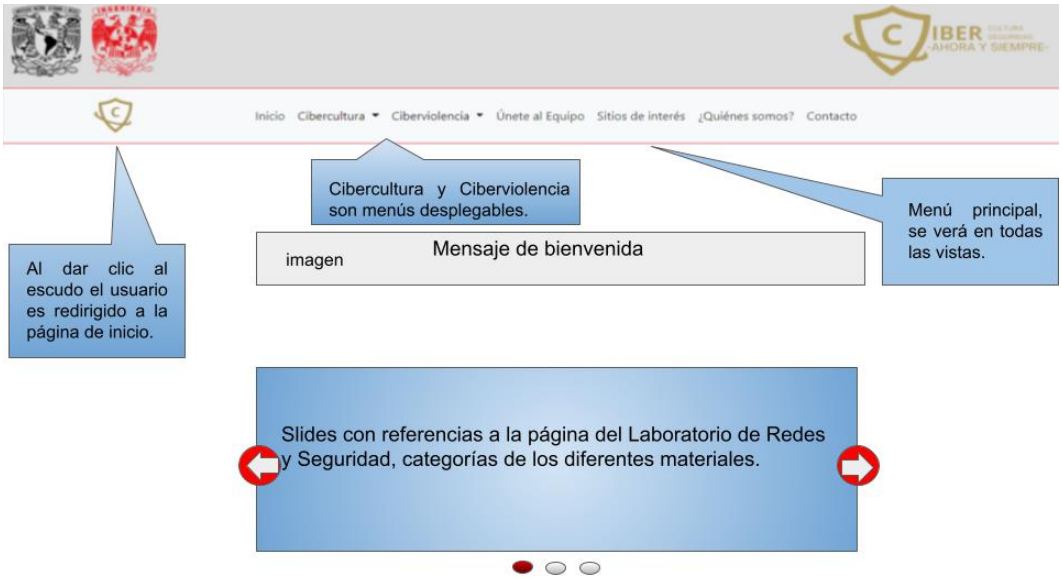


Figura 2.15 Vista de inicio.

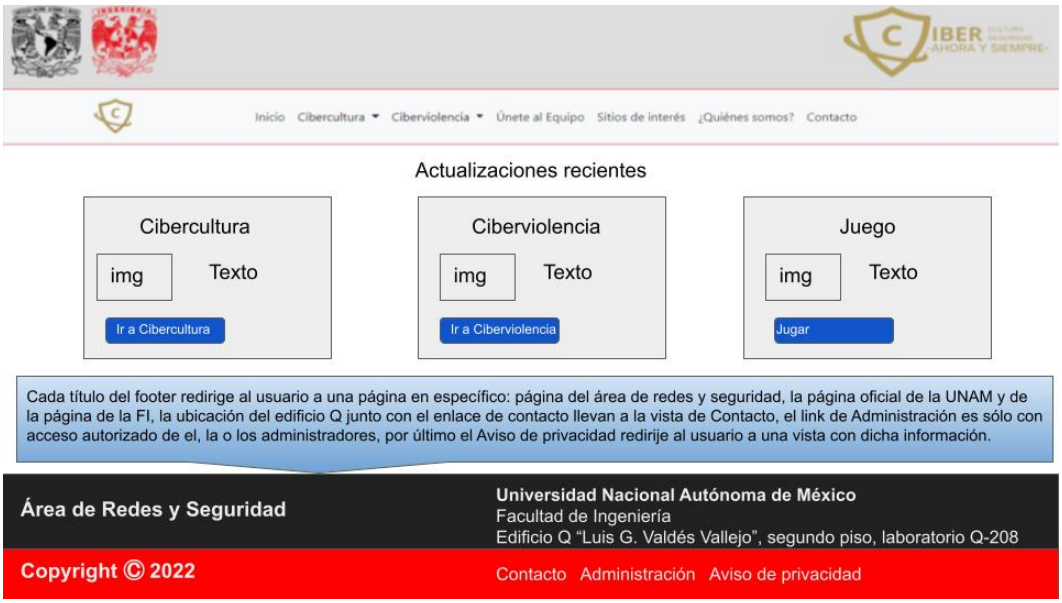


Figura 2.16 Continuación de la vista inicio.

Si el usuario se posiciona en las tarjetas de "Actualizaciones recientes" podrá seleccionar cualquier botón que lo redirigirá a una vista determinada, por ejemplo, cuando el usuario dé clic en el botón de "Ir a Cibercultura" será dirigido al Index de esa categoría, tal como lo muestra la figura 2.17.

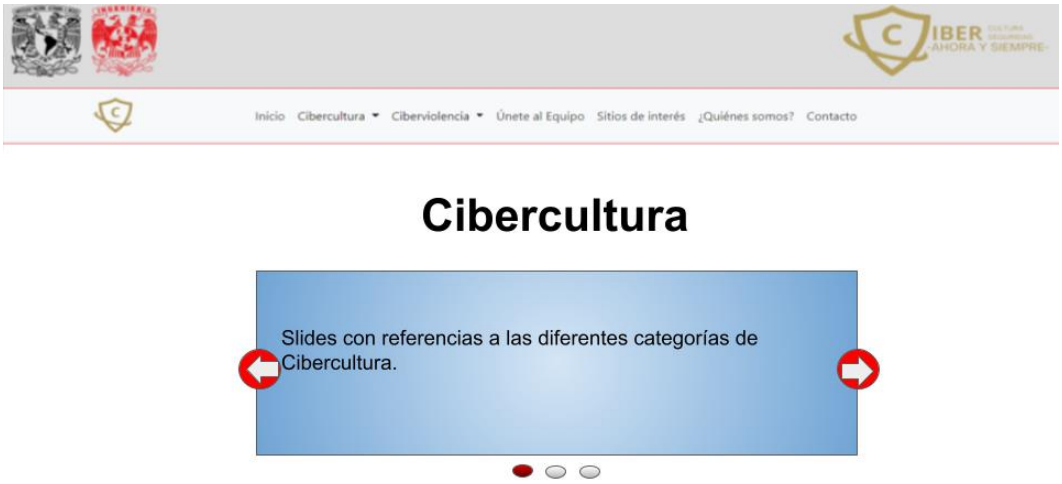


Figura 2.17 Index de Cibercultura.

En caso de que el usuario seleccione dar clic en el botón de “Ir a Ciberviolencia” será dirigido al Index de esa categoría, tal como lo muestra la figura 2.18.

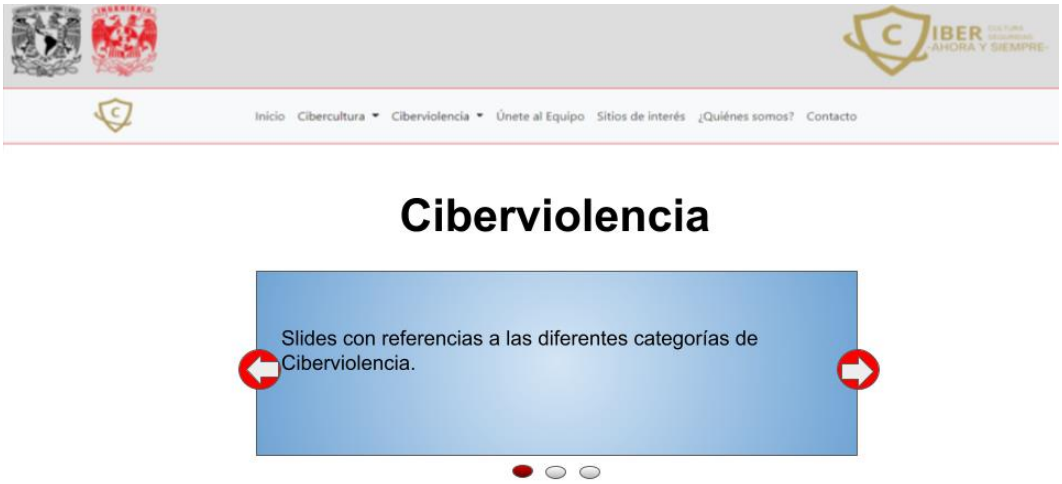


Figura 2.18 Index de Ciberviolencia.

Mientras que, si el usuario da clic en “Jugar”, será redirigido a una vista que muestra que los juegos están en proceso de creación, en cuanto los juegos sean terminados serán colocados en una vista similar a la figura 2.19.

Figura 2.18 Vista de Juegos.

Menús desplegables y sus subcategorías

Regresando al menú principal y sus categorías, la figura 2.20 muestra las subcategorías que puede seleccionar el usuario para observar los distintos materiales desarrollados para el tema de Cibercultura.

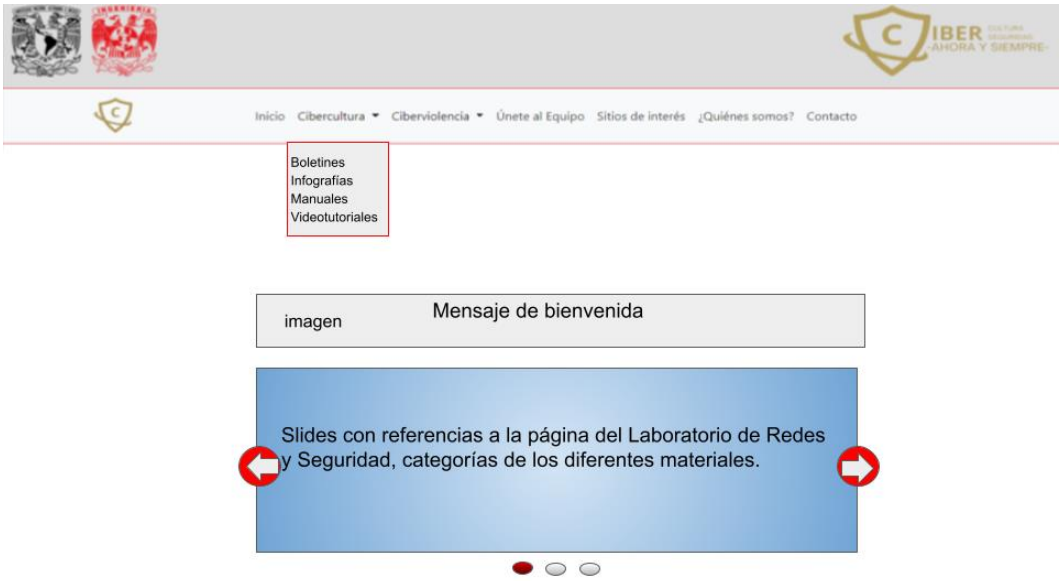


Figura 2.20 Menú desplegable de Cibercultura.

Mientras que la figura 2.21 le muestra al usuario la vista seleccionada, cabe destacar que las vistas de todas las subcategorías poseen la misma estructura, por eso se opta por solo mostrar la de boletines, como se podrá observar cada boletín está contenido en una tarjeta de presentación para que al momento de dar clic en el boletín deseado este se muestre.

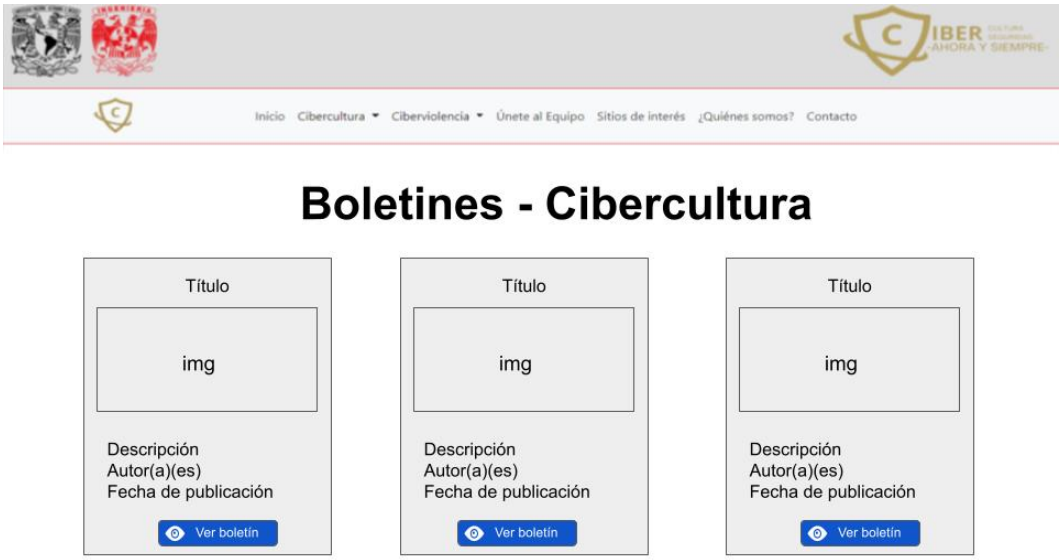


Figura 2.21 Selección de la categoría Boletines – Cibercultura.

La figura 2.22 muestra las opciones del menú desplegable de Ciberviolencia, el cuál posee las mismas categorías que el tema de Cibercultura.

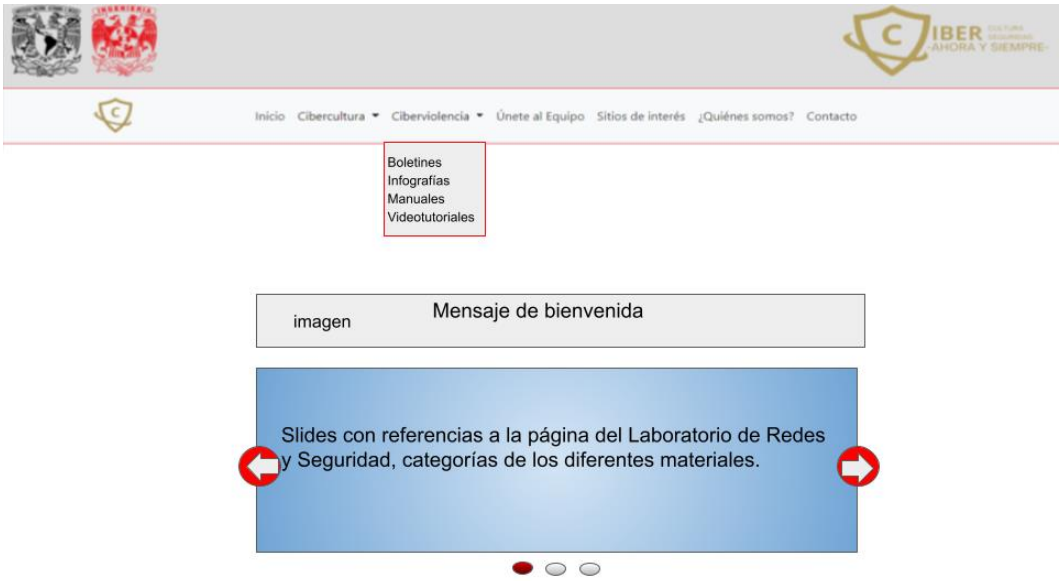


Figura 2.22 Menú desplegable Ciberviolencia.

Al dar clic en la opción deseada, el usuario podrá observar que el material que desea consultar está contenido en tarjetas, las cuales poseen un breve resumen de lo que trata en este caso un boletín de Ciberviolencia (ver figura 2.23).

Otro punto importante es que las imágenes que se utilizarán en ambas secciones (Cibercultura y Ciberviolencia) deberán ser aprobadas para su uso, puesto que se busca generar un entorno de respeto e igualdad de género para que las y los miembros de la comunidad se sientan identificados y llamar así su atención.

Figura 2.23 Selección de la categoría Boletines – Ciberviolencia.

El enlace de Únete al Equipo es una cordial invitación a formar parte del equipo de "Cibercultura en Ciberseguridad: Ahora y siempre" desarrollando materiales, herramientas, juegos, entre otros, con el objetivo de generar conciencia sobre la importancia de la Cibercultura en la ciberseguridad, tal como se muestra en la Figura 2.24.

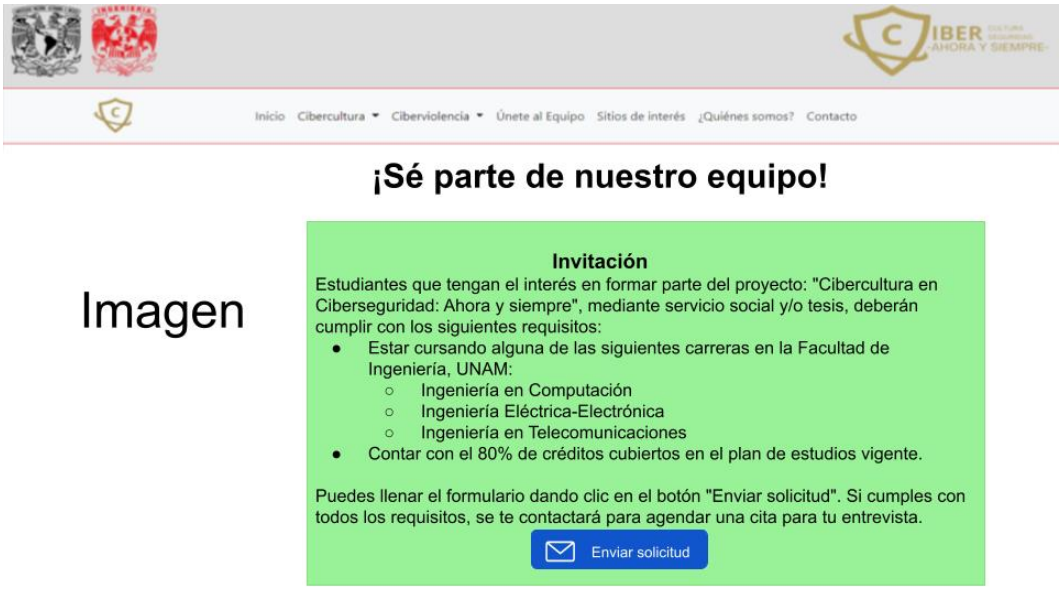


Figura 2.24 Vista de Únete al Equipo.

En caso tal de que las y los alumnos interesados cumplan con los requisitos mencionados pueden llenar un formulario, como el que se muestra en la figura 2.25

para que se les otorgue una entrevista en la que puedan acordar las actividades que deseen desarrollar.

Una vez que el estudiante de clic en Enviar solicitud, le aparecerá una alerta en color verde en la cual se les informa que su información se envió correctamente, en caso de que el formato del historial académico no sea pdf, se le notificará que el único formato permitido es este y no podrá continuar hasta que ingrese un archivo válido.

Figura 2.25 Formulario de solicitud.

El siguiente link de la barra de navegación es el de "Sitios de interés", en dicha vista se pretende proveer a las y los alumnos de la DIE los links más relevantes en sus carreras, al igual que algunos links de la UNAM y otros que puedan serles de utilidad, tal como se muestra en la figura 2.26.

Figura 2.26 Vista de Sitios de Interés.

Al Inicio del sitio web se da una pequeña bienvenida, en esta sección se busca responder a diferentes preguntas, tales como se muestran en la figura 2.27 los mensajes al igual que las imágenes deberán ser revisados por las profesoras a cargo del proyecto, para evitar errores ortográficos y generar mensajes claros para que los usuarios puedan entender a la perfección la misión, visión y objetivos de este gran proyecto.

Figura 2.27 Vista de ¿Quiénes somos?

El último link del menú es el contacto, en el cual se busca dar la ubicación física y los horarios de atención presencial, en caso de necesitar mayor información se provee el correo electrónico del Laboratorio de Redes y Seguridad, como se muestra en la figura 2.28.

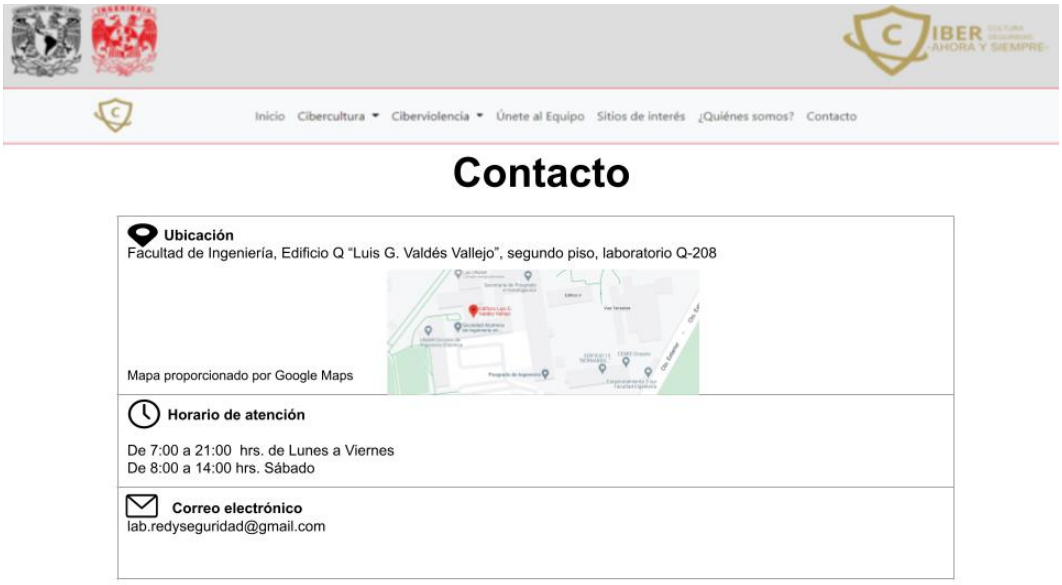


Figura 2.28 Vista de Contacto.

Como se mencionó en la figura 2.16, el footer posee diferentes enlaces a diversas secciones, tanto ajenas a este desarrollo como internas, en la figura 2.29 se muestra el Aviso de privacidad, el cual fue provisto por la página del Laboratorio de Redes y Seguridad, el cual fue colocado dentro de una alerta amarilla para indicar lo importante que es para este desarrollo contar con dicho aviso y que en caso de querer copiar o reproducir dicho sitio las personas sean precavidas y den el crédito correspondiente a dicho proyecto e instituciones que lo avalan.

Figura 2.29 Aviso de privacidad.

Sección administrativa: Esta sección es única y exclusivamente para él o la administradora del sitio web, debido a que en esta área del sitio web se podrán subir los materiales, revisar solicitudes, manejar un histórico de solicitudes y miembros del equipo además de agregar nuevos administradores que podrán ser soporte del administrador principal.

Nota: En varias de las imágenes podrá observar rectángulos plateados, los cuales sirven como protección de datos para ejemplificar los datos sensibles que se podrán manipular en esta sección.

En el mismo footer hay un enlace que dice “Administración”, al dar clic en él se puede observar esta pantalla de inicio de sesión, tal como se muestra en la figura 2.30, en el cual se solicita un nombre de usuario y contraseña, los cuales serán asignados por el o la administradora.

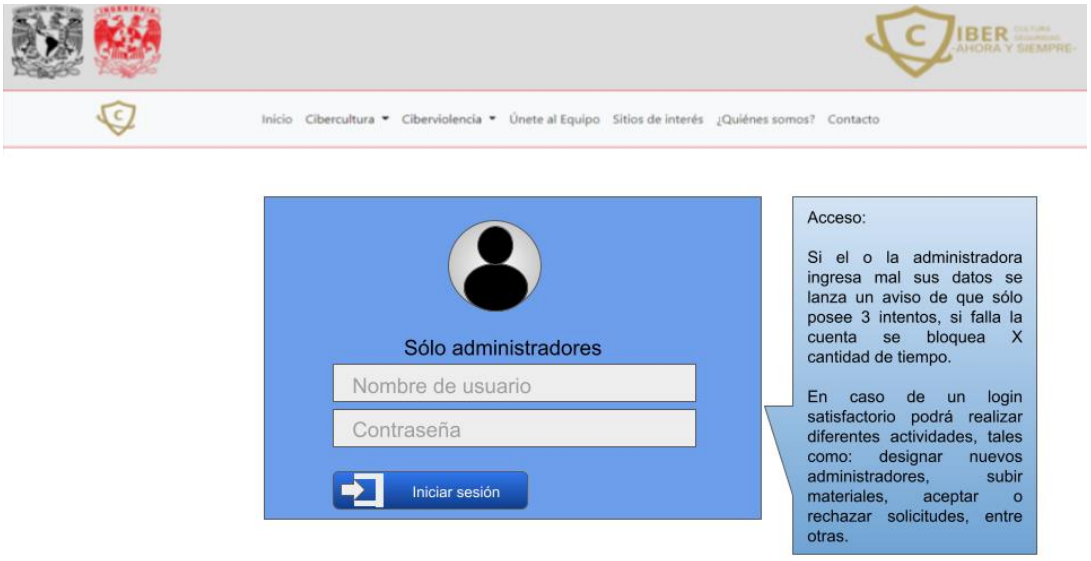


Figura 2.30 Inicio de sesión administrativa.

Cuando el administrador o administradora ingresa correctamente sus datos, la barra de navegación cambia, mostrando dos menús desplegables adicionales, tal como lo muestra la figura 2.31. Además de que se puede observar la lista de opciones del menú desplegable “Administración”.

Figura 2.31 Barra de navegación administrativa.

Elemento del menú desplegable: Administración de materiales

Cuando se dé clic en el enlace de "Administración de materiales", lo primero que verá es una vista Index de estado, como al principio no hay materiales agregados mostrará una alerta como se muestra en la figura 2.32.

Figura 2.32 Lista de materiales inicial.

Al dar clic en el botón que indica la subida de materiales, aparecerá un formulario, tal como se muestra en la figura 2.33, lo que permitirá que se suba el material en su sección correspondiente, contenido en una tarjeta con los datos solicitados, por ejemplo: si se decide subir en la sección de Cibercultura un videotutorial, se

validará que el vídeo esté almacenado en un formato mp4 y no dejará subir ningún archivo que no tenga dicho formato.

Figura 2.33 Formulario para añadir materiales.

Cuando ya existen materiales añadidos, se muestra una tabla como la de la figura 2.34, que además de servir de histórico de materiales se pueden realizar las acciones de "Editar" un material, lo que implicaría una corrección de datos o incluso cambiar de material y la otra opción es "Eliminar" en caso de que querer borrarlo por completo.

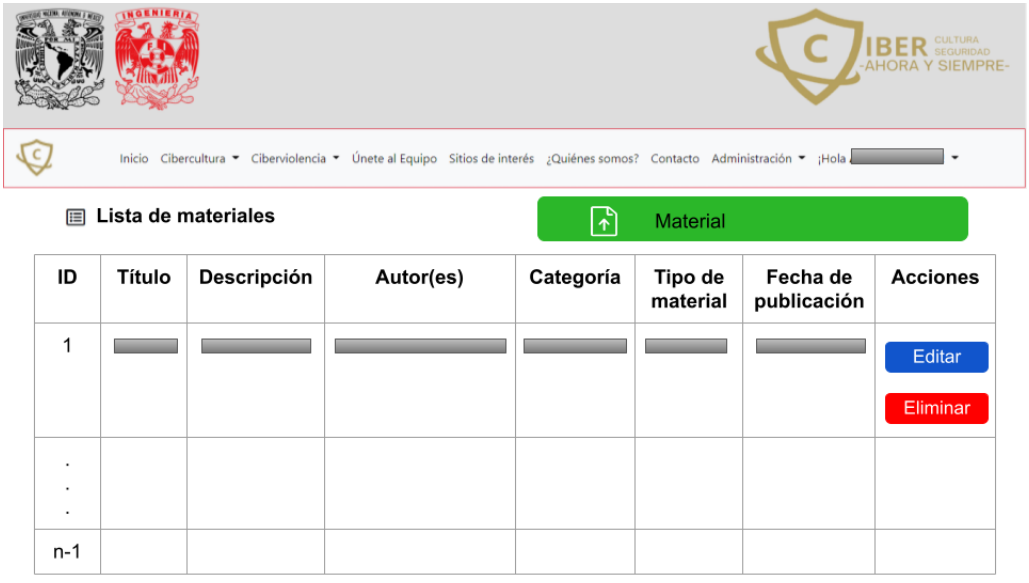


Figura 2.34 Listado de materiales.

Elemento del menú desplegable: Solicitudes

Al igual que en “Lista de materiales” cuando el sitio web está en cero, la vista se encuentra en un estado inicial como el que se muestra en la figura 2.35.

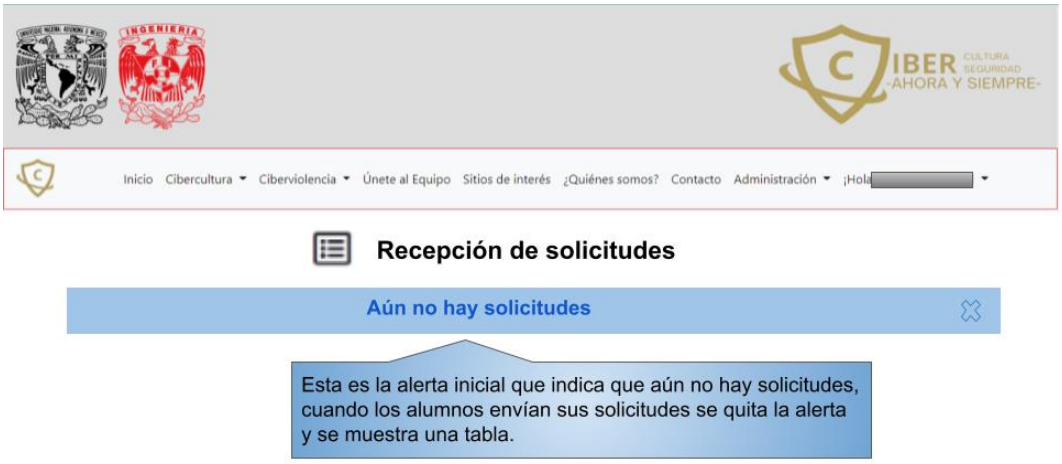


Figura 2.35 Estado inicial de la recepción de solicitudes.

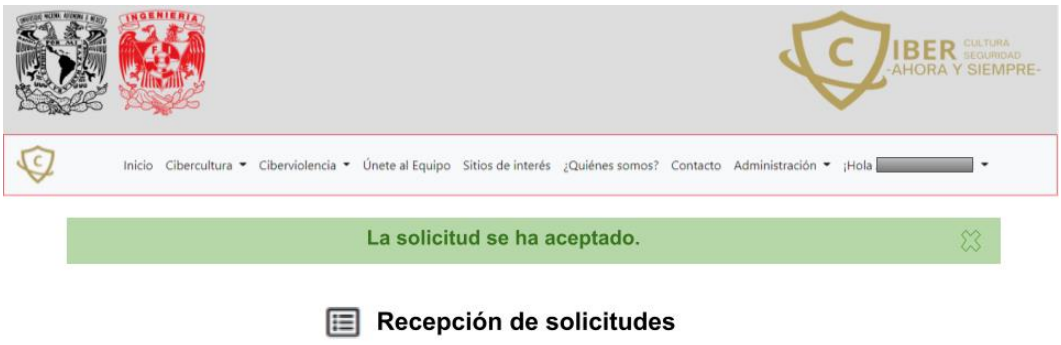
Cuando las alumnas y alumnos ingresen al sitio web en la sección de “Únete al Equipo” y envíen su solicitud, el administrador o administradora podrá revisar las solicitudes en una tabla, tal como se muestra en la figura 2.36.

Figura 2.36 Tabla de recepción de solicitudes.

En dicha tabla podrá dar clic en el botón de “Revisar solicitud”, lo que le dará acceso al formulario que envió el o la solicitante incluyendo su historial académico,

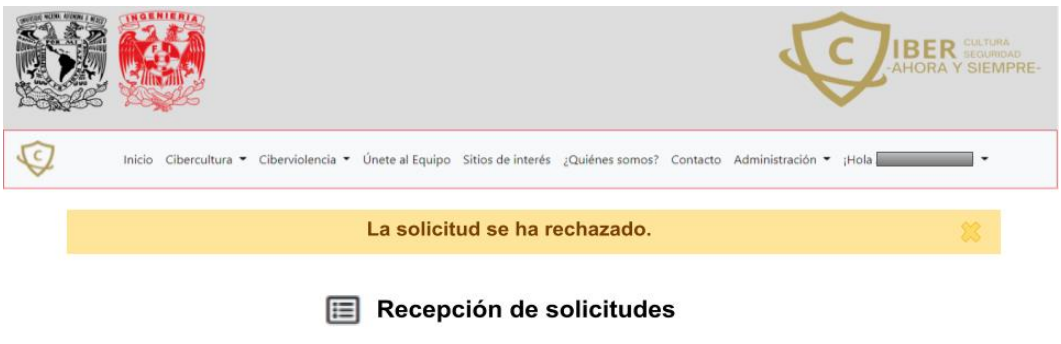
si el estudiante cumple con los requisitos, su solicitud podrá ser aceptada, tal como se muestra en la figura 2.37, en caso contrario se rechaza la solicitud, dando como resultado una vista como la figura 2.38.

Cabe destacar que el “Estado de la solicitud” tiene 3 estados posibles por defecto, “PENDIENTE” cuando la solicitud aún no es revisada, “ACEPTADA” cuando la solicitud arroja un resultado positivo y “RECHAZADA” en caso de un resultado negativo, además al ser revisadas las solicitudes se quita el botón de revisión y muestra la razón de la aceptación o el rechazo, quedando así la tabla como un historial de solicitudes.



ID	No.Cuenta	Nombre(s)	Apellido(s)	Email	Carrera	Fecha de la solicitud	Estado de la solicitud	Acciones
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	dd/mm/aaaa hh:mm:ss	ACEPTADA	ESTA SOLICITUD HA SIDO ACEPTADA

Figura 2.37 Aceptación de la solicitud.



ID	No.Cuenta	Nombre(s)	Apellido(s)	Email	Carrera	Fecha de la solicitud	Estado de la solicitud	Acciones
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	dd/mm/aaaa hh:mm:ss	RECHAZADA	NO CUMPLE CON LOS REQUISITOS

Figura 2.38 Rechazo de la solicitud.

Elemento del menú desplegable: Administrar Equipo

Mismo caso, al no existir solicitudes aún no existen miembros del equipo, por ende, la vista inicial del link "Administrar Equipo" se verá igual a la figura 2.39.

Figura 2.39 Vista inicial de Miembros del Equipo.

Cuando la solicitud ha sido aceptada, esta se podrá encontrar en la información del solicitante que se encuentra en esta sección con los campos de "Actividad(es)", "Inicio de actividades" y "Fin de actividades" con la leyenda "POR ASIGNAR", en la columna de "Asignaciones" podrá encontrar el botón "Asignar actividades", tal como se encuentra en la figura 2.40.

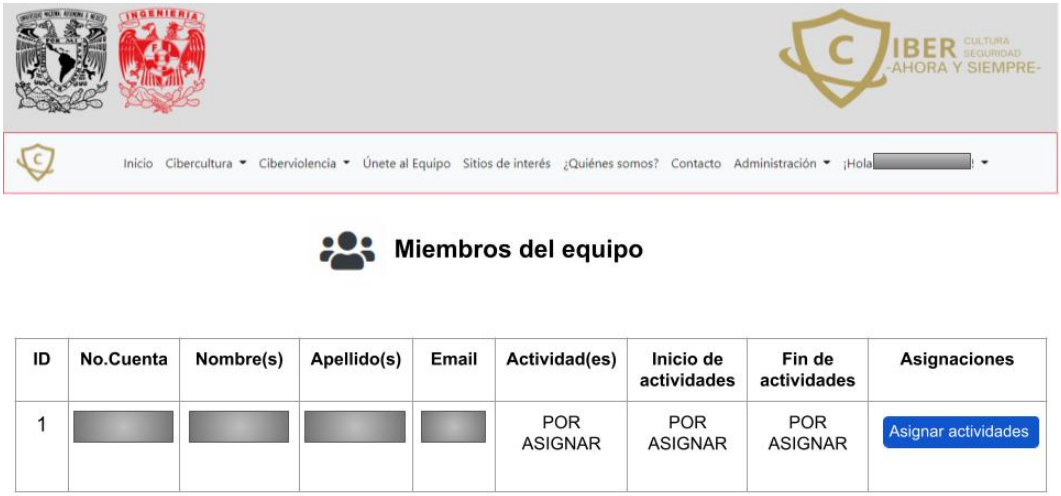


Figura 2.40 Vista con aspirantes a miembros del equipo.

Al dar clic en el botón de “Asignar actividades” podrá observar la información del nuevo miembro del equipo tal como se muestra en la figura 2.41 y acordar los campos previamente descritos.

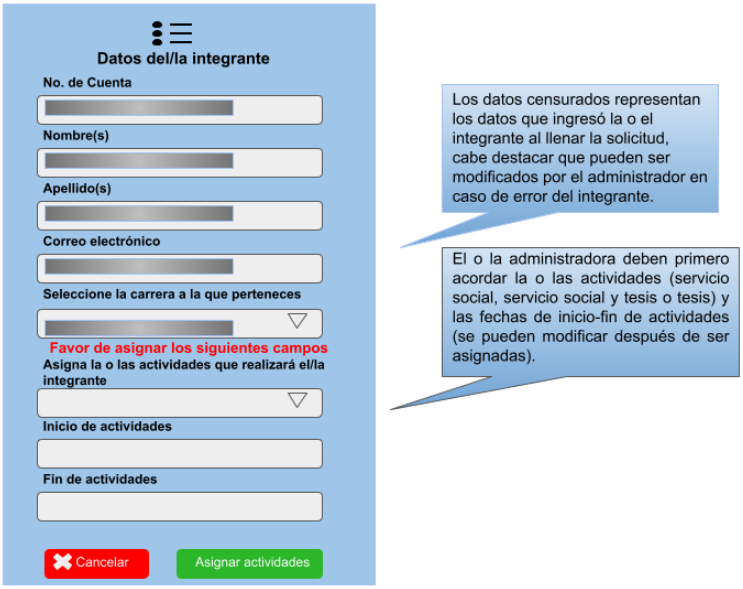


Figura 2.41 Formulario de los datos del/la integrante del equipo.

Al registrar los campos descritos anteriormente dando clic en “Asignar actividades” la página se redirigirá a la vista de Miembros del Equipo y mostrará un resultado como el que se muestra en la figura 2.42.

Figura 2.42 Tabla de los miembros del equipo actualizada.

Elemento del menú desplegable: Lista de Administradores

Se generó un usuario administrador por defecto, el cual puede realizar todas las acciones antes mencionadas, además de registrar nuevos administradores, dicho usuario puede ser eliminado justo después de crear uno nuevo por el superadministrador, cabe destacar que las y los usuarios administradores estarán contenidos en una tabla como se muestra en la figura 2.43.

Figura 2.43 Lista inicial de administradores.

Para registrar nuevos usuarios administradores es necesario llenar un formulario con los datos mostrados en la figura 2.44, al finalizar el superadministrador deberá dar clic en Registrar y el nuevo usuario estará listo para usarse.

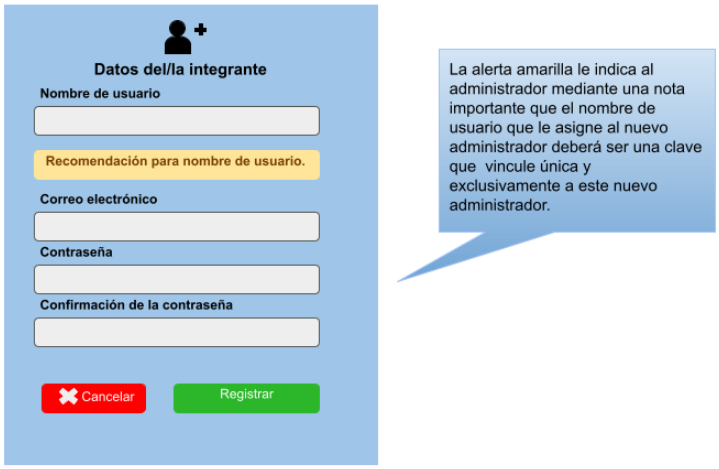


Figura 2.44 Formulario para el registro de administradores.

Cuando se registra un nuevo administrador, se redirige a la vista “Lista de administradores” la cual muestra los cambios como se muestra en la figura 2.45.

Figura 2.45 Actualización de la lista de administradores (registro de un administrador).

Como se mencionó con anterioridad, el superadministrador puede borrar el usuario administrador creado por defecto además de que cualquier administrador puede borrar a los demás administradores hasta este punto del desarrollo, es por ello que se muestra la alerta contenida en la figura 2.46 indicando el peligro que conlleva esta acción.

Figura 2.46 Eliminación de un usuario administrador.

En caso de borrar un usuario, será redirigido a la vista “Lista de administradores” actualizada como se muestra en la figura 2.47.

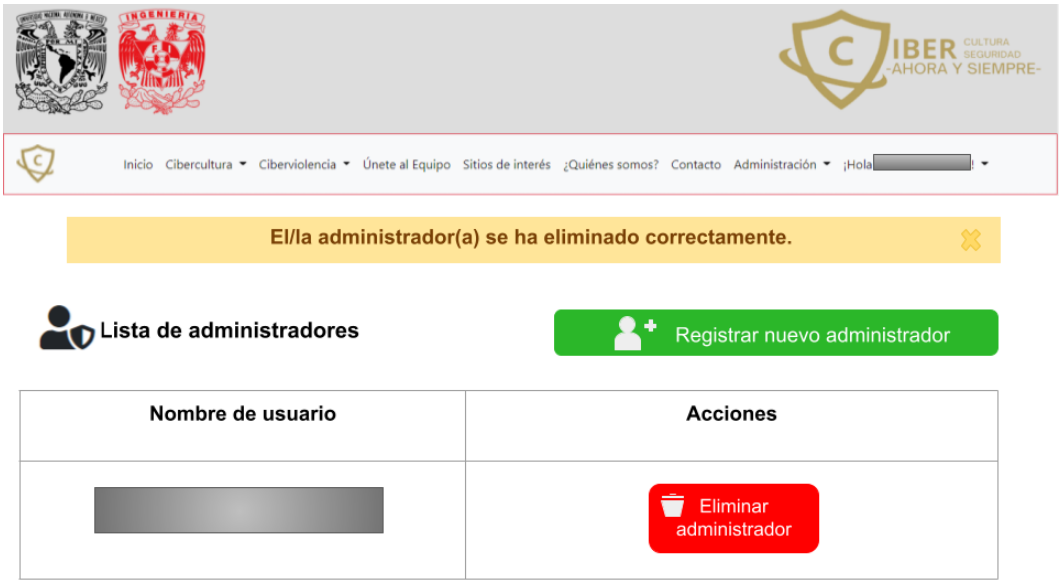


Figura 2.47 Lista actualizada de administradores (eliminación de un administrador).

En la Figura 2.48, se podrá observar que el mensaje de bienvenida al administrador también es un menú desplegable con las opciones de cambio de contraseña y el fin de la sesión.

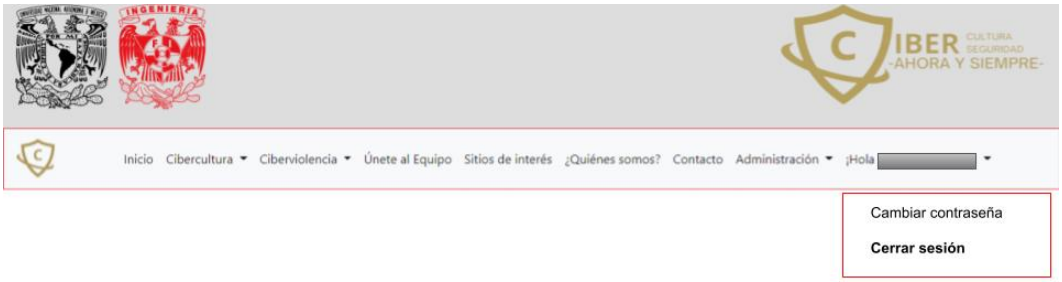


Figura 2.48 Menú desplegable: Sesión administrativa.

Elemento del menú desplegable: Cambiar contraseña

En caso de que se desee cambiar la contraseña cada cierto tiempo, podrá hacerlo llenando un formulario como el que se muestra en la figura 2.49.

Figura 2.49 Formulario de cambio de contraseña.

En caso de que se llenen los campos y se dé clic en el botón de "Cambiar contraseña" se cerrará su sesión activa y se le mostrará una vista como la de la figura 2.50.

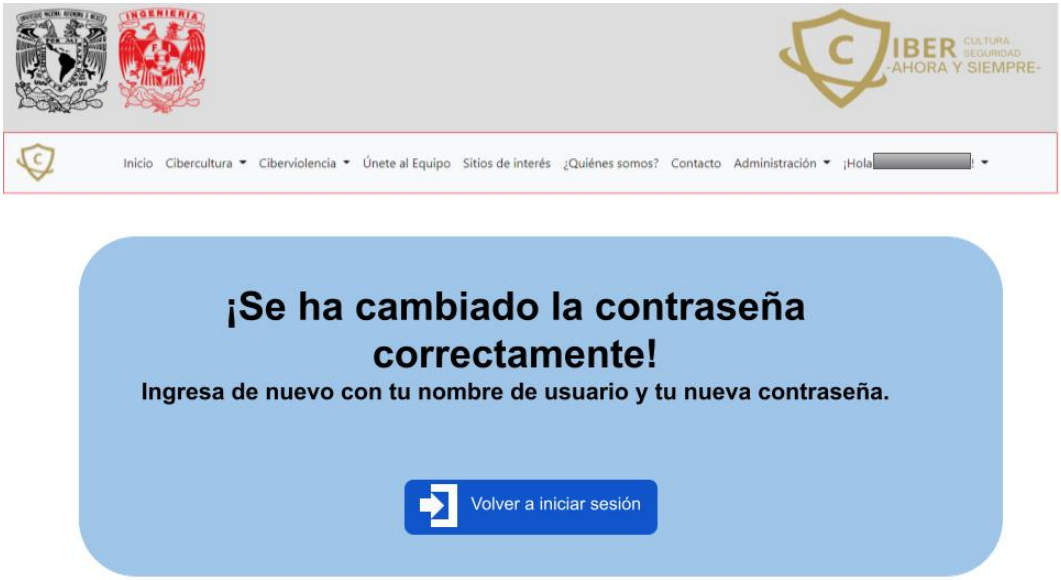


Figura 2.50 Cambio de contraseña.

Elemento del menú desplegable: Cerrar sesión

Cuando el usuario administrativo termina sus labores en el sitio web deberá cerrar su sesión dando clic en dicho elemento del menú desplegable, lo que le mostrará una vista como la que se muestra en la figura 2.51, si no desea cerrar su sesión seguirá viendo la misma barra de navegación, pero en caso de que sí desee cerrar su sesión el resultado será como el de las figuras 2.15 y 2.16.

Figura 2.51 Cierre de sesión.

En este capítulo se planteó todo lo relacionado al diseño web y la experiencia de usuario, por lo que el siguiente capítulo abordará la funcionalidad de este desde la perspectiva del desarrollo web, haciendo énfasis en las herramientas y lenguajes de programación que se utilizaron para crear el sitio web de Cibercultura.

Capítulo 3. Propuesta y desarrollo del sitio web

En este capítulo se expondrán los principales aspectos de la creación de un sitio web a partir del diseño que se mostró en el capítulo anterior, implementando las buenas prácticas del desarrollo web, lo cual incluye la seguridad de este, por otra parte, se realizará un análisis de diferentes herramientas desde los lenguajes de programación más utilizados hasta el hospedaje en un servidor real y funcional.

La principal razón de realizar un análisis de las herramientas que se van a implementar en el desarrollo es la justificación del porqué se usa una y no otra herramienta, ya que es importante resaltar que aunque algunas son muy utilizadas, existen estándares, los cuales poseen mucha documentación en línea, y en caso de existir algún error o problema existen comunidades que resuelven y explican la resolución dichos inconvenientes, por otra parte, existen aplicaciones que son muy amigables para el desarrollador las cuales le facilitan el proceso de la creación de código, adición de plugins, entre otros.

La propuesta del sitio web refleja el entendimiento de los requerimientos del proyecto, dado que este se creará desde cero y debe cumplir con estándares solicitados, el primero es que debe ser una versión institucional, por lo que debe ser similar al sitio web del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería, lo que implica que debe poseer la misma paleta de colores para que este desarrollo sea relacionado a la Facultad de Ingeniería de la UNAM, otro punto importante a considerar es el envío de formularios para pertenecer al equipo de Cibercultura en Ciberseguridad: Ahora y siempre, el cual está acotado a solo alumnos de la DIE (Ingeniería Eléctrica Electrónica, Computación y Telecomunicaciones), dichos alumnos podrán solicitar unirse al equipo como tesista, prestador de servicio social o ambos.

Como podrá observar en el tema “2.2 Boceto del diseño web”, el cual fue aprobado y conforme fue evolucionando el proyecto se fueron quitando y agregando nuevas secciones, las cuales también cuentan con su propio boceto.

A continuación, se explica la metodología que se utilizará en el proceso de crear un sitio web desde cero.

3.1 Consideraciones de las amenazas presentes 2020-2021

A lo largo de los años diferentes organizaciones que se dedican al desarrollo de aplicaciones web han implementado ciertos estándares generados por OWASP (Open Web Application Security), dicho proyecto busca concientizar a los desarrolladores para que implementen mejoras de seguridad en sus diseños, es por ello que se creó el Top ten de las principales amenazas a las que están expuestos

los desarrollos web, aunque existen más amenazas y es por ello que los desarrolladores deben de dar más de sí mismos para proteger las aplicaciones web que se encuentran en sus diferentes fases (desarrollo, producción y comercialización).

Es por lo que antes de iniciar el desarrollo web se realizó una investigación del top ten de los años 2020 y 2021, con el objetivo de minimizar el impacto de los 10 principales riesgos que se muestran a continuación:

Top ten del año 2020:

1. **Inyección:** Las fallas de inyección, como la inyección de SQL, ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a datos sin la debida autorización.
2. **Autenticación rota:** Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.
3. **Exposición de datos sensibles:** Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales. Los atacantes pueden robar o modificar esos datos débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos.
4. **Entidades externas XML (XXE):** Muchos procesadores XML más antiguos o mal configurados evalúan las referencias de entidades externas dentro de los documentos XML. Las entidades externas se pueden utilizar para divulgar archivos internos mediante el controlador de URL de archivos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
5. **Control de acceso roto:** Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder a funciones y / o datos no autorizados.
6. **Mala configuración de seguridad:** La configuración incorrecta de seguridad es el problema más común. Esto suele ser el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben configurarse de forma

segura, sino que también deben actualizarse o actualizarse de manera oportuna.

7. **Cross-Site Scripting XSS:** Esta vulnerabilidad es aprovechada en ataques que permiten ejecutar scripts de lenguajes como JavaScript.
8. **Ataques DoS y DDoS:** La Denegación de servicio es un ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones, mientras que la Denegación de servicio distribuido es un DoS que envía las peticiones desde diversos orígenes, de esta forma es más efectivo, complicado de detener y determinar su origen.
9. **Spam:** El spam es cualquier forma de comunicación no solicitada que se envía de forma masiva.
10. **De fuerza bruta:** Es el intento de descifrar un usuario y/o contraseña con el método de prueba y error utilizando diferentes combinaciones de frases, letras, palabras y números.

Adicionalmente se considera importante mencionar que existen otros riesgos que no se contemplan en este top ten, debido a que existen menores riesgos de ocurrencia en dicho año, tal como las **vulnerabilidades de las APIS y de software conocidas.**

Cabe destacar que OWASP lanza este top ten para concientizar a las empresas, organizaciones y Software Developers sobre el desarrollo web seguro y que estos contemplen implementar mejoras en sus diferentes sistemas y aplicaciones, pero también reconoce que su Top ten no refleja necesariamente todas las vulnerabilidades de software importantes que deben abordarse y que todo aquel que se dedique al desarrollo de software debería considerarlas sobre todo en este panorama en que las amenazas evolucionan y se vuelven cada vez más sofisticadas [40].

Top 10 del año 2021:

En el top ten de este año se crearon tres nuevas categorías, lo que implica que viejas categorías se actualizarán en nombre y alcance, se iniciará este top ten con una imagen comparativa realizada por la propia OWASP del año 2017 y 2021, para posteriormente explicar los cambios a estas categorías de amenazas y vulnerabilidades, mismos que se detallan en su página web [41].

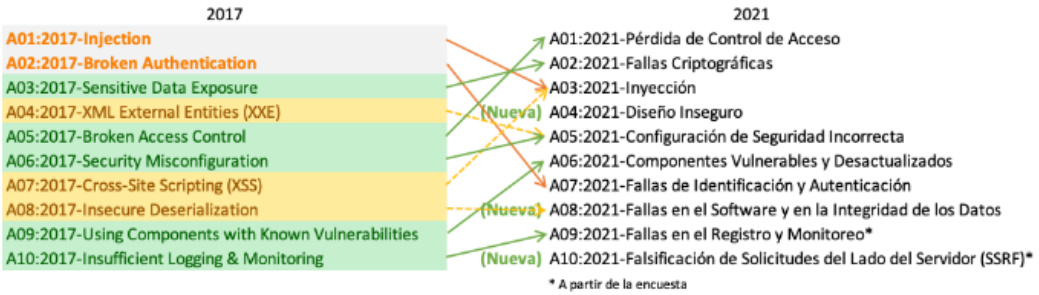


Figura 3.1 Qué ha cambiado en el Top 10 de 2021.

1. La Pérdida de Control de Acceso pasó de la quinta posición en 2017 a ser el riesgo principal de seguridad en desarrollo web del 2021.
2. Los fallos criptográficos pasaron de ser un síntoma general a ser la raíz de la causa de la exposición de datos confidenciales e incluso el compromiso del sistema en cuestión.
3. La inyección desciende hasta la tercera posición y el Cross-site Scripting se considera ya como parte de esta categoría.
4. Para la cuarta posición se ha creado una nueva categoría para ser considerada este 2021: Diseño inseguro, la cual posee un enfoque principal: los riesgos relacionados con las fallas de diseño es el diseño inseguro.
5. Configuración incorrecta de seguridad: Sube una posición desde el último top ten además de que el riesgo que representan las Entidades Externas XML(XXE) se encuentran contempladas en esta categoría. Cabe destacar que existe una mayor presencia de software altamente configurable el cual abre paso a que exista algún tipo de configuración incorrecta.
6. Componentes vulnerables y obsoletos: Antes era denominado como "Uso de Componentes con Vulnerabilidades Conocidas", pasó de la novena posición a la sexta debido a que es un problema conocido que cuesta probar y evaluar el riesgo, lo que hace que el desarrollo web tenga en sí una falla predeterminada al implementar dicho componente.
7. Fallas de Identificación y Autenticación: Anteriormente era la categoría de "Pérdida de Autenticación" y pasó de estar en la segunda a la séptima posición, ahora incluye 33 CWEs (Common Weakness Enumeration) relacionadas con fallas de identificación, las CWE es un sistema de categorías para las debilidades y vulnerabilidades del software. La razón de que esta categoría bajara de nivel se debe a que se ha incrementado el uso de frameworks estandarizados que están ayudando a minimizar el riesgo.
8. Fallas en el software y en la integridad de los datos: Es una nueva categoría, la cual engloba a la categoría A08 (la cual se muestra en la figura 3.1) "Deserialización Insegura". Esta nueva categoría se centra en hacer suposiciones relacionadas con actualizaciones de software, los datos

críticos y los pipelines CI/CD sin verificación de integridad, debido a que estos elementos generan uno de los mayores impactos según los sistemas de ponderación de vulnerabilidades CVE/CVSS (Common Vulnerability and Exposures/Common Vulnerability Scoring System).

9. Fallos de monitoreo y registros de seguridad: Esta categoría subió un peldaño en el top ten actual, además de que antes era conocida como "Registro y Monitoreo Insuficientes", cabe destacar que la actualización de esta categoría no sólo es en el nombre puesto que ahora contempla una mayor cantidad de fallas. La importancia de esta categoría radica en que dichas fallas pueden afectar directamente la visibilidad, las alertas de incidentes y los análisis forenses.
10. Falsificación de solicitudes del lado del servidor (SSRF): El proyecto OWASP tiene su propia comunidad, la cual mediante una encuesta votaron que es importante la creación de esta categoría (ganó el primer lugar) y plantearse este escenario y calcular los posibles riesgos, pero citando al equipo de OWASP: "Los datos muestran una tasa de incidencia relativamente baja con una cobertura de pruebas por encima del promedio, junto con calificaciones por encima del promedio para la capacidad de explotación e impacto".

3.2 Herramientas de desarrollo web

El desarrollo web implica otorgar las funcionalidades requeridas por el diseño al sitio web, la migración de este a un servidor que le otorgue desde este lado las herramientas necesarias para poder responder a las peticiones de los clientes y procurar que la comunicación cliente-servidor sea segura desde cualquier dispositivo con el que los usuarios acceden desde Internet.

En esta sección se detalla el proceso de selección de lenguajes de codificación y de programación, algunos de los IDES y editores de código contemplados que facilitan el llevar a cabo el proceso de desarrollo de un sitio web dinámico, responsivo y que cumpla con los requerimientos técnicos y gráficos mostrados en "2.2 Boceto del diseño del sitio web".

Además de estas herramientas básicas se implementarán un framework llamado ASP.NET Core el cual es de código abierto, multiplataforma y de alto rendimiento que permite agilizar el proceso de desarrollo reutilizando módulos y herramientas, para el front-end se utilizará Bootstrap, el cual es responsivo e implementa la arquitectura Modelo-Vista-Controlador, misma que se implementa en ASP.NET Core, también se utilizará una biblioteca de iconos vectoriales y estilos CSS llamada fontawesome para resaltar ciertos elementos del sitio web, junto con el

plugin de un carrusel, el cual se utilizará para mostrarle a los miembros de la comunidad las diferentes secciones del sitio web.

Para la sección administrativa mostrada en "2.2 Boceto del diseño del sitio web" se implementará y configurará una API (Interfaz de Programación de Aplicaciones), llamada Identity que servirá para autenticar al usuario administrador y que a su vez este pueda subir los materiales en sus respectivas secciones, revisar las solicitudes, acordar entrevistas con los candidatos seleccionados, acordar las actividades que estos van a realizar, agregar o eliminar a distintos administradores. Es importante resaltar que dicha API fue desarrollada para funcionar en conjunto con ASP.NET Core.

3.2.1 Lenguajes de programación

A continuación, se muestra la tabla 3.1, la cual es una comparativa de los lenguajes más utilizados en el desarrollo web, la cual es una cita traducida de Nimap Infotech [42], dicha tabla aborda las características de ambos lenguajes.

Tabla 3.1. *Comparativa de lenguaje de desarrollo web.*

HTML5	PHP
Lenguaje de codificación para el navegador.	Lenguaje de codificación para el servidor.
Los navegadores solo entienden HTML y no PHP.	Los fragmentos de código PHP se procesan en el servidor y HTML se devuelve al navegador como salida.
Para ejecutar código HTML solo se requiere del navegador.	Para ejecutar una declaración o código PHP, se necesita un servidor compatible con PHP como XAMPP.
HTML 5 es la última versión de HTML (nuevas etiquetas en imagen, vídeo, figuras).	PHP 7 es la última versión de PHP.
HTML es procesado por el navegador.	PHP primero es procesado por el servidor y HTML es el resultado que pasa al navegador.

Se puede usar para crear páginas web estáticas.	Usando PHP se pueden crear páginas web dinámicas.
Para mostrar páginas web, no hay otra opción que HTML para los navegadores.	Para la programación del lado del servidor hay muchas opciones como ASP.NET, JSP, PERL, RUBY y PHP.
HTML y JavaScript se utilizan como tecnologías Front-End	PHP se utiliza como tecnología de servidor o Back-end.

Elección del lenguaje con el que se llevará a cabo el desarrollo web

Ambos lenguajes son complementarios y tienen sus ventajas, pero es conveniente trabajar con el estándar, el cual es HTML5 junto con CSS y JavaScript, debido a que este se considera la base del desarrollo web, es fácil de aprender, existe mucha información sobre este, además de que muchos frameworks implementan el lenguaje de marcado y las hojas de estilo de CSS (las cuales pueden ser modificadas al gusto del programador o codificador) para el front-end debido a la compatibilidad que tienen los buscadores con la tecnología móvil, otra ventaja es que HTML5 proporciona soporte para audio y video, ya que estos se reproducen nativamente sin necesidad de añadir un plugin externo.

Para realizar el back-end del sitio web se implementarán los lenguajes C# y JavaScript, los cuales serán utilizados para agregar funcionalidades, por lo que a continuación se mencionarán sus respectivas características.

C# (See Sharp)

C# es un lenguaje de programación orientado a objetos y a componentes, además de contar con seguridad de tipos, el uso de C# permite a los desarrolladores crear muchos tipos de aplicaciones sólidas y seguras que se ejecutan en .NET.

Cabe resaltar que este lenguaje de programación tiene sus raíces en la familia de lenguajes C lo que resulta familiar para los programadores de C, C + +, Java y JavaScript [43].

JavaScript

JavaScript es un lenguaje de programación que le permite a los desarrolladores implementar funciones complejas en páginas web, en este caso se utilizarán scripts para controlar los formatos permitidos al momento de subir los archivos, tales como

el historial académico, por ende, las vistas no serán estáticas, pues mostrarán cambios como la actualización de contenido, el mapa de la ubicación, reproductor de vídeo, entre otros [44].

En cuanto al servidor se optará por un servidor web Apache, para la base de datos se utilizará SQL, las principales razones de utilizar estas herramientas es que son gratuitas, open source y que existe documentación de cómo implementarlas.

3.2.2 Herramientas de programación (Editores e IDES, Frameworks, Arquitectura, NuGet, API y plugins)

A continuación, se realizará un análisis de las diferentes herramientas que se requerirán a lo largo de este desarrollo, el cual inicia con una comparativa de Editores de texto y los IDEs, los diferentes servidores web, las bases de datos y algunos frameworks que se explicarán más adelante.

Análisis de Editores e IDEs (Entorno de Desarrollo Integrado): Es importante resaltar que un editor es diferente a un IDE, ya que el primero es simple, básico y ligero, ya que su función es muy general y se puede ampliar mediante plugins específicos que aumenten su capacidad de trabajo, mientras que el segundo cuenta con una interfaz gráfica elaborada y sumamente intuitiva que facilita trabajar en grandes proyectos ahorrando tiempo con una integración de diferentes herramientas [45].

1. **Notepad++:** Editor de código fuente con soporte para diversos lenguajes de programación, gratuito y de código libre cabe destacar que su distribución es únicamente para Windows.
   En la página oficial de descargas se ofrece una gran variedad de plugins que el programador puede requerir para trabajar en una gran variedad de entornos [46].
2. **HTML-Kit:** Editor de páginas web muy potente orientada a programadores web ya que para hacer uso de este programa se requiere escribir código HTML, cuenta con dos vistas, la de código y la de previsualización [47].
3. **Visual Studio Community 2019:** Un completo IDE extensible y gratuito para crear aplicaciones modernas para Windows, iOS y Android, además de aplicaciones web y servicios en la nube de Microsoft Azure [48].
4. **Visual Studio Code:** Editor de código fuente desarrollado por Microsoft para Windows, Linux, macOS y web [49].

Tabla 3.2. *Comparación de Editores e IDEs para la creación y diseño web.*

Herramienta	Características
Notepad++	• Coloreado de código para más de 40 lenguajes de programación diferentes, entre los que se incluyen todos los que un desarrollador web podría requerir, como HTML, JavaScript, ASP, SQL, PHP, CSS, Python, Ruby, etc. • Permite definir el resaltado de sintaxis para nuevos lenguajes de programación que necesite el usuario. • Autocompletado de código. • Multi-Documento. • Multi-Vista, un ejemplo de esto es tener dos versiones del mismo documento. • Permite realizar acciones de Buscar / Reemplazar utilizando incluso expresiones regulares para definir los patrones a reemplazar. • Detección automática del estado del documento, que puede ayudarnos en caso de que se quiera guardar un archivo que había sido modificado por otro usuario o programa. • Otras utilidades como Zoom, soporte para varios idiomas, puntos de marca, resaltado de paréntesis u sangría, creación de macros, etc.
HTML-Kit	• Reconoce casi todos los lenguajes de creación web (HTML, ASP, JavaScript, PHP). • Resalta el código de manera conveniente. • Comandos útiles para la edición. • Corrige la sintaxis de HTML. • Permite la edición de documentos XML. • Plugins. • Permite la edición de sitios directamente desde Internet, crear plantillas o grabar archivos en formato UNIX.
Visual Studio Community 2019	• Instalación ligera y modular. • Posee herramientas de código abierto. • Flexibilidad para crear e implementar aplicaciones web modernas.

	• Productividad: cuenta con una avanzada compatibilidad con los marcos web más potentes como son: Angular, jQuery, Bootstrap, Django, Backbone.js y Express. • Pruebas: se puede someter el código a un conjunto de pruebas seleccionadas por el desarrollador. • Control de versiones Git y GitHub. • Permite desarrollar aplicaciones para la Web con ASP.NET, Node.js, Python o JavaScript, por lo que facilita el cambio entre lenguajes y tipos de proyecto con el editor de HTML5, CSS3 y JavaScript. • ASP.NET Core y .NET Core (código abierto) funcionan en Windows, Mac y Linux. • De forma predeterminada cuenta con la instalación de Bootstrap 4, el cual es un framework de CSS, HTML y JavaScript. • Permite realizar implementaciones en cualquier servidor web con la posibilidad de escalar el servicio o implementación a la nube de Microsoft Azure. • Visual Studio incluye herramientas de ayuda como IntelliSense (para el código JavaScript del lado cliente), CodeLens (para obtener información en detalle en una única línea) y el depurador (permite diagnosticar errores de forma local o remota, en cualquier explorador o en la nube). • Administradores de paquetes (LibMan, NuGet, NPM): NuGet ofrece bibliotecas detalladas del lado servidor de .NET, la herramienta ligera Administrador de bibliotecas le permite al desarrollador adquirir bibliotecas del lado cliente y así obtener sólo aquellos archivos que se requieran de los marcos populares y los paquetes de bibliotecas, y el administrador NPM, ofrece herramientas y utilidades.
Visual Studio Code	• IntelliSense: herramienta capaz de autocompletar variables, funciones, lista las opciones de variables, funciones, además de proporcionar información de los parámetros que requiere un método. • Código de depuración directamente desde el editor.

	• Comandos Git incorporados, los cuales permiten tener un manejador de versiones del proyecto en desarrollo, restaurar a un estado anterior y el trabajo colaborativo. • Extensible y personalizable: permite instalar extensiones para agregar nuevos idiomas, temas, depuradores y para conectarse a servicios adicionales. Las extensiones se ejecutan en procesos separados, lo que garantiza que no ralentizará el editor. • Permite realizar implementaciones en cualquier servidor web con la posibilidad de escalar el servicio o implementación a la nube de Microsoft Azure.

Elección de herramienta para la programación del sitio web

Los editores de texto son fáciles de utilizar para cualquier programador ya que este se enfoca a escribir el código y el programa resalta las sentencias particulares de cada lenguaje de programación además de presentar "ayuda" al momento de escribir el código, como es el caso del autocompletado, se pueden agregar los plugins conforme se necesitan hasta igualar a un IDE, una desventaja que se encontró en el caso de HTML Kit es que no posee una tercera vista que muestre el resultado de la escritura del código, al igual con Notepad + +, si el programador desea ver el desarrollo (pasar de código a visual) se requiere descargar e instalar un cliente FTP (Protocolo de Transferencia de Datos) y seleccionar un proveedor de hosting, en cambio los IDEs son herramientas potentes que ya incluyen herramientas para facilitar la productividad reduciendo el tiempo de investigación de plugins específicos. El IDE Visual Studio Community 2019 (versión gratuita de Visual Studio de Microsoft) contiene muchas herramientas de código abierto multiplataforma, además de que están desarrolladas con lo último de las tecnologías actuales como es la Inteligencia Artificial, gracias a la IA se ofrecen recomendaciones personalizadas de cómo mejorar el código, posee herramientas específicas para el desarrollo web permitiendo y soportando los lenguajes, marcos y frameworks más utilizados del desarrollo web, otro punto destacable es que este IDE posee su propia versión cliente de varios servidores web, como es el caso de IIS Express para cuando se ejecuta la aplicación en un entorno Windows o Kestrel cuando se ejecuta en una distribución de Linux.

Cabe destacar que se seleccionó el IDE de Visual Studio Community, por las ventajas previamente mencionadas, además de ser muy intuitivo facilita el trabajo del programador al crear las subcarpetas en el repositorio y todas las carpetas

pueden ser consultadas en cualquier momento, también se pueden observar las diferentes vistas, consulta del rendimiento, uso de memoria, herramientas de autenticación y el protocolo HTTPS.

Una desventaja de este IDE es que no es posible realizar la descarga en Linux, se menciona ya que el desarrollo será migrado en su totalidad a un entorno Linux, es por ello, que al implementar el sistema operativo Ubuntu 20.04 se hará uso del editor Visual Studio Code para realizar modificaciones al código y que este funcione en dicho sistema.

Frameworks implementados en la creación de Cibercultura

ASP.NET Core 5.0

Este sitio web implementará el framework de ASP.NET Core en su versión 5 puesto que es multiplataforma, de código abierto y de alto rendimiento. Las ventajas de trabajar con dicho framework son las siguientes [50]:

- Es sencillo y modular.
- Diseñado para la capacidad de prueba.
- Seguridad estricta: menor intercambio de información y rendimiento mejorado.
- Plataforma unificada para la creación de la interfaz web y las APIs web.
- Herramientas que simplifican el desarrollo web (MVC, Bootstrap v4 y Angular).
- Permite efectuar implementaciones locales y en la nube.
- Integración de marcos del lado cliente modernos y flujos de trabajo de desarrollo.

El IDE de Visual Studio Community 2019 al momento de crear el proyecto con ASP.NET Core 5 con arquitectura MVC carga dos frameworks para el desarrollo web que implementan dicha arquitectura, los cuales son Bootstrap 4 y Angular, los cuales son muy conocidos en el desarrollo front-end. En la tabla 3.3 se puede observar la comparación entre ambos frameworks [51].

Tabla 3.3. *Comparación entre AngularJS y Bootstrap.*

Framework	Diferencias	Características	Ventajas
AngularJS	Desarrollado por Google, proporciona diversos componentes que ayudan al programador a estructurar la aplicación web y organizar el proyecto de manera satisfactoria. Se debe de tener en claro la lógica de negocios que se va a implementar (la cual se representa mediante los controladores). Su función es tomar los datos mediante el controlador respectivo, para procesarlos utiliza el modelo y al final los envía al usuario mediante una vista, la cual mantiene una comunicación bidireccional con el controlador, por lo que puede llamar funciones o eventos, mismos que pueden mandar llamar a más métodos.	Angular posee cinco diferentes tipos de frameworks para lograr un desarrollo front-end más fluido (dependerá del objetivo del proyecto saber cuál es el más indicado para implementar), los cuales son: AngularUI Bootstrap, Angular Foundation, Ionic framework y Mobile Angular UI. Trabaja con las arquitecturas: JavaScript y MVC. Se puede implementar en el diseño de aplicaciones móviles. Posee recursos de configuración tales como el enlace de datos, enrutamiento e inyección de dependencias.	Integración automática de los múltiples componentes de la arquitectura MVC. Intuitivo en cuanto a los elementos de HTML5. Angular no requiere complementos o frameworks adicionales. Es compatible con características adicionales. Realiza por sí mismo la prueba o test unitarios para comprobar el correcto funcionamiento de las unidades individuales.
Bootstrap	Desarrollado por Twitter, el cual pasó	El diseño de las vistas se adapta	El desarrollo front-end es rápido ya que

	a formar parte de una comunidad de código abierto, por lo que se puede implementar fácilmente y está al alcance de cualquier persona que guste de la programación, posee componentes de CSS y JavaScript, facilitando el trabajo del desarrollador front-end. Para tomar la entrada de datos de un usuario y procesarla, Bootstrap implementa formularios, los cuales pueden estar diseñados de forma horizontal o vertical, estos poseen controles de forma textual (.form-control) que ayudan a controlar los datos. Posteriormente revisa los modelos de datos creados y muestra al usuario la información requerida mediante una vista (el proceso final es igual al de Angular).	automáticamente de acuerdo con las dimensiones que se le otorga a nivel de programación, por lo que el usuario podrá consultar el sitio web desde cualquier dispositivo. Proporciona diseños de estilos y estructura tanto de CSS y JavaScript que se pueden implementar en los elementos de interfaz en conjunto con HTML5.	proporciona funcionalidad CSS y bloques predefinidos, los cuales se pueden personalizar de acuerdo con las necesidades del sitio web. Garantiza la consistencia sin importar la forma en la que se realice el desarrollo. Uniformidad en los diferentes buscadores web (la salida es igual sin importar el navegador que utilicé el usuario). Trabaja con un diseño de cuadrícula (máximo de 12 columnas, las cuales pueden ser fijas por tamaños extra small, small, medium, large, extra large, diseño automático, fluido, entre otros) para cargar los datos.

Elección de framework para el desarrollo front-end

Las principales razones de seleccionar a Bootstrap como framework de front-end es que se adecua a la metodología de diseño responsivo adaptable a los dispositivos móviles además de las características que se mencionan a continuación.

Como se mencionó con anterioridad Bootstrap versión 4 es un framework de CSS, HTML y JavaScript, entre las características más relevantes de esta herramienta se encuentra que es multiplataforma, de código abierto, por otra parte, en su página web oficial existe una excelente documentación de los diferentes elementos que componen este framework además de ofrecer ejemplos de aplicación con opción a modificar a gusto de los desarrolladores.

Una desventaja de Bootstrap 4 es que no incluye una sección de iconos a utilizar en el diseño web (flechas, símbolos de play, de señalización, de redes sociales, entre otros), por lo cual se implementará el framework de Font Awesome, el cual se explica a continuación.

Font Awesome

Es la biblioteca de iconos vectoriales y estilos CSS, con el cual se complementará la parte visual del diseño web. Otro punto importante de este framework es que existen dos versiones, la de paga y la gratuita, por lo que se utilizará la versión gratuita, la cual contiene una extensa variedad de iconos que se pueden implementar.

Arquitectura Modelo-Vista-Controlador (MVC)

Patrón de arquitectura que permite separar las responsabilidades de la interfaz de usuario (Vista), la lógica de negocios de la aplicación (Controlador) y los datos que maneja dicha aplicación (Modelo), es decir, MVC permite la programación modular descrita en la Figura 8, en donde cada componente tiene su propia responsabilidad, por ejemplo los controladores son los encargados de recibir la petición de “https” de acuerdo a la regla de ruteo que se disponga, después de un procesamiento responde a la petición tratando de satisfacer lo que le piden, la respuesta normalmente es una vista [52].

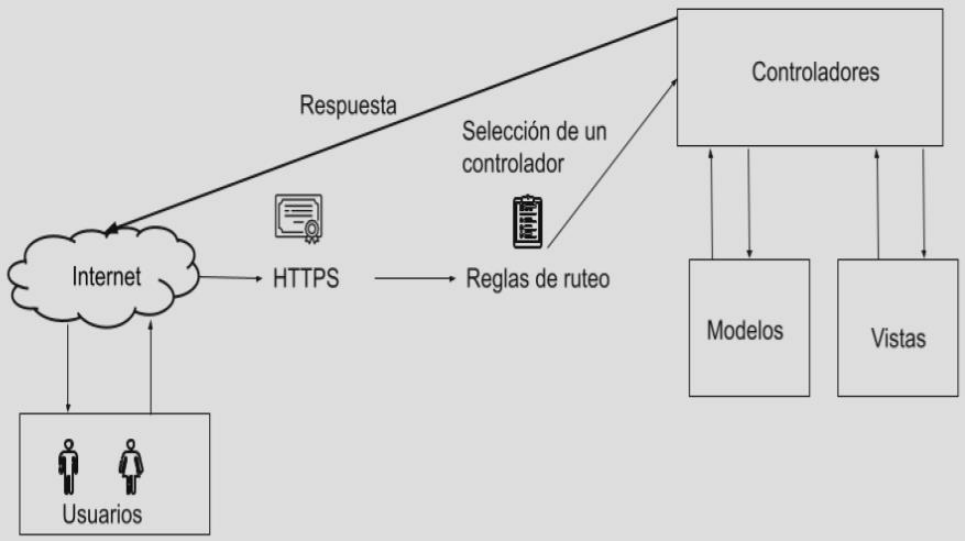


Figura 3.2 Arquitectura MVC.

NuGet

En los desarrollos web que implementan .NET y .NET Core se requiere consumir códigos útiles para poder implementar ciertas acciones tales como: el acceso a datos, la gestión de bases de datos, la implementación de interfaces como la de ASP.NET Core Identity, las cuales son específicas para EF Core[1] y otras como la compilación de las vistas en tiempo de ejecución todo esto mediante diferentes paquetes NuGet, por lo que a continuación se explica que es un NuGet, qué información contiene y de dónde se pueden obtener.

NuGet es una herramienta desarrollada con el objetivo de proveer a cualquier plataforma de desarrollo moderno un mecanismo mediante el cual los desarrolladores puedan crear, compartir y consumir código útil, es común que dicho código se incluye en "paquetes", los cuales contiene código compilado como lo son los DLL junto con otro contenido necesario como son otros archivos relacionados con ese código y un manifiesto descriptivo que incluye información como el número de versión del paquete.

NuGet es el mecanismo compatible con Microsoft para compartir código, por lo que se puede decir que este es un administrador de paquetes que define cómo se crean, alojan y consumen los paquetes para .NET y .NET Core, los cuales se pueden encontrar en el IDE de Visual Studio Community de forma gráfica, a su vez se pueden realizar diferentes acciones tales como buscar, descargar, actualizar y

[1] EF Core: su función principal es servir como intérprete entre dos tecnologías fundamentadas en distintos principios por un lado la programación orientada a objetos y por el otro las bases de datos relacionales y no relacionales.

eliminar dichos paquetes, mientras que en Visual Code dichos paquetes se descargan, actualizan y eliminan mediante línea de comandos, dichos paquetes se pueden buscar desde Internet en la plataforma de nuget.org.

De acuerdo con la documentación de Microsoft [53] se define a un paquete NuGet como "(...) un único archivo ZIP con la .nupkg extensión que contiene código compilado (DLL).
(...)
Los consumidores de paquetes obtienen esos paquetes de hosts adecuados, los agregan a sus proyectos y luego llaman a la funcionalidad de un paquete en su código de proyecto. Luego, NuGet se encarga de todos los detalles intermedios."

ASP.NET Core Identity

Es una API que admite la funcionalidad de inicio de sesión de la interfaz de usuario (UI), se utiliza para administrar usuarios, contraseñas, datos de perfil, roles, confirmación de la cuenta mediante correo electrónico, entre otros [54].

Cabe destacar que Identity tiene sus propios modelos (tablas en la base de datos) para realizar las operaciones previamente explicadas además de que los usuarios pueden crear su cuenta con la información de inicio de sesión que se almacena en Identity o pueden usar un proveedor de inicio de sesión externo, como es el caso de vincular su cuenta de Facebook o Google.

Owl Carousel

Es un plugin para añadir diapositivas o carruseles a las páginas o sitios web. Está preparado para ser implementado en todos los dispositivos, se puede maquetar al gusto fácilmente y tiene infinidad de opciones como otros plugins.

Para poder implementarlo sólo se debe de añadir en el encabezado en el archivo de estilos, los scripts necesarios junto con la llamada al plugin [55].

3.3 Tipos de Hosting

El hosting es un servicio de alojamiento, el cual permite la publicación de una página web o aplicación en Internet, existen diferentes tipos de hosting de paga y gratuitos, esto se debe a que este servicio es almacenado en uno o varios servidores, en el o en los cuales se almacenan todos los archivos y datos de la página web o aplicación para que esta funcione correctamente.

Es por lo que a continuación se muestran los principales tipos de hosting con sus principales características, ventajas y desventajas [56]:

1) Compartidos: En este tipo de hosting se comparten los recursos del servidor, por dar ejemplos: la CPU, el procesador y la memoria RAM, entre las diversas páginas web que están alojadas en él.
   a) Ventajas:
      i) Es el hosting más económico del mercado.
      ii) Fácil de manejar e instalar.
   b) Desventajas:
      i) Si hay algún problema con algún proyecto alojado, puede afectar al resto de los proyectos.
      ii) Menor flexibilidad.
      iii) Al compartir recursos, la velocidad y disponibilidad del sitio web pueden verse afectadas.

   Nota 1: Este tipo de Hosting se recomienda para proyectos que no requieran de mucho espacio para almacenar la información ni necesidades especiales.

2) Cloud: En el caso del hosting en la nube, el proyecto es alojado en varios servidores interconectados en la nube, por lo que no está alojado en un solo servidor, esta característica suele ser útil, ya que en caso de que, si un servidor fallara, el resto de los servidores compensa la pérdida de recursos. Otra característica de este servicio es que el hosting en la nube puede ser:
   - Hosting compartido.
   - Hosting Virtual.
   - Hosting dedicado.

   a) Ventajas:
      i) Es más eficiente que el hosting dedicado.
      ii) Se adapta a las necesidades del proyecto en tiempo real.
      iii) Posee la mejor disponibilidad.
      iv) Gran capacidad de adaptación.
      v) Al contar con el respaldo de varios servidores, ofrece una mejora de seguridad.
   b) Desventajas:
      i) Para la gestión se requieren conocimientos avanzados.
      ii) Su precio es elevado.
      iii) Como los recursos son variables, los costos también.
      iv) Implicaciones legales en cuanto al tráfico de datos personales entre países.

   Nota 2: Servicio recomendado para grandes proyectos como aplicaciones que requieran Software como Servicio (SaaS).

3) VPS: Es un servicio proporcionado por un servidor físico que es fraccionado virtualmente para que cada proyecto funcione de manera independiente con recursos propios. Lo que implica que las páginas web alojadas en ese servidor no se vean afectadas en cuanto al rendimiento, aunque no compartan recursos las páginas web o proyectos, este tipo de hosting no es dedicado.
    a) Ventajas:
        i) Posee una mayor flexibilidad en comparación con el hosting compartido.
        ii) Si un proyecto presenta alguna falla no afecta al resto de los proyectos alojados.
        iii) Alternativa económica al hosting dedicado.
    b) Desventajas:
        i) Dispone de una parte de los recursos totales del servidor.
        ii) Es más costoso que el hosting compartido.
        iii) El nivel de configuración y uso es más complicado que el hosting compartido.

    Nota 3: Útil en proyectos que tengan requerimientos y configuraciones específicas, además de que requieran mayor capacidad de almacenamiento en el servidor, es una buena opción para cuando no se tiene el capital para contratar un hosting dedicado.

4) Dedicado: Este hosting se caracteriza por ofrecer servicios a un único cliente, por lo que los recursos de software y hardware del servidor son exclusivos del proyecto y las especificaciones que este tenga.
    a) Ventajas:
        i) El rendimiento no se ve afectado por el tráfico.
        ii) Permite que el sitio web opere de manera óptima.
        iii) Garantiza mayor flexibilidad, velocidad y acceso.
        iv) Tiene mayores recursos.
        v) Posee una mayor seguridad.
    b) Desventajas:
        i) Costoso.
        ii) Complicado de configurar y mantener.

    Nota 4: Es el servicio de hosting más recomendado para grandes proyectos, los cuales requieren de un servidor completo para alojar su proyecto.

Elección de tipo de hosting
De todas las opciones antes mencionadas y realizando un análisis de las ventajas y desventajas de cada servicio, se optó por utilizar el hosting compartido, ya que el área de Redes y Seguridad de la Facultad de Ingeniería ofreció alojar el sitio web en su servidor, por lo que se tendrá que cumplir con ciertas normas que nos indique la persona responsable del servidor.

3.4 Migración del sitio web al servidor Linux

Para poder llevar a cabo la migración de manera exitosa se realizaron cambios en el gestor de bases de datos, la exportación de la base de datos del proyecto, en el servidor web, pasando de IIS Express a Kestrel cuando se cambió de sistema operativo Windows a una distribución Ubuntu, Kestrel opera en conjunto con Apache como proxy reverso debido a la modificación de la configuración inicial del proyecto para admitir el proxy reverso, para hacer las pruebas se montó una máquina virtual con un servidor simulando las especificaciones que fueron indicadas en un principio, para subir los archivos del sitio web se utilizó Webmin (herramienta gráfica web que permite administrar archivos de configuración y de carga de programas sin la necesidad de usar SSH), aunque se pudo usar PuTTY para administrar el servidor virtual implementando SSH.

Para conocer el proceso con mayor detalle deberá consultar el Anexo: Manual del sitio web "Cibercultura en la ciberseguridad: Ahora y siempre" apartado "Migración del proyecto al sistema operativo Ubuntu 20.04". Debido a que este desarrollo web se realizó siguiendo las especificaciones del Laboratorio de Redes y Seguridad.

3.4.1 Servidores web (IIS Express, Kestrel, Apache y Apache como proxy reverso)

Servidor web
Es un dispositivo compuesto de hardware y software, al igual que una computadora, con la diferencia de que posee una mayor capacidad de procesamiento de datos, con el fin de atender las peticiones de los clientes, los cuales pueden ser otros servidores, computadoras, dispositivos móviles y de red para proveerlos de un servicio web específico.

Otra función de los web servers es el alojamiento de sitios y páginas web, los cuales están compuestos de archivos como lo son imágenes, archivos de texto, videos, entre otros. Estos archivos son transmitidos a los usuarios a través de los navegadores web mediante los protocolos http y https [57].

IIS Express
IIS Express fue desarrollado por Microsoft, es una versión ligera del servidor de aplicaciones web, este viene integrado en las distintas versiones de Visual Studio, la ventaja de este servidor es que resulta sencillo probar las configuraciones reales en él sin necesidad de instalar alguna otra herramienta, ni tener ejecutando otro servicio en segundo plano durante la realización de las pruebas [58].

Kestrel
Kestrel es un servidor web que está integrado con el framework ASP .NET Core, lo cual lo convierte en un servidor multiplataforma funcional.

La desventaja con la que cuenta es que no incluye todas las opciones de configuración que permiten al administrador(a) del servidor personalizarlo, gestionarlo y ofrecer un nivel de seguridad alto como lo harían Apache, Nginx o IIS [59].

Apache
Apache es un proyecto de software de código abierto que busca implementar servidores web con el objetivo de crear una implementación de código fuente robusto, comercial y gratuito para todas las plataformas [60].

La principal razón de utilizar Apache en este desarrollo se debe a la estabilidad y seguridad que proporciona como servidor web.

Apache como proxy reverso
El objetivo de un proxy reverso es generar una capa que separa y oculta del cliente toda la infraestructura interna, para ejemplificar en la figura 3.3 se muestra que un cliente realiza una petición, quien la recibe es Apache configurado como un proxy reverso (recordando que este provee al sitio web de una extensa configuración de seguridad en comparación con Kestrel), este la entrega al servicio interno (Kestrel, el cual no es un servidor web nativo de Linux y como tal no existen instrucciones en dicho sistema para configurarlo), este procesa la petición y entrega la respuesta al proxy para que a su vez este la entregue al cliente, como se puede observar la comunicación que se realiza internamente se lleva a cabo de forma no segura y la comunicación externa es con el protocolo https.

Motivos por los cuales es necesario implementar el proxy reverso

1) Seguridad
   a) Facilita la implementación de certificados SSL.
   b) Apache es conocido por que es fiable, robusto y flexible.
   c) Permite aplicar una capa lógica, filtrado y redireccionamiento adicional antes de que las conexiones entrantes lleguen a la aplicación web.

2) Escalabilidad
   a) Se puede usar el proxy reverso para balancear la carga.

   Nota: La traducción más adecuada para el reverse proxy es proxy inverso, por lo que las menciones subsecuentes al reverse proxy se harán como proxy inverso.

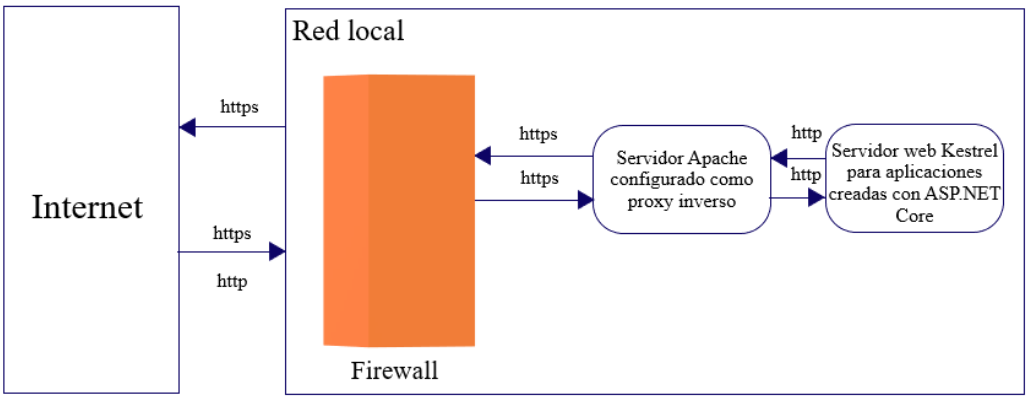


Figura 3.3 Explicación del funcionamiento de Apache proxy inverso y Kestrel.

3.4.2 La importancia de MariaDB en el desarrollo del sitio web

MariaDB es un sistema manejador de bases de datos (DBMS), el cual está muy relacionado con MySQL, esto es, porque uno de los desarrolladores y fundadores de MySQL, Michael "Monty" Widenius, decidió mantener el proyecto como software libre.

Una de las principales características de MariaDB es que, al ser un sistema de software libre, la misma comunidad puede dar soluciones, actualizaciones y mejoras a dicho sistema, sin tener que esperar tanto tiempo a que un sólo equipo de desarrollo se encargue de ello. Otra característica importante es que MariaDB ofrece compatibilidad con cualquier sistema operativo, desde Linux, Windows y MacOS. Asimismo, MariaDB a través del tiempo ha ido implementando mejoras en la velocidad de manejo de datos y de las consultas.

Otra característica importante que se tomó en cuenta para el desarrollo del proyecto y con la que cuenta MariaDB es que existen distintos tipos de extensiones y frameworks que se adaptan completamente con MariaDB, pues en este caso ASP .NET cuenta con una extensión que es compatible con este sistema manejador de bases de datos y que nos ayudó a implementar de una manera eficiente y rápida todos los modelos necesarios para el proyecto del sitio web [61].

Adicionalmente a todas las características mencionadas, la decisión de implementar MariaDB para este proyecto fue también el hecho de que en el servidor donde se aloja actualmente el sitio web, ya contaba con este sistema y se solicitó que la implementación se adaptara al mismo.

3.4.3 Elementos adicionales al sitio web para su correcto funcionamiento en el servidor

Los siguientes elementos se implementaron para darle funcionalidades más robustas al sitio web del lado del servidor, como lo son Certbot para la creación del certificado que se utiliza para habilitar el puerto 443 para el uso del protocolo seguro de transferencia de hipertexto (HTTPS).

El archivo de virtual host realiza el proceso de traducir la IP en un nombre de dominio mediante DNS (Sistema de Nombres de Dominio). Para poder lograr la implementación de un nombre de dominio, se realizó el trámite por medio de la Facultad de Ingeniería, la cual fue la encargada de llevar a cabo la petición a la Universidad Nacional Autónoma de México de que se le otorgara al sitio web un dominio. Una vez aceptada la solicitud, la Facultad entregó el dominio para poder hacer uso e implementarlo en el servidor y hacer las configuraciones necesarias para el sitio web.

Gracias al archivo de servicio se logra hacer que el sitio web funcione como un servicio background más del servidor y que este siempre esté funcionando en segundo plano y que en caso de un fallo el sitio trate de reactivarse cada 10 segundos.

Algunos de los elementos que son visibles para los usuarios son el nombre de dominio y el HTTPS que se puede observar en la liga del sitio web (`https://cibercultura.fi-b.unam.mx/`), mientras que otros son imperceptibles para ellos, pero estos archivos ayudan a dar respuesta a las peticiones que los clientes le realizan al servidor desde cualquier parte de Internet.

3.4.3.1 Archivo de configuración de VirtualHost

Se crea un archivo de host virtual para que este aloje a Apache como proxy inverso, el cual apuntará al servidor Kestrel que se ejecuta en local, desde un punto de vista de seguridad, Microsoft recomienda que Kestrel no esté expuesto a peticiones wildcard.

A continuación, se muestra un archivo básico de configuración de virtual host para implementar Apache como proxy inverso y este se comunique a su vez con Kestrel, obtenido de la página Microsoft Docs [62].

```
<VirtualHost *:*>
    RequestHeader set "X-Forwarded-Proto"
    expr=%{REQUEST_SCHEME}
</VirtualHost>

<VirtualHost *:80>
    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:5000/
    ProxyPassReverse / http://127.0.0.1:5000/
    ServerName www.example.com
    ServerAlias *.example.com
    ErrorLog ${APACHE_LOG_DIR}helloapp-error.log
    CustomLog ${APACHE_LOG_DIR}helloapp-access.log common
</VirtualHost>
```

En el archivo anterior se indica que Apache es el que acepta el tráfico proveniente de Internet en el puerto `80` el cual se usa para la navegación web de forma no segura (http), el servidor Apache por defecto otorga la dirección `127.0.0.1` y `:5000` se indica el puerto en que el servidor Kestrel acepta la comunicación con Apache de forma no segura de manera bidireccional, el dominio `www.example.com` la conversión de la dirección IP del sitio web que es atendido por este virtual host y el `*.example.com` es un alias que redirige a los usuarios al mismo sitio web, en este caso se debe contar con el dominio del sitio web, el cual se acordó que fuera `www.cibercultura.fi-b.unam.mx`

3.4.3.2 Certificado de autenticación

Let's Encrypt es una autoridad de certificación (AC), gratuita, automatizada y abierta, la cual proporciona certificados SSL para que el sitio web posea el Protocolo seguro de transferencia de hipertexto (HTTPS).

Esta AC utiliza un software que usa el protocolo ACME, el cual corre en el hospedaje web, cuando se tenga acceso al servidor mediante el Shell se podrá usar

el cliente ACME llamado Certbot para automatizar la emisión e instalación de certificados SSL sin tiempo de inactividad [63].

Por lo que para obtener un certificado gratuito para el dominio del sitio web de cibercultura.fi-b.unam.mx se deberá demostrar control sobre dicho dominio, el archivo de host virtual, además de tener acceso Shell, una vez que Certbot valide estos requisitos en el Shell del servidor, este puede ser configurado para otorgar todos los certificados a los sitios web alojados en el servidor o solo a el que se le indique [64].

En este caso solo se utilizará Certbot para otorgarle el certificado SSL al sitio web, además de realizar la instalación de este en el servidor, se deberá agregar un complemento para garantizar que se renueve periódicamente el certificado, tal como se muestra en la siguiente línea:

```
sudo apt install certbot python3-certbot-apache
```

El siguiente paso es comprobar la configuración del host virtual, debido a que Certbot deberá encontrar un archivo de host virtual adecuado al sitio web dentro de los archivos de configuración. Para hacer esto deberá seleccionar el host virtual adecuado, para eso deberá escribir el path del mismo, como se muestra a continuación.

```
sudo nano /etc/apache2/sites-available/nombredomnio.conf
```

Buscará las siguientes líneas en el archivo, en caso de no tenerlas deberá escribirlas.

```
...
    ServerName www.example.com
    ServerAlias *.example.com
...
```

Si tiene estas líneas significa que esta correcto y que después de generar el certificado Certbot podrá actualizar este host virtual para permitir las conexiones https.

Como se mencionó con anterioridad, Certbot ofrece diferentes alternativas para obtener un certificado SSL a través de complementos.

El siguiente complemento se encargará es de Apache y sirve para reconfigurar Apache y volver a cargar la configuración en caso de ser necesario.

```
sudo certbot –apache
```

Al aplicar el comando anterior, Certbot le solicitará que responda ciertas preguntas para configurar el certificado SSL, entre ellas le solicita un correo electrónico válido para que se le envíen correos para recordarle sobre la renovación.

Después de contestar todas las preguntas, Certbot le mostrará enumerados los nombres de dominios que se encuentran en el servidor y deberá seleccionar el que corresponda a este sitio web y presioné ENTER.

Lo que le mostrará un resultado similar al que se muestra a continuación [65]:

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for your_domain
http-01 challenge for www.your_domain
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-
available/your_domain-le-ssl.conf
Enabled Apache socache_shmcb module
Enabled Apache ssl module
Deploying Certificate to VirtualHost /etc/apache2/sites-
available/your_domain-le-ssl.conf
Enabling available site: /etc/apache2/sites-
available/your_domain-le-ssl.conf
Deploying Certificate to VirtualHost /etc/apache2/sites-
available/your_domain-le-ssl.conf
```

Certbot le preguntará si desea que el tráfico de HTTP sea redirigido a HTTPS o no, con este paso se termina de configurar el certificado, el cual ya está instalado y cargado en la configuración de Apache.

El último paso es verificar que la configuración se ha aplicado correctamente ingresando en el buscador la siguiente URL `https://cibercultura.fi-b.unam.mx/` al dar clic, el sitio web deberá ser cargado además de tener el candado que indica que la conexión es segura.

3.4.3.3 Archivo de servicio

Este archivo `unit` se crea y configura dentro del servidor, con el objetivo de que el sitio web, el cual es administrado por Apache se mantenga activo como un

servicio, además de que en caso de que la aplicación deje de funcionar se reinicie cada cierto tiempo.

A continuación, se muestra un ejemplo de un archivo de servicio en un sistema operativo CentOS, el cual fue obtenido de Microsoft Docs.

```
[Unit]
Description=Example .NET Web API App running on CentOS 7

[Service]
WorkingDirectory=/var/www/helloapp
ExecStart=/usr/local/bin/dotnet
/var/www/helloapp/helloapp.dll
Restart=always
# Restart service after 10 seconds if the dotnet service
crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=dotnet-example
User=apache
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=multi-user.target [66]
```

En la sección `Unit` se agrega una descripción del servicio que se está creando, en este caso se podría poner en `Description = Cibercultura en ASP.NET Core 5.0 running on Distribución de Linux.`

En la sección de `service` se escribe en el `WorkingDirectory` se describe la dirección en la que se iniciará el servicio, en `ExecStart` se indica la ruta desde dónde se ejecuta el sitio web en el caso del archivo de ejemplo se puede observar que el archivo que se ejecuta es un .dll de la aplicación hello.
`Restart` indica que si existe algún fallo en la aplicación el servidor deberá intentar levantar la aplicación como un archivo de background cada 10 segundos como lo indica el `RestartSec`.

Si la aplicación no se cierra en un tiempo determinado se emite una `SigKill` igualada al valor de `SIGINT`.

Otro elemento del apartado de servicio es el `SyslogIdentifier=dotnet-example`, este nombre puede ser un nombre arbitrario, como por ejemplo `aspdotnet-cibercultura`.
En el `User=apache` se deberá seleccionar al usuario administrador de la aplicación.

Por último, en el campo de `Environment=ASPNETCORE_ENVIRONMENT=Production`, se puede poner el o los ambientes correspondientes, los cuales debieron ser indicados en el archivo de configuración de la aplicación, es decir, si en la aplicación solo se especificó el ambiente de desarrollo, este archivo deberá indicar developer, mientras que si en dicho archivo se especificó un entorno de desarrollo, pruebas o producción estos se deberán indicar en este archivo.

Para finalizar el archivo se encuentra la sección de Install con el campo de `WantedBy=multi-user.target`, lo que indica el target al que pertenece este `Unit`, lo que provoca que el gestor del sistema y de los servicios de Linux mediante el comando de `systemctl enable <nombre_del_servicio>.service` cree los enlaces simbólicos necesarios dentro del target multi-user.target.wants sin necesidad de hacerlo manualmente con el propósito de que el servicio se ejecute automáticamente al arrancar el target [67].

Capítulo 4. Resultados y Mantenimiento

En este último capítulo se mostrarán pruebas del correcto funcionamiento del sitio web, mostrando los resultados obtenidos de los procesos realizados para el diseño y desarrollo del sitio web.

Se mostrarán pruebas desde el buscador web de que este cuenta con un certificado de autenticación propio, esto se llevó a cabo mediante configuraciones realizadas a un servidor web real que alberga distintos sitios web que poseen sus propios certificados, por lo que se tomó en cuenta que dichas configuraciones no afectarán a los demás sitios y certificados.

En las pruebas se muestra una versión anterior del sitio web, debido a que se solicitaron cambios que ayudarían a mejorar el presente proyecto, como lo fue el cambio de dueño del sitio web, antes era el Laboratorio de Redes y Seguridad, ahora pertenece al Área de Redes y Seguridad, por otra parte, se agregó un formato válido a los materiales, debido a que algunos de los materiales que fueron desarrollados y expuestos ante este equipo de desarrollo funcionan mejor en formato .gif.

Se dará respuesta a la hipótesis planteada al inicio del trabajo "¿Por qué es tan importante la ciberseguridad en la vida personal, estudiantil y laboral?".

Por último, podrá consultar el sitio web vía Internet (`https://cibercultura.fi-b.unam.mx/`) desde cualquier dispositivo, aprender y reforzar su ciberseguridad por medio de la cibercultura que presentan los materiales creados y desarrollados por alumnos, los cuales fueron validados por los docentes que forman parte de este proyecto.

4.1 Pruebas del sitio web

Antes de montar el sitio web en el servidor se realizó la migración del proyecto a un sistema operativo Linux para probar que este funcionaba correctamente en dicha plataforma, por lo que se realizaron las instalaciones del editor de Visual Studio Code, ASP.NET Core 5.0, MariaDB y complementos para que el proyecto se conectará exitosamente con la base de datos.

Al extraer el proyecto de Windows se puede notar que se deja de trabajar con el servidor web de IIS Express, el cual funciona únicamente para este sistema operativo, otro elemento que deja de funcionar al salir de dicho sistema es la Autoridad Certificadora por lo que las comunicaciones que eran realizadas con HTTPS pasan a ser HTTP y empieza a funcionar el servidor web Kestrel debido a un archivo de configuración del proyecto que contempla este cambio de plataforma.

Para observar dicha comparación del funcionamiento del proyecto se pueden observar las figuras 4.1 y 4.2.

Figura 4.1Prueba realizada desde Windows.

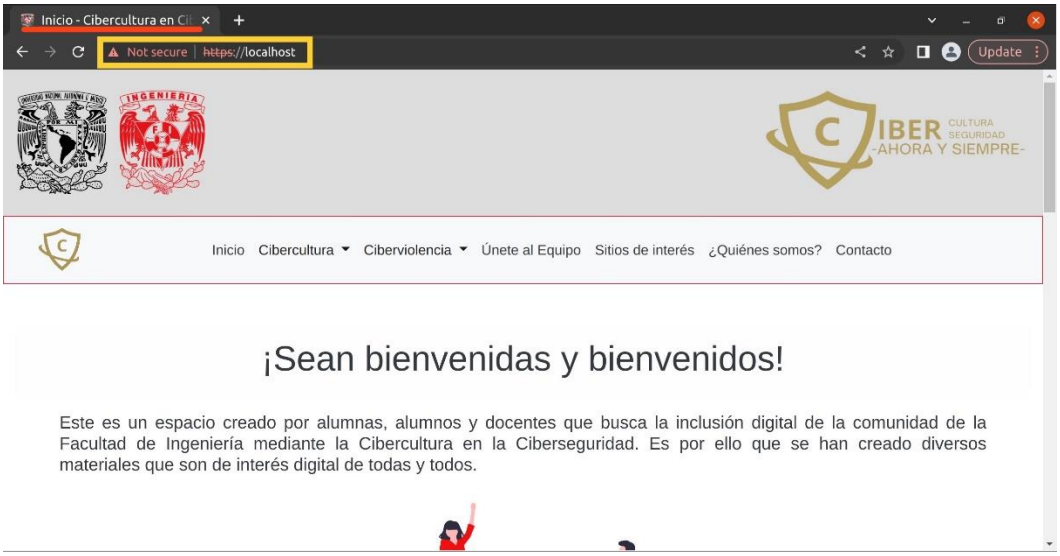


Figura 4.2 Prueba realizada desde Linux.

Los elementos para resaltar de ambas figuras son que en el rectángulo rojo que se muestra en la pestaña del navegador web la posición del usuario dentro del sitio, por ejemplo: Vista-Cibercultura en Ciberseguridad, en ambos casos se observa que el usuario se encuentra posicionado en Inicio y le seguirá la frase -Cibercultura en Ciberseguridad.

La comparación de la ejecución del proyecto en Windows vs. Linux radica en la cápsula amarilla que presentan ambas figuras, debido a que en Windows el IDE de

Visual Studio Community tiene integrada una autoridad certificadora (AC) local que brinda una conexión segura (https) con el servidor web IIS Express, mientras que en Visual Code se realiza una conexión no segura con Kestrel en Linux.

Al pasar la prueba de migración se procedió a hacer la transferencia del proyecto a un servidor virtual para probar el correcto funcionamiento del sitio y la base de datos. En la figura 4.3 se observa el sitio web desde un dispositivo móvil probando que el sitio funciona desde cualquier dispositivo dentro de la red de prueba.

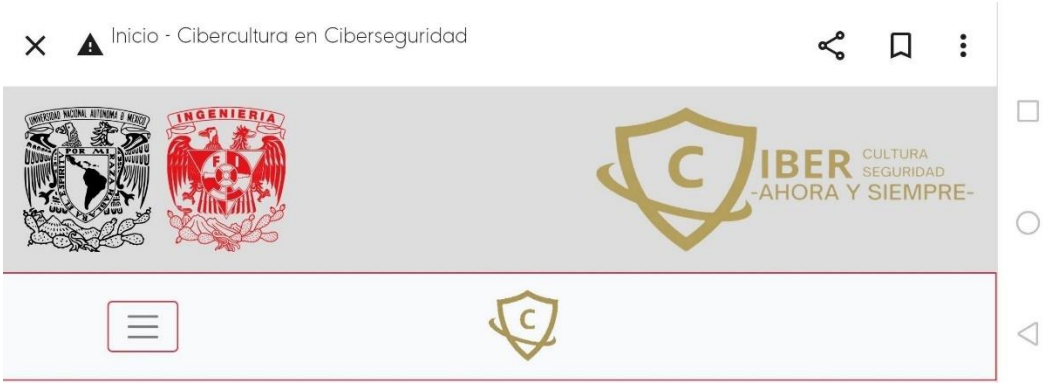


Figura 4.3 Sitio web desde un dispositivo móvil.

En la figura 4.4 se observa que la base de datos funciona correctamente debido a que el usuario administrador logra iniciar sesión. Después del inicio de sesión se probaron distintos materiales, los cuales se mostrarán más adelante.

Figura 4.4 Prueba de inicio de sesión.

El administrador es el responsable de publicar los distintos materiales, revisar, aceptar o rechazar solicitudes, llevar un histórico de los miembros del equipo, entre otros, por lo que se ejemplifican los aspectos más sencillos para comprobar que la interacción de la base de datos y el sitio web es funcional.

La primera prueba en llevarse a cabo del lado de la administración fue el llenar el formulario para la publicación de un material, en la figura 4.5 se muestra dicho formulario.

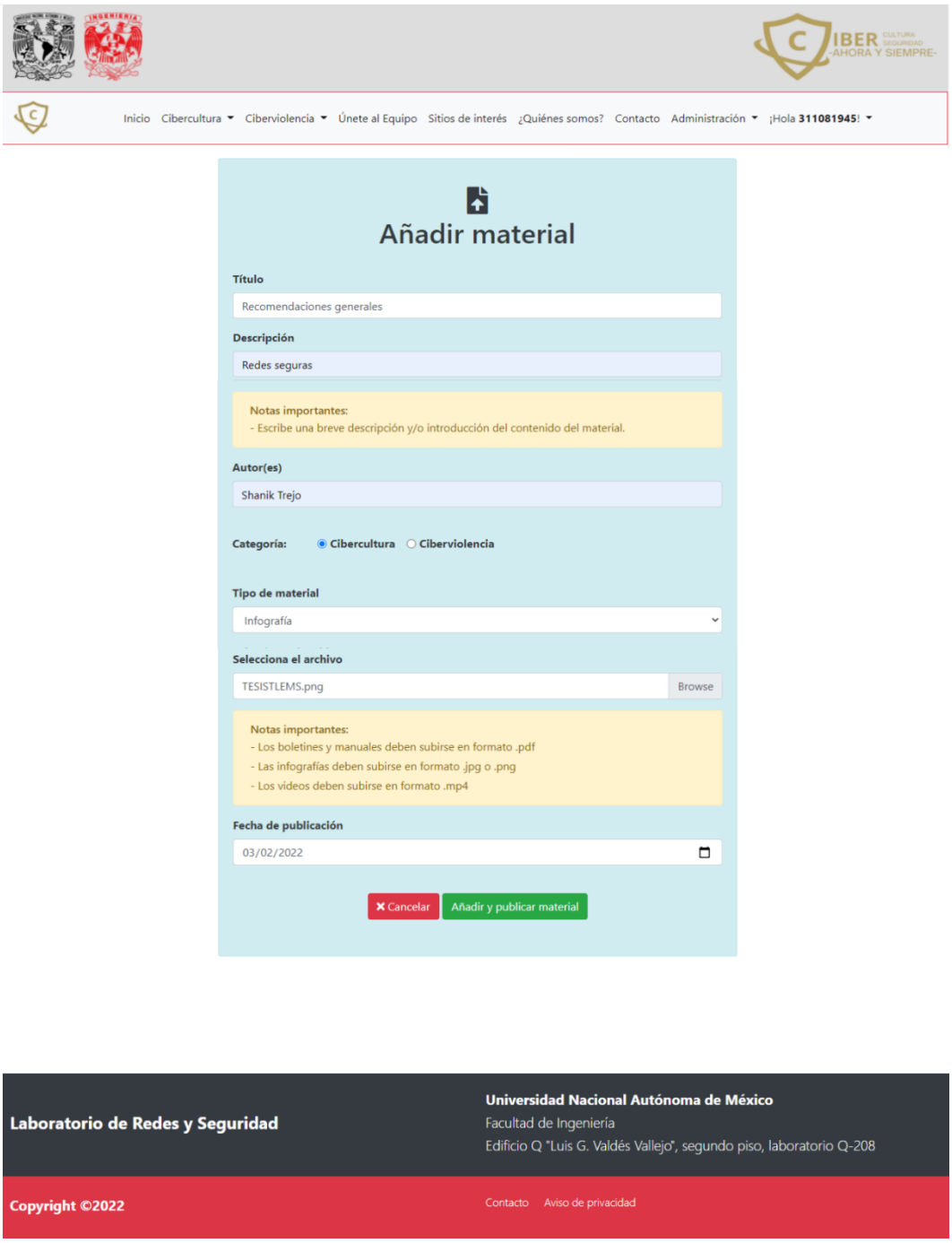


Figura 4.5 Ejemplo de la publicación de un material.

En la figura 4.6 se puede observar que el administrador ya ha subido distintos materiales, los cuales se le presentan en una tabla, la cual le permite realizar las operaciones de editar o eliminar cualquier material, además de que se le indica mediante una alerta que la operación realizada se llevó a cabo con éxito.

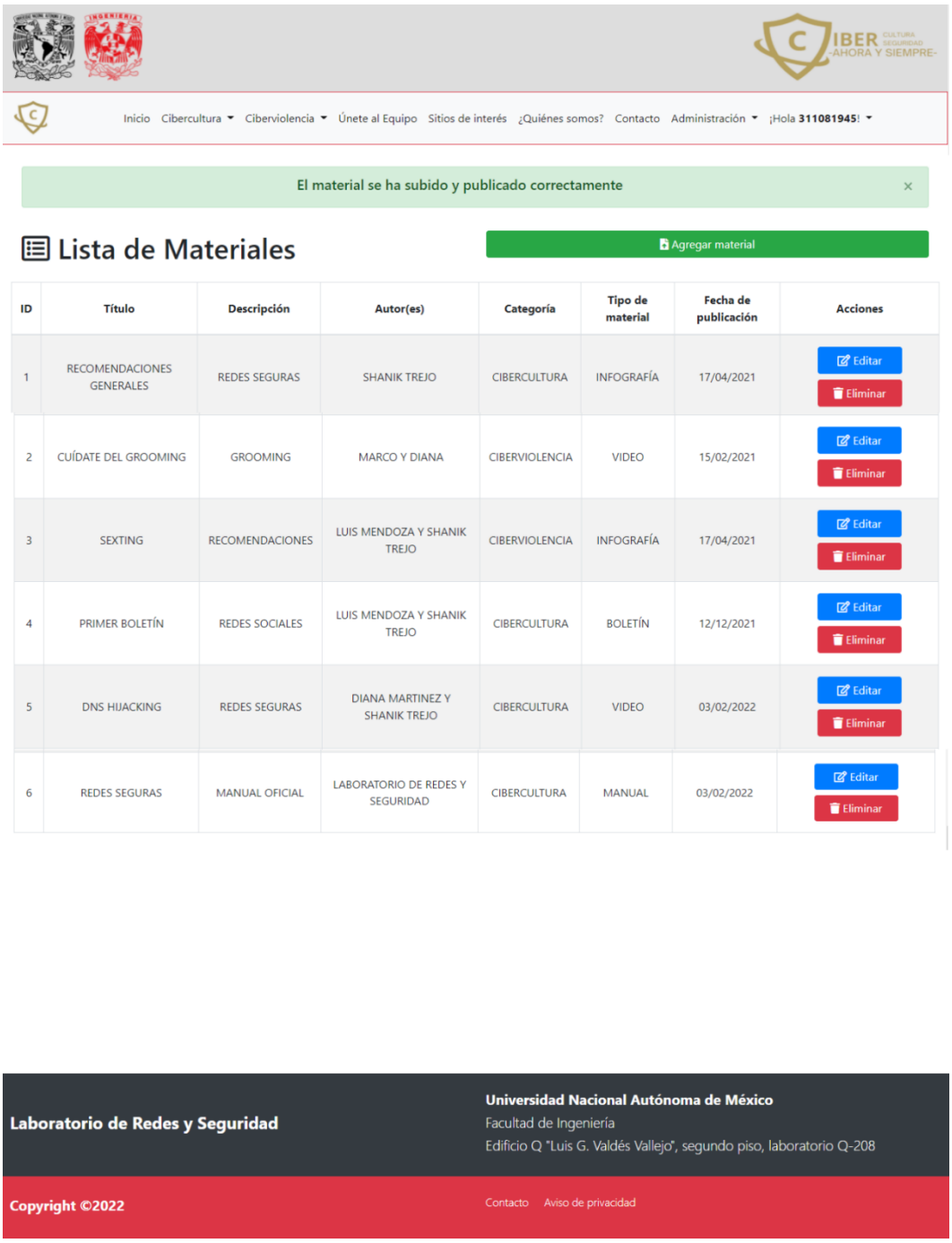


Figura 4.6 Ejemplo de la administración de los materiales.

En la figura 4.7 se observa que el administrador requiere realizar alguna modificación al material #1, por lo que en la lista de materiales se debe dar clic en "Editar" para modificar algún campo del material. En caso contrario se puede "Cancelar" la operación sin afectar el proceso.

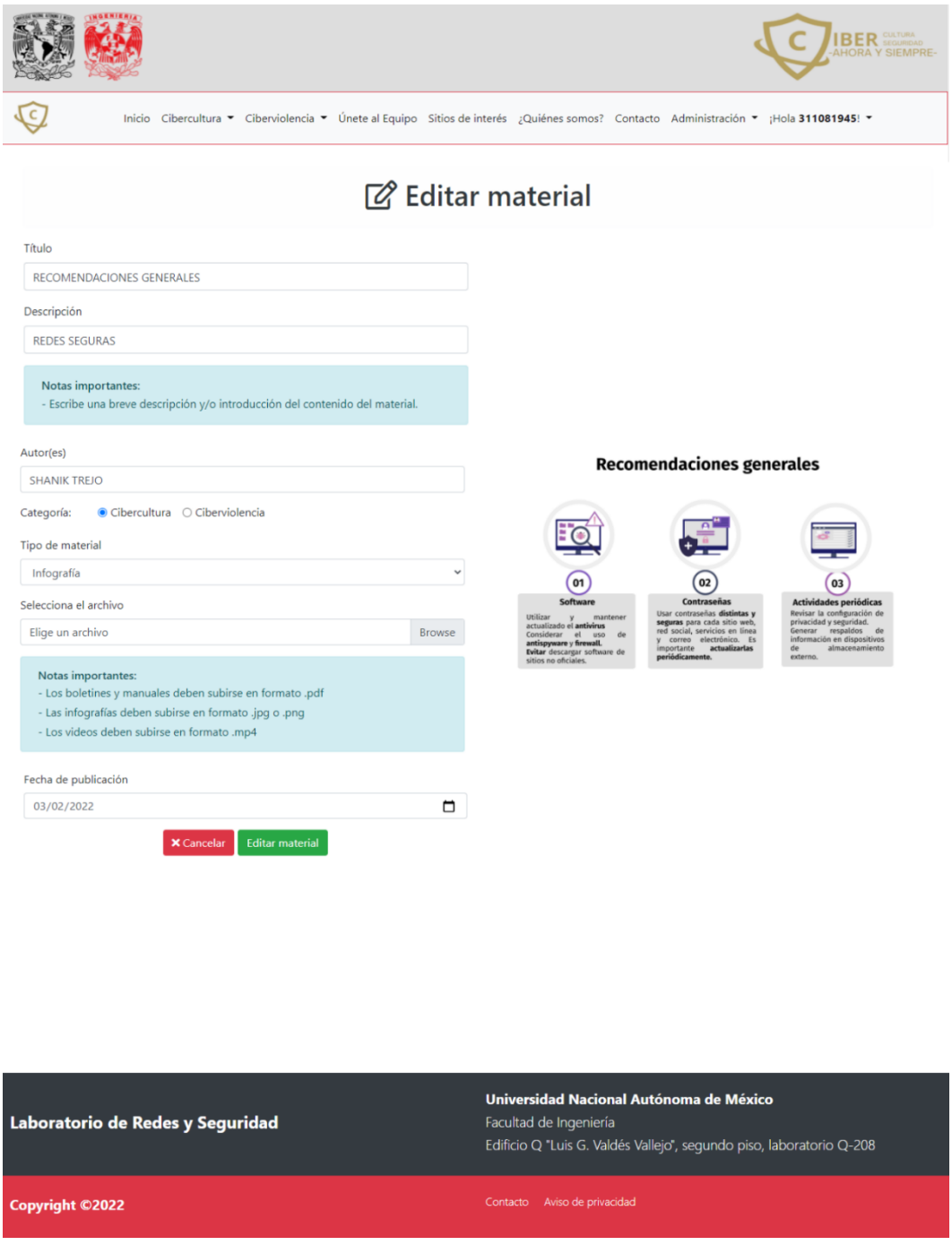


Figura 4.7 Edición de un material.

En la figura 4.8 se muestra una vista previa del material, así como los datos de este y los procesos para “Eliminar el material” y/o “Cancelar”, según se requiera.

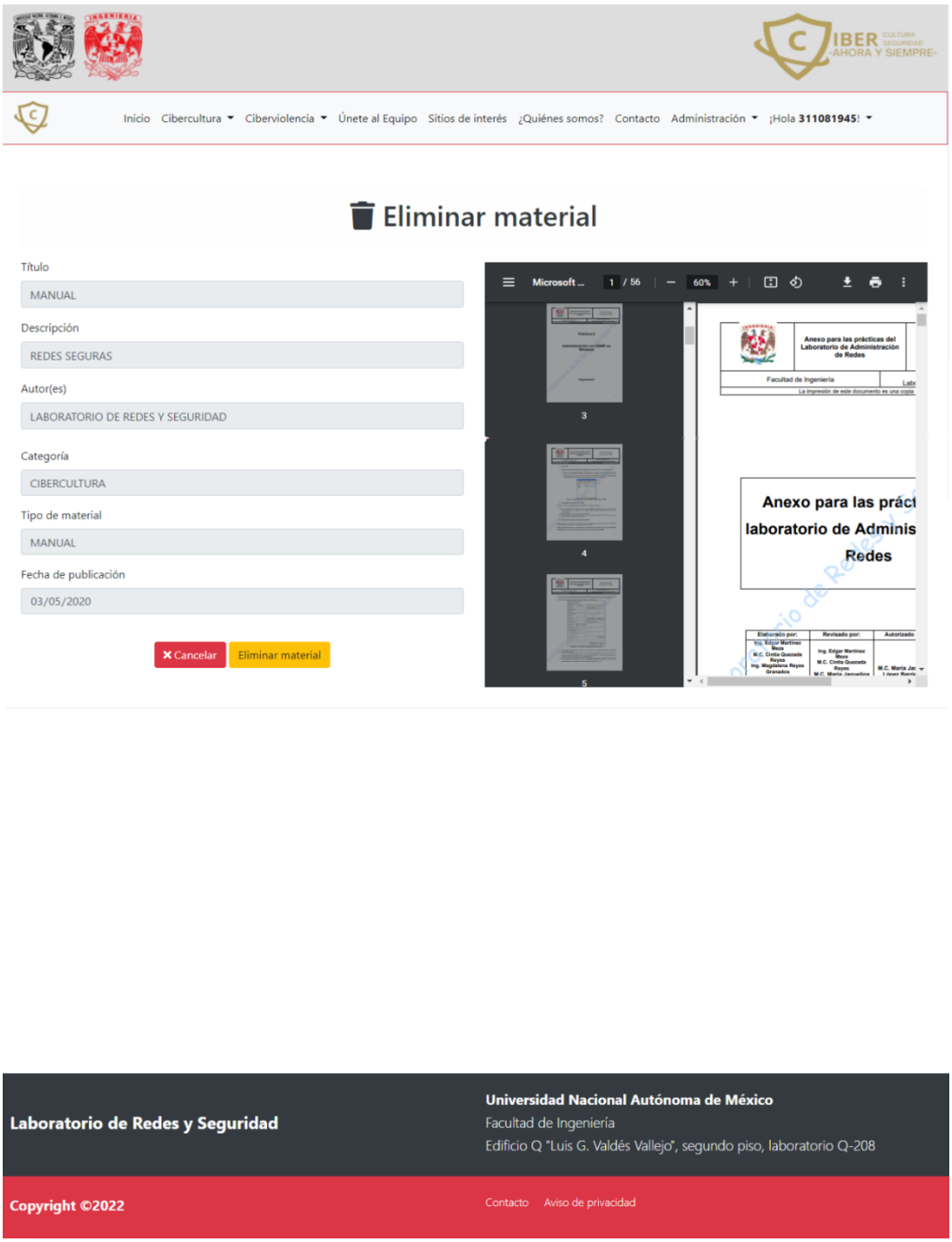


Figura 4.8 Eliminación de un material.

Nota: Para saber cómo se mostrarán los materiales de prueba desde la perspectiva de la Comunidad de la Facultad de Ingeniería podrá ser consultado en el anexo "Manual del usuario final".

A continuación, se muestra una prueba del apartado "solicitud para formar parte del equipo de "Cibercultura en Ciberseguridad: Ahora y siempre" vista desde la perspectiva de la comunidad de la Facultad de Ingeniería.

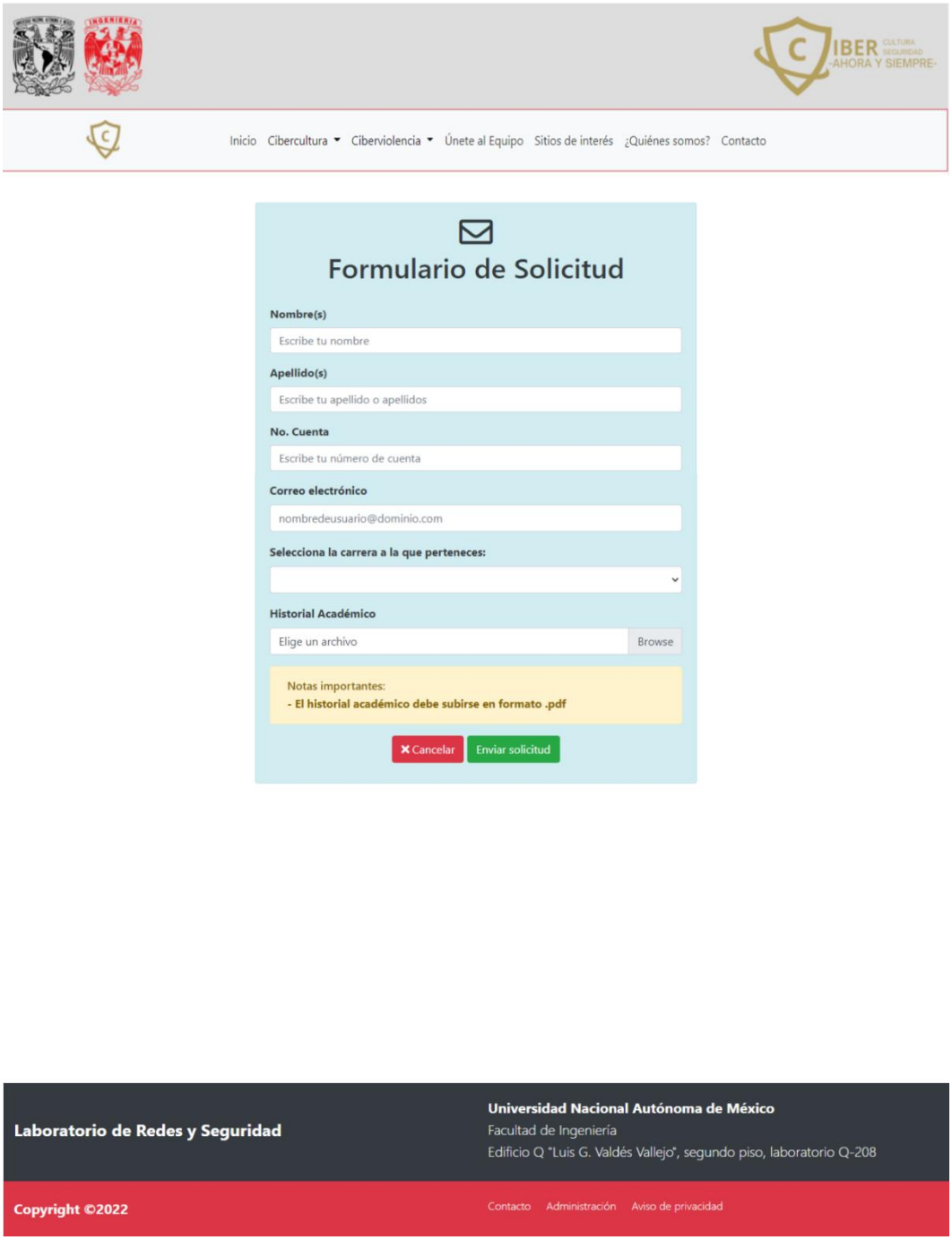


Figura 4.9 Ejemplo del envío de una solicitud para formar parte del proyecto.

En la sección administrativa “Revisión de la solicitud #1”, se muestra la solicitud recibida (ver figura 4.10) y se podrá aceptar y/o rechazar, según sea el caso. Adicionalmente el administrador puede no ejecutar ninguna acción dando clic en “regresar” al menú “Solicitudes”.

Figura 4.10 Revisión de una solicitud para formar parte del equipo.

En caso de que la solicitud sea aceptada, el administrador se pone en contacto con el postulante para la verificación de la información recibida, así como del proceso de las actividades a realizar en el tiempo asignado. Ver figura 4.11.

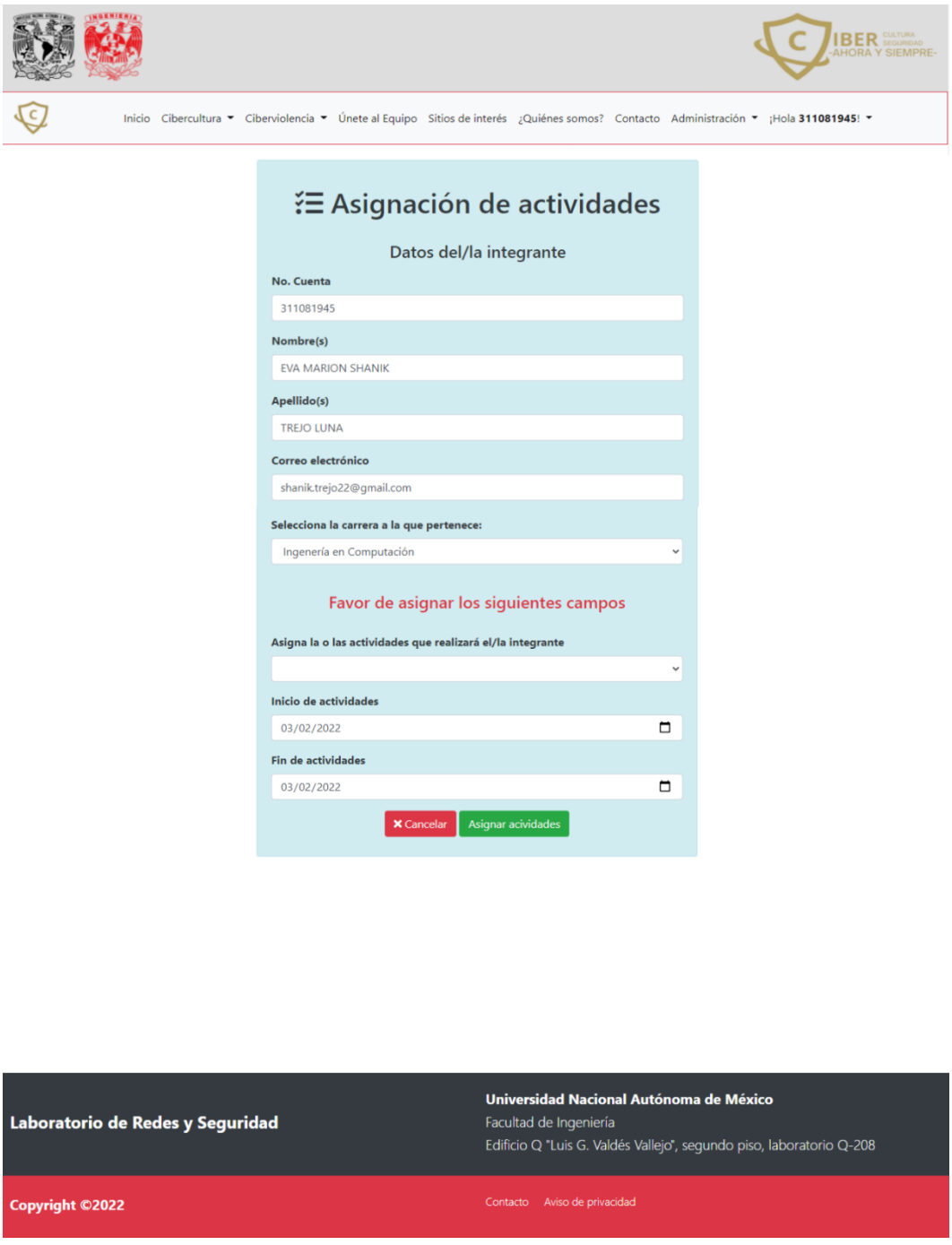


Figura 4.11 Ejemplo de asignación de actividades.

Al dar clic en el botón de Asignar actividades, se retorna al administrador a la tabla de Miembros del equipo, como se muestra en la siguiente figura.

Cabe destacar que las actividades pueden ser editadas en cualquier momento.

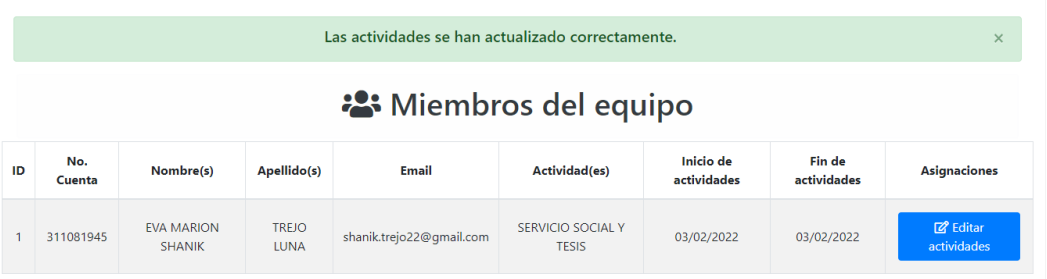


Figura 4.12 Actividades asignadas.

4.2 Resultados

Como resultados se puede mostrar la página web ya funcional, montada en el servidor; contando así con un nombre de dominio propio y a su vez con su certificado que permite las conexiones seguras mediante el protocolo HTTPS utilizando el puerto 443.

Para poder obtener este resultado final, fue necesario realizar la solicitud de un nombre de dominio para que este sitio web pudiera operar como un sitio independiente de los sitios existentes en el servidor. Dicho nombre de dominio fue solicitado por el departamento de la Facultad de Ingeniería.

Una vez obtenido el nombre de dominio, se realizaron las configuraciones necesarias para habilitar el host en el servidor y así iniciar el proceso de certificación de la página.

Finalmente, una vez habilitado el sitio en el servidor, con ayuda de la herramienta Certbot, fue posible generar las llaves privadas y los certificados para habilitar el acceso a la página mediante el puerto 443 a través del protocolo HTTPS. Adicional a esto, fue necesario la creación de un script que se encargara de la renovación periódica del certificado para que, de esta manera, siempre se mantenga una conexión segura.

Se observa en las figuras 4.13 a 4.15, el sitio web ya accesible desde Internet (`https://cibercultura.fi-b.unam.mx/`), así como su certificado.

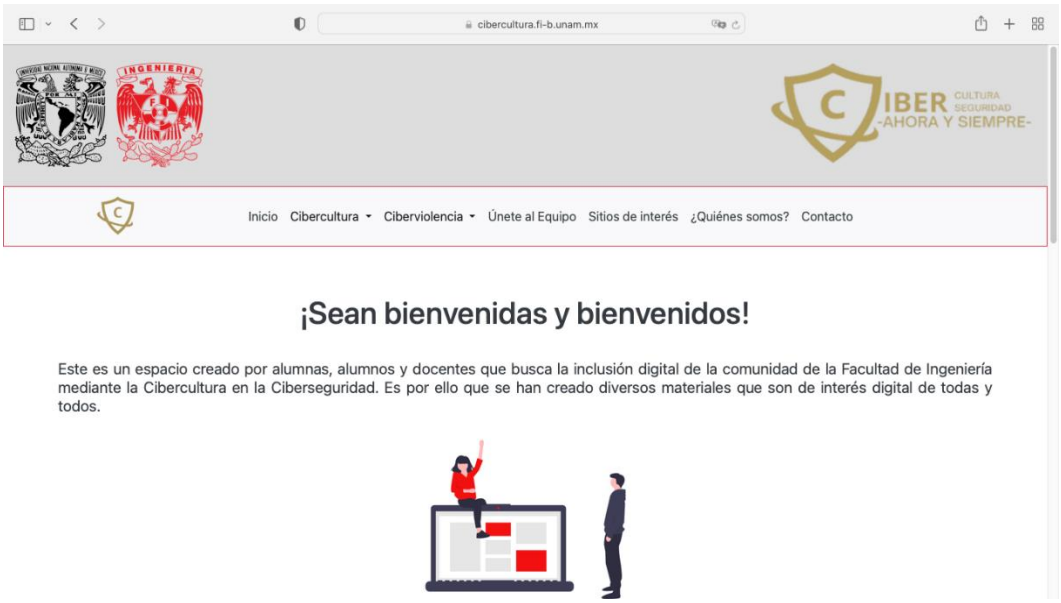


Figura 4.13 Visualización desde un navegador web en una computadora.

Figura 4.14 Visualización móvil.

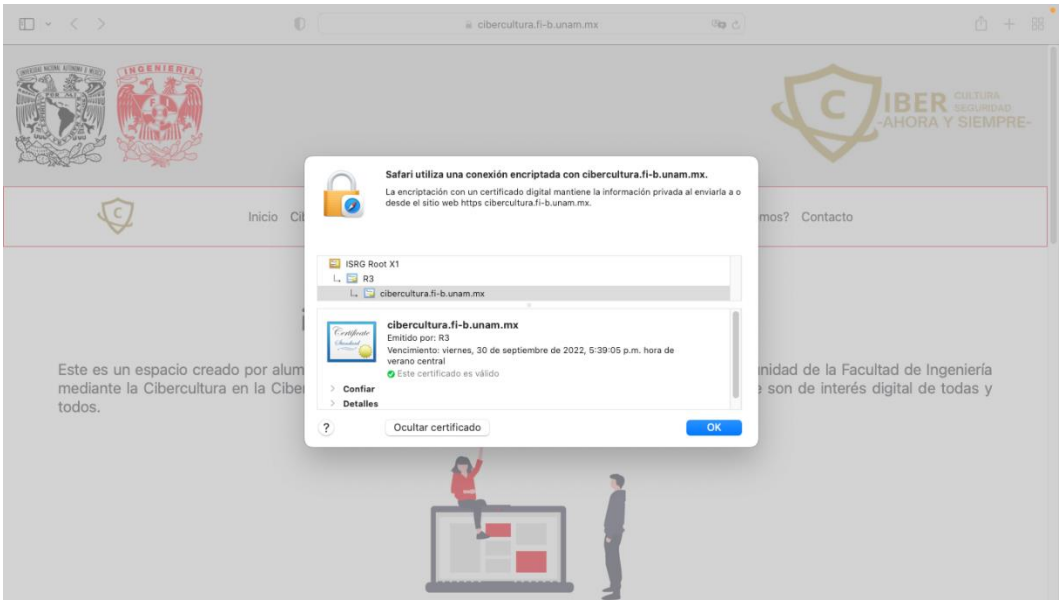


Figura 4.15 Certificado del sitio web.

En cuanto al mantenimiento del sitio web, es importante mencionar que conforme a las actualizaciones que requiera el proyecto se podrá consultar el anexo "Manual de creación del sitio web "Cibercultura en la ciberseguridad: Ahora y siempre" apartado "Desarrollo en Windows". En este anexo se puede obtener información acerca de la estructura del proyecto para poder llevar a cabo los cambios y nuevas implementaciones que sean necesarias, además de actualizar los paquetes que requiere el proyecto para su funcionamiento.

4.3 Respuesta a la hipótesis

La hipótesis planteada al inicio de este proyecto fue ¿Por qué es tan importante la ciberseguridad en la vida personal, estudiantil y laboral?

Al inició se planteó que la Ciberseguridad que las empresas proporcionan al ofrecer sus servicios en Internet podrían ser deficientes y que podrían mejorarse, pero también nosotros como individuos podemos fortalecer la seguridad de las aplicaciones o servicios que utilizamos diariamente en esta era digital hiperconectada mediante el uso y fomento de la cibercultura como respuesta a posibles riesgos y amenazas en Internet, sobre todo aquellas que traen consecuencias del mundo virtual al físico, puesto que detrás de cada username existe una persona que puede verse afectada física, mental, emocional o económicamente por no poderse proteger adecuadamente en el ciberespacio.

Es por ello que surge esta propuesta, la creación de un sitio web actualizado con frecuencia que promueva la Cibercultura en la Ciberseguridad todo el tiempo, mediante diversos materiales, los cuales buscan generar conciencia en la Comunidad de la Facultad de Ingeniería, con el fin de que los miembros de la comunidad adquieran las buenas prácticas y diversas medidas para disminuir los riesgos a los que puedan estar expuestos en el mundo digital, proveyéndoles de diversos métodos y herramientas para proteger su información además de que estos miembros sean capaces de ayudar a amigos, familiares y compañeros en la adopción de la Cibercultura en su vida diaria.

4.4 Liberación del sitio web

Después de realizar las pruebas correspondientes y de verificar que el sitio web creado en ASP.NET Core 5.0 funciona en un entorno de sistema operativo y servidor Linux, lo siguiente fue realizar la "Guía rápida de migración al servidor", la cual podrá ser consultada en el apartado de "Anexos", dicha guía fue enviada a revisión al encargado o encargada de administrar el servidor y realizar los cambios que fueran requeridos, una vez que se realizaron las modificaciones solicitadas, se prosiguió a alojar el sitio web en el servidor junto con los archivos de configuración, servicio y el certificado que asegura que el sitio web implementa el protocolo https (Protocolo Seguro de Transferencia de Hipertexto), la importancia de implementar https es garantizar a los usuarios que el sitio web es seguro y que sus datos estarán protegidos (en caso de enviar una solicitud de postulación al equipo de Cibercultura en Ciberseguridad: Ahora y Siempre). Además de que los datos que ingresen los administradores, tales como nombre de usuario y contraseña no sean interceptados, pues ellos son los responsables de subir los materiales y dar seguimiento a las candidaturas y miembros del equipo.

Conclusiones

A lo largo de este trabajo escrito hemos mencionado la importancia de los avances tecnológicos, en especial de Internet y los dispositivos con los que la comunidad se conecta a esta gran red; ya sea para fines educativos, sociales o de trabajo. Además de mencionar los conceptos básicos relacionados con el prefijo ciber, el cual está íntimamente ligado a Internet y a la identidad digital que las personas asumen en el ciberespacio. Esta tecnología es capaz de conectar a personas con intereses en común en distintas partes del mundo, pero también es utilizada con propósitos negativos, desde el ciberacoso hasta ciberviolencia a personas, empresas y naciones, por lo que también es importante identificar las vulnerabilidades, amenazas y ataques que suelen ser comúnmente perpetradas a través de Internet.
Es por ello que surge el proyecto "Cibercultura en Ciberseguridad: Ahora y Siempre", con el cual se busca crear un espacio de divulgación y participación comunitaria por parte del estudiantado y profesorado de la Facultad de Ingeniería, así como de voluntarios que quieran participar y aportar contenido e información valiosa acerca de estos temas.

Dentro de las categorías del sitio web se puede encontrar un apartado llamado Cibercultura, el cual es el espacio que se utiliza para crear campañas de concientización y fomentar las buenas prácticas para crear un entorno seguro en el ciberespacio, así como para reducir los posibles riesgos a los que todas y todos nos encontramos expuestos.

Por otro lado, el apartado Ciberviolencia es la categoría donde se puede encontrar el contenido relacionado con las campañas de concientización acerca de temas más específicos en cuanto a violencia digital e información útil que pueda ayudar a la comunidad a identificar estas acciones que puedan afectar su integridad, así como la de sus conocidos. Adicional a ello, se podrá encontrar tutoriales de cómo prevenir y evitar que estas acciones se sigan realizando en el Internet.

Teniendo en consideración lo anteriormente mencionado, se tomó la decisión de aplicar los conocimientos adquiridos a lo largo de la licenciatura para poder realizar este proyecto, pues gracias a dichos conocimientos y con ayuda de las herramientas correctas fue que se pudo desarrollar el sitio web propiamente para este proyecto, el cual se espera que la comunidad de la Universidad Nacional Autónoma de México así como del público en general se sume a este proyecto y visite este sitio para poder generar un cambio en nuestra sociedad y poder lograr difundir la Cibercultura en el ciberespacio.

Anexos

Glosario de términos

AC (Autoridad de Certificación): Es una entidad de confianza responsable de emitir y revocar los certificados digitales utilizados en las transacciones y firmas electrónicas.

AP o WAP (Access Point o Wireless Access Point): También conocidos como Puntos de Acceso en español.

API (Application Programming Interfaces): En español se conoce como Interfaz de Programación de Aplicaciones, las API son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos.

ApplicationDbContext: Subclase de DbContext, es un servicio con ámbito en el proveedor de servicios de aplicación de ASP.NET Core (conocido por ser un contenedor de inserción de dependencias). El contexto se configura para utilizar el proveedor de base de datos, el cual leerá la cadena de conexión de la configuración de ASP.NET Core.

APT (Advance Persistent Threat): En español se le conoce como Amenaza Persistente Avanzada. Es un ataque complejo y de elevado nivel con el objetivo de obtener datos confidenciales durante un largo período de tiempo.

ARPANET (Advanced Research Projects Agency Network): En español se le conoce como Agencia de Proyectos de investigación Avanzada.

ASP.NET Core: Es un framework de código abierto, multiplataforma y de alto rendimiento que permite agilizar el proceso de desarrollo reutilizando módulos y herramientas.

ASP.NET Core Identity: Es una API que admite la funcionalidad de inicio de sesión de la interfaz de usuario (UI).La cual permite administra usuarios, contraseñas, datos de perfil, roles, reclamos, tokens, confirmación por correo electrónico y más.

Back-end: Parte del desarrollo web que se encarga de otorgar las funcionalidades en el servidor, el cual es el encargado de alojar y ejecutar el sitio web.

Bootstrap: Es un framework front-end utilizado para desarrollar aplicaciones web y sitios Mobile First, es decir, que adapta el contenido del sitio a la pantalla del dispositivo del usuario.

Certificados SSL: Es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada.

CID: Son las siglas de la triada de la seguridad informática (Confiabilidad, Integridad y Disponibilidad).

Cibercultura: Representa a diferentes movimientos culturales que se han ido gestando con la evolución de las tecnologías de la información y comunicación sobre el espacio, la realidad, las relaciones humanas y sociales.

Ciberviolencia: Violencia digital a través de las redes sociales, tiene diversas manifestaciones como el ciberbullying, el sexting, el grooming, entre otros, la

forma de actuar del agresor es mediante alguno de los siguientes ejemplos: la difusión de datos e imágenes personales sin el consentimiento de la víctima, amenazas, difamaciones, acoso, humillación, ataques que afectan la libertad de expresión entre otras.

CLI (Command-Line Interface/Interfaz de Línea de Comandos) : Es una interfaz de texto, a la que se accede mediante comandos en prompts, en lugar de usar el mouse a través de la interfaz gráfica del usuario (GUI). CLI también se denomina símbolo del sistema operacional Windows, o terminal/pantalla de comando en macOS.

Código QR: Proviene del inglés Quick Response code, por lo que en español se traduce como código de respuesta rápida, este es la evolución del código de barras.

CONDUSEF: Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

COVID-19: Enfermedad infecciosa provocada por el virus SARS-CoV-2.

CPU (Central Processing Unit): En español se conoce como Unidad Central de Procesamiento, es un componente de hardware que se encuentra dentro de un dispositivo programable (computadoras, smartphones y otros dispositivos inteligentes). Su trabajo es interpretar las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y externas.

CRUD: acrónimo de "Crear, Leer, Actualizar y Borrar" (del inglés: Create, Read, Update and Delete),que se usa para referirse a las funciones básicas en bases de datos o la capa de persistencia en un software.

CSS: Del inglés Cascading Style Sheets o en español Hojas de estilo en cascada.

CVE/CVSS (Common Vulnerability and Exposures/Common Vulnerability Scoring System):CVE significa vulnerabilidades y exposiciones comunes. CVE es un glosario que clasifica las vulnerabilidades. El glosario analiza las vulnerabilidades y luego utiliza el Sistema de puntuación de vulnerabilidad común (CVSS) para evaluar el nivel de amenaza de una vulnerabilidad. Una puntuación CVE se usa a menudo para priorizar la seguridad de las vulnerabilidades.

CVV (Card Verification Value) o CVC (Card Verification Code): En español Valor de Verificación de Tarjeta (CVV) o Código de Verificación de Tarjeta (CVC) dicho valor de verificación o código de verificación suele estar compuesto por tres dígitos que son establecidos por las compañías que fabrican las tarjetas bancarias.

CWE (Common Weakness Enumeration): Es un sistema de categorías para las debilidades y vulnerabilidades del software.

DbContext: Es una instancia que representa una sesión con la base de datos y se puede usar para consultar y guardar instancias de sus entidades. DbContext es una combinación de los patrones Unidad de trabajo y Repositorio.

DBMS (DataBase Management System): El sistema manejador de bases de datos se utiliza como una interfaz entre la base de datos, el usuario y las distintas aplicaciones utilizadas.

DDL(Dynamic Link Library): Es una biblioteca de vínculos dinámicos que cumplen con el objetivo de proveer de una serie de archivos que constan de código ejecutable y demás partes de una app, los cuales hacen posible la utilización de las aplicaciones que se instalan en la computadora.

Desarrollo web: Proporciona diversas funcionalidades al sitio implementando lenguajes de programación.

DIE: Son las siglas de División de Ingeniería Eléctrica.

Dirección IP: Es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "Protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local. Por lo que las direcciones IP son el identificador que permite el envío de información entre dispositivos en una red. Contienen información de la ubicación y brindan a los dispositivos acceso de comunicación, lo que le facilita al Internet el poder diferenciar entre distintas computadoras, routers y sitios web que se encuentran interactuando dentro de él.

Diseño web: Es la parte que se encarga de lo visual del sitio web contemplando la experiencia de usuario usando herramientas enfocadas al diseño sin implementar lenguajes de programación.

DNS (Domain Name System): En español se conoce como Sistema de Nombres de Dominio. Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados tanto a Internet como a redes privadas que asocia a las direcciones IP de los sitios web con el nombre del dominio que tienen registrado.

DoS (Denial of Service): La Denegación de Servicio es un ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

DDoS (Destributed Denial of Service): La Denegación de Servicio Distribuido es un DoS que envía las peticiones desde diversos orígenes, de esta forma es más efectivo, complicado de detener y determinar su origen.

Editor de código: Es un programa ligero que no exige mucha RAM (Random Access Memory, en español Memoria de Acceso Aleatorio) o procesador, en dónde se puede abrir y crear un archivo a la vez y guardarlo en una carpeta además permite agregarle plugins para realizar muchas más funciones, por ejemplo, hacer que pueda soportar múltiples lenguajes con el objetivo de volverlo más potente.

EF Core (Entity Framework Core): Su función principal es servir como intérprete entre dos tecnologías fundamentadas en distintos principios por un lado la programación orientada a objetos y por el otro las bases de datos relacionales y no relacionales.

FI: Facultad de Ingeniería.
Fontawesome: Biblioteca de iconos vectoriales y estilos CSS.
Framework: Es una estructura base utilizada como punto de partida para elaborar un proyecto con objetivos específicos.
Front-end: Es la parte del desarrollo web que parte del diseño frontal del sitio, es decir, implementa los lenguajes de programación y marcado que utilizan los navegadores web, tales como HTML, CSS, JavaScript, PHP y diversos frameworks dedicados a esta.
FTP (File Transfer Protocol): El protocolo de transferencia de archivos es un protocolo de red que se utiliza para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor.
Git: Sistema de control de versiones.
GitHub: Es un portal creado para alojar el código de las aplicaciones de cualquier desarrollador.
GNU/Linux: Familia de sistemas operativos tipo Unix compuesto por software libre y de código abierto. GNU/Linux surge de las contribuciones de varios proyectos de software, entre los que destacan GNU y el kernel Linux.
GUI (Graphical User Interface/Interfaz Gráfica de Usuario): Es una interfaz que se puede utilizar para controlar computadoras, tabletas y otros dispositivos. Las GUI utilizan elementos gráficos como iconos, menús e imágenes para facilitar el manejo del usuario.
HTTP (HyperText Transfer Protocol): El Protocolo de Transferencia de Hipertextos, se encarga de otorgar el acceso a las páginas, sitios y aplicaciones web a través de Internet.
HTTPS (HyperText Transfer Protocol Secure): El Protocolo Seguro de Transferencia de Hipertexto es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus dispositivos y la página, aplicación o el sitio web al que está accediendo.
HTML (HyperText Markup Language): El Lenguaje de Marcas de Hipertexto es el componente más básico de la Web. Define el significado y la estructura del contenido web.
IDE (Integrated Development Environment): El Entorno de Desarrollo Integrado es un sistema de software para el diseño de aplicaciones que combina herramientas comunes para desarrolladores en una sola Interfaz de **Usuario Gráfica (GUI)**.
IdentityDbContext: Clase base para el contexto de la base de datos de Entity Framework utilizada para la identidad.
IFormFile: Es una representación de C# del archivo que se usa para procesar o guardar el archivo.

Index: Es el nombre que comúnmente se utiliza para la página predeterminada que se muestra en un sitio web.
INEGI: Instituto Nacional de Estadística y Geografía.
IP (Internet Protocol): Protocolo de Internet.
IRSF (International Revenue Share Fraud): El Fraude internacional de ingresos compartidos es de tipo telefónico, este utiliza medios técnicos para realizar llamadas no autorizadas a números premium. Los ciberdelincuentes usan teléfonos pirateados, tarjetas SIM robadas y PBX corporativos comprometidos para dirigir llamadas a sus propias líneas o líneas alquiladas con facturación de conexiones entrantes. Otro método de ataque de IRSF es una llamada directa que obliga a la víctima a devolver la llamada a un número premium.
ItemGroup: Conjunto de elementos Item definidos por el usuario para crear su aplicación en MSBuild.
ITU (International Telecommunication Union): En español es la Unión Internacional de Telecomunicaciones.
jQuery: Es una biblioteca de JavaScript minificada de código abierto creada para simplificar las operaciones de JavaScript.
Kernel: Es el núcleo del sistema operativo, este se encarga principalmente de mediar entre los procesos de usuario y el hardware disponible en la máquina.
Layout: Es un esquema que resume y señala la distribución y forma de los elementos dentro de un diseño.
LGBT+: Lesbiana, Gay, Bisexual, Transgénero, Transexual, Travesti, Intersexual y Queer. Al final se suele añadir el símbolo + para incluir todos los colectivos que no están representados en las siglas anteriores.
MacOS: Es un sistema operativo diseñado por Apple que está instalado en todos los equipos creados por la compañía Apple Inc.
MariaDB: Es un sistema manejador de bases de datos (DBMS).
Microsoft (acrónimo de Microordenador y Software): Empresa tecnológica multinacional, la cual desarrolla, fabrica, licencia y da soporte a ordenadores personales, servidores, dispositivos electrónicos y servicios.
MIT (Massachusetts Institute of Technology): Instituto Tecnológico de Massachusetts.
MITM: Man In The Middle u hombre en el medio. Es un ataque que le permite al ciberdelincuente alterar o interceptar los paquetes de información que son transmitidos entre un emisor y receptor, facilitando el secuestro de una conexión autorizada o denegar la capacidad de una persona para usar determinados servicios de red.
MOCIBA: Módulo sobre Ciberacoso.

MSBuild (Microsoft Build Engine): Es una plataforma para crear aplicaciones. Este motor, proporciona un esquema XML para un archivo de proyecto que controla cómo la plataforma de compilación procesa y compila el software.
MVC (Model-View-Controller o Modelo-Vista-Controlador): Es un patrón de arquitectura que permite separar las responsabilidades de la interfaz de usuario (Vista), la lógica de negocios de la aplicación (Controlador) y los datos que maneja dicha aplicación (Modelo).
MX: México.
MySQL: Es el sistema de gestión de bases de datos relacional más extendido en la actualidad al estar basada en código abierto, tiene una versión gratuita y otra comercial, la cual es gestionada por la compañía Oracle.
NuGET: Es un administrador de paquetes compatible con Microsoft para compartir código.
OWASP (Open Web Application Security): Es una metodología de seguridad de código abierto y colaborativa que se utiliza como referente para auditorias de seguridad de aplicaciones web.
PBX (Private Branch Exchange): Central telefónica privada.
PHP (Hypertext Preprocessor): Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.
Pipeline de CI/CD: Los principales conceptos que se atribuyen a un CI/CD son la integración continua (CI), la distribución continua (CD) y la implementación continua (el otro CI).Un pipeline CI/CD es un conjunto de prácticas para incorporar la automatización continua y el control permanente en todo el ciclo de vida. Desde las etapas de integración y prueba, hasta las de distribución e implementación del proyecto de software.
Plugins: Son complementos que añaden funcionalidades extra o mejoras a los programas.
Posicionamiento SEO (Search Engine Optimization): Conjunto de técnicas que se aplican en una página web con el objetivo de mejorar su posición y su visibilidad en los motores de búsqueda de los principales navegadores.
Protocolo ACME (Automated Certificate Management Environment o en español Entorno de Gestión de Certificados Automatizado): El protocolo ACME permite comunicar con la AC directamente del servidor y sirve para la obtención e instalación automática de los certificados SSL/TLS.
Protocolo TLS (Transport Layer Security o Seguridad de la Capa de Transporte en español): Es una versión actualizada y más segura de SSL.
PuTTY: El nombre PuTTY proviene de las siglas Pu: Port unique TTY: Teletipo (por sus siglas en inglés) o Teletipo de puerto único, es un emulador de terminal gratuito que admite varios protocolos de red como SSH.

Razor: En una sintaxis basada en C# que permite usarse como motor de programación en las vistas o plantillas de los controladores de ASP.NET Core MVC.
Scaffolding en ASP.NET Core: Es la generación de áreas, controladores, vistas y páginas con código predefinido.
SDK (Software Development Kit): En español es un kit de desarrollo de software, el cual reúne un grupo de herramientas que les permiten a los desarrolladores la programación de aplicaciones para un sistema, plataforma o lenguaje de programación específico.
SIM (Subscriber Identity Module): El Módulo de Identificación de Abonado es una tarjeta inteligente desmontable usada en teléfonos móviles y módems.
Slidesgo: Plantillas para PowerPoint y Google Slides gratis.
SMS (Short Message Service): Servicio de Mensajes Cortos.
SQL (Structured Query Language): Lenguaje de Consulta Estructurada diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos relacionales.
SSH (Secure SHell): El intérprete de órdenes seguro es un protocolo y que a su vez también es un programa que lo implementa cuya función principal es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.
SSL (Secure Sockets Layer o Capa de sockets seguros en español): Es un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
SSRF (Server Side Request Forgery): La falsificación de solicitudes del lado del servidor es una vulnerabilidad que puede ser aprovechada por un atacante, dicha vulnerabilidad ocurre cuando una aplicación web permite consultas HTTP del lado del servidor hacia un dominio arbitrario elegido por el atacante.
Stuxnet: Malware.
Target Framework (Marco de destino): Se utiliza para especificar el conjunto de APIs que se requieren implementar en la aplicación o biblioteca.
TIC: Tecnologías de la Información y la Comunicación.
UNAM: Universidad Nacional Autónoma de México.
Unix: Es un sistema operativo portable, multitarea y multiusuario.
URL (Uniform Resource Locator): Es la dirección única y específica que se asigna a cada uno de los recursos disponibles de la World Wide Web para que puedan ser localizados por el navegador y visitados por los usuarios.
VoIP (Voice over Internet Protocol): La Voz sobre el Protocolo de Internet es una tecnología que proporciona la comunicación de voz y sesiones multimedia (tales como video) sobre **Protocolo de Internet (IP)**.
WannaCry: Ataque de ransomware.

WhatsApp: Aplicación de mensajería instantánea para teléfonos inteligentes.
WiFi: Wireless Fidelity (Fidelidad Inalámbrica) es la tecnología móvil que se usa para conectar computadoras, tablets, smartphones y otros dispositivos a Internet.
Windows: Es un sistema operativo que se implementa en computadoras, teléfonos inteligentes y otros sistemas informáticos, creados y comercializados por la empresa norteamericana Microsoft.
wwwroot: Esta carpeta es la que actúa como raíz del sitio web, es donde se encontrarán los archivos estáticos requeridos por el sitio web.
XAMPP: Es una distribución de Apache que incluye varios softwares libres. El nombre es un acrónimo compuesto por las iniciales de los programas que lo constituyen: el servidor web Apache, los sistemas relacionales de administración de bases de datos MySQL y MariaDB, así como los lenguajes de programación Perl y PHP. La inicial X se usa para representar a los sistemas operativos Linux, Windows y Mac OS X.
XML (Extensible Markup Language): Es un lenguaje de marcado, al igual que el HTML (utilizado para programar páginas Web), definido y mantenido por el World Wide Web Consortium (W3C). El objetivo del XML se enfoca en la simplicidad, generalidad y usabilidad por parte de toda la Internet.
XSS (Cross Site Scripting): Secuencia de comandos en Sitios Cruzados es una vulnerabilidad típica de las aplicaciones web.
XXE (XML External Entity): Es una vulnerabilidad presente en las aplicaciones que analizan entradas XML.

Cuestionario

El cuestionario se realizó mediante la herramienta de Formularios de Google, el cual tiene por nombre "Cibercultura en la Facultad de Ingeniería (UNAM)", en el año 2020, la razón de utilizar dicha herramienta fue por la practicidad de ser enviada vía Internet al máximo número de estudiantes en plena pandemia del COVID-19, con el objetivo de recopilar información para llevar a cabo un estudio que permitiera identificar el nivel de conocimiento en términos de Seguridad Informática y Ciberseguridad que tienen los integrantes de la comunidad estudiantil que cursan alguna de las diversas carreras que son impartidas en la Facultad de Ingeniería.

Los datos recabados del estudio se utilizaron para determinar las Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de este sector de la comunidad por la persona encargada de crear los materiales, por otra parte este cuestionario se utilizó de base para crear diversos mini cuestionarios por alumnos que prestaron su servicio social en el equipo de "Cibercultura en Ciberseguridad: Ahora y siempre" que fueron respondidos por los docentes para cubrir sus respectivas necesidades, debido a que este cuestionario es de carácter interno sólo se mostrará la estructura de las 16 secciones que éste posee, las cuales incluyen:

La principal razón de haber participado en la realización de dicho cuestionario fue para conocer los requerimientos que se tendrían que tomar en cuenta para la difusión de los materiales que se crearían y solo aceptar los formatos válidos para cada tipo de material.

1) La carrera que estudian los encuestados.
2) El avance académico (por bloques de semestres aprobados).
3) Datos personales.
    a) El rango de edad en el que se encuentran.
    b) Género.
4) Dispositivos con los que acceden a Internet (se muestra una lista).
5) Uso de dispositivos ajenos para acceder a cuentas privadas.
6) Tiempo de consulta en diferentes servicios de Internet:
    a) Redes sociales.
    b) Streaming de música.
    c) Streaming de video (series y películas).
    d) Noticias.
    e) Videojuegos.
    f) Banca electrónica.
7) Uso de redes públicas.
    a) Motivos por los que se conectan (en caso de hacerlo) a este tipo de red.
    b) Requisitos para conectarse.

c) Lugares de conexión.
d) Servicios que utilizan.

8) Uso de redes sociales (en caso afirmativo).
   a) ¿Qué redes sociales utilizan? (se muestra una lista).
   b) Tiempo de uso.
   c) Tipos de perfil que tienen.
9) Seguridad en la privacidad.
   a) Aceptan o rechazan la solicitud de amistad de un desconocido.
   b) Bases para aceptar o rechazar la solicitud.
   c) En caso de aceptar la solicitud: Inician la conversación o esperan que la otra persona tome la iniciativa.
10) Seguridad en contraseñas.
   a) Misma contraseña para varios sitios web o distintas.
   b) Afirmación de poseer contraseñas seguras.
   c) Tipos de combinaciones o métodos para crear contraseñas (se muestra una lista).
   d) Conocimiento de las repercusiones de tener contraseñas inseguras.
   e) Medición del nivel de seguridad de contraseñas mediante una herramienta externa.
   f) Acepta o rechaza el almacenamiento automático en diferentes medios.
   g) Medios de almacenamiento de las contraseñas (se muestra una lista).
   h) Conocimiento de los gestores o administradores de contraseñas.
   i) Frecuencia del cambio de contraseñas.
11) Fraudes.
   a) Conocimiento sobre sí se es o fue víctima de algún fraude en Internet.
   b) Señalar el tipo de fraude del que se fue víctima (en caso afirmativo se muestra una lista con opciones).
   c) Tiene conocimiento sobre cómo evitar ser víctima de un delito por Internet.
   d) Conocimiento de a dónde acudir en caso de ser una víctima de un delito por Internet.
12) Antivirus.
   a) La importancia que le dan a contar con un antivirus instalado en los dispositivos electrónicos que utilizan.
   b) Cuentan con antivirus instalados en todos sus dispositivos.
   c) En caso de contar con antivirus mencionar si conocen los beneficios que le ofrecen.
   d) En caso de tener antivirus cada cuanto lo actualiza.
13) Nube.
   a) Uso la nube para almacenar información.
   b) En caso afirmativo:

i) Mencionar cuales son los servicios en la nube que se utilizan (nube: privada, pública e híbrida).
ii) Conoce el nivel de seguridad que brinda o brindan dichas nubes.
iii) De los servicios dónde se almacena su información importante se está seguro de qué solo usted puede acceder a sus archivos.

14) Copias de seguridad.
   a) Creación de copias de seguridad.
   b) En caso afirmativo:
      i) Indicar la frecuencia.
      ii) Indicar los medios.
15) Aplicaciones orientadas a su carrera (se muestra una lista).
16) Aplicaciones diversas.
   a) Uso de aplicaciones de paga.
   b) Tipos de aplicaciones para:
      i) Entretenimiento.
      ii) Hacer compras.
      iii) Salud.
      iv) Finanzas.
      v) Servicios de transporte.
      vi) Reservación de hospedaje.
      vii) Servicios gubernamentales.

La principal razón de haber participado en la realización de dicho cuestionario fue para conocer los requerimientos que se tendrían que tomar en cuenta para la difusión de los materiales que se crearían y solo aceptar los formatos válidos para cada tipo de material.

Nota: El "Análisis de la Encuesta" contiene información que se utilizará para el tema de tesis "Materiales didácticos para fomentar la cibercultura en la Facultad de Ingeniería FI" que fue realizado por Martínez Santana Diana Anayanssi.

Boceto del diseño del sitio web

En este anexo se muestran todos los bocetos creados para el diseño y desarrollo del sitio web, la mayoría de ellos ya fueron explicados en el Capítulo 2 apartado “2.2 Boceto del diseño del sitio web”, por lo que en este anexo se dará mayor énfasis en las vistas dinámicas de las secciones de Cibercultura y Ciberviolencia.

Vistas visibles para la comunidad

Inicio.

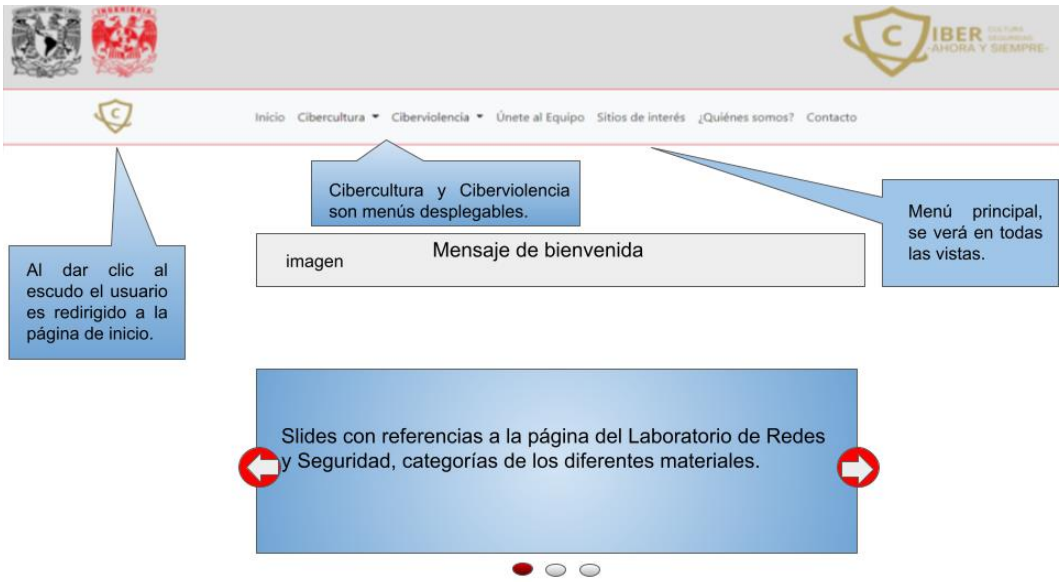


Figura 1. Vista de inicio parte 1.

Menús desplegables y sus apartados:
Cibercultura.

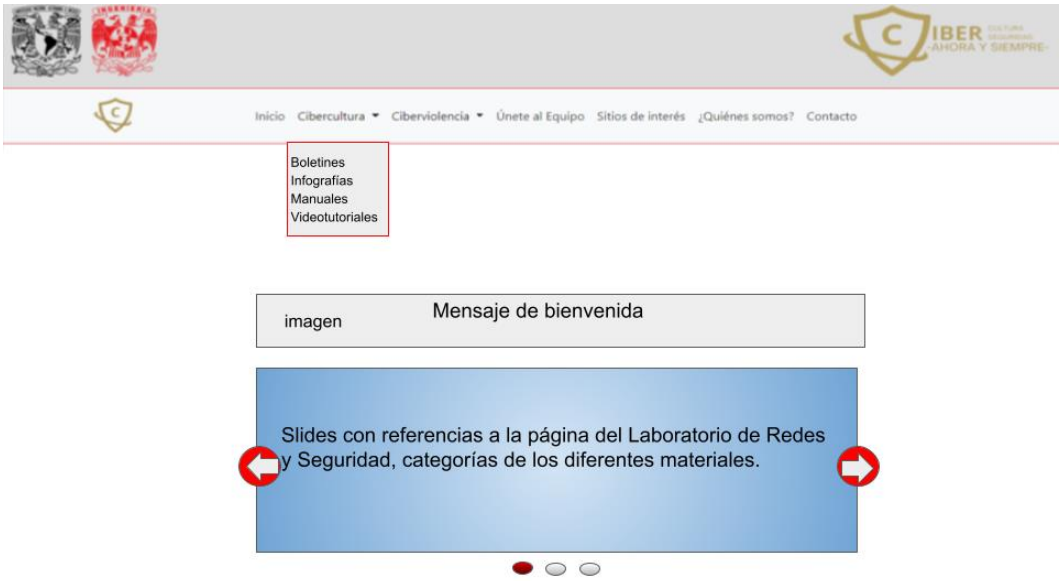


Figura 2. Menú desplegable de Cibercultura.

Ciberviolencia.

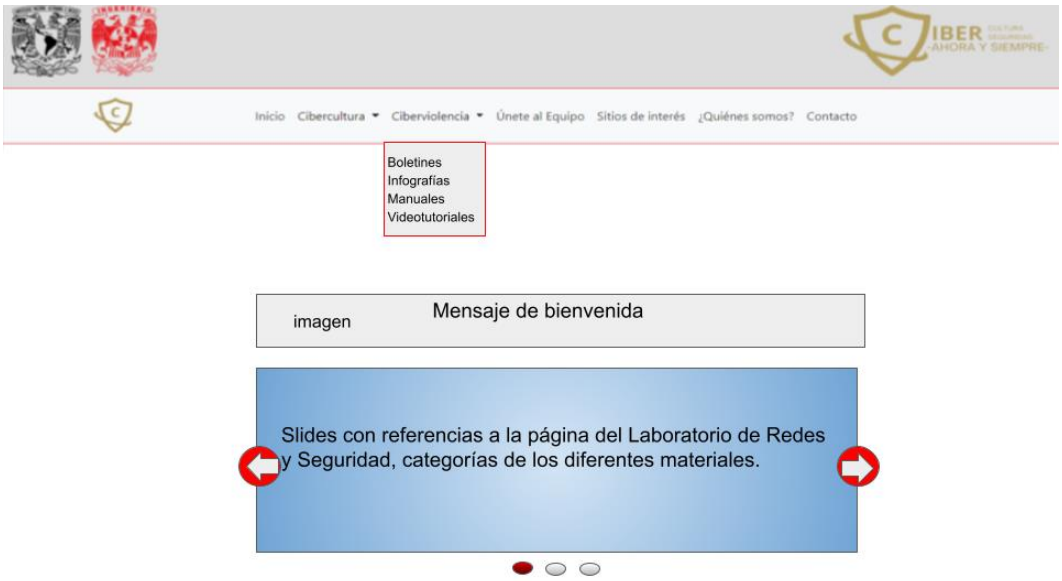


Figura 3. Menú desplegable de Ciberviolencia.

Continuación de la vista de “Inicio” (“Actualizaciones recientes” y enlaces del footer).

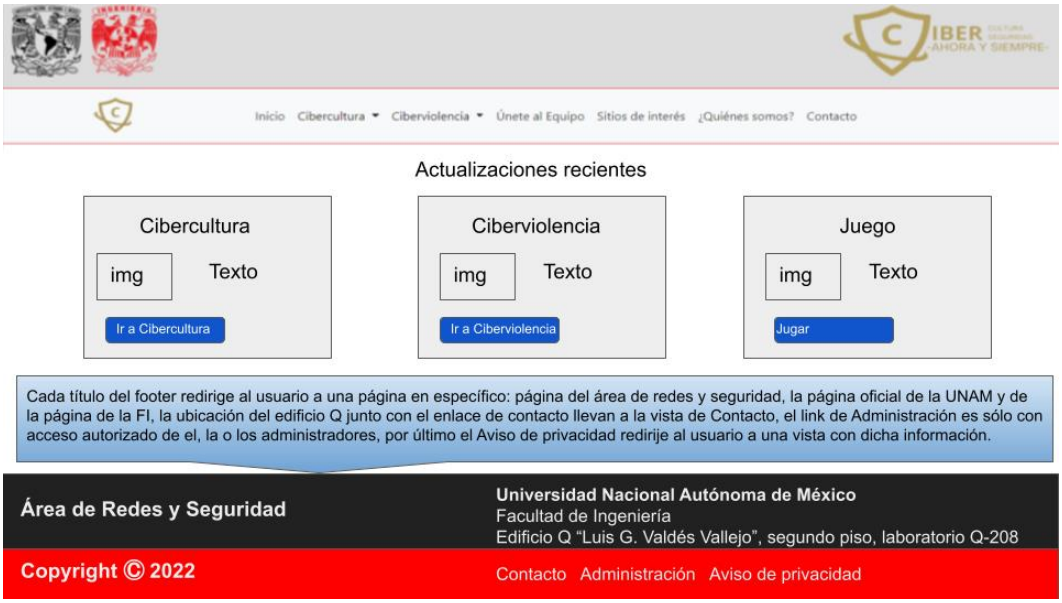


Figura 4. Vista de inicio parte 2.

Ir Cibercultura (Index de Cibercultura).

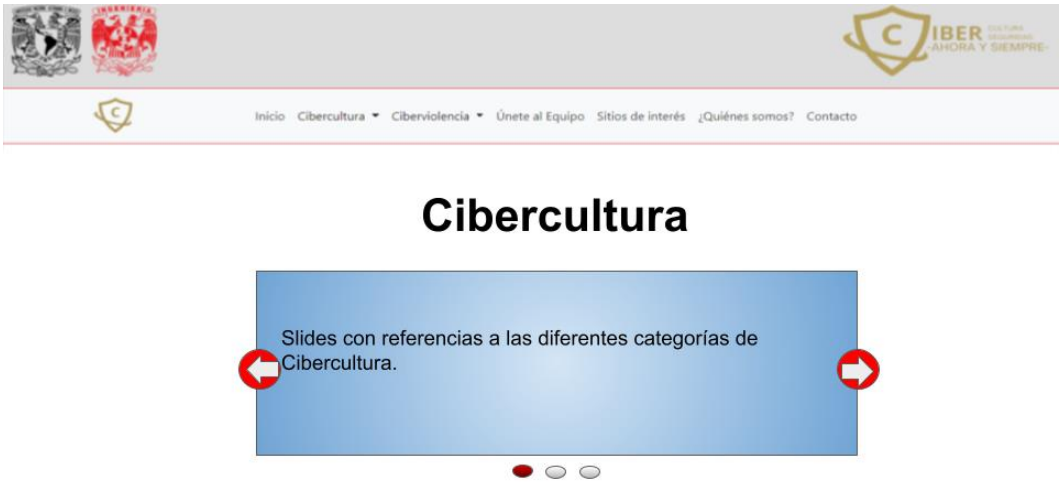


Figura 5. Index de Cibercultura.

Ir Ciberviolencia (Index de Ciberviolencia).

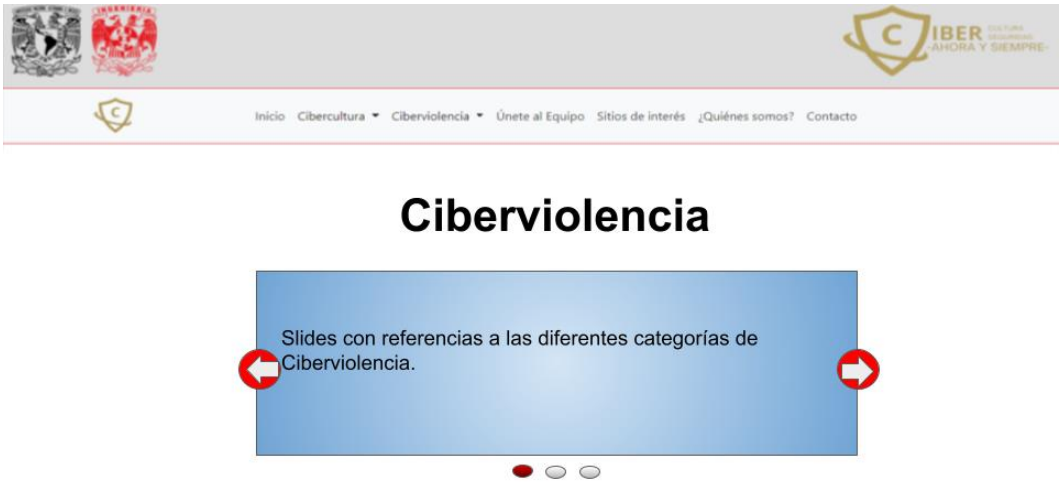


Figura 6. Index de Ciberviolencia.

Jugar (Index de juegos).

Figura 7. Index de Juegos.

Regresando a las opciones del menú principal (Barra de navegación) se puede observar que en las secciones de Cibercultura y Ciberviolencia existe un antes y después de subir los materiales.

Opciones del menú desplegable de Cibercultura:
La sección de “Boletines” antes de que el administrador suba dichos materiales.

Figura 8. Vista inicial de Boletines - Cibercultura.

Actualización de la vista “Boletines” cuando ya existen boletines disponibles.

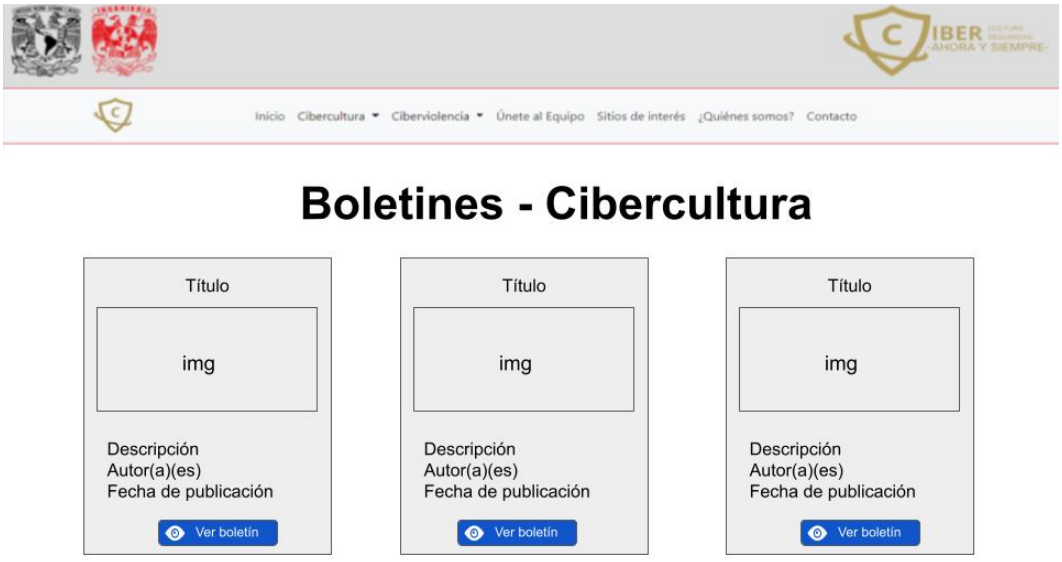


Figura 8.1 Vista de Boletines - Cibercultura con materiales.

La sección de “Infografías” antes de que se publiquen ese tipo de materiales.

Figura 9. Vista inicial de Infografías - Cibercultura.

Actualización de “Infografías” cuando ya existen materiales disponibles.

Figura 9.1 Vista de Infografías - Cibercultura con materiales.

La vista de “Manuales” antes de que se publiquen materiales de dicha categoría.

Figura 10. Vista inicial de Manuales - Cibercultura.

Así se ve la vista de “Manuales” cuando ya existan publicaciones disponibles.

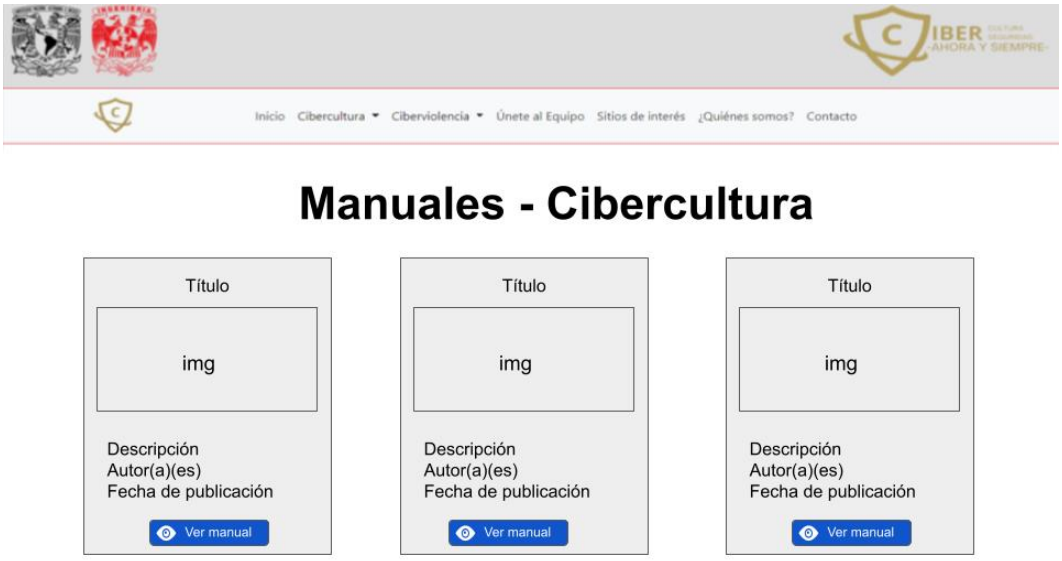


Figura 10.1 Vista de Manuales - Cibercultura con materiales.

La sección de “Videotutoriales” cuando aún no existen materiales disponibles para dicha categoría.

Figura 11. Vista inicial de Videotutoriales - Cibercultura.

Los “Videotutoriales” actualizados cuando ya existen publicaciones de este tipo de material.

Figura 11.1 Vista de Videotutoriales - Cibercultura con materiales.

Opciones del menú desplegable de Ciberviolencia:
Se repite el proceso de mostrar el antes de que existan materiales y el después que es la actualización de las vistas con los materiales publicados.

Boletines antes de existir ese tipo de material.

Figura 12. Vista inicial de Boletines - Ciberviolencia.

Boletines después de publicar ese tipo de material.

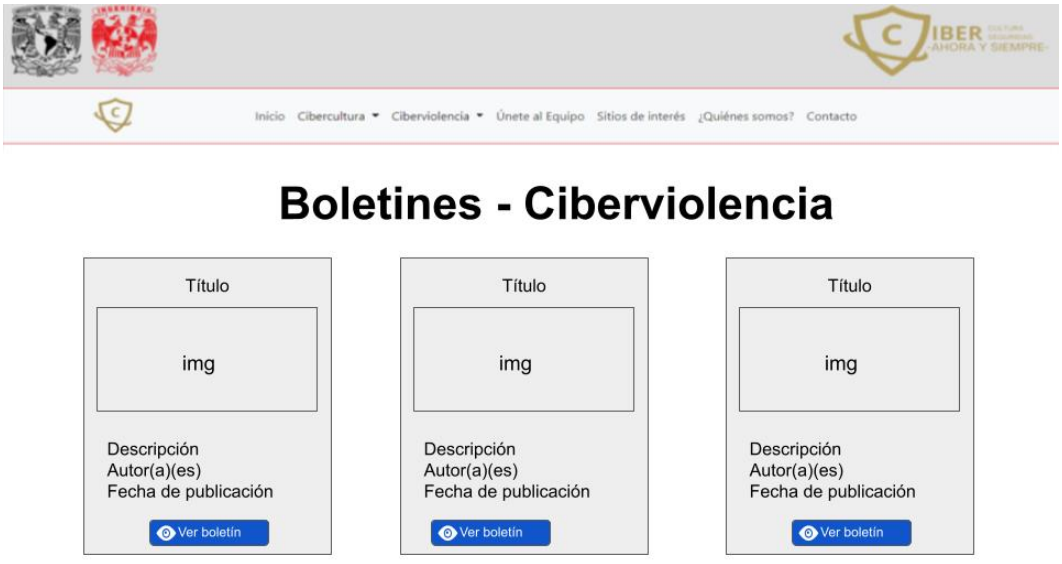


Figura 12.1 Vista de Boletines - Ciberviolencia con materiales.

Infografías antes de subir ese tipo de material.

Figura 13. Vista inicial de Infografías - Ciberviolencia.

Infografías cuando ya existen materiales.

Figura 13.1 Vista de Infografías - Ciberviolencia con materiales.

Manuales antes de la publicación de materiales.

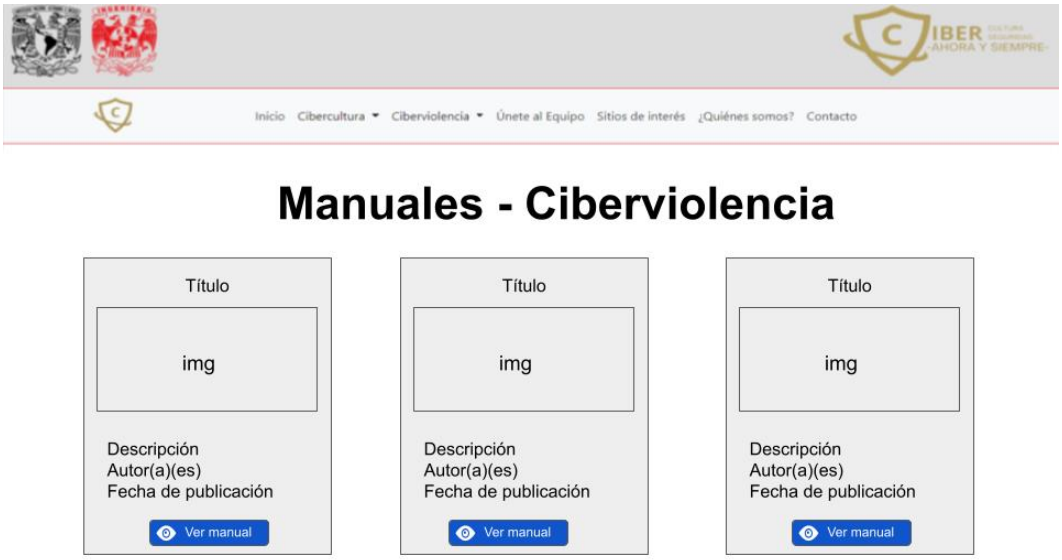


Figura 14. Vista inicial de Manuales - Ciberviolencia.

Manuales cuando ya está actualizado con materiales disponibles para su consulta.

Figura 14.1 Vista de Manuales - Ciberviolencia con materiales.

Videotutoriales antes de la publicación de este tipo de material.

Figura 15. Vista inicial de Videotutoriales - Ciberviolencia.

Videotutoriales cuando se actualiza con materiales disponibles para su consulta.

Figura 15.1 Vista de Videotutoriales - Ciberviolencia con materiales.

Únete al Equipo.

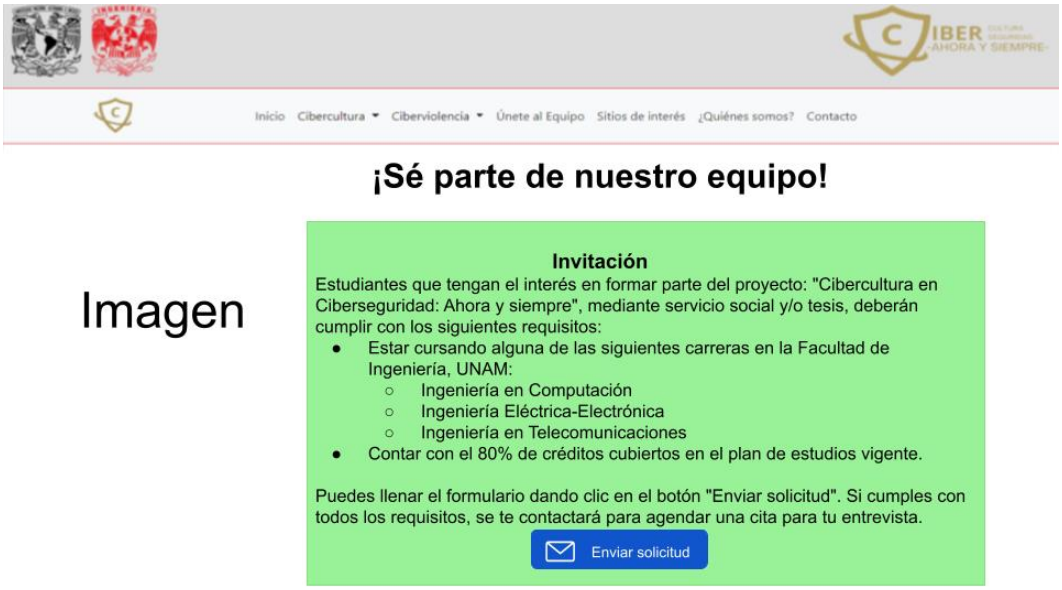


Figura 16. Vista de Únete al equipo.

Al dar clic en “Enviar solicitud” se muestra una vista de estado (formulario de solicitud).

Figura 16.1 Formulario de solicitud para unirse al equipo.

Sitios de interés.

Figura 17. Vista de Sitios de interés.

¿Quiénes somos?.

Figura 18. Vista de ¿Quiénes somos?.

Contacto.

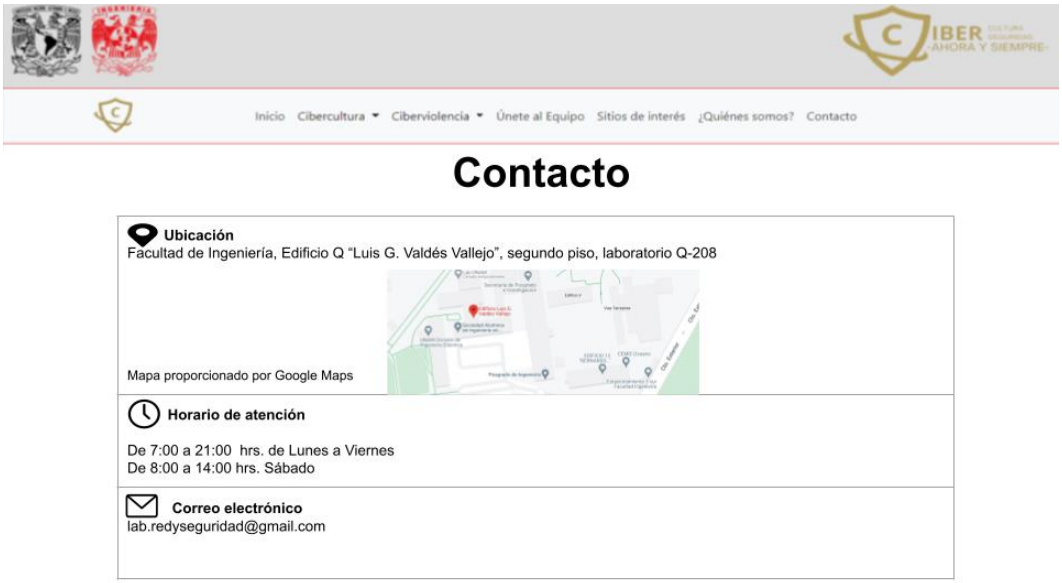


Figura 19. Vista de Contacto.

Enlaces del footer rojo:
Contacto (redirige al usuario a dicha vista).

Aviso de Privacidad.

Figura 20. Vista de Aviso de privacidad.

Administración:
Inicio de sesión.

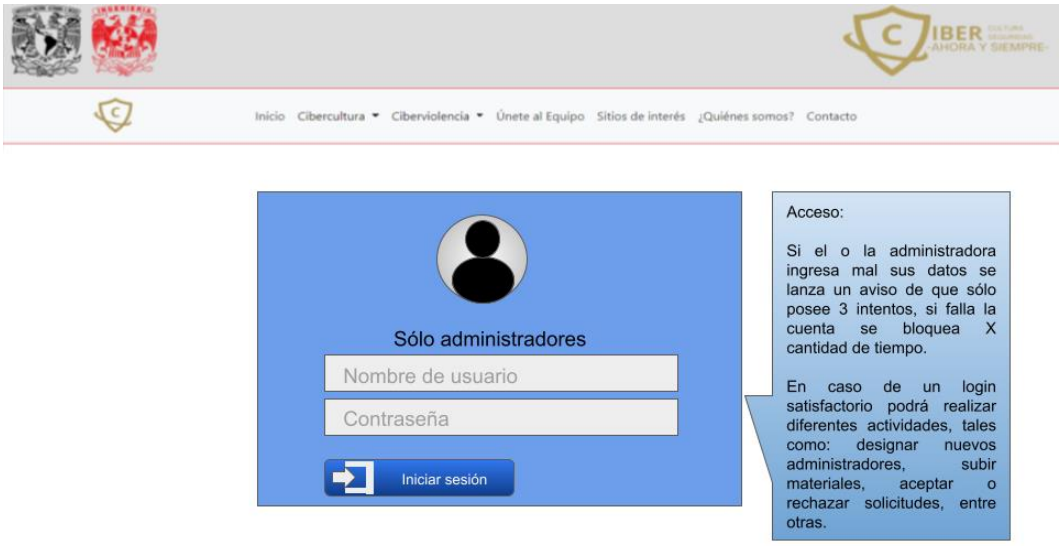


Figura 21. Vista de Login.

Vistas visibles solo para el personal administrativo

Inicio desde la perspectiva administrativa (Ver barra de navegación para comprobar).

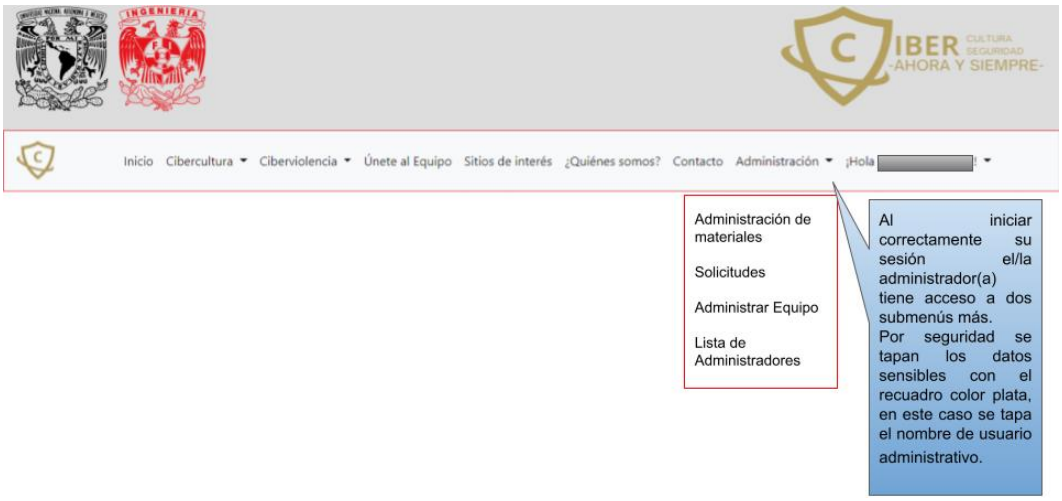


Figura 22. Vista de Inicio desde la perspectiva de la administración.

Opciones del menú desplegable de Administración:
Administración de materiales antes de subir cualquier material (estado inicial).

Figura 23. Vista inicial de Administración de materiales.

Formulario para añadir los materiales.

Figura 23.1 Formulario para añadir materiales.

Vista de la “Lista de materiales” cuando ya existen materiales publicados en el sitio web y las posibles acciones a ejecutar.

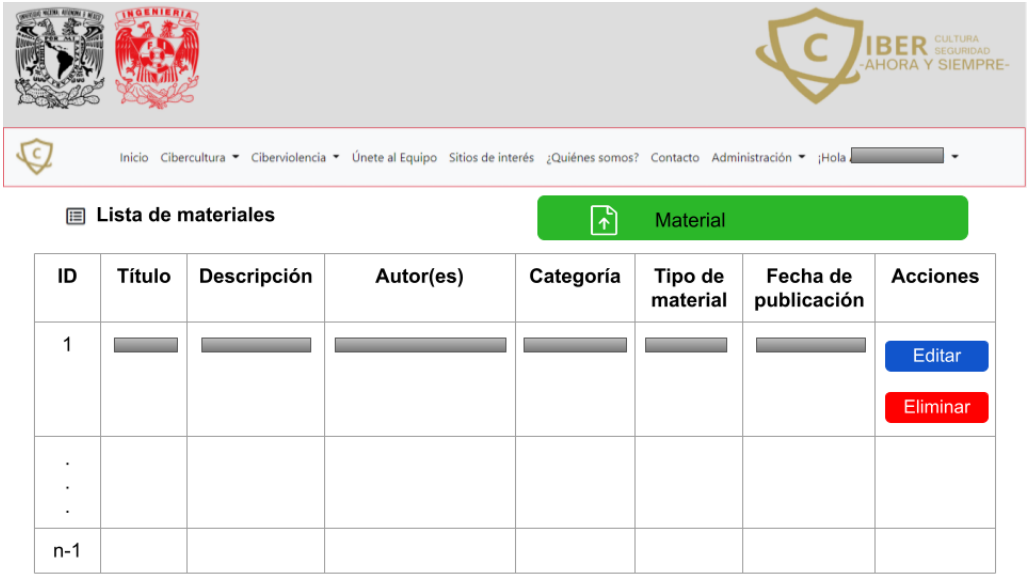


Figura 23.2 Vista de Administración de materiales (Lista de materiales) con materiales añadidos.

Solicitudes: inicialmente muestra una alerta indicando que ningún alumno ha enviado una solicitud para unirse al equipo.

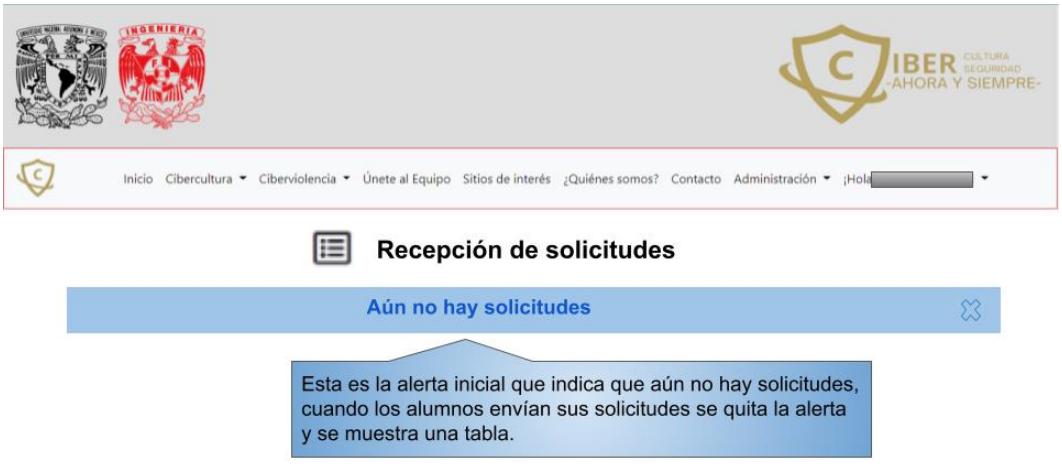


Figura 24. Vista inicial de recepción de solicitudes.

Solicitudes cambia de estado generando una tabla que muestra las solicitudes realizadas por alumnos.

Figura 24.1 Vista de Recepción de solicitudes con formularios.

Al dar clic en el botón de “Revisar solicitud” la vista tiene dos cambios posibles, los cuales son “La solicitud se ha aceptado” y “La solicitud se ha rechazado” como se muestra a continuación.

Alerta que indica que la solicitud ha sido aceptada.

Figura 24.2 Vista de Recepción de solicitudes con solicitudes aceptadas.

Alerta que indica que la solicitud ha sido rechazada.

Figura 24.3 Vista de Recepción de solicitudes con solicitudes rechazadas.

Vista inicial de "Miembros del equipo", la cual indica que todavía no hay integrantes.

Figura 25. Vista de Administrar equipo (Miembros del equipo) inicial.

Cuando la solicitud ha sido aceptada, el nuevo integrante forma parte de “Miembros del equipo”, por lo que el personal administrativo le podrá asignar actividades.

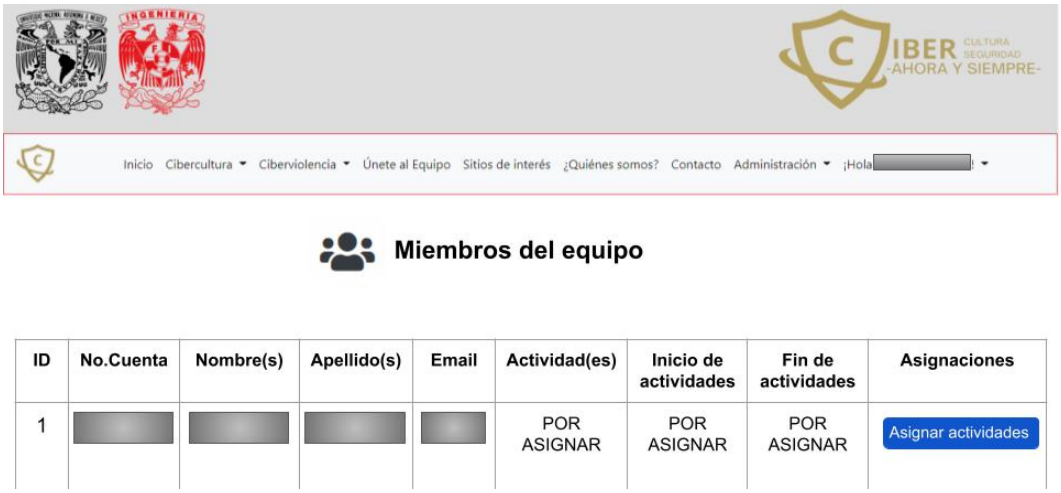


Figura 25.1Vista de Administrar equipo (Miembros del equipo) con integrantes.

Para llevar a cabo el proceso de asignación de actividades, el inicio y fin de estas se realiza mediante un formulario nombrado “Datos del/la integrante” como se muestra a continuación.

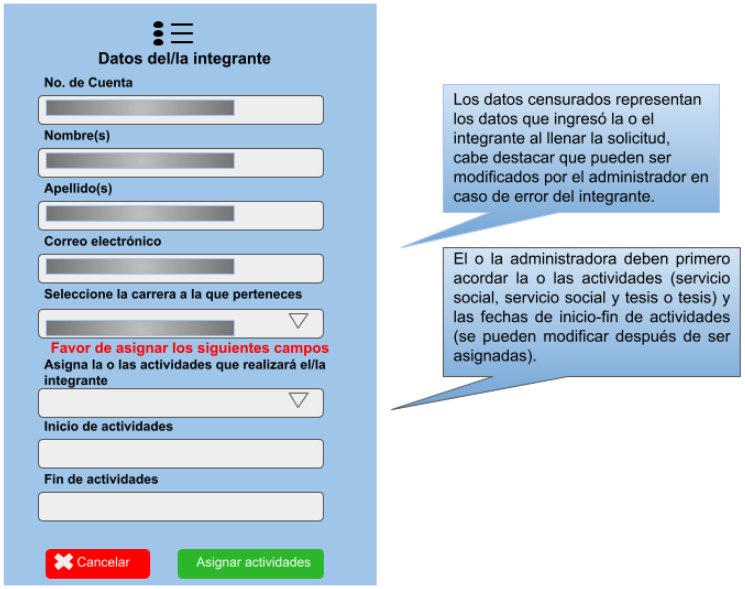


Figura 25.2 Formulario para asignar actividades.

Después de dar clic en el botón de “Asignar actividades”, la vista muestra una alerta que indica que las actividades se han actualizado correctamente y se comprueba viendo los campos cuatro últimos campos de la tabla “Miembros del equipo”.

Figura 25.3 Vista de Administrar equipo (Miembros del equipo) asignación de actividades.

La sección de “Lista de administradores” posee un usuario creado por defecto para otorgar acceso al superusuario.

Figura 26. Lista de administradores.

Al dar clic en “Registrar un nuevo administrador” se muestra el siguiente formulario para poder crear un nuevo acceso.

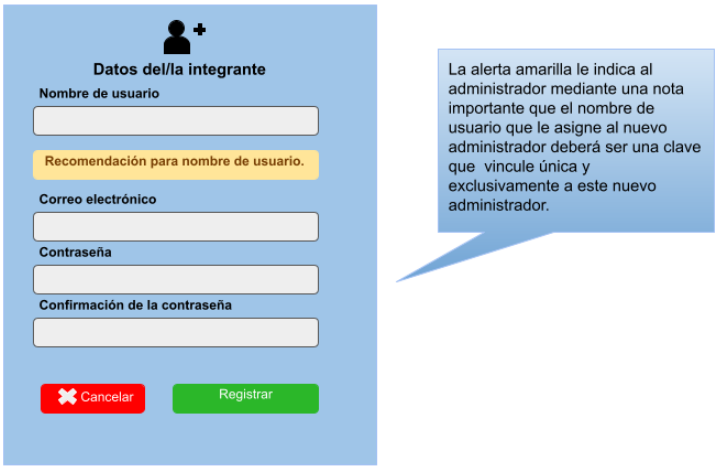


Figura 26.1 Formulario para registrar administradores.

Después de dar clic en “Registrar” se regresa a la vista “Lista de administradores” y se puede observar una alerta indicando el registro de un nuevo(a) administrador(a), además de que este nuevo usuario es registrado en dicha tabla.

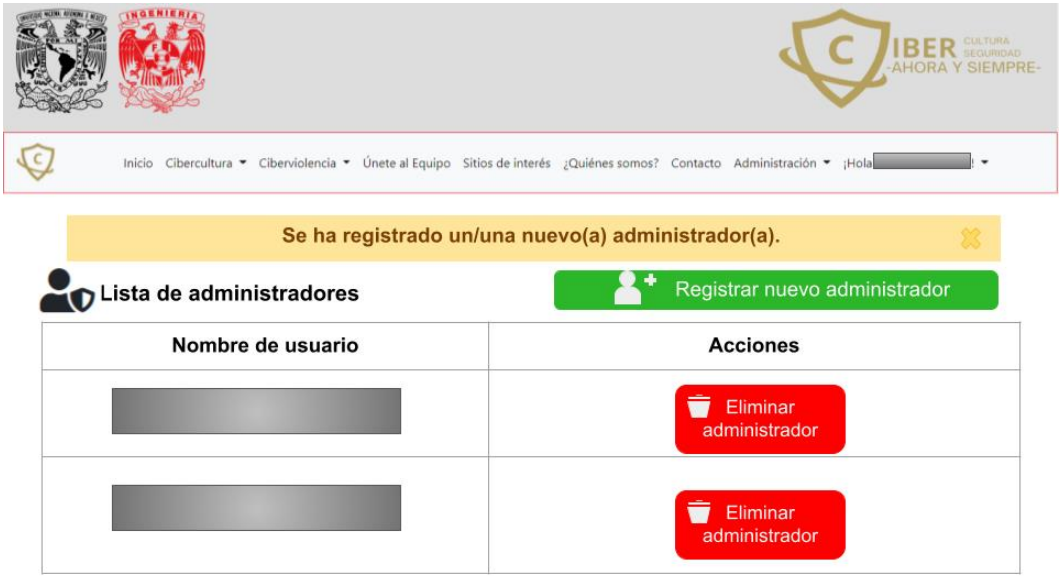


Figura 26.2 Lista de administradores con adición de un administrador.

En caso de desear/requerir “Eliminar administrador” se muestra una alerta como la que se muestra a continuación.

Figura 26.3 Alerta para borrar a un administrador.

En caso de dar clic en “Sí”, se muestra una alerta indicando que el usuario se eliminado correctamente y la tabla se actualiza.

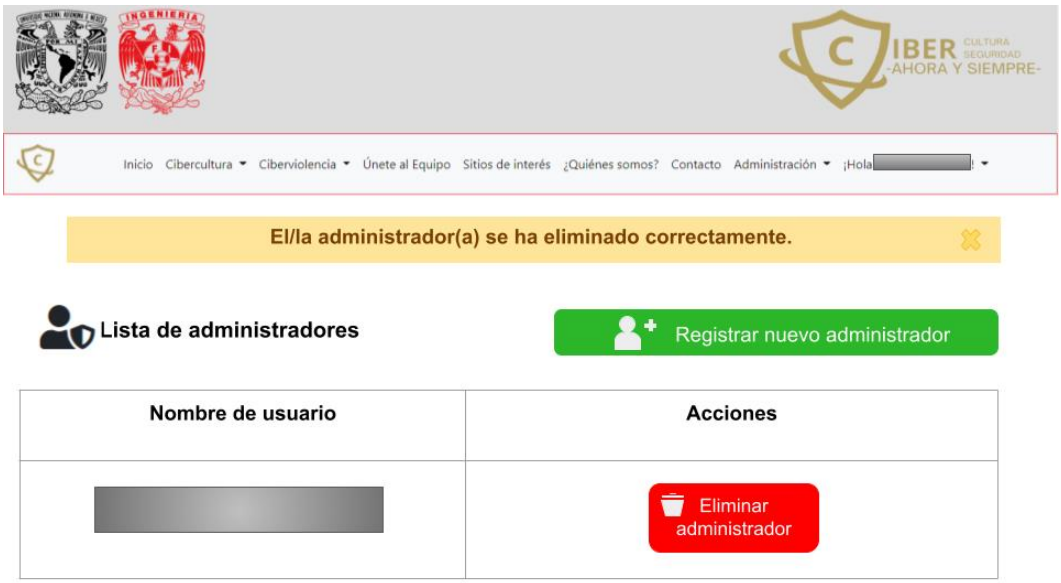


Figura 26.4 Lista de administradores con sustracción de un administrador.

Opciones del menú desplegable de “¡Hola +nombre de usuario!”.

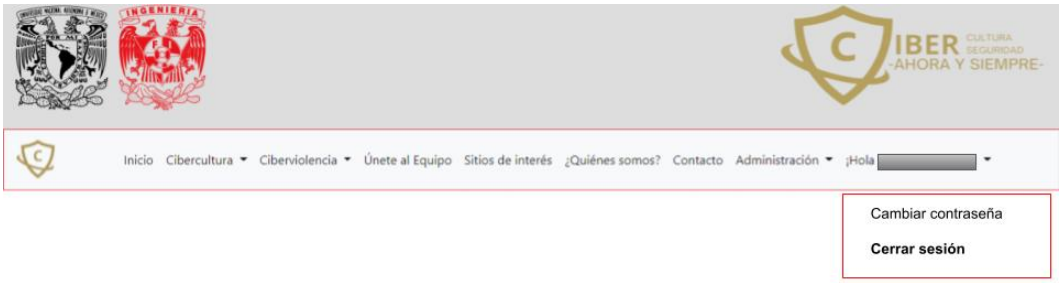


Figura 27. Menú desplegable personalizado.

Al dar clic en “Cambiar contraseña” se muestra un formulario como el que se muestra a continuación.

Figura 28. Formulario para el cambio de contraseña.

Al cambiar la contraseña se muestra la siguiente alerta, indicando que se cerró su sesión y que debe volver a ingresar con su nueva contraseña.

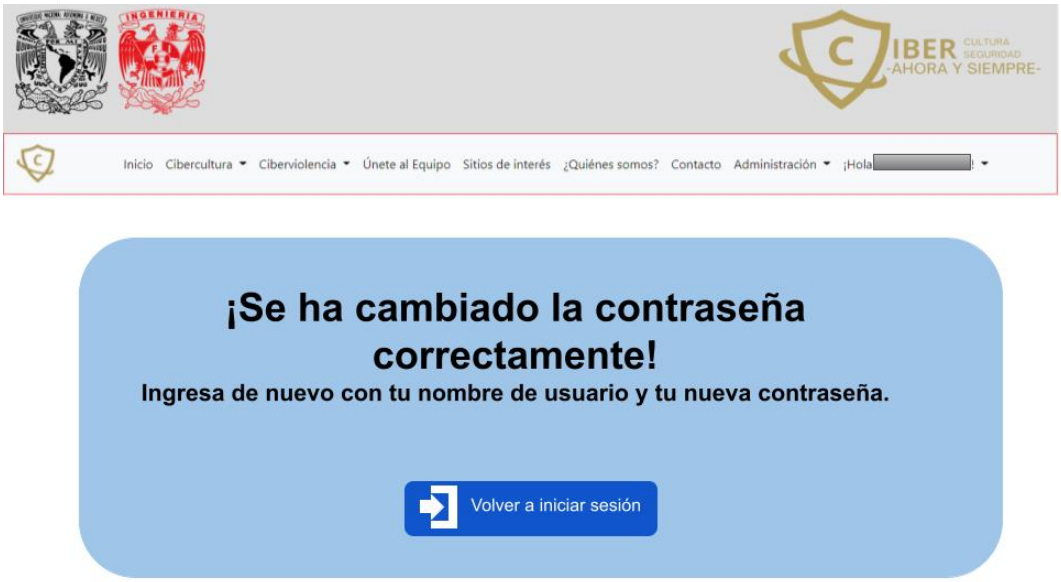


Figura 28.1 Cambio de contraseña.

"Cerrar sesión" es una alerta que muestra la opción de cerrar o no la sesión.

Figura 29. Alerta de cierre de sesión.

Manual de creación del sitio web “Cibercultura en la Ciberseguridad: Ahora y Siempre”

Índice

Desarrollo en Windows 164
Instalación del IDE: Visual Studio Community 2019 164
Creación del proyecto 165
Estructura de las carpetas y archivos del proyecto 166
Estructura del MVC 174
Escalabilidad de la página web 193
Migración del proyecto al sistema operativo Ubuntu 20.04 201
Instalación de ASP.NET Core 5.0 y MariaDB 201
Instalación de Visual Code, C# y exportación de la base de datos 204
Publicación del proyecto y transferencia al servidor 206

Desarrollo en Windows
Instalación del IDE: Visual Studio Community 2019

Para obtener el IDE es necesario realizar la descarga de este en la página oficial de Microsoft https://visualstudio.microsoft.com/es/vs/community/. Así como se ve en la Figura 1, en la cual ya se obtuvo el IDE y se procede a su instalación.

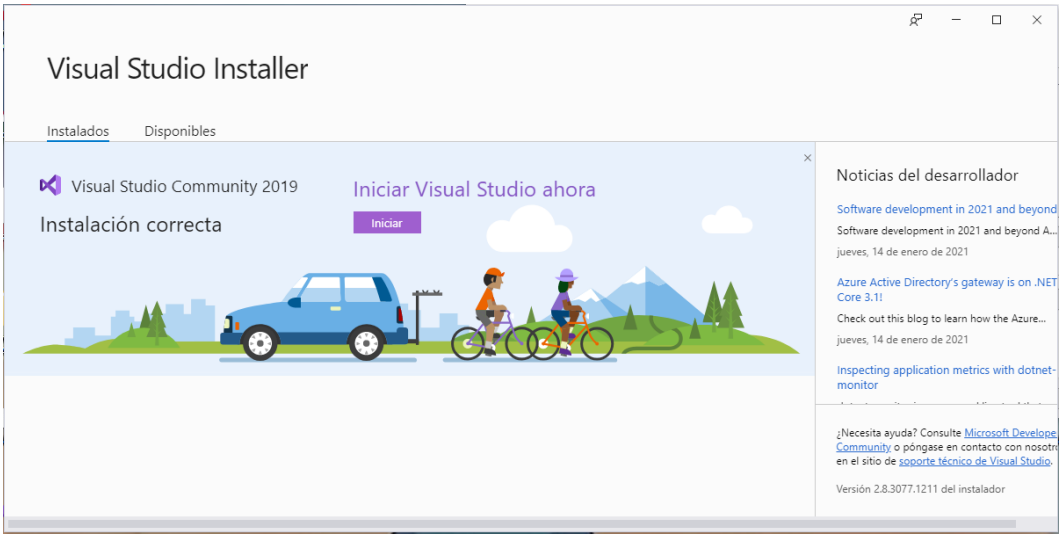


Figura 1. Instalación de Visual Studio Community 2019.

Para este desarrollo se optó por trabajar con la actualización de ASP.NET Core, en su versión 5.0.6, por lo cual se descargó directamente de la siguiente página web: https://dotnet.microsoft.com/download
Nota: Actualmente el IDE ya posee esta actualización por defecto, pero se muestra el proceso que se siguió para la realización del proyecto.

La recomendación que se hace mediante la página web de Microsoft es realizar la descarga de Hosting Bundle como se muestra en la Figura 2.

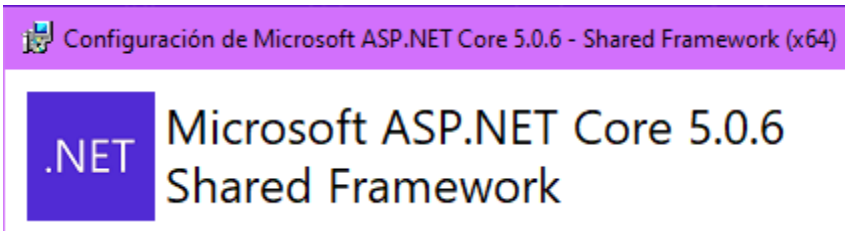


Figura 2. Instalación de ASP.NET Core.

Creación del proyecto

En Visual Studio Community 2019 deberá seleccionar la opción de crear un nuevo proyecto, posteriormente seleccionar "Aplicación web ASP.NET Core con C#", dé clic en "Siguiente", por lo que aparecerá una ventana como se muestra en la Figura 3, en dicha ventana deberá configurar el proyecto: asignar un nombre al proyecto, en este caso "CiberculturaV2", dejar los valores de "Ubicación" y "Nombre de la solución" como lo sugiere el IDE, dé clic en "Crear".

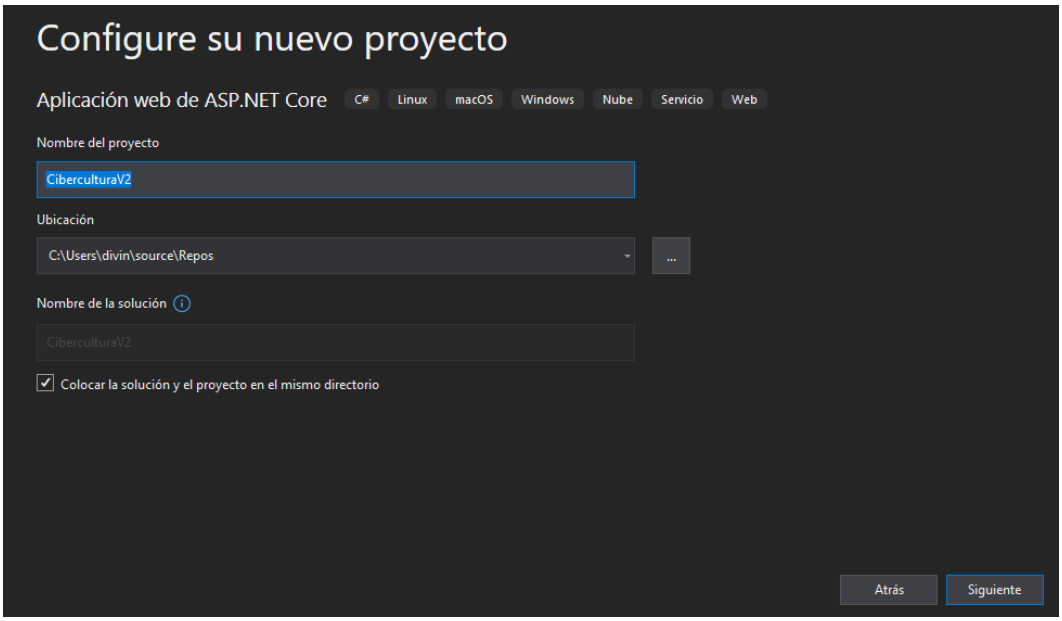


Figura 3. Configuración del proyecto.

La siguiente acción del IDE es mostrar una ventana como se muestra en la Figura 4, por lo que deberá seleccionar los siguientes elementos del formulario: .NET Core, ASP:NET Core 5.0, la plantilla de Aplicación web de ASP.NET Core (Modelo-Vista-Controlador), en el lado derecho, en la sección de "Avanzado" seleccionar "Configurar para HTTPS" y "Enable Razor runtime compilation", estas se habilitan para crear una página web con el protocolo de transferencia de hipertexto seguro y el Enable Razor runtime compilation permite que cuando se realicen cambios a la vista no se tenga que volver a compilar el proyecto, basta con guardar los cambios y refrescar el navegador, finalmente dé clic en "Crear".

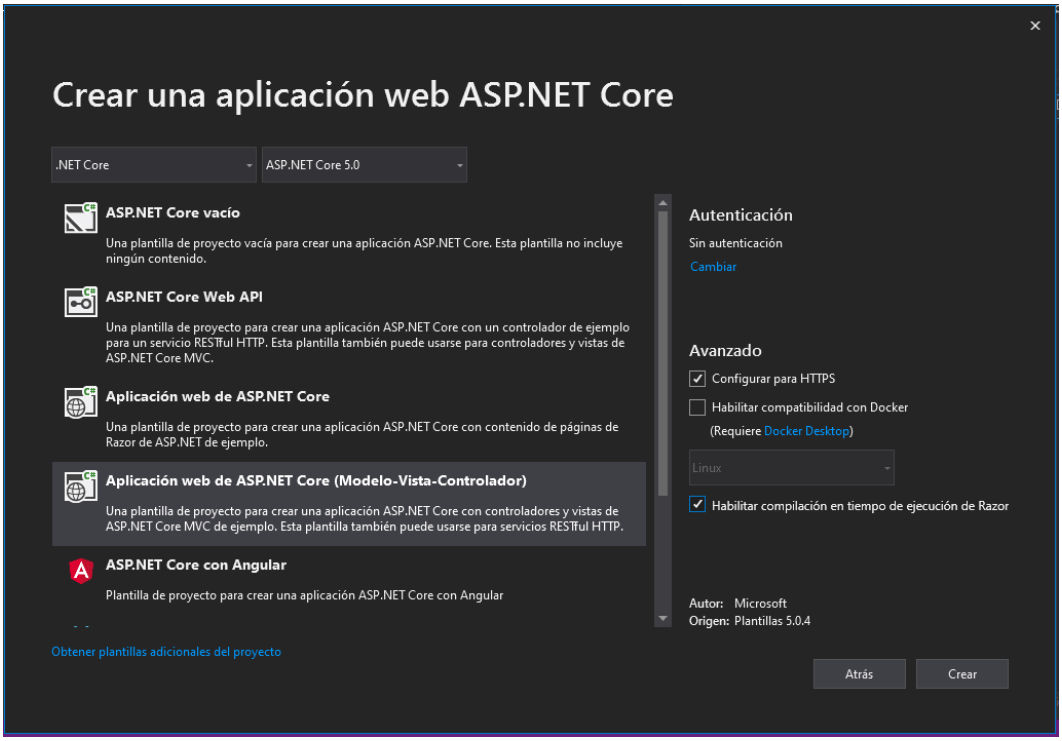


Figura 4. Creación de la aplicación web ASP.NET Core.

Estructura de las carpetas y archivos del proyecto

A continuación, se explicará la estructura de las carpetas del proyecto, dé clic en la solución CiberculturaV2, se desplegarán los elementos y carpetas previamente configurados del proyecto, como se puede observar en la Figura 5.

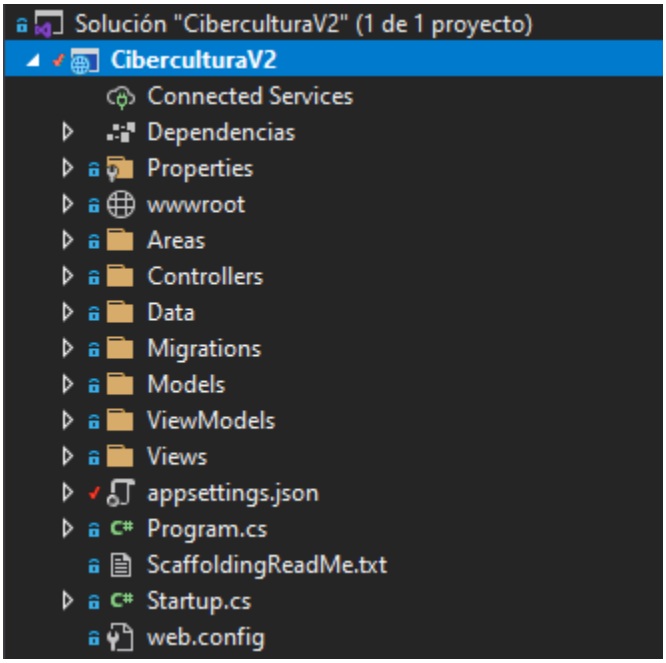


Figura 5. Carpetas y programas base del proyecto.

Dé doble clic en la carpeta del proyecto CiberculturaV2, al hacerlo se abrirá un archivo de tipo .csproj que muestra el SDK web de ASP.NET Core para compilar la aplicación, de los elementos que se pueden observar son: el Target Framework (.NET Core) y el ItemGroup en donde se cargaran todas las extensiones y paquetes de NuGet que se instalaron mediante Visual Studio, inicialmente sólo contiene el TargetFramework que indica la versión 5.0 de .NET Core y el en la sección de ItemGroup: Razor, conforme se avanzó en el proyecto se pueden observar que se han agregado más elementos, como son NuGet y extensiones de fontawesome (no se requieren todos los elementos de fontawesome, por lo que aparece que no se utilizan), como se muestra en la figura 5.1.

```
<Project Sdk="Microsoft.NET.Sdk.Web">

  <PropertyGroup>
    <TargetFramework>net5.0</TargetFramework>
    <CopyRefAssembliesToPublishDirectory>false</CopyRefAssembliesToPublishDirectory>
  </PropertyGroup>

  <ItemGroup>
    <PackageReference Include="Microsoft.AspNetCore.Diagnostics.EntityFrameworkCore" Version="5.0.13" />
    <PackageReference Include="Microsoft.AspNetCore.Identity.EntityFrameworkCore" Version="5.0.13" />
    <PackageReference Include="Microsoft.AspNetCore.Identity.UI" Version="5.0.13" />
    <PackageReference Include="Microsoft.AspNetCore.Mvc.Razor.RuntimeCompilation" Version="5.0.13" />
    <PackageReference Include="Microsoft.EntityFrameworkCore.SqlServer" Version="5.0.13" />
    <PackageReference Include="Microsoft.EntityFrameworkCore.Tools" Version="5.0.13">
      <PrivateAssets>all</PrivateAssets>
      <IncludeAssets>runtime; build; native; contentfiles; analyzers; buildtransitive</IncludeAssets>
    </PackageReference>
    <PackageReference Include="Microsoft.VisualStudio.Web.CodeGeneration.Design" Version="5.0.2" />
    <PackageReference Include="Pomelo.EntityFrameworkCore.MySql" Version="5.0.4" />
  </ItemGroup>

  <ItemGroup>
    <Folder Include="wwwroot\Files\HistorialesAcademicos\" />
    <Folder Include="wwwroot\Files\Materiales\" />
  </ItemGroup>

  <ProjectExtensions><VisualStudio><UserProperties appsettings_1json__JsonSchema="" /></VisualStudio></ProjectExtensions>

</Project>
```

Figura 5.1 CiberculturaV2.csproj.

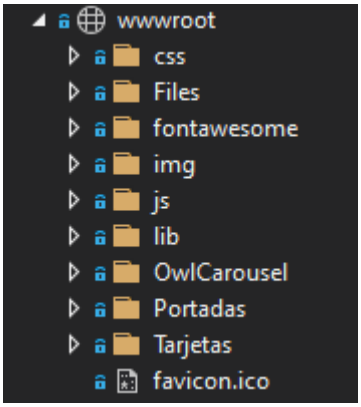


Figura 5.2 Carpeta wwwroot.

La carpeta **wwwroot**, la cual se muestra en la figura 5.2, es una carpeta que se crea por defecto al crear el proyecto, el objetivo de esta carpeta es almacenar todos los elementos estáticos que contendrá el proyecto, por lo que, en su interior almacena

varias subcarpetas que posee el propio proyecto, tales como la de css, que contiene la hoja de estilos del proyecto, de esta podemos destacar que va a contener las características necesarias para dar estilo a la barra de navegación, los botones contenidos en dicha barra, contenido gráfico, tales como los Carruseles de imágenes y el mapa,html y footer, con el objetivo de brindar un estilo propio que siga el principio de diseño responsivo, otra subcarpeta es la de js, la cual contiene una hoja site.js con comentarios para escribir códigos de JavaScript (no se crearon scripts en dicha hoja), la carpeta lib (Figura 5.3) contiene los archivos que Microsoft pre carga para el desarrollo web, como son los frameworks Bootstrap v4 y Angular, junto con scripts de validación que ambos frameworks requieren para operar, los cuales son proporcionados por jQuery, pero se encuentran inhabilitados, en caso de que el desarrollador no los requiera, dado que el desarrollo requiere los scripts de jquery se habilitaron al agregarlos a la hoja de diseño maestra del proyecto: _Layout, en la sección de scripts.

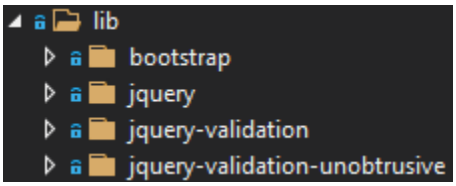


Figura 5.3 Subcarpetas de lib.

El favicon.ico es un ícono simple que utiliza la aplicación en la pestaña de navegación, por lo cual se eliminó y se generó uno con el logo a color de la Facultad de Ingeniería y se agregó a la carpeta de wwwroot, para poder habilitarlo se deberá agregar en el head de _Layout, como se mostrará más adelante.

Debido a las necesidades del desarrollo se crearon varias carpetas, como la de Files, la cual contiene dos subcarpetas: Materiales e HistorialesAcademicos, una es para organizar los materiales generados tanto para Cibercultura y Ciberviolencia, mientras que la otra es para que los postulantes puedan subir su Historial Académico para realizar su servicio social y/o tesis con el equipo de Cibercultura y Ciberseguridad: Ahora y siempre.

Carpetas creadas que contienen imágenes: la de img es la cual almacena el header de los escudos de la Universidad Nacional Autónoma de México, la Facultad de Ingeniería, el logo del proyecto, entre otras. La carpeta de Portadas son imágenes diseñadas como portadas para las diferentes secciones de la página web que son implementadas en los carruseles principal, el de Cibercultura y el de Ciberviolencia, mientras que la carpeta Tarjetas son aquellas imágenes que se utilizarán para cada tipo de material. Cabe destacar que estas últimas están estandarizadas, las portadas

poseen un ancho de 1143 por un alto de 405 píxeles y las tarjetas poseen un ancho de 1076 por un alto de 597 píxeles.

Nota: Para agregar una carpeta de manera global, dé clic derecho sobre la solución y seleccione "Agregar", se desplegará otro menú, de este seleccione "Nueva Carpeta", en caso de agregar una nueva carpeta dentro de otra, repetir los pasos anteriores (posicionarse en la carpeta, ejemplo: wwwroot, dé clic derecho, seleccionar "Agregar" y "Nueva carpeta").

Dado que el proyecto se desarrolló con Bootstrap v4 y al notar que no posee iconos propios, se optó por utilizar un framework de CSS que se especializa en ofrecer iconos vectoriales de manera gratuita y de paga, por lo que se optó por seleccionar los iconos que ofrece de manera gratuita, para implementar dicho framework se procedió a realizar la descarga de su página web oficial https://fontawesome.com/v5.15/how-to-use/on-the-web/referencing-icons/basic-use, el siguiente paso es descomprimir la carpeta que se descarga y agregar la carpeta de fontawesome a la carpeta a wwwroot, por otra parte, se implementó el mismo carrusel que utiliza la página de Laboratorio de Redes y Seguridad, el cual es Owl Carousel, por lo que de igual manera se obtuvo de su página web oficial https://owlcarousel2.github.io/OwlCarousel2/docs/started-welcome.html y se agregaron los elementos necesarios para que ambos funcionen correctamente.

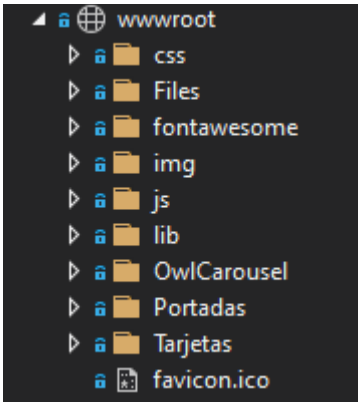


Figura 5.4 Subcarpetas de root.

Nota: Los nuevos elementos que se deseen agregar como subcarpetas de img, Files, frameworks o scripts de jQuery entre otros, es recomendable agregarlos en **wwwroot.**

La carpeta de "Models" va a contener la interacción con la base de datos, donde a cada modelo le va a corresponder una tabla en la base de datos, en la carpeta de "Controlador" se crearán los controladores, "Vista" es donde se creará la

aplicación, es decir, todo aquello que el usuario va a poder observar en pantalla (texto, tablas, formularios, imágenes entre otros), se enviará al controlador y del controlador usa el modelo para mostrarle al usuario el contenido en su pantalla.

Archivos

Appsettings.json: Es un fichero que permite establecer las variables de ejecución de la aplicación, en el cual se puede especificar si se tendrá un único fichero o tener un fichero por entorno (de desarrollo, producción, lanzamiento, entre otros).
Cabe resaltar que en este archivo se configura la cadena de conexión con el servidor y la base de datos que se va a implementar, junto con el Logging el cual se puede modificar dependiendo del sistema operativo en el que se implementará la aplicación (Linux, macOS y Windows), dicho proceso se explica más adelante.

Programs.cs: Es un archivo de configuración Host genérico de .NET que se encarga de encapsular los recursos de la aplicación, es usado para invocar al archivo Startup cuando se carga la aplicación.

Startup.cs: Es una clase usada en el framework de ASP.NET Core, es utilizado para introducir el código de inicialización, en este archivo se personalizan las configuraciones de los middlewares que guiarán el proceso de las peticiones, en ConfigureServices se realiza la inyección de dependencias, por lo que todas las configuraciones requeridas se harán en dicho método, lo que les permitirá a los controladores acceder a dichos datos.
En caso de requerir nuevos servicios y/o configuraciones deberán ser inicializados en dicho archivo.
Configure es el método que contiene los middlewares, los cuales permiten acceder al redireccionamiento, como a archivos estáticos (wwwroot), el de routing y autorización.

web.config: Archivo de configuración que permite extender hasta 2GB los materiales.

Figura 6. Cadena de conexión para SQL Server 2019 y Logging para Microsoft.

Nota: Para que la aplicación pueda interactuar con la base de datos se deberá configurar con la autenticación de SQL y que esta permita las conexiones remotas,

dichos parámetros se configuran en la administración de la base de datos y se agregan a la cadena de conexión.

Configuración de la cadena de conexión para conectarse a la base de datos
En el proyecto se creará una nueva carpeta, dé clic derecho en CiberculturaV2, se desplegará un menú, seleccione la opción "Agregar", se desplegará una lista de opciones, seleccione "Agregar nueva carpeta", le asignará el nombre de Data, dé clic derecho en dicha carpeta, agregue una "Clase", la nombrará ApplicationDbContext.

La clase se agrega con los elementos necesarios tanto de using cómo el namespace y el public class ApplicationDbContext al cual se le agregó la herencia de la clase DbContext, la cual es nativa de ASP.NET Core.

En esta clase se instancian los modelos que serán creados ya que estos van a tener una interacción con la base de datos, como se puede observar en la Figura 6.1 ya se encuentran declarados los modelos creados para este desarrollo, AdminMaterial se creó con el objetivo de administrar los materiales y Solicitud para recibir, aceptar o rechazar y dar seguimiento a las solicitudes de alumnos y alumnas interesados en participar en el proyecto de "Cibercultura en Ciberseguridad: Ahora y siempre".

```
//Proyecto de Tesis: Trejo Luna Eva Marion Shanik
using CiberculturaV2.Models;//Instancia a la clase Models
using Microsoft.EntityFrameworkCore;//Se instala para poder utilizar ApplicationDbContext(mapeo de los modelos que serán cargados)

namespace CiberculturaV2.Data
{
    //Clase heredada de DbContext
    19 referencias
    public class ApplicationDbContext : DbContext
    {
        //contructor
        0 referencias
        public ApplicationDbContext(DbContextOptions<ApplicationDbContext> options) : base(options)
        {

        }
        //Instancia a los modelos previamente creados
        //Modelo:AdminMaterial Instancia:AdminMaterial
        22 referencias
        public DbSet<AdminMaterial> AdminMaterial { get; set; }//Administracion de material
        //Modelo: AdminEquipo Instancia: AdminEquipo
        //NOTA: se debe de realizar otra migración para cargar los registros en la DB

        12 referencias
        public DbSet<Solicitud> Solicitud { get; set; }//Recepción de las solicitudes
    }
}
```

Figura 6.1 ApplicationDbContext.

Para poder aplicar DbContext al proyecto se deben descargar los siguientes paquetes NuGet, dichas descargas las podrá hacer desde el CLI de NET o desde Visual Studio. En este caso se realizaron las descargas desde Visual Studio, por lo que se explicará cómo realizar dichas descargas de paquetes NuGet en caso de requerir instalar más paquetes o actualizar los que ya se tienen.

Pasos por seguir: En el menú superior seleccione la opción de “Herramientas”, se desplegará un menú, de este deberá seleccionar “Administrador de paquetes NuGet”, se desplegará un submenú y le dará clic a la opción “Administrar paquetes de NuGet para la solución”. Se le mostrará una pantalla similar a la figura 6.2, para agregar un NuGet se deberá posicionar en la pestaña “Examinar” y buscar qué elementos se desean agregar, en la Figura 6.2 se muestra la descarga de Microsoft.EntityFrameworkCore.Sql, en este caso dé clic al primero, del lado derecho se muestra el paquete, seleccione el checkbox de “Proyecto” y en automático se activa la del proyecto, buscar la versión más reciente para ASP.NET Core 5 (ya que actualmente Microsoft liberó ASP.NET Core 6 y dichos paquetes NuGet no son compatibles con la versión del proyecto), posteriormente de clic en “Instalar” se abrirá una ventana para revisar la licencia de clic en “Aceptar” y así finaliza la descarga del paquete.

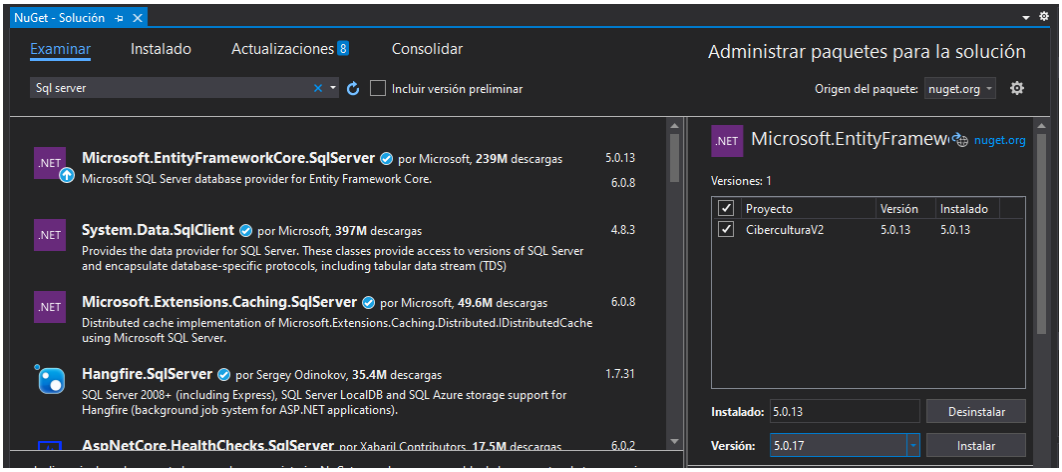


Figura 6.2 Instalación de Microsoft.EntityFrameworkCore.SqlServer.

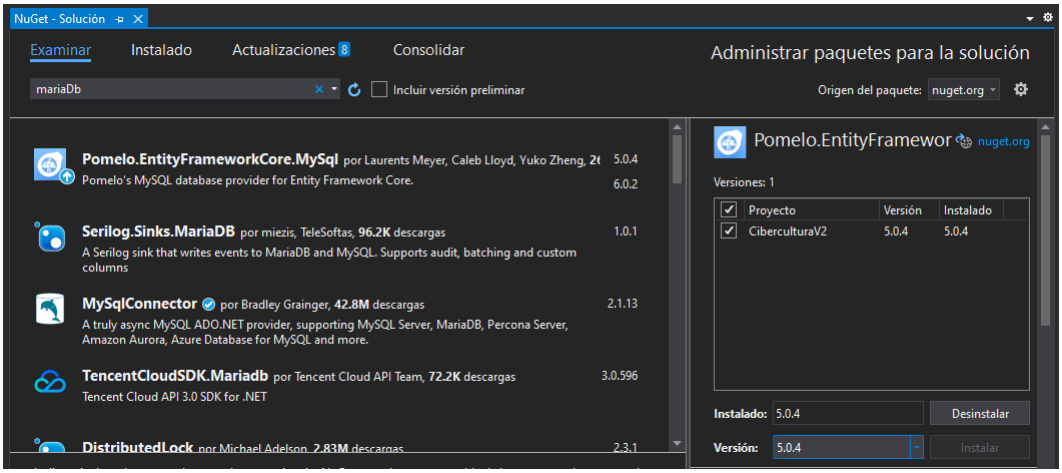


Figura 6.3 Instalación de Pomelo.EntityFrameworkCore.MySql.

Nota: En un principio se realiza la instalación de `Microsoft.EntityFrameworkCore.SqlServer`, puesto que se contempló hacer uso del SQL Server de Microsoft, es por ello que cuando se realice la migración a Linux se instalará el NuGet de **Pomelo.EntityFrameworkCoreMySql** desde dicho sistema operativo para poder implementar la base de datos MariaDB, como se muestra en la figura 6.3.

Después de realizar los pasos anteriores deberá agregar la cadena de conexión en el archivo de startup.cs en la sección de ConfigureServices, como se muestra en la figura 6.4, al agregar dicho código, marcará error ya que se deben agregar los siguientes using:

- using Cibercultura V2.Data;
- using Microsoft.Entity Framework Core;

Los cuales le serán sugeridos por la propia herramienta de "Acciones rápidas".

```
2 referencias
public IConfiguration Configuration { get; }

// This method gets called by the runtime. Use this method to add services to the container.
0 referencias
public void ConfigureServices(IServiceCollection services)
{
    //Configuración de cadena de conexión
    services.AddDbContext<ApplicationDbContext>(options =>
    options.UseSqlServer(Configuration.GetConnectionString("DefaultConnection")));

    services.AddControllersWithViews();
}
```

Figura 6.4 Cadena de conexión.

Estructura del MVC

Modelos: Clases que representan los datos de la aplicación y que utilizan la lógica de validación para hacer cumplir las reglas comerciales para esos datos.

Vistas: Archivos de plantilla que su aplicación utiliza para generar dinámicamente respuestas HTML.

Controladores: Las clases que manejan las solicitudes entrantes de navegación, recuperar los datos del modelo y especifique plantillas de vista que devuelven una respuesta al navegador.

El primer paso para implementar el MVC es crear un modelo, siguiendo estas instrucciones:

Posicionarse en la carpeta de Models, dar clic derecho y seleccionar la opción de "Agregar", lo que abrirá otro submenú y deberá seleccionar la opción "Clase", como se muestra en la Figura 7.

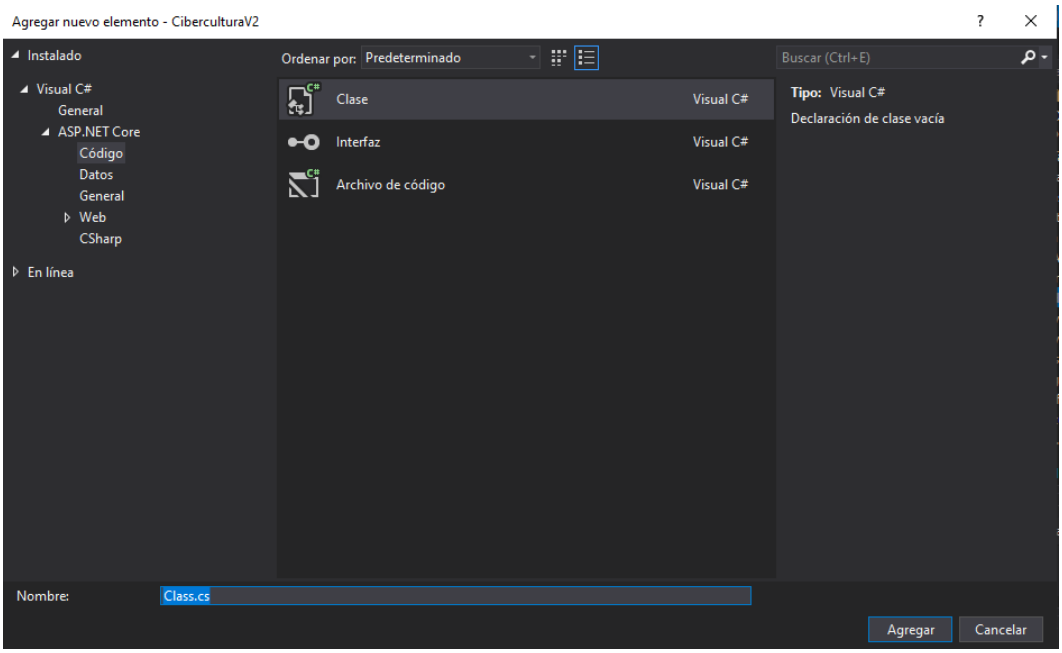


Figura 7.Creación de una clase Modelo.

Por convención propia se estableció que el nombre de los modelos se encontrará en singular para poder diferenciarlos de los controladores, los cuales serán nombrados en plural para poder diferenciarlos.

Al agregar la clase se utiliza la data notación de C# para darle los atributos necesarios a la clase (modelo), junto con sus respectivas validaciones.

Todos los modelos generados poseen comentarios que facilitan la comprensión de las líneas de código.

De manera gráfica se presentan los atributos y tipos de datos de los modelos para un mayor entendimiento, de igual forma se explicará la función de estos.

Los atributos son aquellos elementos que permitirá la funcionalidad e interacción con la base de datos, mientras que los controladores tendrán la función de ser un intermediario entre la página web y los usuarios.

El primer modelo que se creó fue el de la administración de los materiales y el cual será explicado después de observar la Tabla 1.

Tabla 1. *Modelo AdminMaterial.*

	Id	**Título**	**Descripción**	**Autores**	**Categoría**	**Tipo**	**ArchivoUrl**	**Archivo (*)**	**ArchivoName**	**ArchivoExt**	**FechaPublicacion**
Tipo de dato	int	string	string	string	string	string	string	IFormFile	string	string	DateTime

El **Id** es de un valor entero, a lo largo del proyecto es utilizado como llave primaria autoincremental y su principal objetivo es ser un registro numérico único para los materiales, las solicitudes o de los miembros del equipo.

El **Título** es una cadena de caracteres con un tamaño máximo de 50, el cual es utilizado para que el administrador pueda realizar las operaciones de crear, leer, actualizar y eliminar (CRUD por sus siglas en Inglés) y que a su vez los visitantes del sitio puedan visualizar el material, mediante un elemento gráfico conocido como tarjeta que lo contiene y es visible tanto para el administrador y los visitantes, cabe destacar que la única operación que pueden realizar los visitantes hacia los materiales es la lectura.

La **Descripción** es igual una cadena de caracteres con un tamaño máximo de 150, la cuál es utilizada para señalar de manera breve de qué trata el material, posee las mismas características tanto para el administrador como para los visitantes.

El campo de **Autores** le permite al administrador dar el crédito a los alumnos y alumnas que desarrollen los materiales, como parte de su servicio social y/o tesis.

La **Categoría** es también una cadena de caracteres, la cual no posee un tamaño máximo debido a que al momento de crear la página web solo se cuentan con dos categorías **Cibercultura** y **Ciberviolencia**, dichos elementos no tienes que ser escritos por el administrador ya que esta sección en el formulario web se lleva a cabo mediante una selección de radios.

Tipo es una cadena de caracteres, la cual se le solicita al administrador como un elemento de opción múltiple en el formulario, las opciones disponibles hasta el momento son **Boletín, Infografía, Manual** o **Vídeo.**

ArchivoUrl es el path completo de la localización del archivo en el servidor. Se utiliza para que el sistema operativo para que borre dicho material.

Archivo es de tipo IFormFile, el cual se utiliza para cargar archivos en ASP.Net Core MVC.

ArchivoName es una cadena de caracteres que se implementa para almacenar el material con un nombre único.

ArchivoExt se utiliza para validar el tipo de archivo que se va a utilizar, los cuales son: **pdf, png, jpg, gif** y **mp4** en los respectivos materiales, ejemplo: si es manual o boletín solo se permite cargar archivos pdf, si son infografías sólo permite subir archivos jpg, png y gif, en el caso de los vídeos solo permite mp4, en caso de querer subir una infografía con formato pdf se podrá subir más no visualizar.

C# posee en su notación de datos un tipo de dato llamado Date Time, el cual es implementado con el nombre de **FechaPublicacion** para seleccionar la Fecha de la publicación; En esta sección del formulario se presenta un calendario del mes y año en curso, por lo que el administrador puede seleccionar la fecha de la creación del material (en caso de conocerla) o poner la fecha en que este lo recibe o lo sube a la página web.

Nota 1: Estos campos son obligatorios y le son solicitados al administrador (excepto el **Id** ya que ese es autoincremental y no editable) al momento de subir un material mediante un formulario web con la validación del lado del servidor en los modelos creador y la validación del cliente en las vistas de Create, Edit y Delete,

en caso de que la vista Index posea un botón este también tendrá su propia validación mediante un span.

Nota 2: Otro elemento que no es requerido es **Archivo** el cual no está mapeado con el objetivo de no generar una columna de este atributo en la base de datos.

A continuación, se muestran los atributos del modelo Solicitud, en las tablas 2 y 3, el cual se implementa para la solicitud, el proceso de seguimiento hasta la culminación de ser miembro del equipo de "Cibercultura en Ciberseguridad: Ahora y Siempre".

Tabla 2. *Modelo Solicitud parte 1.*

	Id	**No. Cuenta**	**Nombres**	**Apellidos**	**Correo**	**Eres**	**Carrera**	**OtraCarrera**	**Status**	**FechaSolicitud**	**Actividad**
Tipo de dato	int	string	string	string	string	string	string	string	string	DateTime	string

Tabla 3. *Modelo Solicitud parte 2.*

	Fecha_Inicio	**Fecha_Fin**	**ArchivoUrl**	**Archivo (*)**	**ArchivoName**
Tipo de dato	DateTime	DateTime	string	IFormFile	string

Los siguientes campos serán implementados en un formulario web y quien tendrá la opción de llenarlos serán los alumnos al momento de enviar su solicitud, la cual no podrán modificar después de enviarla.

No. Cuenta representa al número de cuenta de los alumnos interesados en realizar su servicio social y/o tesis en el equipo "Cibercultura en Ciberseguridad: Ahora y Siempre", por lo que es una cadena de caracteres con un tamaño mínimo de 9 caracteres y puede alcanzar hasta 15.

Nombres y **Apellidos** son cadenas de caracteres con un máximo de 50 caracteres cada uno.

Email es una cadena de caracteres, pero en las validaciones necesarias para el servidor se le especifica que el tipo de dato es EmailAddress.

Eres atributo diseñado con el objetivo de seleccionar mediante un formulario con radios las opciones de Estudiante y Docente, pero por cuestiones del proyecto se deshabilitó este atributo.

Carrera atributo diseñado para contener las 13 carreras de la Facultad de Ingeniería, pero por cuestiones de cambio de requerimientos, se limitó a las 3 carreras pertenecientes a la DIE (Ingeniería en Computación, Ingeniería Eléctrica Electrónica e Ingeniería en Telecomunicaciones), de manera visual esta información se le solicita a los interesados mediante un formulario que ya contiene habilitadas las carreras, por lo que sólo tendrá que seleccionar la carrera a la que pertenece, es por ello que este atributo es una cadena de caracteres.

Otra Carrera atributo diseñado y deshabilitado por cambio en los requerimientos, su objetivo era que si el interesado no fuera un alumno o alumna de la Facultad de Ingeniería podría de igual forma especificar la carrera de la que es proveniente, en Carrera se encontraba un valor de Otra y al seleccionarla, se activaría un script con un campo en blanco para que él o la interesada pudiera escribir el nombre de la carrera de la que proviene.
ArchivoUrl es el path completo de la localización del archivo en el servidor. Se utiliza para que mediante el sistema operativo se pueda borrar el historial académico de los alumnos rechazados o que ya concluyeron su proceso.

Archivo es de tipo IFormFile, el cual se utiliza para cargar archivos en ASP.Net Core MVC.

ArchivoName es una cadena de caracteres que se implementa para almacenar el historial académico de cada postulante con un nombre único, el cual es su número de cuenta.

Los siguientes campos no son manipulados ni por el o la interesada en ser un miembro del equipo ni el o la administradora, ya que su función es automatizar el proceso de seguimiento de la solicitud agregando dos columnas, las cuales son las de **FechaSolicitud** que muestra la fecha y hora exacta en la que se realizó la solicitud debido a que es de tipo DateTime pendiente y la fecha en la que se envió la solicitud, junto con **Status** que posee como valor inicial pendiente y puede cambiar a aceptar o rechazar la solicitud al dar clic en el botón Revisar solicitud.

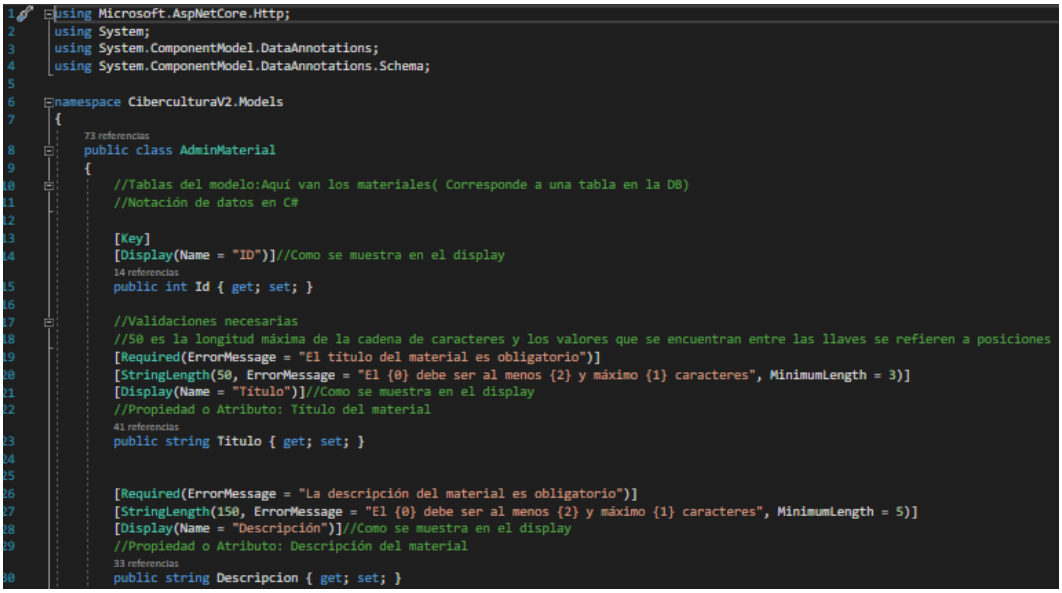
En caso de que la solicitud sea aceptada pasará de ser una solicitud a una administración de equipo, en esta sección se acordarán las actividades a realizar, ya sea tesis, servicio social o tesis y servicio social, almacenando la opción

seleccionada en **Actividad**, al llegar al acuerdo de actividades también se agregan las columnas de **Fecha_Inicio** y **Fecha_Fin** de las actividades a realizar, de dichas fechas sólo se mostrará la fecha sin hora exacta en la que se realizó dicho proceso.

Nota: las vistas y formularios donde serán implementados todos estos atributos serán explicados más adelante, debido a que estos se aplican en Controladores y Vistas.

A continuación, se muestran los modelos de AdminMaterial y Solicitud, en las figuras 7.1 a 7.4, los cuales poseen los atributos necesarios para poder interactuar con la aplicación y que gracias a ellos se podrá tener un registro de los materiales y solicitudes, mientras que con los controladores se podrá tener una interacción con las vistas y los usuarios, realizando las siguientes acciones: crear los materiales, editarlos y eliminarlos.

Nota: En la sección de comentarios donde dice "//Validaciones necesarias" se refiere a las validaciones que se deben realizar del lado del servidor.



```
using Microsoft.AspNetCore.Http;
using System;
using System.ComponentModel.DataAnnotations;
using System.ComponentModel.DataAnnotations.Schema;

namespace CiberculturaV2.Models
{
    73 referencias
    public class AdminMaterial
    {
        //Tablas del modelo:Aquí van los materiales( Corresponde a una tabla en la DB)
        //Notación de datos en C#

        [Key]
        [Display(Name = "ID")]//Como se muestra en el display
        14 referencias
        public int Id { get; set; }

        //Validaciones necesarias
        //50 es la longitud máxima de la cadena de caracteres y los valores que se encuentran entre las llaves se refieren a posiciones
        [Required(ErrorMessage = "El titulo del material es obligatorio")]
        [StringLength(50, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 3)]
        [Display(Name = "Título")]//Como se muestra en el display
        //Propiedad o Atributo: Título del material
        41 referencias
        public string Titulo { get; set; }


        [Required(ErrorMessage = "La descripción del material es obligatorio")]
        [StringLength(150, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 5)]
        [Display(Name = "Descripción")]//Como se muestra en el display
        //Propiedad o Atributo: Descripción del material
        33 referencias
        public string Descripcion { get; set; }
```

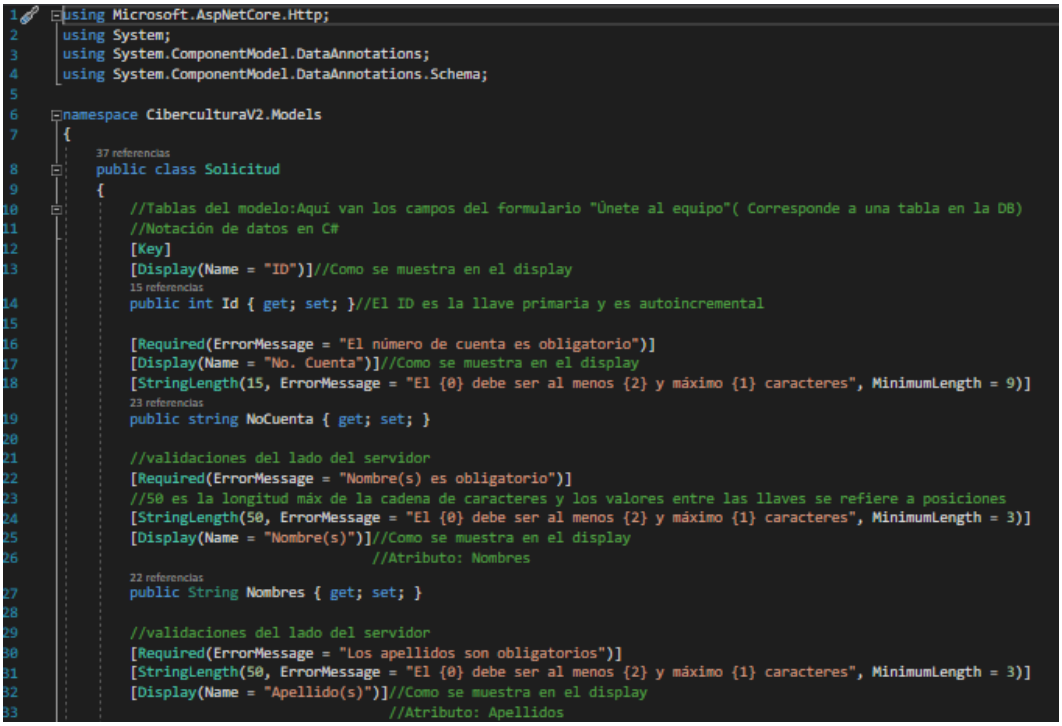
Figura 7.1 Creación del Modelo: AdminMaterial parte 1.

```
        //Validaciones necesarias
        //50 es la longitud máxima de la cadena de caracteres y los valores que se encuentran entre las llaves se refieren a posiciones
        [Required(ErrorMessage = "El título del material es obligatorio")]
        [StringLength(50, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 3)]
        [Display(Name = "Autor(es)")]//Como se muestra en el display
        //Propiedad o Atributo: Autores del material
        33 referencias
        public string Autores { get; set; }

        //Validaciones necesarias
        [Required(ErrorMessage = "La categoría es obligatoria")]
        [Display(Name = "Categoría")]
        41 referencias
        public string Categoria { get; set; }

        //Validaciones necesarias
        [Required(ErrorMessage = "El tipo de material es obligatorio")]
        [Display(Name = "Tipo de material")]
        39 referencias
        public string Tipo { get; set; }

        //Validaciones para la ubicación
        [Required(ErrorMessage = "La ubicación es necesaria")]
        5 referencias
        public string ArchivoURL { get; set; }

        //Validaciones necesarias para la extensión
        [NotMapped]
        10 referencias
        public IFormFile Archivo { get; set; }

        //Validaciones para el nombre del archivo
        [Required(ErrorMessage = "El nombre del archivo es necesario")]
        17 referencias
        public string ArchivoName { get; set; }
```

Figura 7.2 Creación del Modelo: AdminMaterial parte 2.

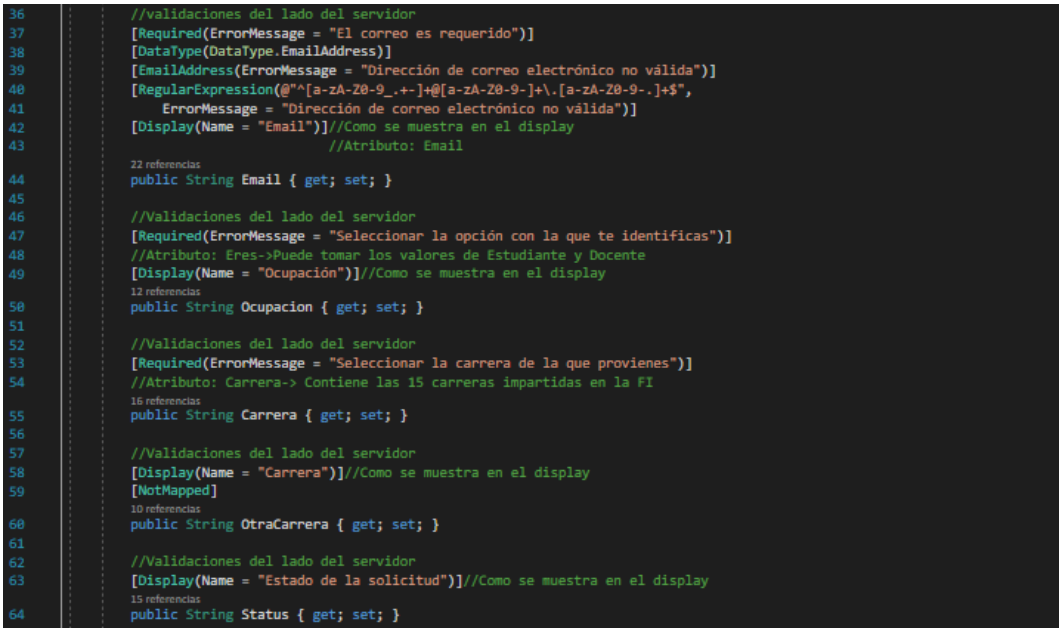
```
        //Validaciones para la extensión
        [Required(ErrorMessage = "La extensión es necesaria")]
        37 referencias
        public string ArchivoExt { get; set; }

        //Validaciones necesarias
        [Required(ErrorMessage = "La fecha es obligatoria")]
        [DataType(DataType.Date)]//Para mostrar solo la fecha sin la hora exacta
        [Display(Name = "Fecha de publicación")]//Como se muestra en el display
        //Propiedad o Atributo: Fecha
        27 referencias
        public DateTime FechaPublicacion { get; set; }
    }
}
```

Figura 7.3 Creación del Modelo: AdminMaterial parte 3.



```
using Microsoft.AspNetCore.Http;
using System;
using System.ComponentModel.DataAnnotations;
using System.ComponentModel.DataAnnotations.Schema;

namespace CiberculturaV2.Models
{
    37 referencias
    public class Solicitud
    {
        //Tablas del modelo:Aquí van los campos del formulario "Únete al equipo"( Corresponde a una tabla en la DB)
        //Notación de datos en C#
        [Key]
        [Display(Name = "ID")]//Como se muestra en el display
        15 referencias
        public int Id { get; set; }//El ID es la llave primaria y es autoincremental

        [Required(ErrorMessage = "El número de cuenta es obligatorio")]
        [Display(Name = "No. Cuenta")]//Como se muestra en el display
        [StringLength(15, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 9)]
        23 referencias
        public string NoCuenta { get; set; }

        //validaciones del lado del servidor
        [Required(ErrorMessage = "Nombre(s) es obligatorio")]
        //50 es la longitud máx de la cadena de caracteres y los valores entre las llaves se refiere a posiciones
        [StringLength(50, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 3)]
        [Display(Name = "Nombre(s)")]//Como se muestra en el display
                                     //Atributo: Nombres
        22 referencias
        public String Nombres { get; set; }

        //validaciones del lado del servidor
        [Required(ErrorMessage = "Los apellidos son obligatorios")]
        [StringLength(50, ErrorMessage = "El {0} debe ser al menos {2} y máximo {1} caracteres", MinimumLength = 3)]
        [Display(Name = "Apellido(s)")]//Como se muestra en el display
                                       //Atributo: Apellidos
```

Figura 7.4 Creación del Modelo: Solicitud parte 1.



```
        //validaciones del lado del servidor
        [Required(ErrorMessage = "El correo es requerido")]
        [DataType(DataType.EmailAddress)]
        [EmailAddress(ErrorMessage = "Dirección de correo electrónico no válida")]
        [RegularExpression(@"^[a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\.[a-zA-Z0-9-.]+$",
            ErrorMessage = "Dirección de correo electrónico no válida")]
        [Display(Name = "Email")]//Como se muestra en el display
                                 //Atributo: Email
        22 referencias
        public String Email { get; set; }

        //Validaciones del lado del servidor
        [Required(ErrorMessage = "Seleccionar la opción con la que te identificas")]
        //Atributo: Eres->Puede tomar los valores de Estudiante y Docente
        [Display(Name = "Ocupación")]//Como se muestra en el display
        12 referencias
        public String Ocupacion { get; set; }

        //Validaciones del lado del servidor
        [Required(ErrorMessage = "Seleccionar la carrera de la que provienes")]
        //Atributo: Carrera-> Contiene las 15 carreras impartidas en la FI
        16 referencias
        public String Carrera { get; set; }

        //Validaciones del lado del servidor
        [Display(Name = "Carrera")]//Como se muestra en el display
        [NotMapped]
        10 referencias
        public String OtraCarrera { get; set; }

        //Validaciones del lado del servidor
        [Display(Name = "Estado de la solicitud")]//Como se muestra en el display
        15 referencias
        public String Status { get; set; }
```

Figura 7.5 Creación del Modelo: Solicitud parte 2.

```
66          //Validaciones necesarias
67          [DataType(DataType.Date)]//Para mostrar solo la fecha sin la hora exacta
68          [Display(Name = "Fecha de la solicitud")]//Como se muestra en el display
            12 referencias
69          public DateTime FechaSolicitud { get; set; }
70
71          //Validaciones del lado del servidor
72          [Required(ErrorMessage = "Seleccionar la carrera de la que provienes")]
73          //Atributo: Carrera-> Contiene las 15 carreras impartidas en la FI
74          [Display(Name = "Actividad(es)")]//Como se muestra en el display
            13 referencias
75          public String Actividad { get; set; }
76
77          //Validaciones necesarias
78          [Required(ErrorMessage = "La fecha es obligatoria")]
79          [DataType(DataType.Date)]//Para mostrar solo la fecha sin la hora exacta
80          [Display(Name = "Inicio de actividades")]//Como se muestra en el display
            7 referencias
81          public DateTime Fecha_Inicio { get; set; }
82
83          //Validaciones necesarias
84          [Required(ErrorMessage = "La fecha es obligatoria")]
85          [DataType(DataType.Date)]//Para mostrar solo la fecha sin la hora exacta
86          [Display(Name = "Fin de actividades")]//Como se muestra en el display
            7 referencias
87          public DateTime Fecha_Fin { get; set; }
88
89          //Validaciones para la ubicación
            5 referencias
90          public string ArchivoURL { get; set; }
91
92          //Validaciones necesarias para la extensión
93          [NotMapped]
            8 referencias
94          public IFormFile Archivo { get; set; }
```

Figura 7.6 Creación del Modelo: Solicitud parte 3.

```
96          //Validaciones para el nombre del archivo
            4 referencias
97          public string ArchivoName { get; set; }
98      }
99  }
100
```

Figura 7.7 Creación del Modelo: Solicitud parte 4.

En la figura 7.8 podrá observar que en la carpeta Models se encuentran los modelos correspondientes a los materiales y a equipo.

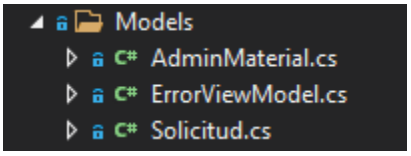


Figura 7.8 Carpeta Models.

Nota 1: ErrorViewModel.cs es creado por defecto y sirve para manejar los errores que se susciten en la aplicación de ASP.NET Core.

Nota 2: Después de crear los modelos y declararlos en **ApplicationDbContext** puede crear una primera migración para poder interactuar con la base de datos, para hacer esto, deberá posicionar en la barra superior de Visual Studio, dar clic en **"Herramientas"**, cuando se despliegue el menú seleccionar **"Administrador de paquetes NuGet"**, después se mostrará un submenú y deberá dar clic en **"Consola del Administrador de paquetes"**, en la parte inferior del IDE se mostrará la consola, y escribirá el siguiente comando: **`add-migration [nombre que desee poner a la migración]`**, ejemplo:

`PM> Add-Migration MiPrimerMigracion`, si sus modelos están correctos y declarados en ApplicationDbContext, la consola le mostrará los siguientes mensajes:

```
Build started...
Build succeeded.
To undo this action, use Remove-Migration.
```

El `Add-Migration` genera una carpeta llamada `Migrations` y los scripts necesarios para subir y eliminar las tablas (de los modelos) de la base de datos.
El siguiente paso, es subir las tablas a la base de datos con el siguiente comando:

`PM> update-database`, si el proceso fue correcto le aparecerán los siguientes mensajes:

```
Build started...
Build succeeded.
Done.
```

Por lo que se podrá ir al Management Studio, dar clic en refrescar el servidor, deberá desplegar la carpeta de Bases de datos y podrá observar que ya se encuentra la base de datos que se declaró en la cadena de conexión en el `appsettings.json` con las tablas previamente creadas.

El segundo paso es crear un controlador, por cada modelo se debe generar mínimo un controlador, pero esto dependerá de las especificaciones requeridas.

Por ejemplo, para el modelo Solicitud se crearon 3 controladores diferentes, uno es para que las y los alumnos interesados en formar parte del equipo de “Cibercultura en ciberseguridad: Ahora y siempre” puedan enviar su solicitud; otro para que el o la administradora puedan visualizar, revisar, aceptar o rechazar las solicitudes y por último un controlador que ayuda al administrador a tener un histórico de los miembros del equipo.

Instrucciones para crear y manipular un controlador
Deberá posicionarse en la carpeta de Controllers, dar clic derecho, seleccionar “Agregar”, se desplegará un submenú y le dará clic en “Controlador”. Posteriormente se abrirá una ventana con múltiples opciones, de la cual deberá seleccionar la opción de “Controlador de MVC en blanco”, como se muestra en la siguiente figura, dará clic en “Agregar” y aparecerá una nueva ventana con el título de Controller.cs en la cual podrá escribir el nombre que desee darle al controlador.

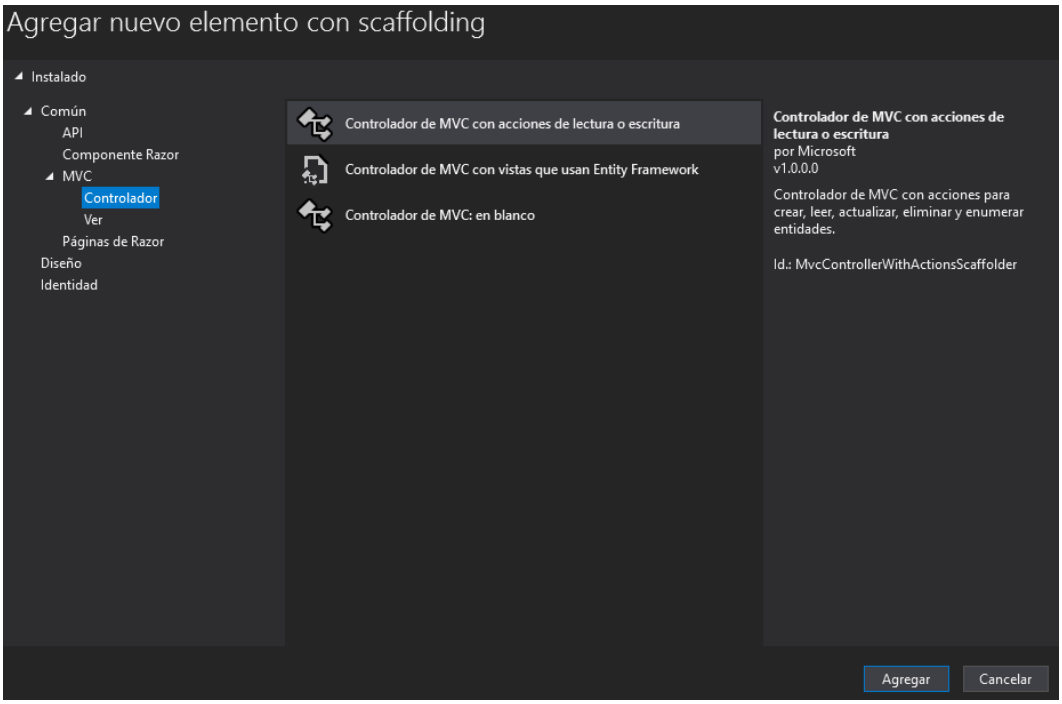


Figura 8.Agregar un nuevo controlador.

Para este proyecto se utilizó el mismo nombre que el modelo previamente creado agregando una letra "s", por ejemplo: para el modelo de AdminMaterial se generó el controlador AdminMaterials, al elegir el nombre de cada controlador se le debe dejar la palabra Controller al final (`AdminMaterialsController.cs`).

Nota: Los modelos se crearon en singular y los controladores en plural debido a ciertas operaciones que se realizan con ambos y esta es una forma de poder diferenciarlos, pero no es obligatorio que al crear nuevos controladores siga esta recomendación, ejemplo de ello es el controlador Equipo, lo que sí es requerido es dejar en el nombre la palabra Controller para que este funcione correctamente.

En la figura 8.1 se muestra la carpeta Controllers, la cual contiene inicialmente a HomeController para posteriormente contener a los controladores que se crearon, más adelante se explicará el porqué de la creación de cada uno, cabe destacar que cada controlador posee comentarios explicando las bibliotecas que usa y fragmentos de código que explican su funcionamiento.

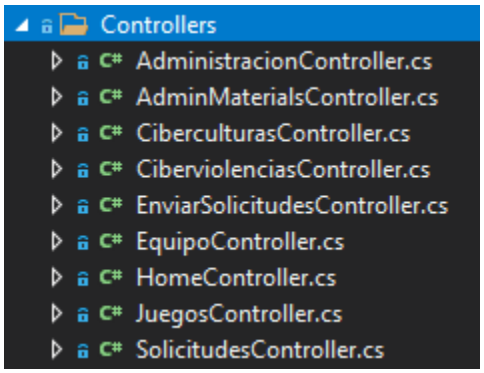


Figura 8.1 Contenido de la carpeta Controllers.

El primer controlador a explicar es aquel que se crea por defecto cuando se configura el proyecto, `HomeController`, el cual posee un objeto público llamado HomeController que se puede utilizar por defecto si se desea implementar un inicio de sesión desde la Vista de inicio **Index** (IActionResult Index ()), los cambios que sufrió este controlador fue que se le agregó la interacción con la base de datos, los modelos, ASP.NET Core MVC y las vistas (IActionResult) que no requieren un modelo (**Acerca,SitioSugeridos, Contacto y Privacy**), ya que su principal objetivo es permitir la lectura de datos, cabe destacar que se pudo crear un controlador diferente para albergar dichas vistas, pero se optó por incluirlas en este por ser el principal; lo que demuestra que puede existir un controlador que no posea acceso a un modelo, pero sí contener vistas sin cambio en su código de estado HTTP.

Controladores creados y su objetivo

Un elemento en común de los controladores creados son los códigos de estado HTTP como son Create, Edit, Delete e Index.

AdminMaterialsController

El objetivo de este controlador es poder subir, editar y eliminar cualquier tipo de material.

Explicación de las operaciones realizadas en los estados HTTP:

El Index es la vista principal, esta tiene un botón de “Agregar material” y muestra una lista con los materiales que se han subido a la página web, en caso de no existir materiales, muestra un mensaje de “Aún no hay archivos subidos”; cuando se le dé clic al botón de “Agregar material” se cambia de estado HTTP a Create, esta vista tiene un form-group con los atributos del modelo **AdminMaterial** (Título, Descripción, Autores, Categoría, Tipo, los atributos relacionados con el Archivo y

la Fecha de publicación) y a su vez posee un objeto que permite subir y grabar el archivo, editar su nombre y crear su path en el servidor. El estado de Post create valida el archivo (que se haya seleccionado un archivo y que este tenga un formato válido) para posteriormente pasar los atributos a la página de Index con los datos ingresados, pero cambiando la entrada (minúsculas o mayúsculas y minúsculas) por una salida en mayúsculas. El estado de Edit primero valida el material mediante el **Id**, si el Id es cero o nulo se retorna un NotFound, en caso de existir el material lo muestra.

El estado de Post Edit muestra el material dentro de un form-group con los atributos editables, en caso de editar algún elemento se guardan los cambios y se regresa a la vista de Index, si se cambia el archivo se borra el anterior y se guardan los cambios.

El estado de Delete y Post Delete funcionan de manera similar al Edit, solo que en este estado se borra el material de la carpeta Files y del almacenamiento interno de la base de datos y servidor.

CiberculturasController
El objetivo de este controlador es almacenar, visualizar e impedir la copia de los materiales pertenecientes a Cibercultura, junto con los detalles de cada tipo de material (Boletines, Infografías, Manuales y Vídeos).

Explicación de las vistas de Ciberculturas:
Como en AdminMaterials se suben los archivos, estas vistas poseen mayores elementos de front-end, por ejemplo; Index es la vista principal que muestra un carrusel con las vistas a cada tipo de material (Boletines, Infografías, Manuales y Vídeos).

A su vez este controlador tiene las vistas individuales de los tipos de materiales: Boletines, Infografías, Manuales y Vídeos, los cuales se muestran mediante una lista de elementos (tarjetas diseñadas con el framework de Bootstrap, la cual contiene diversos elementos, tales como el título, una portada y botón que redirige a una página Details), mientras que las vistas que tienen la terminación Details (ejemplo: BoletinDetails) muestra una visualización del material en cuestión, el cual no permite la descarga del material.

CiberviolenciasController
Los objetivos de este controlador es el almacenamiento, visualización y restringir la copia de los materiales pertenecientes a Ciberviolencia, junto con los detalles de cada tipo de material (Boletines, Infografías, Manuales y Vídeos).

Explicación de las vistas Ciberviolencias:
Index es la vista principal que muestra un carrusel (Owl Carousel) con portadas que redirigen al usuario a cada tipo de material (Boletines, Infografías, Manuales y Vídeos) y al igual que cibercultura, los materiales se listan mediante tarjetas que poseen un botón que redirige a las vistas de Details que restringen la copia de los materiales.

Controlador para las y los alumnos
EnviarSolicitudesController
Contiene una vista Index la cual contiene una invitación a ser parte del equipo de Cibercultura en Ciberseguridad: Ahora y siempre junto con un botón que le permite a las y los interesados en llenar un formulario web, por lo que los estados HTTP que les son permitidos a los alumnos son Create y Post Create, por lo que el objetivo de este controlador es procesar las solicitudes de servicio social y/o tesis dentro del equipo sin darles la opción de editar o eliminar la solicitud.

Explicación de las operaciones realizadas en los estados HTTP de EnviarSolicitudes:
En Create se muestra el form-group que contiene parte de los atributos del modelo Solicitud (Nombres, Apellidos, Número de cuenta, Correo electrónico, Carrera e Historial académico), en Post Create se realizan diversas validaciones, entre ellas que se haya seleccionado un archivo para ingresar en el campo de historial académico en formato pdf, se cambian las entradas del solicitante a todas en mayúsculas, con excepción del correo electrónico, los campos que no se piden se agregan de manera automática a una tabla que pertenece al administrador, la cual se podrá observar en SolicitudesController, los campos del modelo solicitud que no se le solicitan a las y los alumnos son Ocupación al cual se le pasa una cadena ESTUDIANTE (debido a que se deshabilitó la opción de docente), Fecha de la solicitud, se agrega la fecha y hora exacta en la que se realizó la solicitud, a Status se le pasa una cadena PENDIENTE, los campos Actividad se manda una cadena vacía, las fechas de inicio y fin también se agregan como la fecha en la que se hizo la solicitud para que el administrador realice las acciones pertinentes.
En caso de proporcionar correctamente los datos, se agrega la solicitud a la base de datos, se guardan los cambios, se retorna a Index y se manda una alerta con un mensaje de “La solicitud se ha enviado correctamente”.

Controladores Administrativos

SolicitudesController

Este controlador contiene un Index, en el cual se listan todas las solicitudes y atributos mencionados en el controlador anterior, las acciones que puede realizar el administrador son las siguientes:

Revisar las solicitudes, obtener el historial académico de cada alumno, el cual tiene de nombre el número de cuenta del alumno, garantizando el nombre único, en caso de ser aceptada, se guardan los cambios en el Index de este controlador cambiando su status de PENDIENTE a ACEPTADA, junto con una alerta de "La solicitud se ha aceptado", en el campo de acciones se muestra el mensaje de "ESTA SOLICITUD HA SIDO ACEPTADA", dichos campos se listan de igual forma en el Index de EquipoController para modificar los atributos de actividades, fecha de inicio y fin, por otra parte, si la solicitud es rechazada, el status cambia de PENDIENTE a RECHAZADA, se manda una alerta de "la solicitud se ha rechazado", eliminando el el historial académico, pero no el registro, quedando como un histórico de las solicitudes, en el campo de acciones se muestra el siguiente mensaje "NO CUMPLE CON LOS REQUISITOS".

EquipoController

Los estados de HTTP que contiene este controlador son el Edit y Post Edit, junto con una vista Index que muestra la lista de los integrantes del Equipo de Cibercultura en Ciberseguridad: Ahora y siempre.

El motivo por el cual se puede editar dicha lista es por la existencia de un botón de "Editar actividades" lo cual permite seleccionar las actividades que realiza cada integrante y su fecha de inicio y fin de las mismas, la primer validación que se hace en Asignaciones (Edit) es identificar al miembro del equipo mediante su Id, si el Id es cero o nulo se retorna un NotFound, en caso de encontrarse el miembro del equipo se procede a realizar los cambios y se salvan en Post Edit el cual retorna a la vista de Index.

Nota: Por defecto se genera el método **public IActionResult Index**, Index es el encargado de llamar a una vista que aún no está creada por lo que deberá realizar los siguientes pasos:

Al seleccionar Index y dar clic derecho, se abrirá un menú del cual seleccionará "Agregar vista...", se desplegará una ventana y seleccionará "Agregar Vista de Razor", posteriormente le aparecerá una ventana como se muestra en la figura 9, lo

cual es para agregar una vista, que por defecto es Index, pero se puede modificar con el nombre deseado.

Deberá seleccionar la opción de “Usar página de diseño”, dar clic en “...”, se abrirá una nueva ventana, busque la carpeta “Views”, se desplegarán otras dos carpetas y seleccionará “Shared”, por último, dé clic en la opción _Layout para que tome los elementos globales de dicha página. Dando como resultado la ruta mostrada en la misma figura 9.

Nota: Una página de diseño es la que aplica el mismo diseño a las demás páginas o vistas (ejemplos: header, barra de navegación y footer) a las demás páginas como es el caso de _Layout.

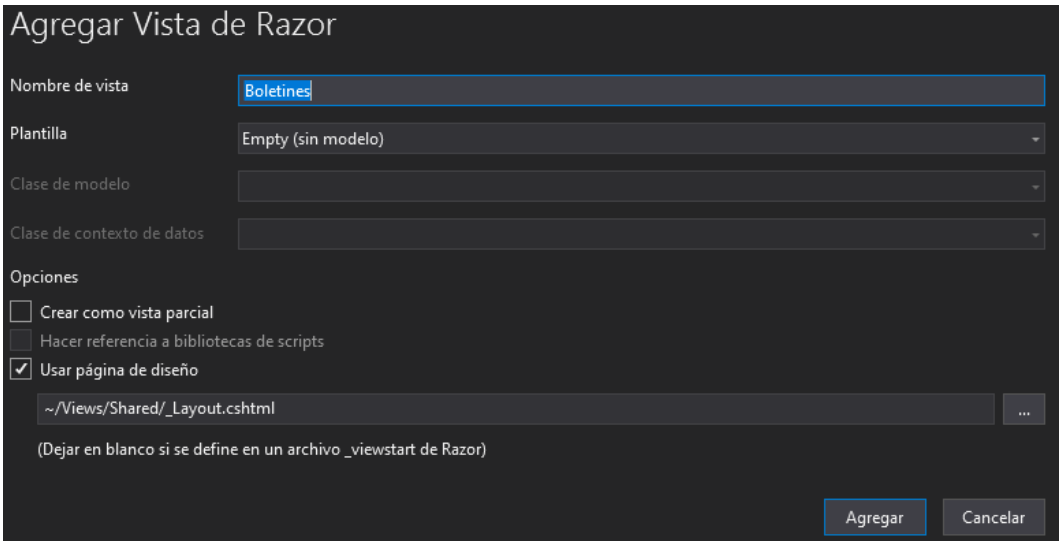


Figura 9. Creación de la Vista Boletines.

La vista que usted cree será una página de Razor, por lo que posee inicialmente los elementos básicos para visualizar su contenido sin la necesidad de utilizar las etiquetas de HTML, pero en este desarrollo se optó por utilizarla para mantener una estructura, las páginas de Razor permiten visualizar contenido de HTML, el uso de frameworks que funcionen con otros estándares de diseño web, tales como JS y CSS.

Se implementará el framework de Bootstrap v4.x, el cual se incluye al crear el proyecto, pero que deberá de añadir mediante una etiqueta <link> en _Layout, de igual manera la hoja de estilos de site.css, Owl Carousel, fontawesome y sus correspondientes scripts.

En la figura 9.1 se muestran las carpetas creadas desde los controladores con sus respectivos IActionResult (las vistas).

Nota 1: En caso de querer agregar un elemento visual se puede acceder a la documentación oficial de Bootstrap y observar el código de ejemplo del elemento que se desee agregar `https://getbootstrap.com/docs/4.0/getting-started/introduction/`.

Nota 2: En caso de requerir un icono para un botón o vista puede ir a `https://fontawesome.com/` y buscar uno que sea de su agrado, de preferencia, antes de buscar un icono seleccione la categoría "Free" para que el buscador le muestre los iconos gratuitos, posteriormente deberá seleccionar el que sea de su agrado y seleccionar "Start Using This Icon", se le mostrará un fragmento de código que deberá copiar y pegar en una etiqueta label, button, o h1-h6 (por citar ejemplos).

Nota 3: Cada vista contiene comentarios, pero los que podrían ser un riesgo de seguridad serán omitidos.

Nota 4: Se repite el procedimiento, en el controlador se selecciona el método Index, el cual se puede modificar a cualquiera que sea de su preferencia o ejemplifique mejor la acción.

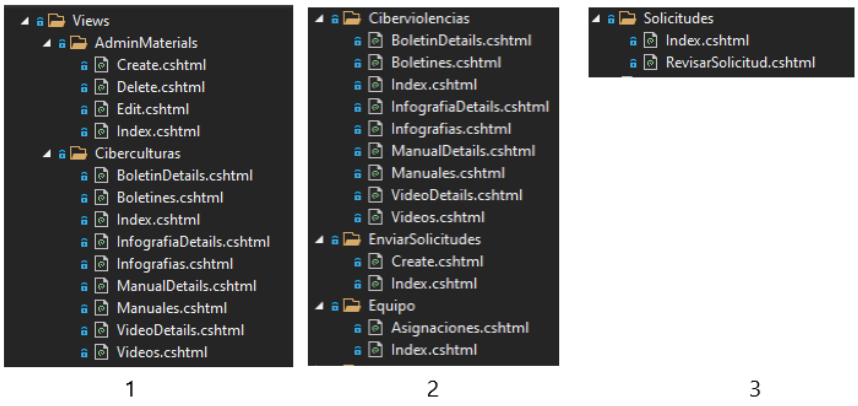


Figura 9.1 Vistas creadas.

Explicación de la subcarpeta Shared

La subcarpeta Shared se crea por defecto al crear el proyecto (mismo caso que la subcarpeta Home), en esta se encuentra la vista _Layout, la cual es la vista maestra de la página web, en ella se encuentra la barra de navegación y todos los elementos globales que desee mostrar, como, por ejemplo: agregar un nuevo botón a la barra

de navegación o un menú desplegable, el footer, dichos elementos deberán ser agregados en esta vista.

El archivo de _ValidationScriptsPartial invoca a las bibliotecas de jquery para realizar la validación de los datos que se encuentran en los formularios o scripts propios.

El archivo Error se mostrará en pantalla cuando ocurra un error inesperado, como podría ser el haber creado un modelo, pero sin vista, entre otros.

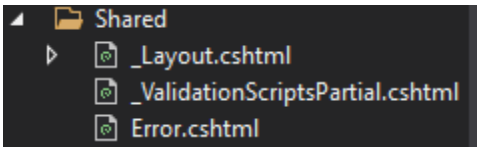


Figura 9.2 Subcarpeta Shared.

La vista que se explicará más a detalle es _Layout por ser la que contiene los elementos globales, tales como el header, la barra de navegación y el footer.

Como se mencionó con anterioridad _Layout es la vista maestra, y como toda vista contiene los elementos estándar de una página web en HTML5, los cuales identifican a la página con el <DOCTYPE html>, <html lang= “es”>,</html> , se seleccionó el lenguaje español debido a que el desarrollo se realizó en este lenguaje, otros elementos característicos son el <head>,</head>, <body>,</body>, <header>,</header>,<footer> y </footer>.

De manera gráfica se puede observar en la figura 9.3 la estructura html de _Layout, que se analizará más adelante.

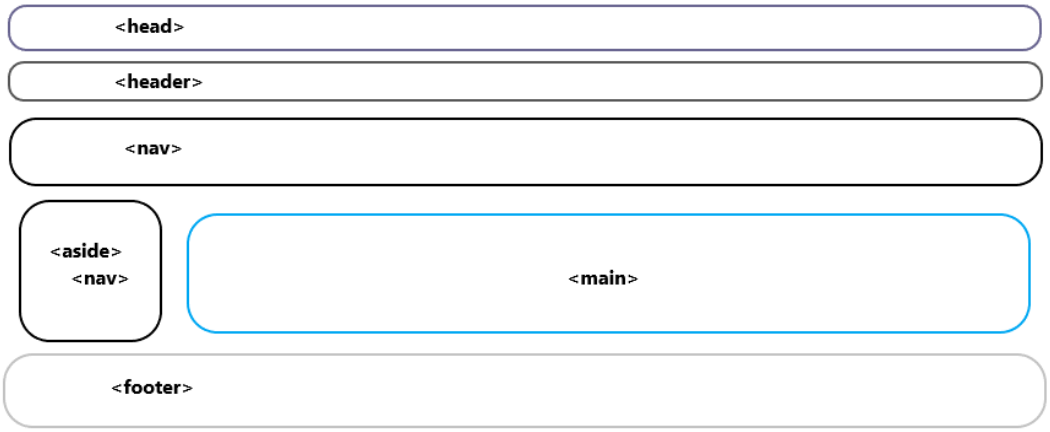


Figura 9.3 Estructura de _Layout.

En la sección de **<head>** de _Layout contiene el código comentado explicando el porqué de cada elemento, los cuales tienen como objetivo interactuar con el navegador web, otro punto que se destaca del head es el elemento <link rel=icon href="~/vid/favicon.ico" /> el cual es un icono del escudo de la Facultad de Ingeniería el cual fue hecho para que se mostrará en la pestaña del buscador web que utilicen los usuarios y está contenido en la carpeta wwwroot.

La etiqueta header almacena un contenedor fluido que se adapta al tamaño de la pantalla del dispositivo que utiliza el usuario, dicho contenedor es de color gris y alberga los escudos de la UNAM, la FI y el logo del proyecto.

La etiqueta de nav corresponde a la barra de navegación y los elementos que la componen, es decir, el color de fondo, el color de los bordes, , los botones que dirigen a los usuarios a las diferentes vistas junto con los menús desplegables de Cibercultura y Ciberviolencia. Dicha barra se puede colapsar y posicionarse en el costado izquierdo de la página.

En la sección de main se visualiza encapsula el contenido de cada una de las vistas, es por lo que se creó la figura 9.4 de la vista Index de la carpeta Home, para ejemplificar el renderizado de esta y las demás vistas.

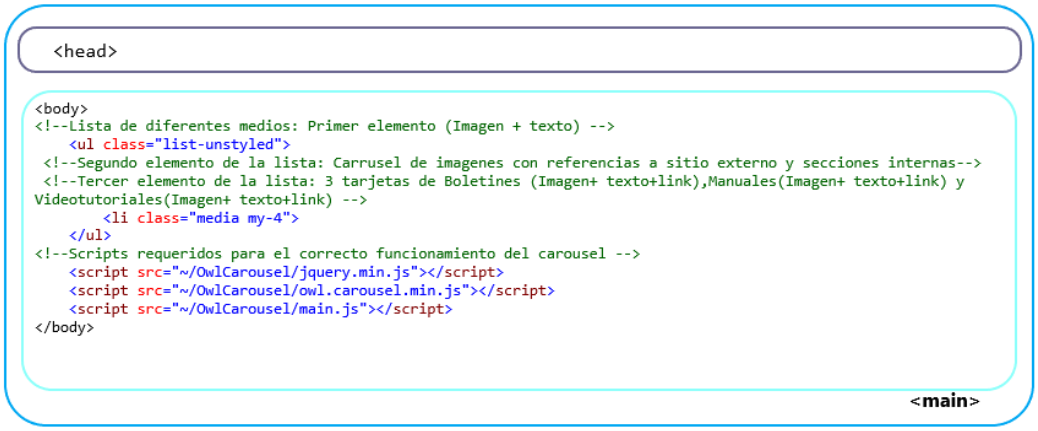


Figura 9.4 Contenido de main.

El footer se divide en 2 partes, una de ellas está configurada para mostrar en color negro los datos de la UNAM y la FI en columnas diferentes, las cuales tienen enlaces a la página del laboratorio de Redes y Seguridad, en la dirección física del laboratorio se redirige a la vista de contacto con el objetivo de mostrar el mapa ,mientras que la segunda parte está configurada para ser de color rojo, mostrar el Copyright y los enlaces al contacto, la sección administrativa y el aviso de privacidad.

Escalabilidad de la página web

ASP.NET Core Identity

Cuando se creó el proyecto se seleccionó sin autenticación, pero dado que se creó una sección administrativa, se deberá implementar un superadmin que pueda generar nuevos usuarios administradores, asignar roles y privilegios dentro de la aplicación, es por ello que se requiere hacer uso de la autenticación para evitar que cualquier persona pueda ingresar a dicha sección.

Se consideró conveniente generar un Registro, Login, Logout, Lockout y se solicitó un reset de contraseña en caso de olvidarla o requerir cambiarla cada cierto tiempo.

Para poder implementar dichas vistas se optó por implementar Identity FrameWork Core para autenticar a los usuarios, por ello se escaló el proyecto siguiendo estos pasos:

1) Agregue los siguientes paquetes NuGet: microsoft.aspnetcore.diagnostics.entityframeworkcore versión 5.0.13 y microsoft.aspnetcore.identity.entityframeworkcore versión 5.0.13.
2) Modifique el archivo de ApplicationDbContext, en la siguiente línea de código: public class ApplicationDbContext : DbContext por **public class ApplicationDbContext : IdentityDbContext<IdentityUser>** además deberá agregar los using recomendados por la herramienta:
   a) using Microsoft.AspNetCore.Identity;
   b) using Microsoft.AspNetCore.Identity.EntityFrameworkCore;
3) Diríjase al "Explorador de soluciones", dé clic derecho en CiberculturaV2, busque la opción de "Agregar", se desplegará otro menú del lado derecho, de clic en "Nuevo elemento con Scaffolding", se abrirá una nueva ventana, del lado derecho seleccionará "Identidad", en el centro aparecerá otra vez "Identidad", puede seleccionar "Agregar" o simplemente de clic 2 veces en "Identidad", el proyecto le mostrará una ventana como la que se muestra en la figura 10.

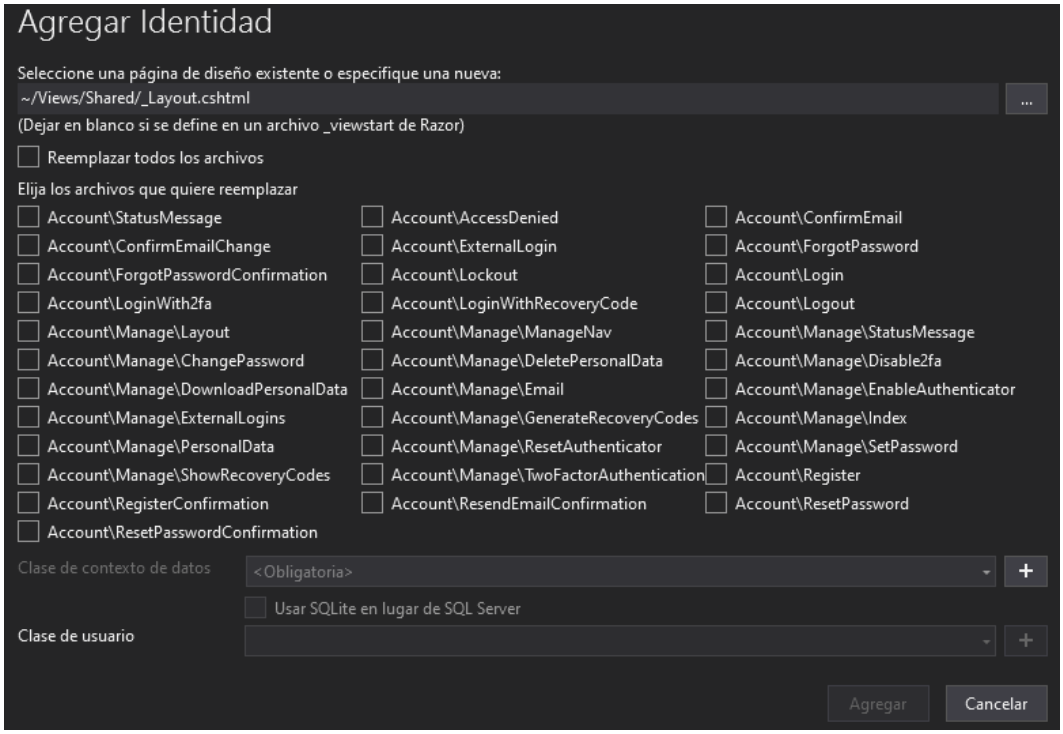


Figura 10. Identity.

4) Seleccione las Páginas de Razor que ya vienen creadas y que poseen sus propios modelos y controladores. En este caso puede seleccionar las que se mencionaron con anterioridad: Register, Login, Logout, Lockout e incluso las de ConfirmEmail, ForgotPassword y ResetPassword, después deberá seleccionar "Clase de contexto de datos", El IDE le sugerirá que cree una clase nueva, pero no es necesario, dado que ya cuenta con ApplicationDbContext, por lo que escribirá lo siguiente: CiberculturaV2.Data.ApplicationDbContext y dará clic en "Agregar". La estructura de la cadena anterior es el nombre de la solución. la carpeta donde se encuentra la clase de contexto. nombre de la clase de contexto de datos.

   Nota 1: Puede conservar dichas páginas o puede crear propias, ya que Identity proporciona sus propios modelos y atributos que pueden ser aprovechados.

   Nota 2: Al aplicar el Scaffolding se agregan nuevas carpetas como se muestra en la figura 10.1, además de que en la carpeta Shared se agrega una nueva vista llamada _LoginPartial, la cual no se implementa ya que se implementa un condicional en _Layout.
5) Borre la carpeta de Migrations del proyecto y la base de datos de Microsoft SQL Server Management Studio, proceda a ejecutar los siguientes comandos en la terminal: **Add-Migration MigracionIdentity** y **update-database**. En los archivos creados en la carpeta de Migrations podrá observar las tablas de Identity como se muestra en la figura 10.2.

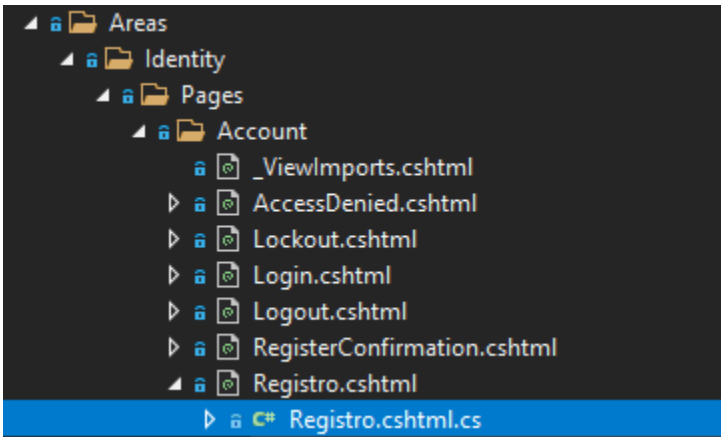


Figura 10.1 Identity FrameWork Core.

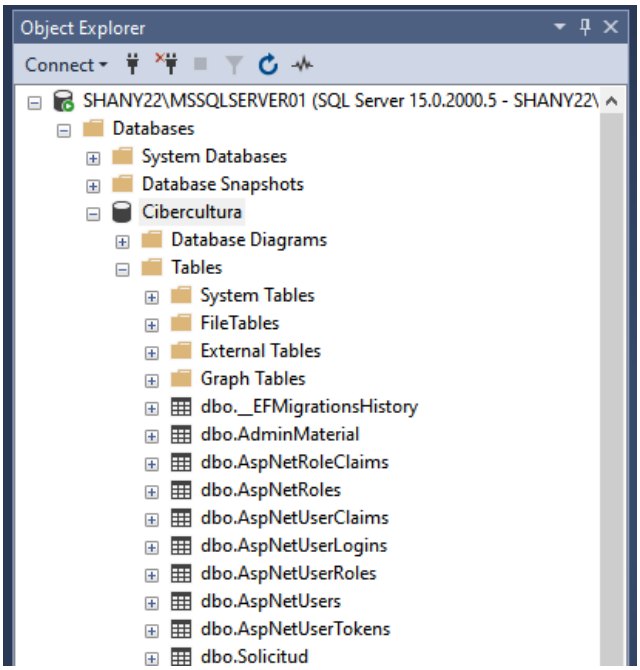


Figura 10.2 Tablas creadas para el proyecto y las de ASP.NET (Identity).

6) Modifique el archivo de Startup.cs con el siguiente código en `color verde y letra Courier New` para agregar Identity y el proxy inverso:

```
using CiberculturaV2.Data;
using Microsoft.AspNetCore.Builder;
using Microsoft.AspNetCore.Hosting;
using Microsoft.AspNetCore.Identity;
using Microsoft.AspNetCore.HttpOverrides;
//(Otras instrucciones using...)
using System.Net;

namespace CiberculturaV2
```

```
{
  public class Startup
  {
    public Startup(IConfiguration configuration)
    {
       Configuration = configuration;
     }
    public IConfiguration Configuration { get; }
    public void ConfigureServices(IServiceCollection
    services){
      //Configuración de las páginas de Razor
      services.AddRazorPages();
      //Configuración de cadena de conexión
      services.AddDbContext<ApplicationDbContext>
      (options =>options.UseSqlServer(Configuration.
      GetConnectionString("DefaultConnection")));

      services.Configure<ForwardedHeadersOptions>
     (options =>{Options.KnownProxies.Add
     (IPAddress.Parse(“”));});

      //Configuración de Identity
      services.AddIdentity<IdentityUser,IdentityRole>
      ().AddEntityFrameworkStores<ApplicationDbContext>
      ();

      services.AddControllersWithViews();
      //Configuración por defecto del inicio
      // de sesión y bloqueo
      services.Configure<IdentityOptions>(options =>
      {
        //Username

        settings.options.User.AllowedUserNameCharacters=
        "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTU
        VWXYZ0123456789";
        options.User.RequireUniqueEmail = false;

        //Password settings.
        //Se requiere el uso de dígitos del 0-9

        options.Password.RequireDigit = true;

        //Requiere el uso minúsculas

        options.Password.RequireLowercase = true;

        //Requiere caracteres no alfanuméricos

        options.Password.RequireNonAlphanumeric = true;

        //Requiere el uso de mayúsculas.
```

```
            options.Password.RequireUppercase = true;

            //la longitud min. requerida es de 12

            options.Password.RequiredLength = 12;

            //Requiere el número de caracteres distintos en
            // la contraseña.

            options.Password.RequiredUniqueChars = 1;

            //Lockout settings.
            //La cantidad de tiempo que un usuario se
            //bloquea
            //cuando se equivoca demasiadas veces.

            options.Lockout.DefaultLockoutTimeSpan =
            TimeSpan.FromMinutes(10);

            //Número de intentos de acceso con error hasta
            //que se bloquea un usuario, si el bloqueo está
            //habilitado

            options.Lockout.MaxFailedAccessAttempts = 3;
            //Determina si se puede bloquear un nuevo
            //usuario.

            options.Lockout.AllowedForNewUsers = true;
            });
        }

// This method gets called by the runtime. Use this
method to configure the HTTP request pipeline.

     public void Configure(IApplicationBuilder app,
    IWebHostEnvironment env){
    if (env.IsDevelopment())
    {
       app.UseDeveloperExceptionPage();
       app.UseForwardedHeaders();
    }
    else
    {
       app.UseExceptionHandler("/Home/Error");
       app.UseForwardedHeaders();
       app.UseHsts();
    }
```

```
app.UseForwardedHeaders(new ForwardedHeadersOptions
{
    ForwardedHeaders = ForwardedHeaders.XForwardedFor |
    ForwardedHeaders.XForwardedProto
});


app.UseHttpsRedirection();

app.UseStaticFiles();

app.UseDefaultFiles();

app.UseRouting();

//Se utiliza para implementar la autenticación

app.UseAuthentication();

app.UseAuthorization();
app.UseEndpoints(endpoints =>{
endpoints.MapControllerRoute(
      name: "default",
      pattern: "{controller=Home}/{action=Index}/{id?}");
 endpoints.MapRazorPages();
   });
      }
   }
}
```

7) Modifique _Layout para implementar Identity con el siguiente código `color verde y letra Courier New`, mientras que las instrucciones en verde y letra Times es para modificar el HTML:

```
@using Microsoft.AspNetCore.Identity
@inject SignInManager<IdentityUser> SignInManager
@inject UserManager<IdentityUser> UserManager


 @if (SignInManager.IsSignedIn(User))
   {
        <!-- código de la barra de navegación (menú)>
        <!-- Desde la perspectiva de la administración>
        <!-- ejemplo: controlador vista display>
        <!--Logout-->
       <li class="nav-item dropdown active">
       <a class="nav-link dropdown-toggle"
        id="navbarDropdown1" role="button"
        data-toggle="dropdown" aria-haspopup="true"
        aria-expanded="false">
        ¡Hola <b>@User.Identity.Name.ToUpper()</b>!
       </a>
       <div class="dropdown-menu border
```

```
          border-danger" aria-labelledby="navbarDropdown">
          <a class="nav-link" asp-controller="Administracion"
           asp-action="ChangePassword">Cambiar contraseña</a>
          <a class="nav-link" id="logout"
           asp-area="Identity" asp-page="/Account/Logout"><b>
           Cerrar sesión</b>
          </a>
          </div>
          </li>
}
else
{
          <!--Código de la barra de navegación>
          <!--vista de la comunidad>


 }

    <div class="container-fluid">
        <main role="main" class="pb-3">
            @RenderBody()
        </main>
    </div>

    <!-- Inicio del Footer con 2 columnas de texto-->
    @if (SignInManager.IsSignedIn(User))
    {
        <!-- footer desde la perspectiva administrativa>
        <!--Contacto>
        <!--Aviso de privacidad>

    }
    else
    {
            <!-- footer desde la perspectiva comunidad>
<!--Contacto>
            <a id="login" asp-area="Identity" asp-
             page="/Account/Login" class="text-white
             font-weight-light">Administración</a>
                
            <!--Aviso de privacidad>

    }
```

8) Se creó AdministracionController para generar los siguientes estados HTTP:
   a) Lista de administradores.
   b) Cambio de contraseña (se requiere conocer el password actual para poder crear uno nuevo).
   c) Eliminar administrador.
9) Se creó una carpeta llamada ViewModels para que se puedan generar clases que le permitirá acceder a los diferentes atributos de los modelos que implementa Identity, modelos que no son visibles para los desarrolladores, pero que en

Microsoft SQL Server Management Studio podrá observar las tablas, atributos y tipos de datos que se implementan, en este caso generaron 3 clases nombradas: Registro, Login y ChangePassword.

10) Páginas de Razor creadas:
    a) Lista de administradores.
    b) Cambio de contraseña (se requiere conocer el password actual para poder crear uno nuevo).
    c) Eliminar administrador.

Estas páginas contienen dos archivos: uno es la página con terminación .cshtml y otro es el controlador con terminación .cshtml.cs en este archivo se aplican los estados HTTP, en el caso de Login se generó una alerta para advertir al administrador que, en caso de escribir mal la contraseña en 3 intentos, la cuenta se bloquea por 10 minutos, sin importar que en el cuarto intento ingrese correctamente la contraseña. Por lo que tendrá que esperar 10 minutos para volver a intentar acceder a su cuenta.

Nota 1: Por cuestiones de seguridad a los controladores administrativos se les debe implementar la biblioteca Identity y la siguiente línea de código, ambas resaltadas en color verde:

```
using Microsoft.AspNetCore.Identity;
namespace CiberculturaV2.Controllers
{
    [Authorize]
    public class _Controller : Controller
```

Nota 2: Para registrar a un administrador se requiere el RFC o número de cuenta del administrador, correo electrónico y una contraseña de 12 caracteres, la cual requiere de letras mayúsculas, minúsculas, números y caracteres especiales. Además, después de crear un nuevo administrador no se queda su sesión iniciada, sino que tendrá que iniciar sesión con su RFC o número de cuenta y contraseña.

Nota 3: Para agregar una página de Razor, deberá posicionarse en la carpeta “Areas”, busque la subcarpeta “Pages” de clic en ella y encontrará la subcarpeta “Account” de clic derecho, seleccione “Agregar” y dé clic en “Nuevo elemento”, busque dentro de la ventana “Página de Razor vacía”, escriba un nombre de identificación, dé clic en “Agregar” y de esta manera podrá crear un controlador y una página de Razor.

Migración del proyecto al sistema operativo Ubuntu 20.04

Instalación de ASP.NET Core 5.0 y MariaDB

Los comandos que deberá aplicar los encontrará con el siguiente tipo de fuente `Courier New`, cuando en el comando se especifique acciones relevantes sobre el proyecto la fuente se verá de la siguiente forma: `Courier New.`

Abra una terminal y escriba los siguientes comandos:
Instalación de los paquetes requeridos para Ubuntu 20.04

```
wget
https://packages.microsoft.com/config/ubuntu/20.04/packages
-microsoft-prod.deb -O packages-microsoft-prod.deb
```

```
sudo dpkg -i packages-microsoft-prod.deb rm packages-
microsoft-prod.deb
```

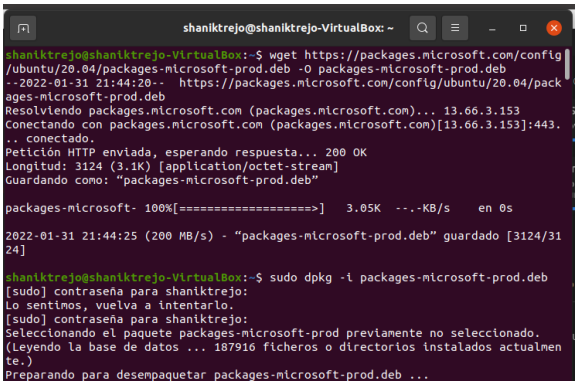


Figura 1. Instalación de los paquetes.

SDK de .NET
Actualización de los repositorios:

```
sudo apt-get update
```

Instalación del transporte https:

```
sudo apt-get install -y apt-transport-https
```

Actualización de los repositorios:

```
sudo apt-get update
```

Instalación del SDK de .NET:

```
sudo apt-get install -y dotnet-sdk-5.0
```

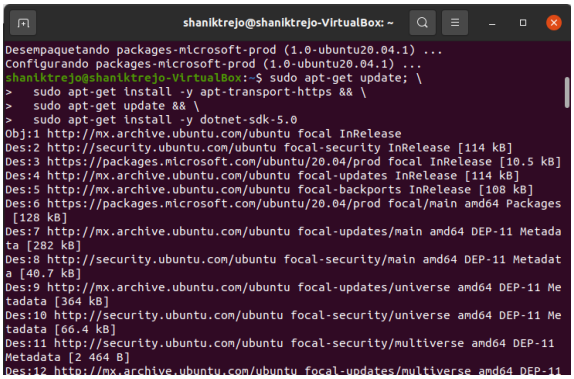


Figura 2. Instalación del SDK de .NET.

Runtime de ASP.NET Core 5.0

Actualización de los repositorios:

```
sudo apt-get update
```

Instalación del transporte https:

```
sudo apt-get install -y apt-transport-https
```

Actualización de los repositorios:

```
sudo apt-get update
```

Instalación del runtime de ASP.NET 5.0:

```
sudo apt-get install -y aspnetcore-runtime-5.0
```

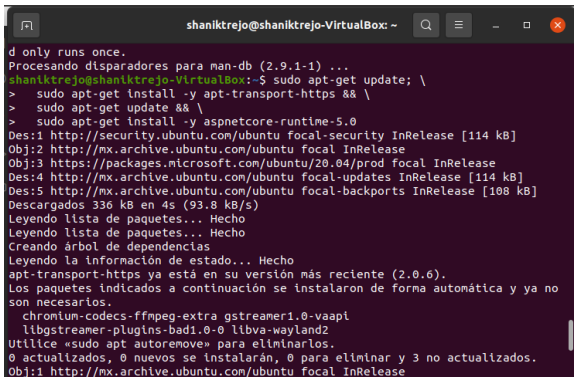


Figura 3. Instalación de Runtime.

.NET EF Database

Instalación de la herramienta en su versión más reciente para ASP.NET Core 5.0:

```
dotnet tool install --global dotnet-ef --version 5.0.14
```

Actualización de la herramienta:
```
dotnet tool update --global dotnet-ef --version 5.0.14
```

Actualización del repositorio:
```
sudo apt update
```

Instalación de MariaDB:
```
sudo apt install mariadb-server
```

Configuración de MariaDB:
```
sudo mysql_secure_installation
```

- El instalador de mariadb le hará una serie de solicitudes, tales como el introducir una contraseña **root** para la base de datos actual, como no ha establecido una de clic en **Enter** para indicar la falta de contraseña.
- La siguiente pregunta que le hará será si desea configurar una contraseña para la base de datos, por lo que deberá escribir **N** y dar **Enter**.
- Para las siguientes preguntas escriba **Y** + **Enter** para aceptar los valores predeterminados.
  Para ajustar la autenticación y privilegios de usuario.

  Creación de cuenta administrativa:
  ```
  sudo mysql

  MariaDB [(none)]> GRANT ALL ON *.* TO
  'XXXXX'@'localhost' IDENTIFIED BY 'XXXXX' WITH GRANT
  OPTION;
  ```

  Donde XXXX en "`XXXXX'@'localhost`" es e el nombre de del usuario y XXXXX después de `IDENTIFIED BY` es la contraseña que se le asignará al usuario.

  Vacíe los privilegios:
  ```
  MariaDB [(none)]> FLUSH PRIVILEGES;
  ```

  Salir:
  ```
  MariaDB [(none)]> exit;
  ```

  Comprobación de la creación del usuario:
  ```
  mysqladmin -u XXXXX -p versión
  ```

  Donde XXXX es el nombre del usuario.

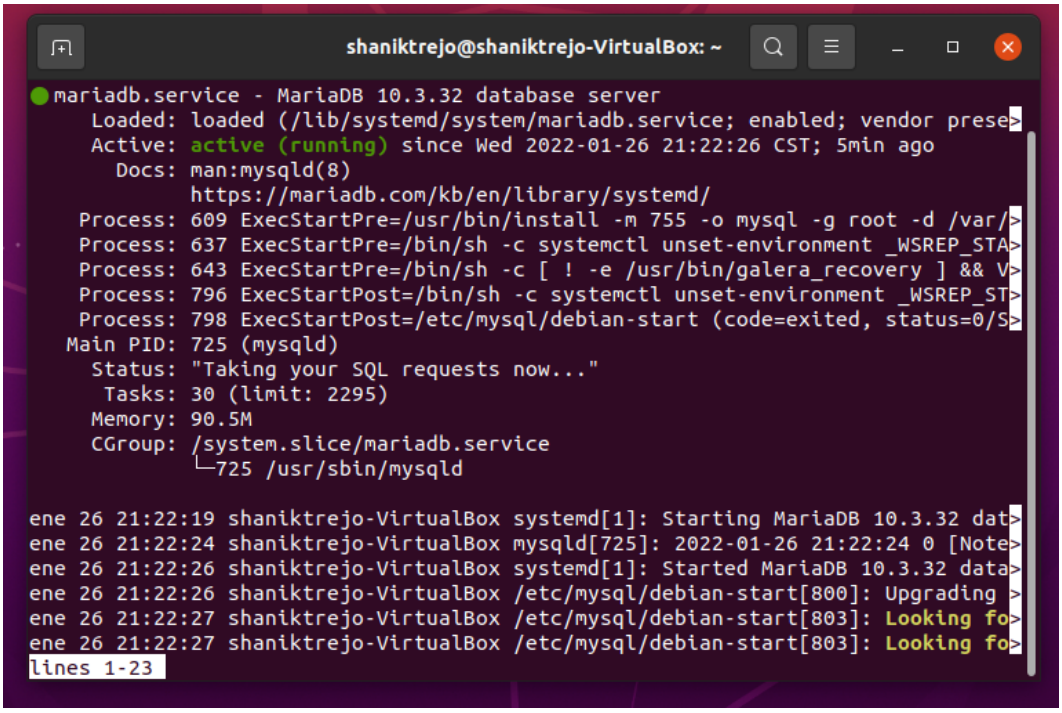


Figura 4. Comprobación de MariaDB

Instalación de Visual Code, C# y exportación de la base de datos

En la misma terminal escriba el siguiente comando:

```
snap install --classic code
```

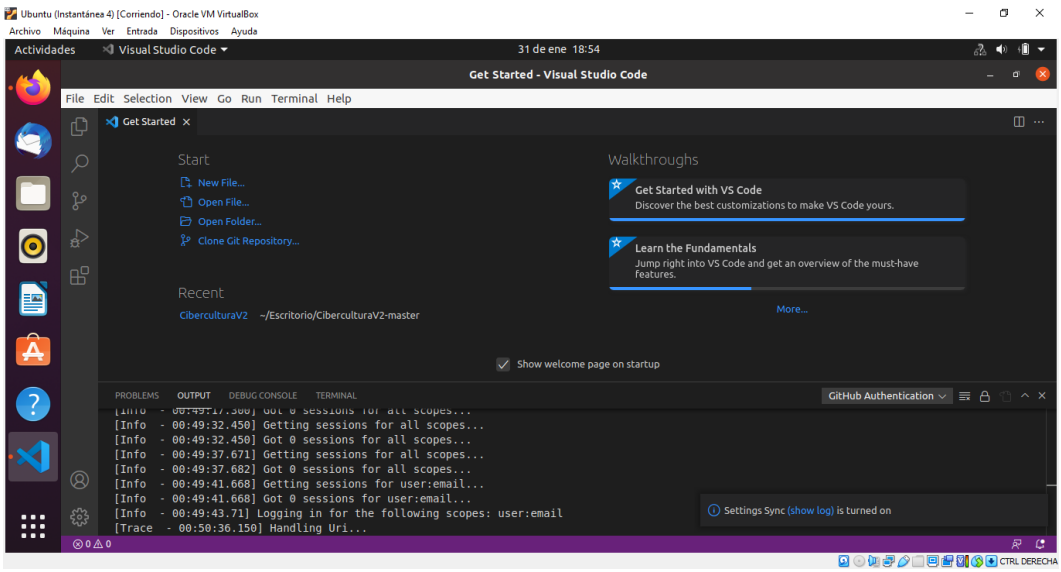


Figura 5. Visual Studio Code.

El proyecto se migró usando la carpeta de la solución, se abrirá en Visual Studio Code, por lo que al revisar los archivos como por ejemplo un modelo o controlador, se observa que el editor no tiene integrado el lenguaje C# de Microsoft por lo que se procede a instalarlo de manera gráfica como se muestra en la figura 6.

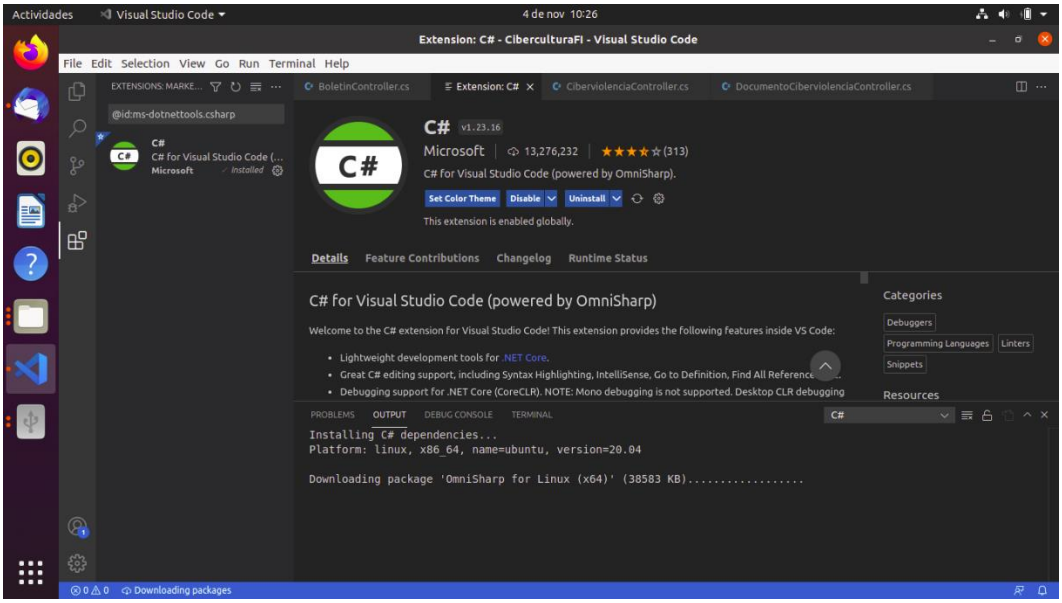


Figura 6. Instalación del lenguaje C# para VS Code.

Para probar el correcto funcionamiento del proyecto en este editor y sistema operativo se deberán ejecutar los siguientes comandos, dentro de la terminal de VS Code.

Compilar el proyecto:

```
dotnet build
```

Actualizar la base de datos:

```
dotnet ef database update
```

Ejecutar la aplicación:

```
dotnet run
```

Se creó un usuario administrador desde el buscador web, mismo que será exportado junto con la base de datos del proyecto.

Exportación de la base de datos del proyecto

Comando general:

```
sudo mysqldump -u username -p name of new database > name of database.sql
```

Aplique el siguiente comando particular:

```
sudo mysqldump -u root -p XXXXX > XXXXX.sql
```

Donde XXXX será el nombre de la nueva base de datos y XXXXX.sql es el nombre de la base de datos a importar.

Agregar el siguiente paquete para que la aplicación pueda acceder a la base de datos:

```
dotnet add package Microsoft.EntityFrameworkCore.Design --versión
5.0.14
```

Publicación del proyecto y transferencia al servidor
Indique la ruta en la que se va a generar la publicación del proyecto

Comando:

```
dotnet publish -c Release -o /rutacompleta (path)
```

La siguiente figura ilustra el proceso de publicación del proyecto.

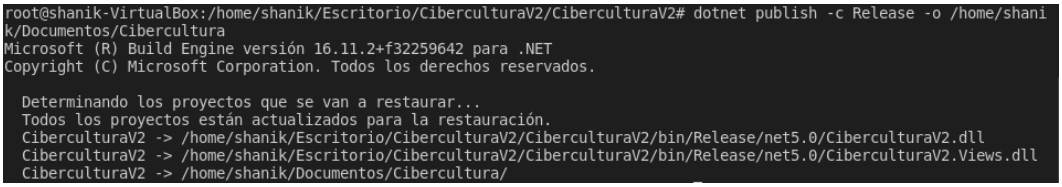


Figura 7. Publicación del proyecto.

Comprima la publicación del proyecto con el siguiente comando:

```
zip -r nombredelacarpeta.zip /rutacompleta (path)
```

Vaya a su servidor y creé la carpeta que albergará el proyecto con el siguiente comando:

```
sudo mkdir /var/www/html/[redacted]
```

La transferencia al servidor se realizará mediante la interfaz web de Webmin la cual realiza la transferencia sin usar Secure Shell (SSH), pero se puede realizar con cualquier cliente que implemente el protocolo de transferencia de archivos (FTP).

Aplique el siguiente comando para editar el archivo del repositorio del servidor:

```
sudo nano /etc/apt/sources.list
```

Agregue al final del archivo el siguiente repositorio:

```
deb http://download.webmin.com/download/repository sarge
contrib
```

Descargue la llave del repositorio de Webmin y agregue la al repositorio del servidor con la siguiente instrucción:

```
wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo
apt-key add
```

Actualice el repositorio:

```
sudo apt-get update
```

Instale Webmin con el siguiente comando:

```
sudo apt-get install webmin
```

Abra una pestaña en su buscador e ingrese `https://IPdelServidor:Puerto`. Por defecto Webmin opera desde el puerto 10000, en caso de desconocer la IP de su servidor aplique el comando de `ifconfig` en la terminal para conocerla, en este caso el servidor tiene una IP de `192.168.1.79`, por lo que deberá escribir: `https://192.168.1.79:10000`. El buscador le dirá que es un riesgo de seguridad, por lo que deberá aceptar el riesgo para poder realizar la conexión con el servidor, como se muestra en la siguiente figura.

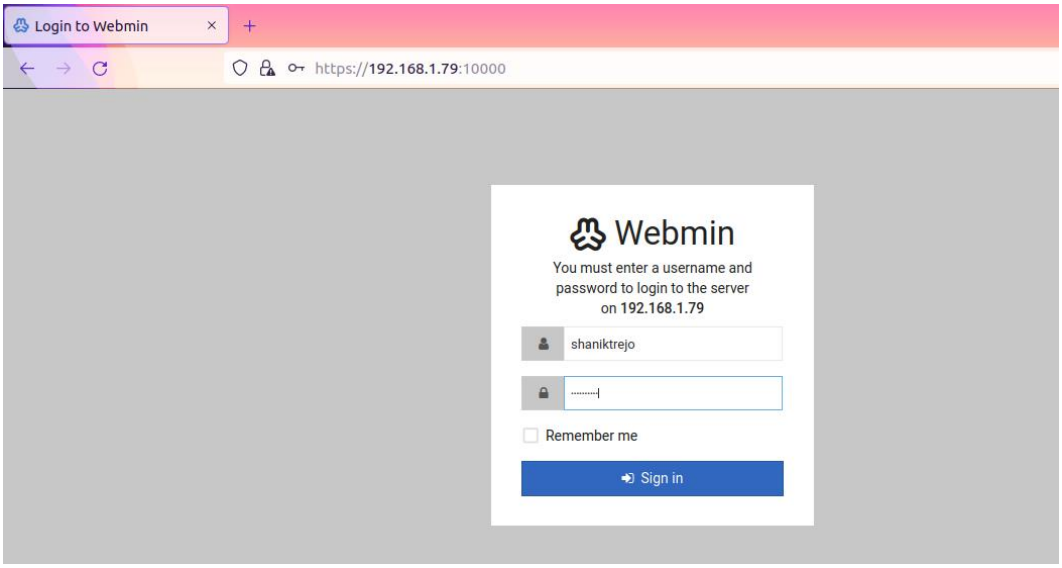


Figura 8. Login de Webmin.

En el menú izquierdo de Webmin busque la opción Tools (figura 8.1 Menú principal), dé clic en File Manager, verá las carpetas que contiene el servidor,

busque la carpeta var, dé clic en ella, agregue la carpeta www, cuando esté creada de clic en ella y podrá observar que se creó la carpeta html, además podrá observar que del lado derecho el botón desplegable de File tendrá que dar clic en él y seleccionar la opción de Upload to current directory (figura 8.2 Transferencia de archivos).

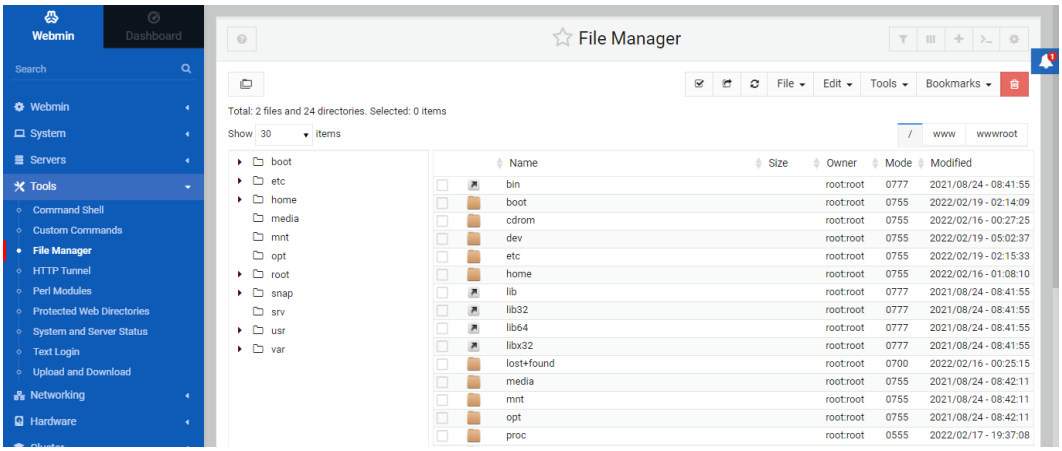


Figura 8.1 Administrador de archivos del servidor.

En su computadora con sistema operativo Ubuntu busque el archivo CiberculturaV2.zip y colóquelos en el espacio de “Drag and drop files here or click to select” de la figura 8.2.

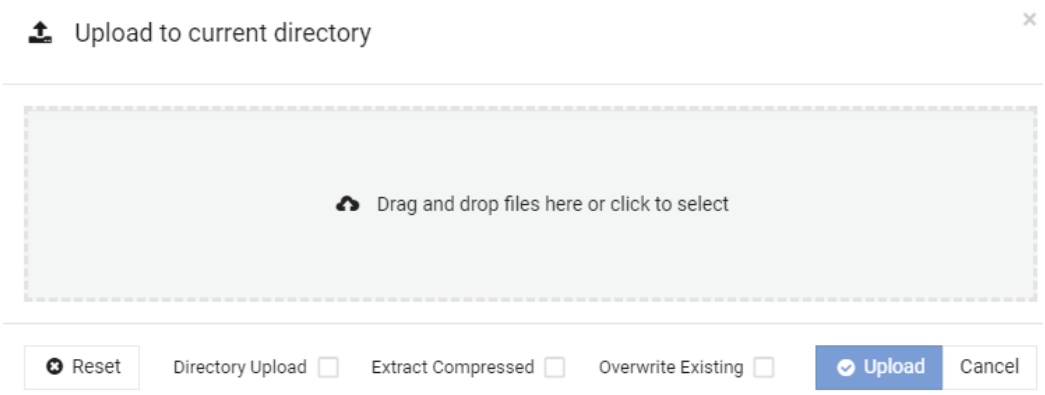


Figura 8.2 Transferencia de archivos.

Opciones para la extracción de archivos:
Opción 1. Interfaz Gráfica de Usuario (GUI): Posteriormente dé clic en Extract para descomprimir los archivos.

Opción 2. Interfaz de Línea de Comandos (CLI) en el servidor: Podrá descomprimir el proyecto en dicha carpeta, para hacerlo deberá escribir el siguiente comando en la terminal del servidor: `unzip Cibercultura.zip`

Podrá observar en el panel de File manager que los archivos ya se encuentran descomprimidos en sus respectivas carpetas.

Opción 3. Utilización de una máquina virtual: Para poder transferir los archivos finales a un sistema operativo igual al que se ocuparía y con el fin de realizar pruebas y ajustes. Es por lo que otra opción a considerar es la utilización de una máquina virtual que mediante ella se pueden compartir los archivos entre la máquina host y la virtual de una manera rápida y sencilla.

Manual del usuario final

Conozca el sitio web oficial del proyecto: “Cibercultura en Ciberseguridad: Ahora y siempre” (Ver figura 1).

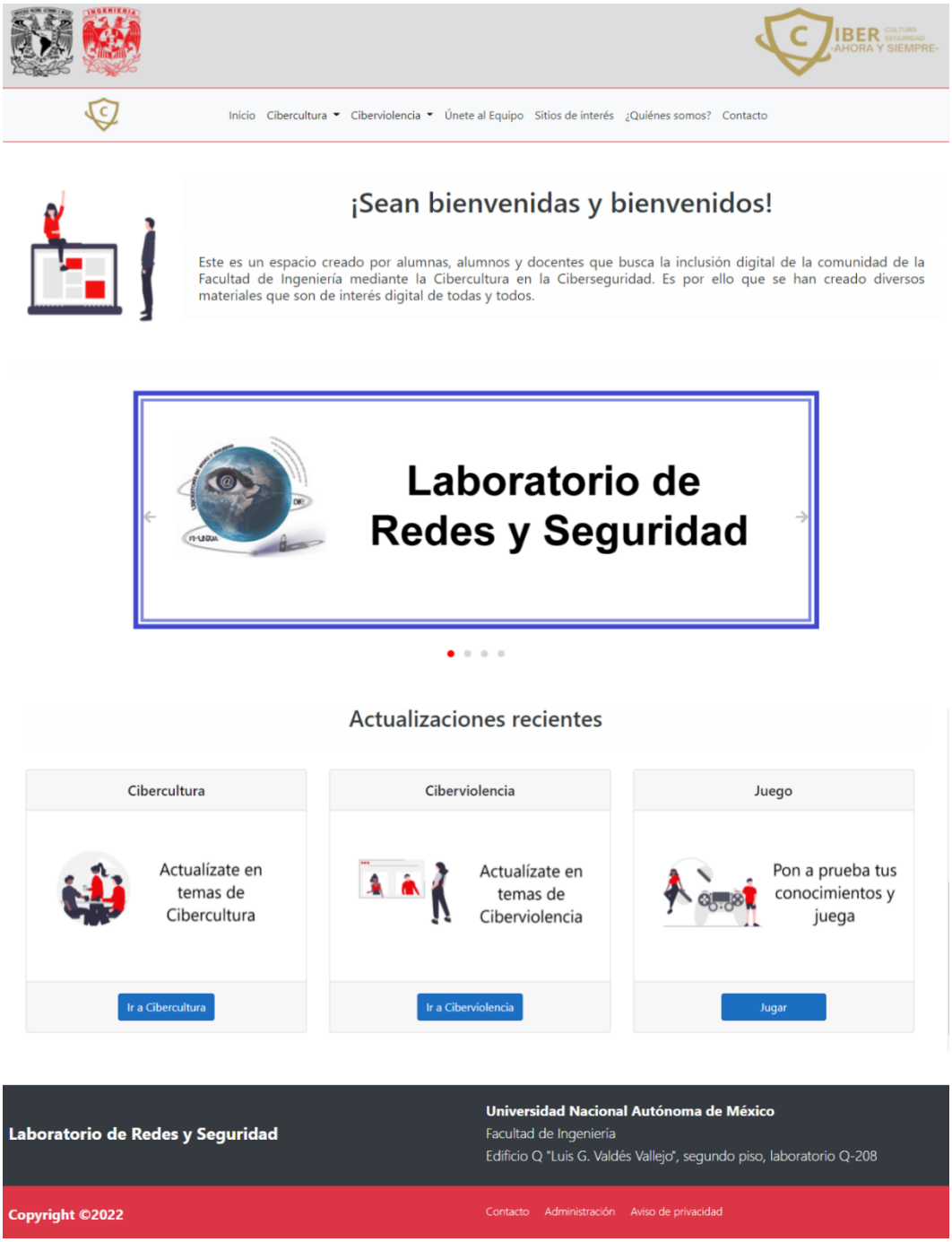


Figura 1.Inicio de https://cibercultura.fi-b.unam.mx/.

Barra de navegación

La barra de navegación (ver figura 2) contiene diferentes enlaces dentro de la página web, por ejemplo, si da clic en el logo del proyecto o el texto de “Inicio”, el resultado que verá será la figura 1.

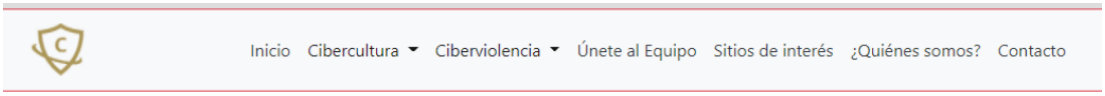


Figura 2. Barra de navegación.

Dé clic en el menú desplegable de “Cibercultura” y observará las categorías que esta contiene (ver figura 2.1), al dar clic en el menú desplegable de “Ciberviolencia” podrá observar que se despliegan las opciones a elegir, como se muestra en la figura 2.2.

Figura 2.1 Menú desplegable de Cibercultura.

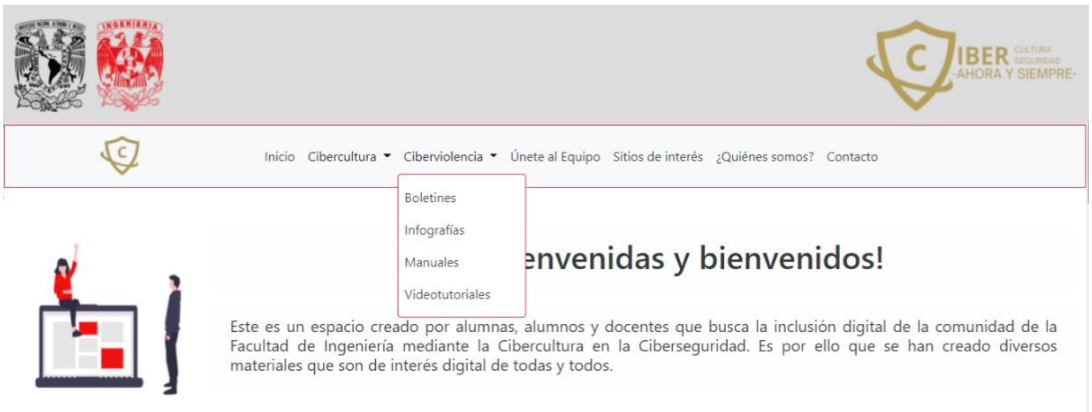


Figura 2.2 Menú desplegable de Ciberviolencia.

Si da clic en “Únete al equipo”, será redirigido a una nueva sección del sitio web, tal como se muestra en la figura 2.3.

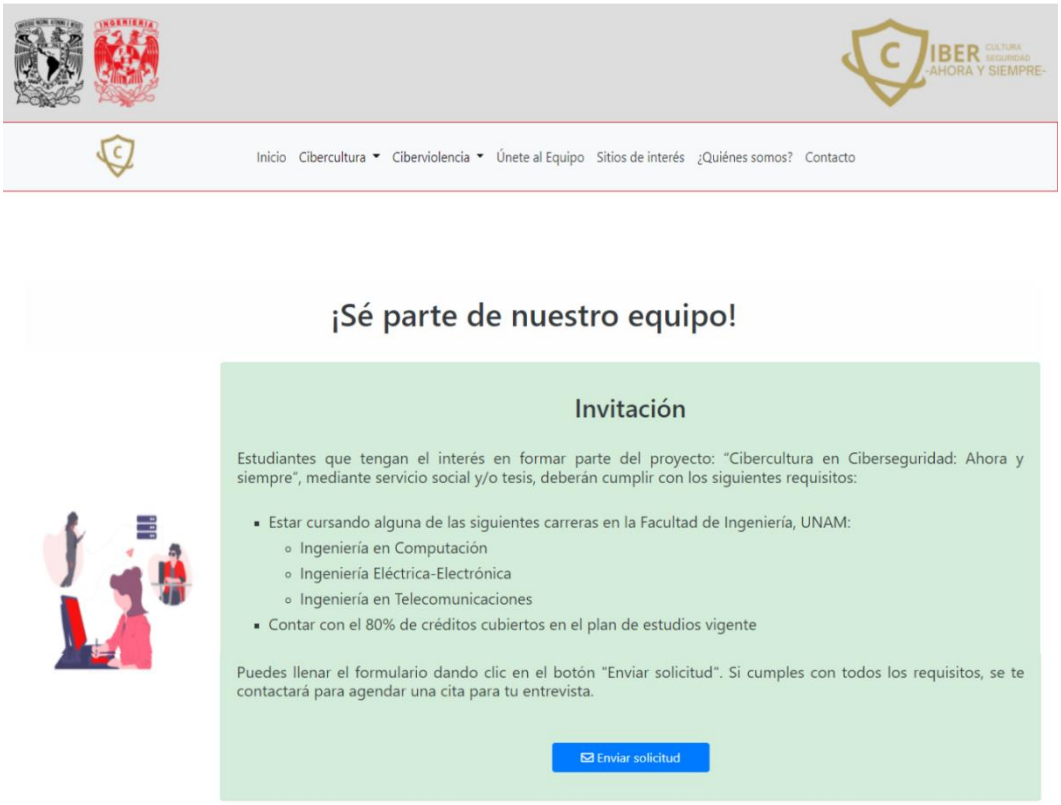


Figura 2.3Página inicial de Únete al equipo.

En “Sitios de interés” se muestra una lista de enlaces que pueden ser de utilidad a los estudiantes a lo largo de su carrera, tal como se muestra en la figura 2.4.

Figura 2.4Página de Sitios de interés.

Al dar clic en “¿Quiénes somos?” Se le mostrará una bienvenida, la visión, misión y objetivos del equipo de Cibercultura en Ciberseguridad: Ahora y siempre (ver figura 2.5).

Figura 2.5Página de ¿Quiénes somos?.

El último elemento de la barra de navegación es “Contacto” (ver figura 2.6) en esta sección podrá observar un mapa de la dirección física del Laboratorio de Redes y Seguridad, el horario de atención y correo electrónico.

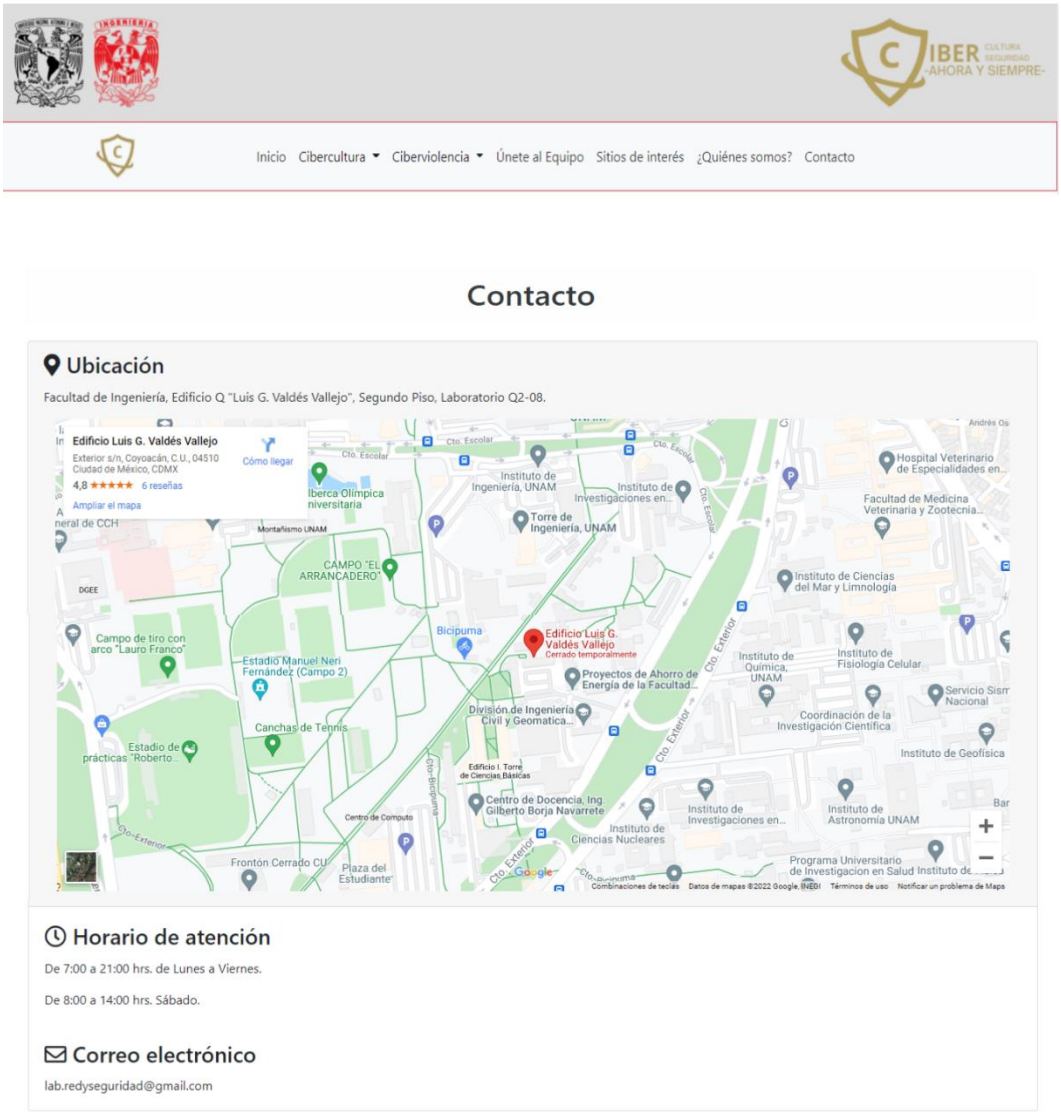


Figura 2.5Página de Contacto.

Cuerpo de la página web

En el cuerpo de la vista inicial puede observar una cordial bienvenida al sitio web, un carrusel de imágenes que al dar clic en cada una de ellas será redirigido a un elemento en específico, pero esta acción se realizará abriendo una nueva pestaña en su navegador web.

Figura 3.Cuerpo del inicio del sitio web.

La sección de “Actualizaciones recientes” se muestran 3 tarjetas diferentes, cuando seleccione Ir a (Cibercultura, Ciberviolencia o Jugar) será redirigido a la vista principal de dicha sección, tal como se muestra en las siguientes figuras.

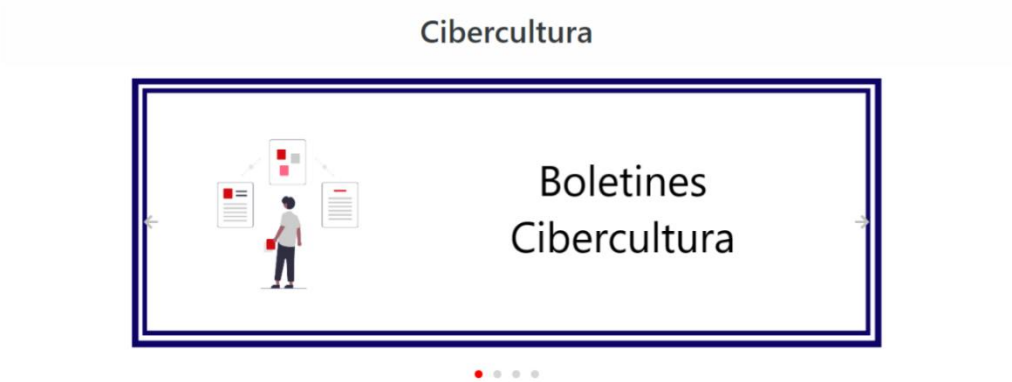


Figura 3.1Index de Cibercultura.

Figura 3.2 Index de Ciberviolencia.

Figura 3.3 Index de Juegos.

Como podrá apreciar en dichas figuras, cada sección tiene su propio carrusel con imágenes que representan a los materiales que alberga este espacio (Boletines, Infografías, Manuales y Videotutoriales) con excepción de los juegos, esto se debe a que se encuentran en desarrollo.

Por último, el footer cuenta con enlaces activos que, al dar clic sobre ellos, se abre una nueva ventana en su navegador web para visualizar la página oficial del elemento seleccionado, entre ellos destacan las páginas de la UNAM, FI, la vista de Contacto y el Aviso de privacidad (figura 4).

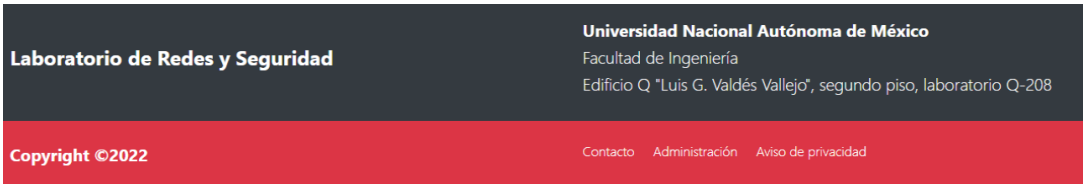


Figura 4. Footer.

Pie de página

Para acceder a la vista de contacto puede hacerlo desde el botón en la barra de navegación, al dar clic en el footer negro (dé clic en la dirección del laboratorio de redes y seguridad) o en el footer rojo dando clic al enlace de contacto. La figura 2.5 muestra el contenido de la vista.

Otros enlaces activos para ser abiertos en otra pestaña del navegador web son:
Laboratorio de Redes y seguridad el cual redirige al usuario a la página oficial del laboratorio (https://redyseguridad.fi-b.unam.mx/Lab/).
Nota: En la última versión del sitio web vigente se cambió al Laboratorio de Redes y Seguridad por el Área de Redes y Seguridad, por lo que el sitio que se abrirá será https://redyseguridad.fi-b.unam.mx/RyS/ (se cumple también para la primera imagen del carrusel que sale en Inicio, mostrando ahora una portada que hace referencia al Área de Redes y Seguridad).

Universidad Nacional Autónoma de México redirige a la página oficial de la UNAM (https://www.unam.mx/).

Facultad de Ingeniería redirige al usuario a la página oficial de la facultad (https://www.ingenieria.unam.mx/).

Nota: Podrá observar un link de Administración al cual no podrá acceder, ya que es un espacio designado para los administradores del proyecto de "Cibercultura en Ciberseguridad: Ahora y siempre".

Con el objetivo de que conozca mejor el sitio web se agregaron los siguientes materiales, pero estos no serán los mismos que encontrará en el sitio web oficial del proyecto, debido a que son materiales que fueron desarrollados para materias

cursadas de la carrera de Ingeniería en Computación y que su único fin era demostrar el correcto funcionamiento del desarrollo web.

Todos los materiales desarrollados se presentan en tarjetas, las cuales poseen un título, portada (imagen alusiva al material y a la comunidad), descripción, autor o autores, la fecha de la publicación y un botón para poder ver el material.

Conozca el apartado de Cibercultura

En la barra de navegación deberá posicionarse en el texto de Cibercultura y dé clic en este, posteriormente dé clic en el texto de Boletines para ver el contenido disponible, en caso de que aún no existan boletines disponibles verá la siguiente página (figura 4).

Figura 4. Boletines de Cibercultura sin materiales disponibles.

En caso de que existan boletines disponibles se verán como se muestra en la figura 4.1.

Nota: En las tarjetas inferiores se muestran referencias a los demás materiales de Cibercultura, lo cual pasará en cada diferente tipo de material.

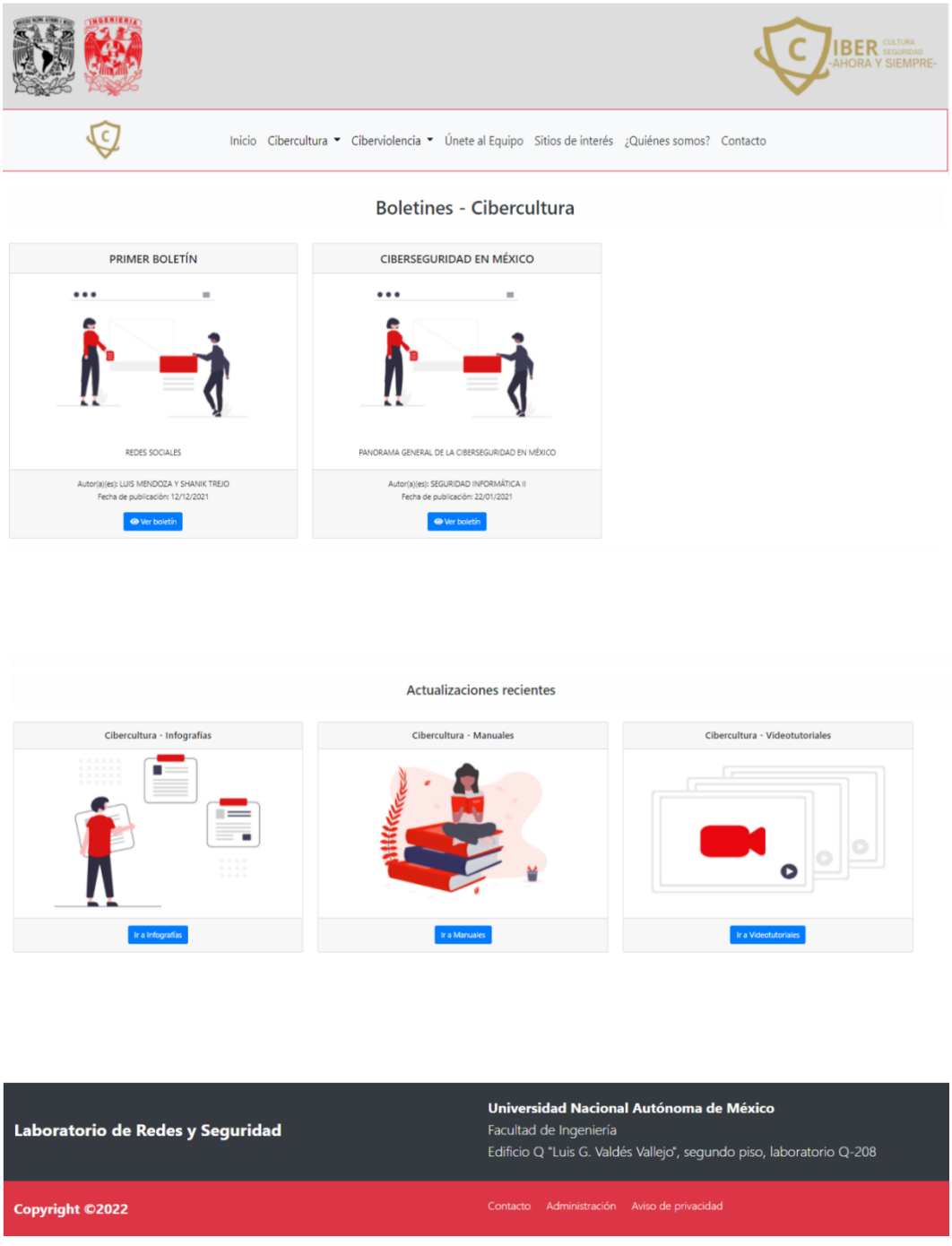


Figura 4.1 Boletines - Cibercultura.

Pulsando el botón que dice “Ver boletín” podrá acceder al material como se muestra en la figura 4.1.1.

Figura 4.1.1Ver boletines de Cibercultura.

Dado que es un pdf podrá cambiar de página con los botones rojos de “Anterior” y “Siguiente”.

El siguiente elemento de Cibercultura es Infografías, en caso de que aún no existan infografías disponibles, la página se mostrará como se muestra en la figura 4.2.

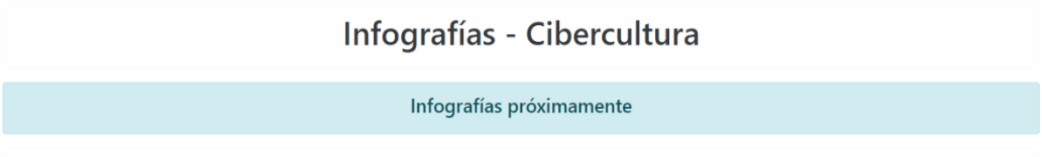


Figura 4.2 Infografías - Cibercultura.

Si ya existen infografías en el sitio web, la página se verá como la figura 4.3.

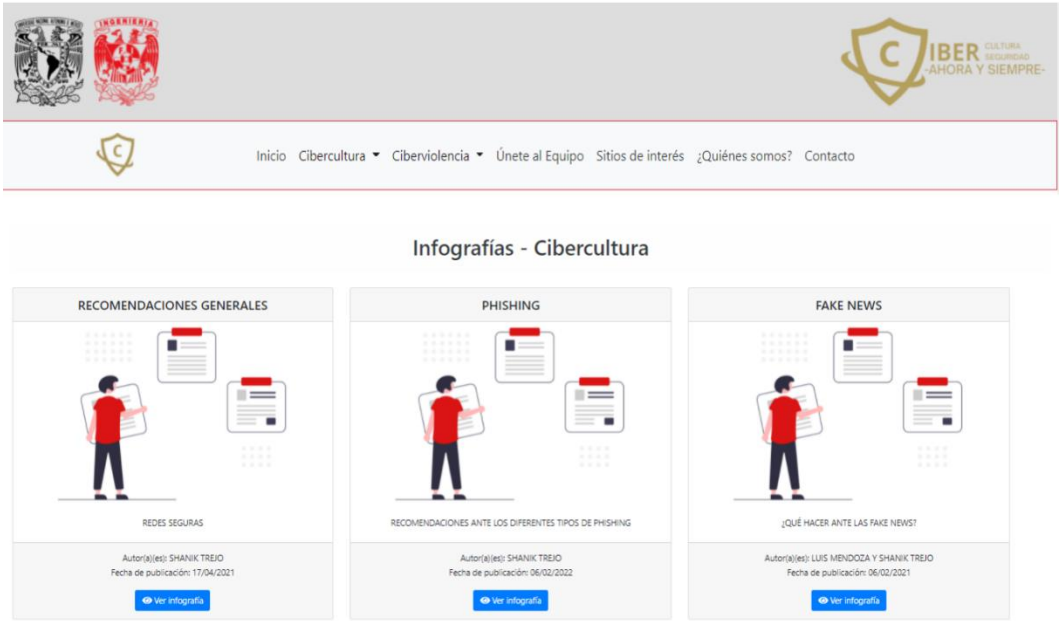


Figura 4.3 Infografías – Cibercultura disponibles.

Dé clic en la Infografía que desee ver, para poder visualizar el material, tal como se muestra en la figura 4.3.1.

Figura 4.3.1Ver infografía de Cibercultura.

El siguiente elemento de Cibercultura son los Manuales, inicialmente está página se encuentra como se muestra en la figura 4.4.

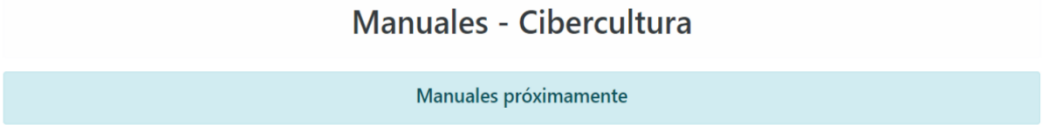


Figura 4.4 Manuales de Cibercultura.

Cuando ya hay manuales disponibles, los podrá observar en tarjetas y para acceder al manual deberá dar clic en el botón de “Ver manual”, tal como se muestra en la figura 4.5.

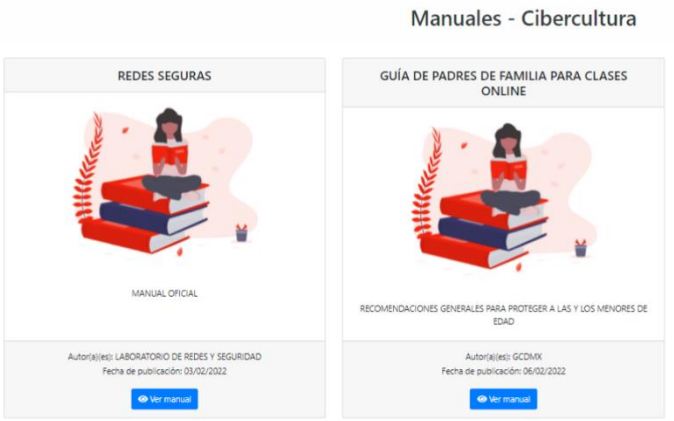


Figura 4.5 Manuales – Cibercultura disponibles.

Al igual que en los boletines podrá cambiar de página dando clic en los botones rojos de “Anterior” y “Siguiente”.

Figura 4.5.1 Ver manual de Cibercultura.

Dado que los manuales tendrán una explicación visual, tendrá que ir a la sección de Videotutoriales para seguir el paso a paso de los manuales, al igual que en los casos anteriores habrá una página inicial que informa que el material estará disponible próximamente (Ver figura 4.6), las tarjetas de los videotutoriales disponibles (Ver figura 4.7) y el videotutorial (Ver figura 4.7.1) desde su respectivo reproductor de mp4.

Figura 4.6 Videotutoriales - Cibercultura.

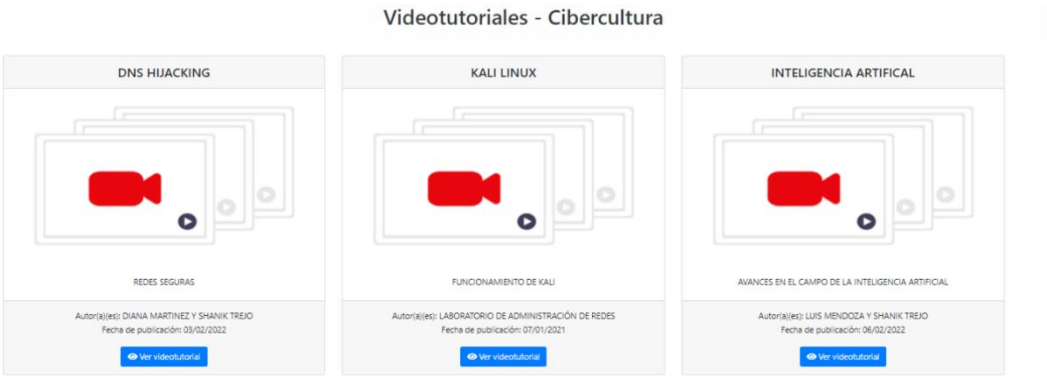


Figura 4.7 Videotutoriales de Cibercultura disponibles.

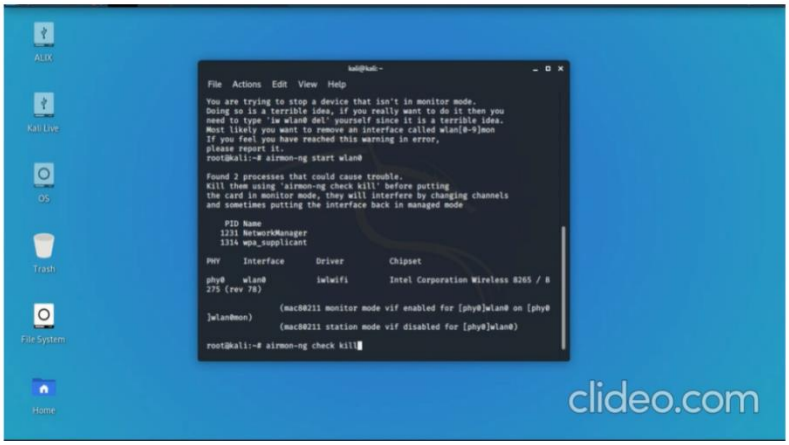


Figura 4.7.1 Ver videotutoriales de Cibercultura.

Conozca el apartado de Ciberviolencia

Los materiales de Ciberviolencia siguen la misma estructura de Cibercultura, por lo que solo se le mostrarán los ejemplos de esta sección sin entrar en más detalles.

Boletines

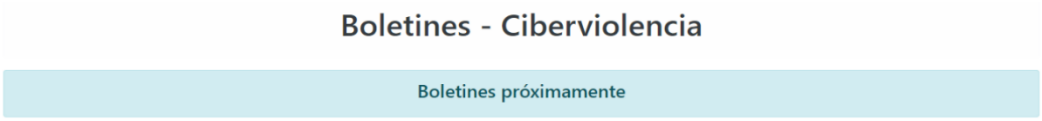


Figura 5. Boletines de Ciberviolencia sin materiales disponibles.

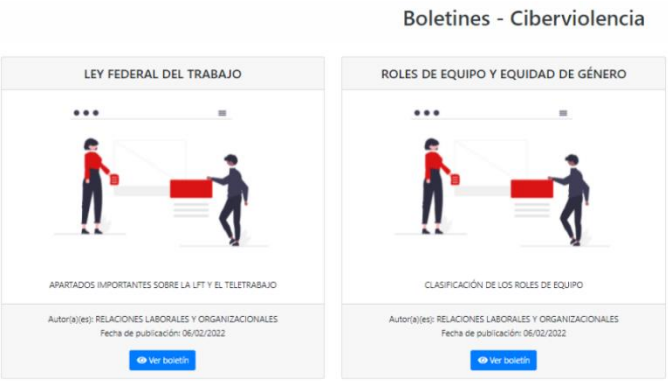


Figura 5.1 Boletines - Ciberviolencia disponibles.

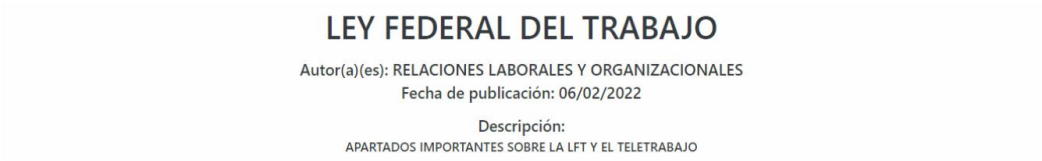


Figura 5.1.1 Ver boletín de Ciberviolencia.

Infografías

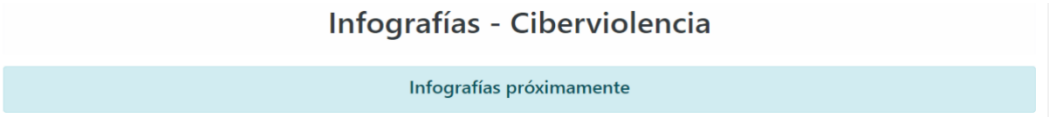


Figura 5.2 Infografías de Ciberviolencia sin materiales disponibles.

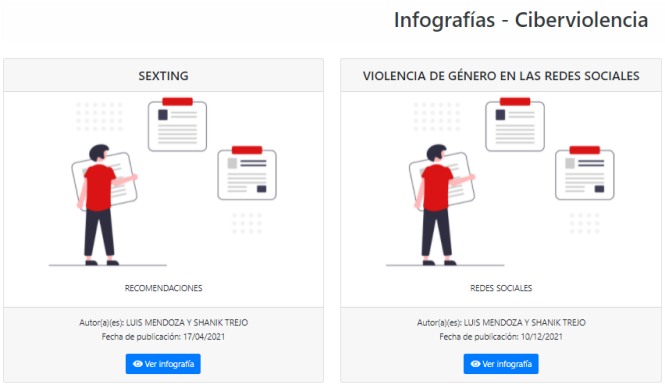


Figura 5.3 Infografías - Ciberviolencia disponibles.

Figura 5.3.1 Ver infografía de Ciberviolencia.

Manuales

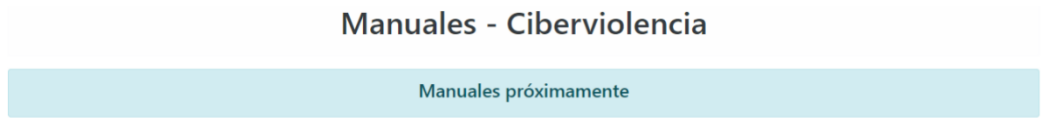


Figura 5.4 Manuales - Ciberviolencia sin materiales disponibles.

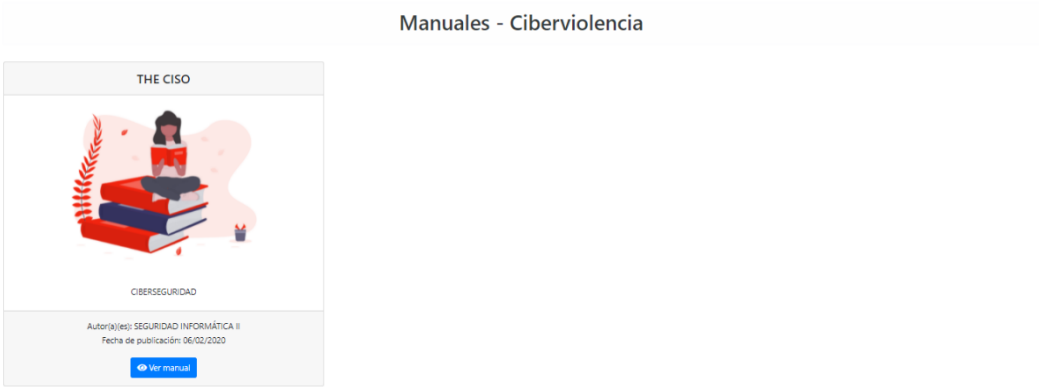


Figura 5.5 Manuales - Ciberviolencia disponibles.

Figura 5.5.1 Ver manual de Ciberviolencia.

Videotutoriales

Figura 5.6 Videotutoriales – Ciberviolencia página inicial.

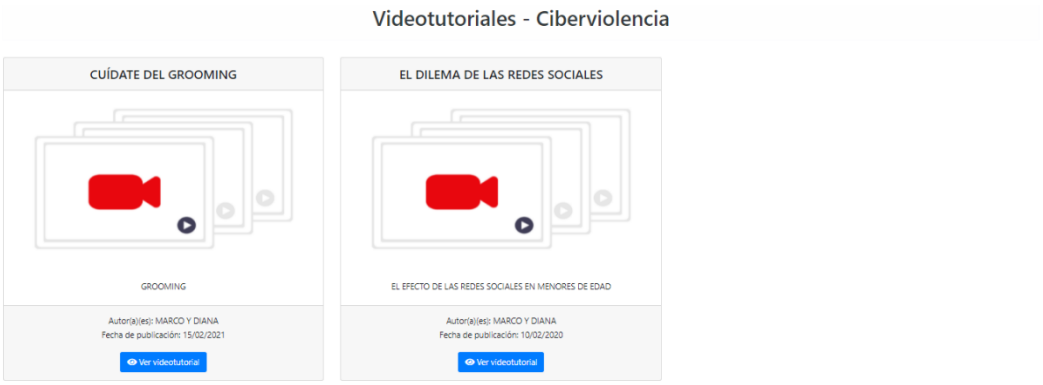


Figura 5.7 Manuales - Ciberviolencia disponibles.

Figura 5.7.1 Ver videotutorial - Ciberviolencia.

¿Cómo unirme al equipo de Cibercultura en Ciberseguridad?

Dé clic en el enlace de "Únete al equipo", en caso de estar interesado/a en realizar su servicio social y/o tesis en el equipo de "Cibercultura en Ciberseguridad: Ahora y siempre" deberá asegurarse de cumplir con los requisitos para enviar su solicitud, para llenarla deberá dar clic en el botón "Enviar solicitud" (figura x) para acceder al formulario web y acordar una entrevista con miembros del equipo.

Nota: Deberá subir su historial académico en pdf y para finalizar dé clic "Enviar solicitud".

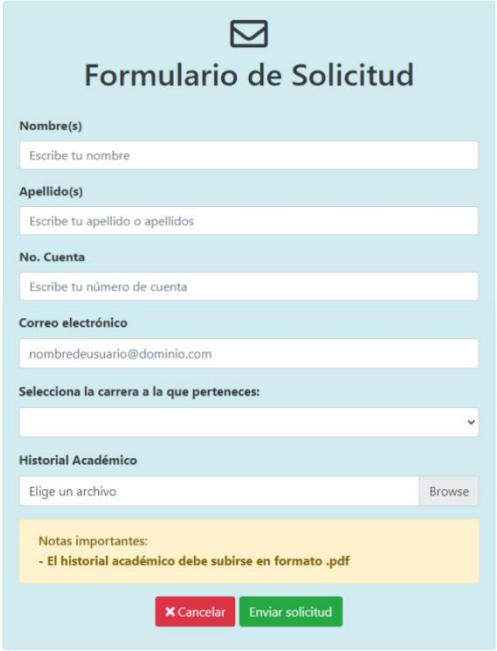


Figura 6. Formulario de postulación al equipo de Cibercultura en Ciberseguridad: Ahora y siempre.

Conoce el aviso de privacidad del sitio web

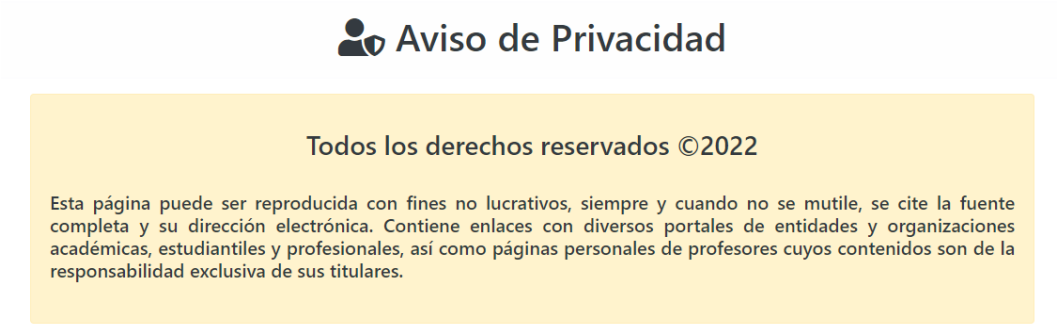


Figura 7. Aviso de privacidad.

Fuentes de información

[45] Agudo, S. (2017, 24 julio). IDEs y editores: ¿qué diferencias hay entre ellos a la hora de escribir código? Genbeta. Recuperado 30 de mayo de 2021, de https://www.genbeta.com/a-fondo/ides-y-editores-que-diferencias-hay-entre-ellos-a-la-hora-de-escribir-codigo

[55] Aguilar, J. (2018, 1 agosto). OWL Carousel. José Aguilar Blog. Recuperado 18 de mayo de 2022, de https://www.jose-aguilar.com/blog/owl-carousel/

[8] Aguirre Romero, J. M. (s. f.). Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. UCM. Recuperado 19 de marzo de 2021, de http://www.ucm.es/info/especulo/numero27/cibercom.html

[31] Albornoz, D. (2019, 6 febrero). Discursos de odio y violencia de género en Internet. Hiperderecho. Recuperado 20 de junio de 2021, de https://hiperderecho.org/2019/02/discursos-de-odio-y-violencia-de-genero-en-internet/#more-5975

[54] Anderson, R. (2022, 9 mayo). Introduction to Identity on ASP.NET Core. Microsoft Docs. Recuperado 19 de mayo de 2022, de https://docs.microsoft.com/en-us/aspnet/core/security/authentication/identity?view=aspnetcore-6.0&tabs=visual-studio

[38] Aquí hay dominios. (2021, 30 enero). Font Awesome ¿Qué es y cómo se usa? Recuperado 19 de enero de 2022, de https://www.aquihaydominios.com/blog/font-awesom-que-es-y-como-se-usa/

[19] Barrera Rubio, P. R. (2020, 3 enero). Realidad y prevención: robo de identidad en México. El Economista. Recuperado 20 de junio de 2021, de https://www.eleconomista.com.mx/opinion/Realidad-y-prevencion-robo-de-identidad-en-Mexico-20200102-0045.html

[62] Boyer, S. (2022, 3 junio). Host ASP.NET Core on Linux with Apache. Microsoft Docs. Recuperado 14 de junio de 2022, de https://docs.microsoft.com/en-us/aspnet/core/host-and-deploy/linux-apache?view=aspnetcore-6.0

[66] Boyer, S. (2022, 3 junio). Host ASP.NET Core on Linux with Apache. Microsoft Docs. Recuperado 14 de junio de 2022, de https://docs.microsoft.com/en-us/aspnet/core/host-and-deploy/linux-apache?view=aspnetcore-6.0

[58] C. (2014, 26 febrero). HERRAMIENTA: IIS Express GUI. campusMVP.es. Recuperado 22 de junio de 2022, de https://www.campusmvp.es/recursos/post/HERRAMIENTA-IIS-Express-GUI.aspx#top

[1] Castells, M. (2002, 10 abril). *Manuel Castells - La dimensión cultural de Internet*. UOC. Recuperado 9 de junio de 2021, de https://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.html

[26] Centro de Estudios Legislativos para la Igualdad de Género & Congreso de la CDMX. (2019, octubre). Violencia digital [Diapositivas]. genero.congresocdmx.gob.mx. https://genero.congresocdmx.gob.mx/wp-content/uploads/2020/07/Violencia-digital.pdf

[64] certbot. (s. f.). Certbot Instructions. Recuperado 16 de mayo de 2022, de https://certbot.eff.org/instructions?ws=apache&os=ubuntufocal

[32] COPRED/Yaaj. (2021, febrero). Informe: Impacto diferenciado ante la COVID-19 en la comunidad LGBT+ en México. https://copred.cdmx.gob.mx/storage/app/media/Encuesta-Impacto-diferenciado-de-la-covid19-en-la-comunidad-lgbttti-en-Mexico.pdf

[11] de la Riva, A. (2020, 28 agosto). Ciberinteligencia, un nuevo paradigma en la ciberseguridad. Criminal Fact. Recuperado 7 de junio de 2021, de https://www.criminalfact.com/ciberinteligencia-un-nuevo-paradigma-en-la-ciberseguridad/

[56] de Souza, I. (2021, 12 febrero). Aprende sobre los tipos de hosting más importantes de la actualidad y sus funciones. Rock Content - ES. Recuperado 22 de mayo de 2021, de https://rockcontent.com/es/blog/tipos-de-hosting/

[57] de Souza, I. (2021, 12 febrero). ¿Qué es un servidor web y para qué sirve en Internet? Rock Content - ES. Recuperado 22 de junio de 2022, de https://rockcontent.com/es/blog/que-es-un-servidor/

[46] Desarrollo web. (s. f.). Editores de código. Recuperado 31 de mayo de 2021, de https://desarrolloweb.com/colecciones/editores-codigo

[47] Desarrollo web. (s. f.). Editores de código. Recuperado 22 de mayo de 2021, de https://desarrolloweb.com/colecciones/editores-codigo

[60] Documentation Group. (s. f.). About the Apache HTTP Server Project - The Apache HTTP Server Project. Apache HTTP Server Project. Recuperado 22 de junio de 2022, de https://httpd.apache.org/ABOUT_APACHE.html

[51] Education-wiki. (s. f.). Angular vs Bootstrap: 4 increíbles diferencias que debes saber. es.education-wiki.com. Recuperado 8 de julio de 2022, de https://es.education-wiki.com/1095456-angular-vs-bootstrap

[39] Espínola, M. G. (2019, 19 junio). La importancia de un menú para el user experience. Paredro.Com. Recuperado 6 de abril de 2022, de https://www.paredro.com/importancia-de-un-menu-y-el-user-experience-sitio-web/

[20] Fernández, J. G. (2020, 24 octubre). Los ciberataques amenazan con colapsar los hospitales: «Sería terrorífico». Expansión.com. Recuperado 27 de junio de 2022, de https://www.expansion.com/economia-digital/companias/2020/10/24/5f915917e5fdea64298b45e1.html

[61] Galvis, A., & Galvis, A. (2020, 28 octubre). HISTORIA MARIADB. MARIA DB. Recuperado 26 de junio de 2022, de https://mariadbuts.wordpress.com/2020/10/27/example-post-3/#:%7E:text=MariaDB%20surge%20a%20ra%C3%ADz%20de,a%20los%20que%20llama%20MariaDB.

[52] gavilanch2. (2018, 3 enero). 1- Introducción a ASP.NET CORE 2 - Qué es MVC | Programando ASP.NET CORE 2 [Video]. YouTube. https://www.youtube.com/watch?v=4FrKuVvISVQ&t=967s

[22] González, C. (2020, 27 abril). Cómo está afectando la expansión del COVID-19 a la ciberdelincuencia. BBVA NOTICIAS. Recuperado 27 de junio de 2022, de https://www.bbva.com/es/como-esta-afectando-la-expansion-del-covid-19-a-la-ciberdelincuencia/

[15] Grupo garatu IT solutions. (2019, 21 junio). Ciberdelincuencia: El fraude en el sector de las telecomunicaciones (Telecom Fraud). Grupo garatu. Recuperado 11 de junio de 2021, de https://grupogaratu.com/fraude-sector-de-telecomunicaciones-telecom-fraud-ciberdelincuencia/

[29] Guardia Nacional CERT-MX. (2021, 23 abril). Tipos de víctimas digitales, tips y recomendaciones. Gobierno de México. Recuperado 20 de junio de 2021, de https://www.gob.mx/gncertmx/articulos/tips-y-recomendaciones-264060

[18] Guardia Nacional CERT-MX. (2021, 23 abril). Vishing. Gobierno de México. Recuperado 20 de junio de 2021, de https://www.gob.mx/gncertmx/articulos/105213

[50] Guerrero, N. (2020, 28 septiembre). ¿Qué es ASP.NET Core? y ¿Cómo funciona?). Programa en Línea. Recuperado 24 de mayo de 2021, de https://www.programaenlinea.net/asp-net-core/

[65] Heidi, E. (2020, 21 mayo). Cómo proteger Apache con Let 's Encrypt en Ubuntu 20.04. DigitalOcean Community. Recuperado 5 de agosto de 2022, de https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-20-04-es

[61] HostingPlus México. (2020, 14 diciembre). Qué es MariaDB y cuáles son sus características | Blog | Hosting Plus México. Hosting Plus. Recuperado 26 de julio de 2022, de https://www.hostingplus.mx/blog/que-es-mariadb-y-cuales-son-sus-caracteristicas/

[27] INEGI. (2021, julio). Comunicado. Módulo sobre Ciberacoso (MOCIBA) (N.º371/21). https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf

[13] INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2021, 19 mayo). Glosario de términos de ciberseguridad: una guía de aproximación para. INCIBE. Recuperado 11 de junio de 2021, de https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[21] INTERPOL. (s. f.). Ciberamenazas relacionadas con la COVID-19. Recuperado 27 de junio de 2022, de https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19

[16] Islas Maldonado, G. (2020, 10 junio). El robo de identidad digital en México. Forbes México. Recuperado 20 de junio de 2021, de https://www.forbes.com.mx/el-robo-de-identidad-digital-en-mexico/

[61] Jankov, T. (2019, 3 octubre). MariaDB vs MySQL, un Resumen sobre las Tecnologías de Base de Datos. Kinsta. Recuperado 26 de julio de 2022, de https://kinsta.com/es/blog/mariadb-vs-mysql/

[63] Let 's Encrypt. (s. f.). Let 's Encrypt - Certificados SSL/TLS Gratuitos. Recuperado 16 de mayo de 2022, de https://letsencrypt.org/es/

[36] Llasera, J. P. (2021, 1 noviembre). Tipografías: Qué son, los diferentes tipos y sus variables tipográficas. Imborrable. Recuperado 29 de septiembre de 2021, de https://imborrable.com/blog/tipografias-que-son/

[12] Marker, G. (2021, 1 junio). Vulnerabilidades informáticas. Tecnología + Informática. Recuperado 21 de junio de 2021, de https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

[37] Mata, P. G. (2021, 27 abril). unDraw.co, ilustraciones gratuitas y de calidad – Marketonomy. Marketonomy - Herramientas de Marketing Online y noticias del sector. Recuperado 2 de octubre de 2021, de https://www.marketonomy.es/undraw-co/

[44] mdn. (2021, 11 febrero). ¿Qué es JavaScript? - Aprende sobre desarrollo web | MDN. Mdn Web Docs. Recuperado 18 de mayo de 2022, de https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

[43] Microsoft. (2022c, marzo 18). A tour of C# - Overview. Microsoft Docs. Recuperado 18 de mayo de 2022, de https://docs.microsoft.com/en-us/dotnet/csharp/tour-of-csharp/

[48] Microsoft. (2021b, noviembre 29). Herramientas web modernas |. Visual Studio. Recuperado 22 de mayo de 2021, de https://visualstudio.microsoft.com/es/vs/features/web/

[49] Microsoft. (2021b, noviembre 3). Visual Studio Code - Code Editing. Redefined. Visual Studio Code. Recuperado 15 de abril de 2022, de https://code.visualstudio.com/

[48] Microsoft. (2021, 12 enero). Visual Studio 2022 Community Edition: descargar la versión gratuita más reciente. Visual Studio. Recuperado 22 de mayo de 2021, de https://visualstudio.microsoft.com/es/vs/community/

[53] Microsoft. (2022b, febrero 2). What is NuGet and what does it do? Microsoft Docs. Recuperado 12 de mayo de 2022, de https://docs.microsoft.com/en-us/nuget/what-is-nuget

[3] Millán, J. A. (1998). *Ciber*. jamillan. Recuperado 7 de junio de 2021, de http://jamillan.com/v_ciber.htm

[35] mimoilus. (s. f.). Psicología del color [Infografía y diseños de logotipo superiores]. Pinterest. https://www.pinterest.com.mx/pin/838795499322088508/

[7] Molina Mateos, J. M. (2013). Conceptos y definiciones | Ciberseguridad y Derecho. molinamateos. Recuperado 7 de junio de 2021, de http://molinamateos.com/content/conceptos-y-definiciones-0

[42] Nimap Infotech. (2019, 9 mayo). PHP vs HTML5 | Server Side Programming and Front End Programming. Recuperado 24 de marzo de 2021, de https://nimapinfotech.com/blog/php-vs-html5/

[33] Observatorio de Violencia de Género en Medios de Comunicación (OVIGEM). (2022, 30 mayo). VIOLENCIA DIGITAL. OVIGEM. Recuperado 14 de junio de 2021, de https://ovigem.org/violencia-digital/

[34] Osan, G. (2022, 29 enero). Principales diferencias entre diseño y desarrollo web. latevaweb. Recuperado 13 de junio de 2022, de https://www.latevaweb.com/diferencia-entre-diseno-web-y-desarrollo-web

[41] OWASP Top 10 team. (s. f.). Inicio - OWASP Top 10:2021. OWASP Top 10 de 2021. Recuperado 15 de abril de 2022, de https://owasp.org/Top10/es/

[5] Oxford University Press (OUP). (s. f.-a). Ciberacosador. Lexico.com. Recuperado 8 de junio de 2021, de https://www.lexico.com/es/definicion/ciberacosador

[5] Oxford University Press (OUP). (s. f.). ciberacoso. Lexico.com. Recuperado 7 de junio de 2021, de https://www.lexico.com/es/definicion/ciberacoso

[6] Oxford University Press (OUP). (s. f.-c). Ciberactivista. Lexico.com. Recuperado 7 de junio de 2021, de https://www.lexico.com/es/definicion/ciberactivista

[4] Oxford University Press (OUP). (s. f.-d). Cibernética. Lexico.com. Recuperado 7 de junio de 2021, de https://www.lexico.com/es/definicion/cibernetica

[25] Pascual, M. G. (2022, 23 mayo). Lazarus, los cibercriminales que roban y extorsionan para el Amado Líder de Corea del Norte. El País. Recuperado 28 de junio de 2022, de https://elpais.com/tecnologia/2022-05-23/lazarus-los-cibercriminales-que-roban-y-extorsionan-para-el-amado-lider-de-corea-del-norte.html

[23] Rebollo, C. (2021, 16 septiembre). Los ciberdelincuentes se reinventan durante la pandemia a través de los códigos QR. El País. Recuperado 27 de junio de 2022, de https://elpais.com/tecnologia/2021-09-16/los-ciberdelincuentes-se-reinventan-durante-la-pandemia-a-traves-de-los-codigos-qr.html

[30] Redondo, M. (2021, 10 marzo). Discriminación en un clic: la homofobia a través de las redes sociales en México. Hipertextual. Recuperado 20 de junio de 2021, de https://hipertextual.com/2018/05/discriminacion-clic-homofobia-traves-redes-sociales-mexico

[67] Rejón, J. (2015, 22 octubre). Linux – El sistema de inicio Systemd – mundotelematico.com. mundotelematico.com. Recuperado 14 de junio de 2022, de https://www.mundotelematico.com/linux-el-sistema-de-inicio-systemd/

[9] Rodríguez, J. A. (s. f.). El Relato Digital. Universidad Javeriana. Recuperado 19 de marzo de 2021, de https://www.javeriana.edu.co/relato_digital/r_digital/cibercultura/cibercultura.html

[2] Rodríguez Munguía, G., Velasco Mejía, A. U., Vicario Solórzano, C. M., & Instituto Politécnico Nacional. (2020, 1 enero). *La Brecha Cibercultural en México*. upiita.ipn. Recuperado 9 de junio de 2021, de https://www.boletin.upiita.ipn.mx/index.php/ciencia/850-cyt-numero-76/1783-la-brecha-cibercultural-en-mexico

[24] RTVE.es. (2021, 9 febrero). La pandemia, la oportunidad perfecta para la ciberdelincuencia. Recuperado 27 de junio de 2022, de https://www.rtve.es/noticias/20210209/pandemia-oportunidad-perfecta-ciberdelincuencia/2074480.shtml

[28] San Martín, N. (2021, 1 mayo). Violencia política afecta más a las mujeres: van 21 asesinadas en este proceso electoral [Comunicado de prensa]. https://www.proceso.com.mx/nacional/2021/6/1/violencia-politica-afecta-mas-las-mujeres-van-21-asesinadas-en-este-proceso-electoral-265040.html

[40] SECURE CODE WARRIOR. (2021). Secure Code Warrior. The OWASP Top 10 . . .and Beyond. Recuperado 15 de abril de 2022, de https://discover.securecodewarrior.com/OWASP-and-beyond.html?utm_source=google&utm_source=cpc&utm_campaign=owasp21&utm_content=keyword&utm_source=google&utm_medium=cpc&utm_term=owasp%2010&utm_campaign=&ad_group=129128046936&ad_ID=554952124798&match_type=p&keyword=owasp%2010&gclid=Cj0KCQjwr-SSBhC9ARIsANhzu15mlJVxFV0t3IuUZoCuEl--Gcq-T3OYmDSN7WydqGKYQY7_skbjP9UaAm_yEALw_wcB

[10] Sierra Gutiérrez, L. I. (2009, junio). La cultura en la era del ciberespacio: Cibercultura. La cultura de la sociedad digital. SciELO. Recuperado 24 de marzo de 2021, de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000100029

[14] sistemius. (2020, 24 noviembre). Ciberdelincuencia: Los 4 delitos informáticos más comunes. Recuperado 11 de junio de 2021, de https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/#:%7E:text=Se%20podr%C3%ADa%20decir%20que%20la,como%20el%20uso%20fraudulento%20de

[59] swhosting. (2020, 30 noviembre). Tutorial: crea una web ASP.NET Core MVC en Linux con Apache. Blog de SW Hosting. Recuperado 22 de junio de 2022, de https://www.swhosting.com/blog/tutorial-crea-una-web-asp-net-core-mvc-en-linux-con-apache/

[17] Trafaniuc, V. (2021, 1 abril). Los 4 principales tipos de fraude cibernético: Ejemplos y formas de prevención. Maplink. Recuperado 20 de junio de 2021, de https://maplink.global/blog/es/tipos-de-fraudes-ciberneticos/