UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“Implementación de buenas prácticas de seguridad en el desarrollo de aplicaciones móviles y web”

TESIS

QUE PARA OBTENER EL TÍTULO DE:

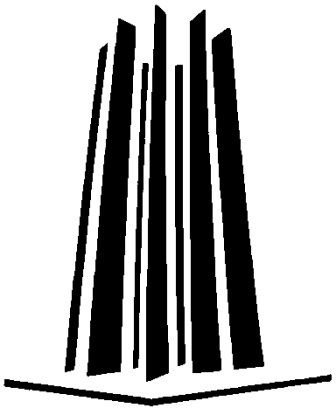
INGENIERO EN COMPUTACIÓN

PRESENTA:

MONROY RUBIO CRISTIAN ALEXIS

ASESOR DE TESIS:

M. en C. JESÚS HERNÁNDEZ CABRERA



Ciudad Nezahualcóyotl, Estado de México,, 2018

Agradecimientos

Índice

Introducción

La tecnología y el uso de dispositivos móviles ha ido creciendo de forma muy rápida durante los últimos años, proporcionando a la sociedad en general una gran cantidad de aplicaciones y sitios web orientados a facilitar las tareas cotidianas que antes podían resultar muy tediosas de realizar, esto ha provocado que la información de las personas sea un activo muy importante para las empresas, las cuales en ocasiones no emplean las medidas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Por esa razón, este trabajo busca proveer una guía en la cual se proporcionen las bases, herramientas, metodologías y buenas prácticas de seguridad enfocadas al desarrollo de sitios web y aplicaciones móviles, ya que son los objetivos más afectados por los atacantes.

Este trabajo se compone de 6 capítulos, a través de los cuales se describen los siguientes temas:

- Capítulo 1: Conceptos básicos necesarios en materia de seguridad de la información, los cuales permitirán la comprensión de los capítulos posteriores de manera más clara.

- Capítulo 2: Se describen los elementos que componen lo sitios web y aplicaciones móviles de manera general, adicionalmente, se detallan los distintos tipos de ataques y vulnerabilidades que afectan exclusivamente a los sitios web y aplicaciones móviles.

- Capítulo 3: Se explica de forma detallada la familia de las normas ISO 27000, con las cuales se puede implementar y auditar un Sistema de Gestión de Seguridad de la Información.

- Capítulo 4: Describe algunas metodologías de desarrollo seguro, las cuales pueden ser adoptadas por una empresa, para tener medidas de protección desde los primeros pasos del desarrollo de sistemas.

- Capítulo 5: Se describen buenas prácticas de desarrollo seguro, con la finalidad de que sirvan como guía y complemento a los temas descritos en el Capítulo 4.

- Capítulo 6: Se describe de manera general el uso de herramientas orientadas a la auditoría de sitios web y aplicaciones móviles, este capítulo en especial está orientado al uso de estas para descubrir vulnerabilidades por parte de la organización y evitar que sean explotadas por atacantes externos.

Objetivos Generales

- Definir una guía que ayude al desarrollo de sitios web y aplicaciones móviles de una manera segura, proporcionando metodologías y buenas prácticas que permitan la creación segura de sitios web y aplicaciones móviles, apegándose a los estándares de seguridad de la información.

- Concientizar a los desarrolladores de sistemas sobre la importancia de crear software de forma segura desde las primeras etapas de desarrollo, para de esa manera mitigar los posibles vectores de ataque y prevenir posibles vulnerabilidades.

Objetivos Particulares

- Mostrar la importancia de la seguridad informática en la actualidad.

- Describir el funcionamiento del malware y el vector de ataque utilizado por los atacantes informáticos.

- Mostrar el correcto uso de herramientas que permitan el aseguramiento de la información dentro de los sitios web y aplicaciones móviles.

- Establecer una correcta implementación de las distintas metodologías para el desarrollo seguro.

- Definir que es importante proteger dentro de un sistema en base a sus necesidades.

- Desarrollar una correcta implementación de las políticas de seguridad, basado en estándares de seguridad de la información.

Capítulo 1

Antecedentes de la Seguridad de la Información

Este capítulo está enfocado en proporcionar una definición completa sobre lo que es seguridad de la información, que busca proteger, de quién, cómo surgió y porqué es tan importante hoy en día.

Además, se describirá lo que es un malware, el surgimiento de este y su evolución, provocando que la seguridad de la información no sea un elemento opcional dentro de los procesos organizaciones, las cuales deben asegurar la confidencialidad, disponibilidad e integridad de la información de sus clientes.

1.1.- ¿Qué es seguridad de la información?

Para poder definir de forma correcta que es la seguridad de la información, primero se debe de entender el concepto de: información, la cual se puede entender como los datos procesados, que tienen un significado importante para alguien, ejemplos de esta definición pueden ser:

- Bases de Datos.
- Documentos.
- Imágenes.

La seguridad se encarga de proteger la información de aquellos que están involucrados con ella dentro o fuera de la organización, ya sean empleados, clientes e incluso proveedores de servicios, a su vez, también se resguardan recursos informáticos como lo son servidores, impresoras, cámaras de seguridad, etcétera., para lograrlo y así, disminuir los riesgos que podrían afectar a los activos.

La seguridad de la información está basada en 3 pilares principales:

- Confidencialidad.
- Integridad.
- Disponibilidad.

También conocidos como CIA (Confidentiality, Integrity, Availability). A continuación, se explican de forma breve.

Confidencialidad.

Está relacionada a que solo el personal autorizado tenga acceso a la información que le corresponda, es decir, busca proteger la información de divulgación y accesos no autorizados.

Algunas técnicas y buenas prácticas utilizadas para garantizar la confidencialidad de la información son:

- *Segregación de tareas* (funciones): Permite clasificar a los usuarios dentro de grupos de acuerdo con los roles que tengan dentro de la organización, generando que solamente puedan acceder a la información necesaria para realizar sus actividades.

- *Cifrado*: Existen una gran cantidad de algoritmos de cifrado, los más utilizados hacen uso de una llave pública y una privada.
  Ambas llaves, son un conjunto de caracteres, los cuales varían de acuerdo al tipo de algoritmo utilizado, para cifrar la información se hace con el uso de la llave privada, posteriormente, se envía el archivo cifrado junto con la llave pública al destinatario, para descifrar la información se hace uso de la llave pública.
  Con esta técnica se asegura que solamente las personas autorizadas recibirán la llave pública que permita descifrar la información y es conocida como cifrado asimétrico y es el más utilizado hoy en día debido a que el cifrado simétrico es considerado como no seguro.

- *Contraseñas*: Método utilizado para el acceso a cualquier aplicativo o equipo, su efectividad radica en su longitud y combinación tanto de números, mayúsculas, minúsculas, caracteres especiales, cambio constante de la misma y la complejidad.

Integridad.

Proporciona la certeza de que la información no ha sido modificada por ningún agente externo durante su transmisión o almacenamiento, ya sea humano o técnico.

Una de las principales técnicas utilizadas para verificar la consistencia de la información, es mediante la suma de verificación, también conocida como algoritmos checksum o hash; los cuales consisten en generar una cadena única del documento, la cual cambiará en caso de que el documento haya sufrido alguna modificación. Si un solo bit cambia, la cadena resultante cambiará completamente.

Disponibilidad.

Permite asegurar que la información se encontrará accesible en todo momento que se solicite.

Existen ciertas medidas que permiten garantizar la disponibilidad, como lo son los respaldos de información y la replicación de la información.

Imagen recuperada de: Infosegur (2013). Objetivos de la seguridad informática. https://infosegur.wordpress.com/tag/disponibilidad/

Otro aspecto importante que tomar en cuenta dentro de la seguridad de la información es el No Repudio, que consiste en asegurar que un usuario no pueda negar que órealizó alguna acción sobre algún equipo, para lograr esto, se debe cumplir con:

- Autenticación.
- Autorización.
- Auditoría.

La *autenticación* es el proceso que permite comprobar que un usuario es quien dice ser, algunos métodos de autenticación son:

- Inicio de sesión, compuesto por un usuario y una contraseña.
- Biométricos.
- Tarjetas inteligentes.

Además, existen los métodos de doble o múltiple autenticación, los cuales proporcionan más seguridad.

La *autorización* está ligada al concepto de gestión de privilegios de acceso y segregación de funciones, es decir, los permisos que tiene un usuario en el sistema y con la información contenida dentro del mismo.

La auditoría, permite llevar un control de las acciones realizadas por los usuarios, es decir, qué, cómo, cuándo y quién realiza acciones en el sistema.

Las bitácoras de sistema y aplicación resultan una herramienta muy útil para el cumplimiento de este punto, debido a que realizan un registro de todas las operaciones de los usuarios en un sistema.

1.2.- ¿Cuándo surgió la seguridad de la información?

La seguridad de la información surgió en el año de 1972, esto a raíz del primer malware informático de la historia llamado Creeper, cuya finalidad era causar afectaciones en una máquina IBM serie 360, la acción realizada por este malware era mostrar un mensaje en pantalla que decía lo siguiente: **“I´m creeper…catch me if you can”**, ante este problema fue creado el primer antivirus, dando con esto el inicio de la seguridad de la información.

Con el paso del tiempo y con el uso cada vez más constante de las computadoras, en la década de los 80´s y principios de los 90´s los especialistas en seguridad de la información centraron su atención en la protección de los equipos de usuario final, esto quiere decir solamente a los ordenadores y al sistema operativo asociado.

Con la llegada del Internet y su principal beneficio, la comunicación entre ordenadores desde cualquier parte del mundo, los atacantes informáticos encontraron una mayor cantidad de vectores de ataque, por lo cual se empezó a buscar la protección de los servidores de los aplicativos y servidores que eran accesibles de manera pública a través de Internet, como medida se optó por el uso de Firewall.

Hoy en día la seguridad de la información enfrenta un gran problema debido al auge en el uso de dispositivos móviles, redes sociales y el uso cada vez más acelerado de las aplicaciones móviles, junto con las nuevas tecnologías de conectividad como WIFI y 4G, ha provocado que no solamente las empresas sean vulnerables ante los atacantes informáticos, sino también la sociedad en general

En un futuro cercano, la seguridad de la información se encontrará ante desafíos más complejos, debido a la llegada de nuevas tecnologías como el Internet de la Cosas (IoT), provocando que cualquier dispositivo inteligente sea vulnerable.

1.3.- Términos comunes usados en seguridad de la información

Una vez definido el concepto de seguridad de la información y el surgimiento y futuro de la misma, es importante conocer los términos utilizados comúnmente dentro de esta área para un correcto entendimiento de las distintas metodologías.

1.3.1.- Activo

Los activos son cualquier elemento que sea relevante para los procesos de la organización, estos a su vez se pueden clasificar en 3:

- Información.
- Infraestructura.
- Usuarios.

La información, como se definió previamente, son los datos que tienen un significado o valía para cualquier persona, se puede considerar como el activo de mayor valor para una organización.

La infraestructura contempla todo lo relacionado a TI, es decir, equipos de cómputo, servidores, conectividad a la red, etcétera., se puede entender como los contenedores que van a almacenar la información.

Finalmente, los usuarios, son todos los individuos que tienen alguna relación con la organización, ya sea empleados, clientes o proveedores y los cuales podrían tener o no algún conocimiento de la información.

1.3.2.- Vulnerabilidad

Una vulnerabilidad es cualquier debilidad de un activo, todos los activos tienen vulnerabilidades en mayor o menor grado, las cuales pueden estar relacionadas a defectos de fábrica para la infraestructura, problemas de salud para los activos relacionados con los usuarios y para la información, no contar con los controles necesarios que garanticen la seguridad de esta en cualquiera de los tres ámbitos de la CIA.

A su vez, las vulnerabilidades se clasifican en:

- Software.
- Hardware.
- Configuración.
- Usuario.

Vulnerabilidad en Software, sucede cuando se existen errores en la lógica de la programación de un sistema, los cuales pueden estar relacionados al uso de funciones no seguras, una falta de correcta validación de los parámetros recibidos por parte de los usuarios, o un incorrecto manejo de errores, provocando que los atacantes puedan inyectar código que se ejecute haciendo uso de los recursos del programa.

Vulnerabilidad en Hardware, puede ocurrir por diversos medios, uno de ellos son los defectos de fábrica, el otro medio que podría provocar un mayor impacto, sucede cuando los equipos (computadoras, servidores, etcétera.) no cuentan con las suficientes medidas de mantenimiento y protección tanto para afectaciones internas y externas.

Vulnerabilidad de Configuración, está ligada a la instalación de software y hardware por defecto, debido a que en ocasiones las herramientas adicionales son vulnerables, por esa razón, es recomendable realizar un análisis de cada uno de los plugins, con la finalidad de instalar solamente lo estrictamente necesario.

Vulnerabilidad de Usuario, involucra de forma directa a todas las personas relacionadas a la organización y es una de las vulnerabilidades más difíciles de solucionar, debido a que es susceptible entre otros a ataques de ingeniería social y phishing, una solución es mantener en constante capacitación y concientización a todo el personal de la organización.

1.3.3.- Amenaza

Es una violación de seguridad potencial, la cual se puede explotar a través de una vulnerabilidad cuando se presentan ciertas circunstancias y puede provocar daño a los sistemas de información produciendo pérdidas materiales, financieras o de credibilidad para la organización. Existen 3 tipos de amenazas:

- Amenazas Humanas.
- Amenazas Físicas.
- Amenazas Lógicas.

Amenazas humanas, está compuesta por los atacantes informáticos y el personal de la organización que tiene algún conocimiento de la información, las vulnerabilidades en esta clasificación están basadas en el desconocimiento o descuido de los usuarios.

Amenazas físicas, suceden sobre la infraestructura de la organización, puede ocurrir debido a defectos de fábrica, fallas en la red, cambios de voltaje, afectaciones físicas como inundaciones o incendios e inclusive por daños perpetrados por el hombre.

Amenazas lógicas, son aquellas que tienen alguna relación con el funcionamiento mismo del sistema, puede ser provocado por alguno de los siguientes elementos:

- Instalación de software malicioso.
- Incorrecta implementación de algún sistema, provocando pérdida de información.
- Uso de canales de comunicación inseguros, generando que la información viaje sin ningún tipo de cifrado durante el envío de esta entre los usuarios.
- Desarrollo inseguro de aplicaciones.

1.3.4.- Riesgo

Es la combinación de la probabilidad de que algún evento suceda y las consecuencias que podría causar a los activos de la organización.

1.3.5.- Impacto

Es la afectación asociada a un riesgo específico, sobre la disponibilidad, confidencialidad e integridad de un activo, estas afectaciones pueden ser monetarias, materiales o de credibilidad hacía la organización.

1.3.6.- Evento

Es cualquier cambio en el comportamiento normal de un sistema, este cambio puede ser planeado (migración del sistema), o accidental (afectación a la disponibilidad de la información), lo cual provocaría que se clasifique como un incidente de seguridad.

1.3.7.- Incidente

Sucede cuando un evento genera un impacto negativo en el sistema de información, es decir, cuando se afecta la confidencialidad, integridad o disponibilidad de la información contenida en el sistema.

1.4.- Tipos de Seguridad de la información

El conocer los distintos tipos de seguridad permite tomar las medidas preventivas, correctivas y reactivas necesarias para la protección de la información en cada una de las clasificaciones y lograr mitigar el riesgo de que una posible vulnerabilidad sea explotada por los atacantes informáticos.

1.4.1.- Seguridad Física.

Involucra todos los accesos físicos a la organización y la protección de los activos contenidos dentro de la misma, para esta categoría es importante tomar medidas que permitan llevar un registro sobre que personas entran y salen de la organización y en qué momento, existen diversos controles, como bitácoras de acceso, cámaras de seguridad, biométricos de entrada, detectores de humo, etcéteraétera.

Este tipo de seguridad se ve amenazada principalmente por los accesos no autorizados, los cuales pueden desencadenar la destrucción, pérdida o robo de la información, desastres naturales y afectaciones en la infraestructura como fallas en la red o sobrecargas eléctricas.

1.4.2.- Seguridad Lógica

La seguridad lógica complementa a la física, se encarga de la protección de los sistemas computacionales y software contenido en los ordenadores o dispositivos utilizados por la organización.

Algunos de los ámbitos que busca proteger esta categoría:

- Ataques externos a través de la red, mediante el uso de Firewall, software antivirus, Honeypot, IDS, IPS, etcétera.
- Intercambio de información, con el uso de protocolos de información seguros y el cifrado de la información.
- Acceso a red interna, a través de VPN, privilegios de acceso a los sistemas.

1.4.3.- Seguridad Humana

Se encarga proteger la integridad de las personas dentro de la organización, tanto de accidentes laborales como externos.

1.5.- Importancia de la seguridad de la información en los sitios web y aplicaciones móviles hoy en día.

Como se ha visto durante el desarrollo de este primer capítulo, la seguridad de la información no solamente se encarga de proteger la información, si no, también el entorno en el cual se desenvuelve.

La seguridad de la información en sitios web y aplicaciones móviles debe ser adoptada en las organizaciones, debido a que las consecuencias de no contar con una correcta implementación de los estándares de seguridad o no desarrollar de forma segura los sistemas que son utilizados por los usuarios pueden provocar desde la divulgación o pérdida de información, hasta el desprestigio de la organización.

Por ello, es importante generar una cultura de seguridad de la información entre los desarrolladores de sistemas, para que generen software funcional y seguro.

Capítulo 2

Tipos de Ataques Informáticos y Malware en sitios web y aplicaciones móviles

En este capítulo se describirá cómo es que se componen los sitios web y aplicaciones móviles, su funcionamiento y evolución a lo largo del tiempo hasta convertirse en herramientas indispensables para la sociedad hoy en día.

Además, se hablará de los atacantes informáticos, su clasificación y que buscan obtener.

Finalmente se definirán los principales ataques informáticos y malware que afectan de manera particular a los sitios web y aplicaciones móviles.

2.1.- Sitios Web.

En esta sección se define que es un sitio web y su evolución desde la creación del primer sitio hasta nuestros días, además de la descripción de manera general de cómo está compuesto un sitio web y la clasificación de este.

2.1.1.- ¿Qué es un sitio web?

Cuando navegamos por Internet consultamos una gran cantidad de sitios web, pero sabemos ¿Qué son en realidad los sitios web?

Un sitio web es un conjunto de archivos electrónicos referentes a un tema en particular, los sitios web están compuestos por páginas web y contienen un dominio asociado que permite el acceso a ellos a través de la red.

Los sitios web son utilizados por cualquier organización ya sea pública o privada, pequeñas o medianas empresas e incluso individuos, permiten la difusión de información, prestación de servicios o comunicación con otras personas alrededor del mundo[1].

2.1.2.- Evolución de los sitios web.

Los sitios web no eran como son hoy en día, como toda la tecnología, debió de adaptarse a las nuevas funcionalidades, navegadores, protocolos e innovaciones, nos sorprendería mucho el pensar que en un inicio los sitios web eran simplemente texto.

Para poder lograr esta evolución, Tim Berners Lee realizó en el año de 1989 una propuesta en la que se describía un sistema de gestión de información, lo que en años posteriores se volvería lo que hoy se conoce como World Wide Web, posteriormente Bernes Lee en el año de 1990 puso en marcha el sistema de hipertexto llamado Enquire, en el cual se podían almacenar piezas de información y conectarlas, además este sistema era multiusuario, es decir, permitía que la información fuera consultada por distintas personas al mismo tiempo.

[1] Milenium, 2017. *Sitios Web.* Recuperado de: https://www.informaticamilenium.com.mx/es/temas/que-son-los-sitios-web.html

Finalmente los sitios web han ido evolucionando de la mano de la World Wide Web, la cual en su versión 1.0 se caracteriza principalmente por ser unidireccional y de contenidos estáticos, es decir, casi no se modificaba el contenido de las mismas y no se realizaban actualizaciones de manera periódica, la información que se publicaba durante esta versión era principalmente cultural, debido a la dificultad que representaba el actualizar este tipo de sitios web, las empresas no pudieron hacer un mejor uso de los mismos.

Posteriormente la Web 2.0 también llamada “La Red Social”, generó el auge de los blogs, wikis, foros y por supuesto las redes sociales, esto gracias a las mejores herramientas de desarrollo web y mejores servidores, esto hizo que la web se volviera colaborativa.

La última versión de la Web, la 3.0, es la web de la nube, las aplicaciones y multi dispositivos, esto debido a que la tecnología permite la conexión a los sitios web desde ordenadores, tabletas, teléfonos inteligentes, además con el uso de la nube, se elimina la necesidad de disponer de sistemas operativos complejos y grandes discos duros para almacenar la información de los usuarios.

2.1.3.- Clasificación de los sitios web.

Una vez explicado el crecimiento de los sitios web, es importante conocer su clasificación, ya que, a partir de ello, se podrá saber de qué tipo de información hacen uso y cuál es su finalidad.

Debido a que el mundo de los sitios web es muy extenso, se usarán como base tres parámetros para su clasificación, los cuales se listan a continuación:

- Visibilidad de contenidos.
- Actualización de contenidos.
- Actividad o fin principal.

Por su visibilidad de contenidos, los sitios web se clasifican de la siguiente manera:

- Intranets.
- Extranets.
- Sitios web públicos.

La *intranet* es una red de computadoras para uso exclusivo de una organización, permite compartir todo tipo de información, esto sucede debido a que usa una tecnología muy similar a la utilizada por el Internet y se basa en los mismos estándares, la diferencia radica en que este tipo de red es privada, estableciendo una comunicación interna entre los individuos de una organización.

Aunque una intranet es una red privada, esta se puede extender hacia internet, esto se logra mediante el uso de VPN (Virtual Private Network).

La *extranet*, es una extensión de la intranet, la diferencia se denota en que solamente se tiene acceso a las computadoras autorizadas, las cuales solamente pueden ser utilizadas por los empleados de la organización, aunque adicionalmente pueden ser utilizadas por personal externo que tenga alguna relación con la misma.

Al igual que la intranet, la extranet permite compartir todo tipo de información, para tener acceso a ella hace uso de un sistema de codificación y contraseñas para dar acceso a los servidores que la contienen.

Los *sitios web públicos*, como su nombre lo dice, pueden ser consultados por cualquier persona desde la red, por lo regular este tipo de sitios no realizan ningún tipo de autenticación y pueden ser encontrados mediante búsquedas de los navegadores web.

Con respecto a la actualización de contenidos, podemos encontrar:

- Sitios web estáticos.
- Sitios web dinámicos.
- Sitios web que combinan ambos tipos.

Sitios web estáticos, están enfocados principalmente a mostrar una información permanente, el usuario no puede interactuar con el sitio web, está compuesto por hipervínculos o enlaces, este tipo de sitios no soportan el uso de bases de datos, correos, se pueden desarrollar de manera muy sencilla, pero para realizar su actualización es muy complicado.

Sitios web dinámicos, la forma en que se encuentran desarrollados permite una mayor interacción con el usuario, adicionalmente pueden hacer uso de una base de datos en la cual se almacena la información que va a ser consultada por el usuario, esperan a que se realice una solicitud y en base a ella, despliegan la información, a diferencia de los anteriores, las actualizaciones son más sencillas de realizar.

Finalmente, la clasificación de los sitios web de acuerdo con la actividad que realizan es la siguiente:

- Comercial o publicitaria.
- Venta.
- Sociales.
- Informativos.
- Buscadores.

Comerciales o publicitarios, tienen como fin dar a conocer a una empresa y los servicios o productos que proporcionan, este tipo de sitios es muy común en las organizaciones, ya que permite brindar atención a sus clientes sin necesidad de que estos últimos se trasladen hasta la empresa.

Venta, también llamados e-commerce, como su nombre lo dice permite realizar la venta de productos de un individuo u organización, a través de internet, este tipo de sitios comúnmente también son dinámicos.

Sociales, son muy conocidos hoy en día, permiten la comunicación entre los usuarios, la información que se genera es completamente hecha por los usuarios, dentro de este rubro podemos encontrar a los foros y las redes sociales.

Informativos, su fin es la difusión o distribución de información pública o privada, a diferencia de los anteriores, son utilizados por especialistas como periodistas, reporteros, etcétera., además la información contenida en estos sitios se actualiza constantemente, dentro de esta clasificación podemos mencionar los periódicos y revistas electrónicas, información del tiempo, de la bolsa de valores, etcétera.

Buscadores, permiten obtener el acceso a los sitios mencionados anteriormente, ya que a partir de una palabra clave o una oración los buscadores le ayudan al usuario a encontrar la información que necesita, entre los más conocidos podemos mencionar Google, Yahoo, Bing, etcéteraétera.

2.1.4.- Elementos de un sitio web.

Para poder desarrollar un sitio web que permita a los usuarios encontrar la información que buscan de manera intuitiva y rápida, es importante conocer los componentes que los conforman, aunque pueden variar de un sitio a otro, los más comunes y relevantes son los siguientes:

- Formulario.
- Logotipo.
- Texto, imágenes, vídeos.
- Nombre de dominio.
- Hipervínculos.
- Botones o pestañas.
- Navegador.
- Footer.

Formularios, son utilizados para que el usuario introduzca datos, comúnmente sirven para el registro y son generados a través de plantillas predeterminadas cuya información es almacenada en una base de datos.

Logotipo, se coloca comúnmente en la parte superior izquierda del sitio y por lo regular es una imagen representativa de la organización, además permite al usuario el regresar a la página principal al momento de seleccionar la imagen.

Texto, las imágenes y vídeos son la información que quiere dar a conocer la organización hacia los usuarios, esta se puede presentar de distintas maneras dependiendo del formato.

Nombre de dominio, también conocido como URL, permite el acceso al sitio desde el buscador, regularmente son nombres descriptivos.

Hipervínculos, ayudan al usuario a acceder a información que se encuentra en otros sitios web, es decir, relaciona distintos sitios web utilizando enlaces.

Botones o pestañas, permiten al usuario acceder a distintas páginas dentro del mismo sitio web, así como también permiten validar los formularios una vez que se ha introducido toda la información.

Navegador, el más común es una barra horizontal, en la cual el usuario puede introducir palabras claves, con las cuales el navegador buscará la información que contenga dichas palabras facilitando con ello la búsqueda de información.

Footer, se encuentra al final del sitio web y contiene la información de Copyright y las redes sociales o información de contacto de la organización.

2.1.5.- Funcionamiento de los sitios web.

Además de conocer los elementos que componen a un sitio web, es necesario conocer su funcionamiento, cómo es que, a partir de una solicitud por parte del usuario, el sitio web realiza la respuesta que contenga la información solicitada en un tiempo de respuesta rápido y de forma eficiente.

Para entender el funcionamiento, es importante conocer el modelo cliente servidor, el cual es el más utilizado en sitios web, debido a su sencillez de implementación y su tiempo de respuesta tan rápido.

El cliente es la computadora o programa que va a realizar una solicitud hacía el servidor, esperando una respuesta con la información solicitada, esta información puede ser una consulta a una base de datos o un archivo que se encuentre dentro del servidor, por su parte el servidor puede también ser un ordenador, un servidor o un programa que responderá a las solicitudes que realice el cliente.

Básicamente, el cliente realiza peticiones hacia el servidor, el cual procesa estas solicitudes y devuelve una respuesta, en los sitios web este tipo de comunicación se realiza por lo regular usando el protocolo HTTP (Hipertext Transfer Protocol) y de forma segura con el protocolo HTTPS (Hipertext Transfer Protocol Secure), de esta manera, toda la información que solicita el usuario hacía el sitio web está por lo regular almacenada en un servidor o en una base de datos, los cuales manejan estas solicitudes y devuelven las respuestas solicitadas.

Los protocolos descritos anteriormente son conocidos también como servicios web y utilizan los puertos 80 y 443 respectivamente.

Existen distintos tipos de servicios, por ejemplo, SSH, FTP, POP3, entre otros. Los cuales cuentan con un puerto en específico para su ejecución, aunque como buena práctica de seguridad se recomienda configurarse de manera distinta.

2.1.6.- Importancia de los sitios web en nuestros días.

Como se ha descrito durante esta sección, los sitios web permiten acceder a una gran cantidad de información, permitiendo que las organizaciones expandan su mercado de negocio y que las personas puedan establecer comunicaciones entre sí alrededor del mundo, provocando que los sitios web sean uno de los principales puntos que buscan vulnerar los atacantes informáticos, ya que muchos de los sitios utilizados por las empresas, contienen información sensible sobre sus clientes, como números de tarjetas bancarias o números de seguro social, por esa razón, es importante reducir el riesgo de que un sitio web sea vulnerable, esto se puede empezar a realizar desde la creación de los mismos.

2.2.- Aplicaciones móviles.

En esta sección hablará de cómo las aplicaciones móviles se han vuelto fundamentales para el desarrollo de la sociedad, se describirá que es una aplicación móvil, como ha evolucionado hasta convertirse en lo que son hoy en día y la clasificación de estas.

2.2.1.- ¿Qué es una aplicación móvil?

También conocidas como Apps, son programas que se instalan en los dispositivos móviles, ya sean teléfonos inteligentes o tabletas y que ayudan al usuario en una tarea específica, ya sea de carácter profesional o de ocio.

El principal objetivo de las aplicaciones móviles es facilitar la vida del usuario, las aplicaciones pueden ser fácilmente descargadas desde las tiendas virtuales que se encuentran dentro de los dispositivos móviles[2].

2.2.2.- Evolución de las aplicaciones móviles.

Las primeras aplicaciones móviles que se desarrollaron datan de finales de los 90´s, eran lo que se conoce como agenda, juegos y editores de audio o ringtones, y han ido evolucionando a lo largo del tiempo de la mano con la innovación de los dispositivos móviles.

Su auge surgió a partir de la creación del iPhone, esto provocó una gran competencia entre los desarrolladores de teléfonos inteligentes, siendo Android uno de los principales, permitiendo que se crearan distintas aplicaciones móviles de acuerdo con las necesidades de cada compañía, otro de los puntos clave dentro su evolución fue el uso de las redes inalámbricas, las cuales permitieron la interacción entre usuarios de distintas partes del mundo y proveyó una mejor funcionalidad para las mismas.

El surgimiento de las Apps Stores impulsó el éxito de las aplicaciones móviles y facilitó la forma en que se distribuyen las mismas, hoy en día podemos encontrar distintas aplicaciones de acuerdo a cada compañía y no solamente ayudan a los usuarios a hacer su vida más fácil, sino que también gran parte de ellas sirven para entretenimiento y comunicación.

[2] Fernández, (2015)*Curso de Apps(I): estructura básica y primera app.* Recuperado de: https://applecoding.com/cursos/curso-apps-estructura-basica

2.2.3.- Clasificación de las aplicaciones móviles.

Debido a la gran cantidad y diferencia de aplicaciones móviles existentes, estas se pueden clasificar de muchas formas, las más importantes, debido a que engloban una gran cantidad de aplicaciones móviles son:

- De acuerdo con el mercado en que han sido desarrolladas.
- De acuerdo con el lenguaje de programación con el que han sido desarrolladas.
- De acuerdo con su tipo.

La primera clasificación, se refiere hacía que dispositivo móvil en específico fue desarrollada la aplicación, generalmente la mayoría de ellas son multiplataforma, existen algunas excepciones en las que debido a la capacidad del dispositivo móvil podrían no funcionar o no cumplir con los requisitos para su ejecución.

La segunda clasificación, permite ordenar las aplicaciones de acuerdo con los distintos lenguajes de programación para el desarrollo de estas, algunos de los más conocidos son Java, C#, C++, HTML5, HTML/CSS/Javascript, entre otros.

La última clasificación a su vez se divide en 3 tipos, los cuales son:

- Aplicaciones Nativas.
- Aplicaciones Web.
- Aplicaciones Híbridas.

Aplicaciones nativas, son aquellas que fueron desarrolladas bajo un lenguaje de programación y entorno específico, este tipo de aplicaciones genera muchas ventajas cuando el sistema operativo cumple con los requisitos para los que se desarrolló, la mayor desventaja de las aplicaciones nativas es que si la organización o el usuario no cumple con los requerimientos o las especificaciones necesarias no se podrá hacer uso de la aplicación.

Aplicaciones web, son desarrolladas comúnmente bajo el lenguaje de programación HTML junto con CSS y Javascript, además se ayudan de un Framework, este tipo de aplicaciones son muy utilizadas para permitir la accesibilidad a los sitios web desde cualquier dispositivo móvil que contenga un navegador, por otro lado, la desventaja es que no hace un uso óptimo de los recursos del sistema.

Aplicaciones híbridas, es una combinación de las aplicaciones web y las aplicaciones nativas, este tipo de aplicaciones es un sitio web adaptado a una aplicación móvil, las ventajas de las aplicaciones hibridas es que son multiplataforma y que por lo regular se encuentran en las Apps Stores, la desventaja es que el diseño varía de acuerdo con cada dispositivo móvil, así como también el uso de los recursos del sistema.

2.2.4.- Componentes de una aplicación móvil.

2.2.4.1.- Android.

A pesar de la gran diversidad de aplicaciones móviles que existen, todas pueden contar con alguno de los siguientes componentes dentro de ellas:

- Activity.
- View.
- Service.
- Content Provider.
- Broadcast Receiver.
- Widget.
- Intent.

Activity, representan el componente principal de la interfaz gráfica de la aplicación móvil, es la ventana o la pantalla de la aplicación.

View, componentes básicos con los que se puede construir una aplicación móvil, estos elementos son, por ejemplo, cuadros de texto, botones, listas desplegables o imágenes, etcétera., son componentes extensibles, ya que el desarrollador puede crear sus propios controles personalizados, lo cual brinda una mayor funcionalidad.

Service, componentes que se ejecutan en segundo plano de la aplicación móvil, es decir, no se requiere de una interfaz gráfica para ver su funcionalidad, estos servicios pueden verse de forma análoga a los procesos dentro de cualquier sistema operativo.

Content Provider, permite a las aplicaciones compartir datos o información entre ellas, estos datos no incluyen los detalles sobre el almacenamiento interno, estructura o implementación, para que las aplicaciones móviles puedan compartir sus datos, estos deben ser definidos previamente durante el desarrollo de esta.

Broadcast Receiver, reacciona ante ciertos mensajes o eventos que ocurran dentro del dispositivo móvil, estos eventos pueden estar relacionados a la cantidad de batería restante, entrada de mensajes, conexión de tarjeta SD, etcétera.

Widgets, elementos visuales que pueden mostrarse en la pantalla principal del dispositivo móvil y permiten al usuario interactuar con las aplicaciones, muestran las aplicaciones activas, pero no en uso, es decir, aplicaciones que se están ejecutando en segundo plano.

Intent, permite la comunicación entre los elementos descritos anteriormente, permite iniciar un servicio, consultar los datos de una aplicación, enviar un mensaje broadcast, etcéteraétera.

2.4.4.2.- IOS

Algunos de los elementos básicos que contienen estas aplicaciones son:

- AppDelegate.
- Main.storyboard.
- ViewController.
- Supporting Files.
- Images.xcassets.
- Launchscreen.xib

AppDelegate, son los elementos básicos necesarios para el arranque, background y cierre de la aplicación.

Main.storyboard, encargado del diseño de la aplicación, permite generar la estructura, navegación e interconexión entre los distintos elementos que la componen.

ViewController, forma parte de la vista que compone la aplicación, es decir, los elementos que verá el usuario al hacer uso de esta.

Supporting Files, contiene todos los recursos necesarios para el funcionamiento de la aplicación.

Images.xcassets, contiene los gráficos relacionados con las pantallas e iconos utilizados dentro de la aplicación.

Launscreen.xib, contiene los mecanismos necesarios para el lanzamiento de la aplicación y su tamaño dentro de cada dispositivo móvil.

2.2.5.- Importancia de las aplicaciones móviles en nuestros días

Las aplicaciones móviles son herramientas utilizadas de forma constante por la mayoría de los usuarios, ya que han provocado que dentro de un dispositivo móvil se tenga una gran cantidad de funciones que antes eran cubiertas por distintos objetos.

El desarrollo de las aplicaciones móviles está enfocado en facilitar la vida de los usuarios, con aplicaciones que permitan mejorar la salud, alimentación y una mejor organización del tiempo, generando un mayor desafío para los especialistas en seguridad de la información, debido a que entre más funcionalidades existan, habrá más puntos de entrada para los atacantes informáticos.

2.3.- Diferencia entre aplicaciones web y móviles

Aunque ambos prestan servicios bajo el mismo medio (teléfonos inteligentes y tabletas), las aplicaciones móviles y web son muy diferentes, las primeras son programas que se pueden descargar e instalar en un dispositivo móvil, mientras que las aplicaciones web son accesibles desde un navegador mientras se tenga una conexión a internet, sin necesidad de que se descargue ningún programa adicional, además algunas aplicaciones móviles no necesitan de conexión a internet para poder hacer uso de ellas una vez que se han descargado.

Otra diferencia significativa es que las aplicaciones móviles permanecen en el dispositivo móvil del usuario prestando un servicio o respondiendo a una necesidad, es decir, su uso es frecuente, mientras que las aplicaciones web, por lo regular, están diseñadas solamente con el fin de informar al público en general.

También se debe resaltar que las aplicaciones móviles pueden no ser compatibles con cualquier dispositivo móvil, mientras que las aplicaciones web, debido a su desarrollo son compatibles en cualquier dispositivo, además las aplicaciones móviles requerir de una descarga, necesitan de un distribuidor que en este caso son las App Store.

Las aplicaciones móviles tienen un mejor manejo de los recursos del sistema, y su accesibilidad es superior, un ejemplo muy claro de esto último se puede observar en el uso de redes sociales.

Por último, las actualizaciones no suceden de la misma manera para ambas aplicaciones, las actualizaciones para aplicaciones web se llevan a cabo sin que el usuario se dé cuenta, esto debido a que es un proceso automatizado, mientras que, para las aplicaciones móviles, los usuarios deben de realizar el proceso de actualización descargando la nueva versión de la aplicación.

2.4.- Atacantes informáticos.

En esta sección se describirán a los distintos tipos de atacantes informáticos y su forma de pensar, es decir, que buscan obtener al momento de realizar un ataque.

2.4.1.- ¿Qué buscan obtener?

Los atacantes informáticos buscan obtener la mayor cantidad de información sensible de un individuo u organización, para posteriormente obtener algún tipo de beneficio, como puede ser económico o reconocimiento social, además, los atacantes pueden ser guiados por su ideología política o religiosa, por lo que buscan el desprestigio de la organización.

La información principal que buscan obtener los atacantes está relacionada información personal, la cual puede ser desde nombres, apellidos, edad, números telefónicos, correos, contraseñas, números de tarjeta, direcciones, entre otros, que les permitan generar un perfil de la víctima.

2.4.2.- Hacker.

Es una persona experta en alguna de las ramas de la informática, dedicada a realizar alteraciones sobre un sistema o dispositivo, con un motivo positivo o negativo, por esa razón, se clasifican en tres tipos:

- White Hat.
- Black Hat.
- Gray Hat.

White Hat, es decir, son conocidos como hacker éticos, son aquellos que buscan vulnerabilidades en los sistemas con el fin de proveer posibles medidas de mitigación y poder corregir los fallos que esta presenta, su fin es el de realizar ataques para mejorar la seguridad de los sistemas computacionales.[3]

Black Hat, son aquellos que buscan las vulnerabilidades de un sistema para conseguir un beneficio monetario, por lo regular este grupo aprovecha las vulnerabilidades más simples, como lo son el error humano, configuraciones por defecto, vulnerabilidades de día cero, etcéteréteraa.

Gray Hat, son aquellos que vulneran un sistema de forma similar a los de Sombrero Negro, pero con la finalidad de ofrecer sus servicios a la organización para poder solucionar esas vulnerabilidades.

2.4.3.- Cracker.

Se encuentran dentro del grupo Black Hat, ya que son individuos que buscan vulnerar un sistema con el fin de obtener beneficios de forma ilegal, estos beneficios por lo regular son económicos, o simplemente realizan un ataque con el fin de desprestigiar a la organización, motivados por sus ideologías.

2.4.4.- Sniffer.

Son atacantes que se ayudan de herramientas de monitoreo de red, para poder obtener información que circula por la misma, se dedican a rastrear, capturar y descifrar los mensajes que viajan por la red hacia internet.

[3]2017. *Definición de atacantes.* Recuperado de: *Notas del Plan de Becarios del Seguridad en Seguridad Informática* de UNAM-CERT.

2.4.5.- Script Kiddie.

Son usuarios que descargan herramientas desde internet y las utilizan sin tener conocimiento de cómo usarlas o del daño que pueden causar.

A pesar de su inexperiencia y sus limitados conocimientos en el área de la seguridad de la información, este tipo de atacantes informáticos son los que más daño causan a las redes y sistemas informáticos.

2.4.6.- Newbie.

Es conocido como un atacante novato, el cual encuentra utilidades o programas dentro de la red y las ejecuta, pero realmente no sabe cuál es el funcionamiento de dichos programas, realmente no puede causar un gran daño hacia un sistema.

2.4.7.- Ciberterrorista.

Este tipo de atacantes, buscan causar pánico y confusión a los usuarios a través de vídeos, imágenes o archivos, esto con fines políticos o religiosos, consigue sus recursos a partir de la extorsión a grandes organizaciones y hacen uso de correos, chats y teléfonos móviles cuyos datos están cifrados, para que no puedan ser localizados de forma sencilla.

2.4.8.- Programadores de malware.

Son expertos informáticos que crean scripts, códigos o bloques de códigos con el fin de vulnerar algún sistema o dejar puertas traseras para un posible acceso, este tipo de programas busca dañar sistemas o aplicaciones del usuario, también pueden ser aplicaciones falsas, las cuales por desconocimiento son descargadas desde la red infectando dispositivos o computadoras, este tipo de atacantes busca que su código se propague lo más posible e infecte a una gran cantidad de equipos.

2.4.9.- Carder.

Es aquel atacante que haciendo uso de herramientas vulnera las tarjetas de crédito y débito, esto con el fin de realizar acciones fraudulentas ya sea desde la web o por teléfono, gastando grandes cantidades de dinero sin el conocimiento del propietario de la tarjeta.

2.4.10.- Phreaker.

Es aquel que busca vulnerar los sistemas telefónicos, la telefonía móvil y voz sobre IP, este tipo de atacantes, se especializan en el funcionamiento de estos sistemas para detectar posibles vulnerabilidades y en ocasiones recibir un beneficio como llamadas gratuitas.

2.4.11.- Spammer.

Son aquellos atacantes que se encargan de enviar correos electrónicos basura, envían de forma masiva correos electrónicos no solicitados a los usuarios o servidores, estos últimos con el fin de generar una denegación del servicio.

El envío de estos correos hacia los usuarios es con el fin de infectar al equipo, debido a que la mayoría de estos contienen malware, aunque también pueden ser con la finalidad de obtener información sensible del usuario o algún beneficio económico.

2.4.12.- Pirata informático.

Son aquellos que se encargan del copiado y distribución de forma ilegal de programas, libros o del contenido intelectual de terceros.

2.4.13.- Exempleados.

Formalmente no son realmente atacantes informáticos como los listados anteriormente, pero conocen las vulnerabilidades que existen en la organización, ya que han interactuado con los sistemas y en ocasiones pudieran mantener accesos a los mismos, provocando que los ataques funcionen exitosamente en la mayoría de los casos.

2.5.- Evolución de los malware y ataques informáticos.

Así como la seguridad informática ha ido evolucionando a lo largo de la historia, los atacantes informáticos han encontrado nuevos métodos de intrusión a los sistemas y han desarrollado malware cada vez más personalizado de acuerdo con el sistema o persona que se desea atacar.

El primer registro que se tiene de un malware fue en el año de 1960, donde surgió el juego llamado CoreWars, el cual fue considerado como un virus, ya que competía junto con las otras aplicaciones del sistema por los recursos del mismo, esto con el fin de tener el control absoluto de la memoria, posteriormente en el año de 1971 surgió el malware Creeper, desarrollado por Bob Thomas, este virus atacaba a los sistemas Tenex a través de ARPANET y al momento de ser descargado por el usuario se auto ejecutaba mostrando el mensaje “I´m the creeper: catch me if you can”, provocando que el usuario no pudiera hacer uso de las aplicaciones de su ordenador.

Posteriormente en el año 1986 surgió un virus llamado Pakistani Brain, el cual buscaba afectar equipos IBM|, este virus atacaba los discos floppy, con lo cual logro propagarse rápidamente en muy poco tiempo, otro malware que se dio a conocer a finales de la década de los 80´s fue el gusano Morris, el cual se propagó a través de miles de estaciones de trabajo alrededor del mundo.

Durante la década de los 90´s, surgió el virus Michelangelo, el cual buscaba infectar el sector de arranque de los disquetes y el sector MBR de los discos rígidos, posteriormente en el año de 1994, surgió el primer ransomware conocido, a diferencia de los conocidos hoy en día, no pedía una recompensa o permitía la liberación de la información mediante una llave o código específico, simplemente, cifraba ciertos sectores del disco duro para que la información no pudiera ser consultada por el usuario, en ciertos sistemas el sector MBR era modificado por uno vacío haciendo que el sistema no pudiera arrancar haciéndolo inutilizable, finalmente en el año de 1997, los atacantes informáticos decidieron cambiar de estrategia de ataque, al dejar de usar malware que se propagara a través del sistema y optaron por usar troyanos, esto, viendo los beneficios económicos que podría traer el robo de identidades y el inicio del phishing a través de los correos electrónicos.

En el año 2000, surgió un gusano muy conocido llamado ILOVEYOU, el cual era enviado a través del correo electrónico, se encontraba almacenado en un adjunto que se hacía pasar por una carta de amor y al ser descargado por el usuario el gusano era capaz de acceder al sistema operativo y extraer los datos de este.

En cuanto a teléfonos móviles, el primer malware surgió en el año 2005, llamado CommWarrior, era capaz te propagarse mediante MMS y Bluetooth, principalmente ataco a teléfonos inteligentes de la marca Symbian, modelo Series 600, a pesar de que sus afectaciones no fueron muy conocidas, este virus generó un impacto importante para los expertos en seguridad informática y antivirus.

Posteriormente en el año 2008, apareció el gusano Stuxnet, uno de los gusanos más conocidos y peligrosos que han existido, el cual marco la nueva era del malware moderno, este gusano se propagaba a través de los sistemas de control industrial y buscaba llegar hasta las instalaciones nucleares iraníes, este gusano no hacía ningún daño a los sistemas solamente buscaba propagarse hasta llegar a los ordenadores de las instalaciones nucleares.

Para el año 2012, apareció Medre, un malware que se encargaba de robar información a través de la extracción de documentos de AutoCAD y buscaba el robo de planos de empresas privadas, especialmente de Perú.

Recientemente se han encontrado distintos malware como Hesperbot y Windigo, el primero es un troyano que atacó a usuarios bancarios a través de phishing, haciéndose pasar por empresas de confianza, una vez que las víctimas introducían sus credenciales en las páginas web falsas diseñadas por los atacantes, estos conseguían sus credenciales de inicio de sesión haciendo un uso indebido de las mismas, mientras que Wendigo, tomó control de 25,000 servidores Unix alrededor del mundo, con los cuales envió millones de mensajes de spam diarios, con el fin de propagar malware, robar información y realizar ataques de denegación de servicio hacia los servidores.

Los malware también han buscado vulnerar los dispositivos móviles y su evolución ha ido en aumento, como ya se mencionó el primer malware para dispositivos móviles surgió en el año 2005, en ese mismo año se encontró el primer backdoor para plataformas móviles y se desarrolló también el primer troyano, el cual estaba designado para robo de datos de los usuarios.

En el 2006, el principal objetivo era el robo de datos y dinero de los usuarios, esto lo lograban haciendo que los dispositivos móviles llamaran a servicios de pago sin conocimiento de sus propietarios.

Durante los años 2007 y 2008, su diseño se expandió para afectar a todo tipo de plataformas, creándose así el primer malware para iPhone y el desarrollo de un antivirus falso llamado FakeAV para los dispositivos móviles.

Para el año 2010 surge Zeus, el cual buscaba atacar a clientes de la banca en línea y robar su información confidencial, en el año 2011 surgió el primer código QR malicioso y finalmente en el 2013, apareció el troyano llamado Obad, considerado el troyano más sofisticado y afectaba sistemas Android, se consideraba así, debido a que tres exploits, un backdoor, un troyano de SMS y funciones de bots, realizando grandes afectaciones a los dispositivos móviles.

En los últimos años, los atacantes han optado por vulnerar sistemas de grandes empresas, extrayendo las bases de datos de los usuarios, dentro de las cuales pueden encontrar información confidencial de los mismos, los casos más conocidos fueron el de la red social Twitter, Linkedin, Sony, Yahoo, estas empresas aceptaron públicamente el robo de información de sus usuarios, en la mayoría de los casos se puso en venta dentro de la red y finalmente el ataque de DDOS más reciente a los servidores de Internet Dyn, el cual afecto a la gran mayoría de las redes sociales como Facebook, Twitter, Instagram, a la aplicación de mensajería Whatsapp, e inclusive a compañías como Spotify, Amazon y Netflix, este ataque fue realizado en conjunto desde distintos puntos del planeta y fue generado durante distintas fases, lo cual provocó que algunas de estas compañías se quedaran sin servicio durante aproximadamente 11 horas .

2.6.- Ataques informáticos.

En esta sección se definirán los distintos tipos de ataques informáticos asociados a los sitios web y aplicaciones móviles, se describirá su funcionamiento, principales afectaciones que causan y qué información buscan obtener.

2.6.1.- ¿Qué son los ataques informáticos?

Un ataque informático es cualquier intento de explotar una vulnerabilidad, realizado por una persona o conjunto de personas, esto con el fin de afectar a los activos de una organización.

Debido a la gran cantidad de ataques que existen, en esta sección solo se tratarán aquellos que afecten a los sitios web y a las aplicaciones móviles.[4]

2.6.2.- DDoS.

Acrónimo de Distributed Denial of Service o Negación de Servicio Distribuido, regularmente sucede cuando el atacante aprovecha una red de computadoras, las cuales contienen un programa que permite al atacante ejecutar comandos de forma remota, esto con el fin de atacar a un objetivo único, para con ello evitar la disponibilidad de un servicio, comúnmente estas computadoras son conocidas como botnets.

[4] 2017: *Tipos de ataques informáticos.* Recuperado de: Notas del Plan de Becarios en Seguridad Informática UNAM-CERT.

Los ataques de DDos funcionan de manera muy sencilla, los sitios web sólo pueden dar servicio a un número limitado de peticiones en un tiempo determinado, cuando sucede un ataque de DDos, los atacantes provocan que el servidor no pueda realizar la respuesta adecuada a todas las peticiones que se realizan desde los distintos equipos, provocando que los usuarios que generan peticiones válidas no reciban una respuesta.

Hay distintos tipos de ataques DDOS, entre los principales encontramos:

- Syn Flood.
- Connection Flood.
- ICMP Flood.
- UDP Flood.

Syn Flood o Inundación de paquetes Syn, es el más común de todos, debido a que es utilizado a través del protocolo TCP, el cual se basa en una comunicación de 3 pasos, de manera general, en el primer paso, el cliente establece una conexión con el servidor enviando una solicitud SYN, posteriormente el servidor en el segundo paso, responde a esta solicitud enviando un paquete SYN/ACK, finalmente el cliente cierra esta comunicación respondiendo al servidor con un mensaje ACK, el ataque SYN Flood, sucede cuando el atacante manda una gran cantidad de solicitudes SYN, a través de direcciones IP inexistentes o no válidas, provocando que el servidor se mantenga en espera de la respuesta para poder cerrar la comunicación.

Connection Flood o Inundación de conexión, como se describió en la definición de DDos, los servidores tienen una cantidad limitada de conexiones simultáneas, este tipo de ataque, se busca ocupar todas las conexiones que puede recibir el servidor.

ICMP Flood o inundación ICMP, para este tipo de comunicación, el servidor responde a las peticiones realizadas por parte de los clientes, la vulnerabilidad radica cuando las peticiones están llenas de información inútil o se realiza la misma petición desde distintas direcciones IP, provocando que se agoten los recursos del sistema.

UDP Flood o Inundación de UDP, se basa en el protocolo UDP y sucede cuando el atacante realiza una gran cantidad de solicitudes a distintos puertos del servidor, esto con el fin de gastar los recursos de este, recursos como memoria RAM, procesador, etcétera., generando que el servidor no pueda procesar todas las solicitudes.

El objetivo principal de los DDos es afectar la disponibilidad de los servidores, para mitigar este tipo de ataques, se pueden mapear las direcciones IP desde las cuales se están realizando las solicitudes para bloquearlas y evitar una afectación mayor al sistema y bloquear esas direcciones para evitar una afectación mayor al sistema.

2.6.3.- XSS.

Del inglés Cross-Site-Scripting, sucede cuando el atacante informático inyecta un código malicioso a un sitio web o aplicación móvil, colocándose en forma de hipervínculo para posteriormente redirigir al usuario a otro sitio web, mensajería instantánea o correo electrónico. Hay dos tipos de XSS:

- Directo o persistente
- Indirecto o reflejado.

XSS directo, consiste en invadir el código HMTL con el que se encuentra desarrollado el sitio web, con etiquetas de tipo <script> y <frame>, provocando que, al momento de ejecutarse ese código en el sitio web, el script pueda ser descargado por el usuario, sin que se percate que ese elemento no forma parte de la página.

Una variante de XSS persistente es llamada XSS Local, su objetivo es aprovecharse de los objetos generados en el sitio web a través de JavaScipt, afectando la página inicial antes de que el navegador la termine de ejecutar, de esta manera el servidor no podrá mitigar esta vulnerabilidad, debido a que se instala de forma local en el ordenador del usuario, sin que este se percate de lo sucedido.

XSS indirecto, consiste en modificar los valores que la aplicación web utiliza para el envío de variables de una página web a otra, enviando los parámetros a través de un mensaje o dentro de la URL, este ataque se realiza comúnmente sobre las cookies, ya que estas permiten identificar al usuario dentro del aplicativo.

La principal afectación que causan este tipo de ataques está relacionada a la disponibilidad del sitio web, debido que el XSS se ejecutará continuamente dentro del equipo del usuario, una de las mejores prácticas para evitar este tipo de ataques, es la sanitización de los parámetros dentro del código del sistema, es decir, no permitir que se ingresen caracteres utilizados en sentencias de lenguajes como Javascript o HTML (<,>,/) con ello, se evita la ejecución del código malicioso dentro del sistema.

2.6.4.- SQL Injection.

SQL Injection o Inyección de SQL, es uno de los ataques más comunes en los sitios web, es explotado por el atacante cuando en los campos de búsqueda acceso, se pueden inyectar o anexar sentencias SQL.

El objetivo principal cuando se realiza este ataque es la obtención de información de la base de datos, la cual puede ser, el manejador que se está utilizando para su gestión, nombres e información de las tablas, etcétera., para ello, el atacante realiza consultas a través de la interfaz gráfica del sitio web o desde la URL, modificando los parámetros que se envían y analizando las respuestas que devuelve el sistema.

Además, los atacantes se ayudan de los métodos GET y POST empleados por los desarrolladores para el envío de información a través de formularios, la diferencia entre GET y POST, es que el primero envía la información en claro, es decir, cualquiera que acceda a la URL del formulario, podría ver la información contenida en el mismo, mientras que el método POST los datos se envían por un canal de información seguro, de tal forma que no puedan ser modificados desde la URL.

Algunas medidas que se pueden tomar para evitar este tipo de ataques son el uso de método POST, sanitización de los parámetros que se envían hacia la base de datos y una correcta configuración del sitio web, para evitar que desde el mismo se generen respuestas del manejador de base de datos.

2.6.5.- Directory Path Traversal.

El objetivo de este tipo de ataque es conseguir acceso a los distintos directorios y archivos de una página web que se encuentran fuera del directorio raíz y a los cuales no tiene acceso un usuario sin privilegios.

Para aprovechar esta vulnerabilidad dentro de los sistemas, los atacantes se ayudan de la URL y los distintos parámetros que muestra al realizarse una solicitud, además hacen uso de caracteres especiales comúnmente conocidos como “dot-dot-slash” (../), los cuales les permiten acceder a los directorios raíz de una página web y a partir de ahí, navegar por todos los ficheros contenidos en la misma.

Para evitar este tipo de ataques, es recomendable realizar una revisión del sistema, para verificar que archivos pueden ser consultados de forma pública, debido a que muchos de los mismos contienen información relacionada a la configuración y administración del sistema.

2.6.6.- Fuerza Bruta.

Un ataque de fuerza bruta es una técnica que permite, mediante la combinación de caracteres obtener las credenciales de acceso al sistema válidas, se apoyan de diccionarios que contienen nombres de usuario y contraseñas comunes, los cuales iteran entre cada uno de los elementos y se aprovechan de errores humanos como:

- Contraseñas débiles.
- Contraseñas compuestas por palabras que se encuentran en un diccionario.
- Contraseñas de longitud corta.
- Nombre de usuario y contraseña similares.

Algunas de las medidas que permiten evitar este tipo de ataques, son:

- Configuración del sitio web para la creación de contraseñas robustas por parte del usuario.
- Bloqueo del usuario después de un cierto número de intentos de inicio de sesión fallidos.
- Retraso de tiempo entre cada intento de inicio de sesión.
- Uso de Captcha.

CAPTCHA acrónimo de Completely Automates Public Turing test to tell Computers and Humans, (Prueba de Turing completamente pública y automática para diferenciar máquinas de humanos), permiten realizar una doble autenticación, debido a que no permite el inicio de sesión, si no se llena de forma correcta el Captcha.

2.6.7.- Ingeniería Social.

Es una técnica en la cual el atacante busca obtener información personal de los usuarios de distintas formas, es uno de los ataques más utilizadas, ya que puede ser aplicada desde un formulario a través de internet, encuestas en línea, hasta encuestas o cuestionarios en la calle y no se requieren conocimientos especializados en sistemas, solamente se debe de saber qué información se quiere obtener del usuario y adaptarlo a las preguntas que se le van a hacer al mismo.

El objetivo de los atacantes al usar esta técnica es conseguir información sensible de los usuarios para posteriormente hacer un uso indebido de la misma, esta información puede ser extraída también desde las redes sociales.

Una forma de evitar la ingeniería social, desde el ámbito de las redes sociales, es restringir el acceso a la información del perfil, la cual solamente debería de ser consultada por conocidos, no brindar información personal si no es necesaria para las acciones que se realizan dentro de un sitio web.

2.6.8.- Phishing.

Realizado comúnmente a usuarios comunes y no a grandes organizaciones como un ataque de DDoS, consiste en el envío de correos que aparentar provenir de una fuente confiable, por lo regular aparentan ser entidades bancarias, que intentan obtener datos confidenciales del usuario, para posteriormente suplantar su identidad, la información que buscan los atacantes son números de tarjeta, claves de usuario, etcétera.

Un ejemplo de esto sucede cuando el usuario recibe un correo electrónico falso que simula proceder una compañía bancaria, este correo contiene un enlace que apunta a una o varias páginas web del banco, replicando casi completamente el aspecto y la funcionalidad del sitio web oficial, para que posteriormente el usuario por desconocimiento introduzca sus credenciales y el atacante pueda almacenarlas para hacer uso de ellas.

Una de las mejores maneras de protegerse de este tipo de ataques realizando campañas de concientización dentro de la organización, en la cual se eduque a los usuarios para que puedan identificar un sitio web falso del original, comúnmente los sitios web oficiales deben de tener al inicio de la URL el protocolo HTTPS, que nos indica que la información que estamos introduciendo en ese sitio va a ir cifrada y no será visible para otros si es que esos paquetes son monitoreados.

2.6.9.- Pharming.

El pharming consiste en suplantar el DNS, con el propósito de conducir al usuario a un sitio web falso.

El DNS organiza los nombres de máquina en una jerarquía de dominio, esta jerarquía se encuentra dividida en 3 partes, la primera es la parte del host o servidor, la segunda el dominio y la tercera el dominio de nivel superior o TLD (Top Level Domain), el DNS permite a un usuario conectarse a un sitio web sin la necesidad de escribir las direcciones IP, facilitando la tarea del usuario al hacer uso de nombres mnemónicos y descriptivos de las empresas.

Para ejemplificar mejor la jerarquía de dominio, se tomará como ejemplo la dirección URL *www.google.com*

- Host/Servidor: www.
- Dominio: google.
- TLD: com.

Existen una gran cantidad de TLD, los más conocidos son: .com, .edu, .gov., .org, .net.

Para que pueda suceder esto, el atacante primero debe de instalar un software malicioso en el ordenador de la víctima, este software puede ser un ejecutable, o un archivo con cualquier tipo de extensión conocida como: .zip, .doc, .rar, etcétera., una vez instalado el programa, el atacante puede re direccionar al usuario a los sitios web falsos, esto se realiza, por ejemplo, cuando el usuario introduce la URL *https://google.com*, el atacante puede hacer que el DNS asociado a Google lo envíe hacia otro sitio web, sin que el usuario se percate de que eso sucedió.

Existen muchas vías por las que el atacante puede hacer que el usuario descargue el software malicioso, entre las más conocidas se encuentran la descarga de programas por parte del usuario, correo electrónico con adjuntos maliciosos.

Para evitar este tipo de ataques, se deben tomar las mismas medidas que para el phishing, es decir, tener los conocimientos mínimos en seguridad, que permitan la identificación de un sitio web falso.

2.6.10.- Cross Site Request Forgery.

Consiste en forzar al usuario a ejecutar peticiones no deseadas a una web en la que se encuentra autentificado sin que este se dé cuenta, el atacante no busca el robo de datos, si no que las peticiones realizadas provoquen algún cambio, dependiendo el nivel de privilegios con los que cuente el usuario afectado es el nivel de riesgo en el que se encuentra el servidor, la principal diferencia con XSS es que aprovecha la confianza del servidor con el usuario, mientras que en el XSS se explota la confianza del usuario hacia el servidor.

El funcionamiento de CSRF es muy simple, el atacante vulnera el código HTML dentro del servidor del usuario, posteriormente la víctima establece una conexión con la aplicación web, introduce las credenciales de acceso al sitio web, una vez iniciada la sesión el usuario comienza a realizar peticiones contra el servidor web sin percatarse de ello.

Las afectaciones de este ataque son diversas, entre las principales se encuentran la suplantación de identidad, ejecución de comandos dentro del sistema, envío de información sensible de una organización o individuo, transferencias de dinero, etcéteraétera.

2.6.11.- Hijacking.

Este tipo de ataque consiste en el secuestro de la cookie de sesión del usuario dentro de un sitio web, se aprovecha de los mecanismos de control utilizados por los sitios web, los cuales por los regular hacen uso de un token de sesión.

Existen diferentes formas de obtener este token, las más comunes son:

- Token de Sesión Previsible: En esta variante de hijacking, el atacante busca predecir el identificador de sesión para poder obtener acceso al aplicativo, esto, obteniendo cierta cantidad de identificadores para poder conocer la estructura de los mismos, así como también el conocer el algoritmo de cifrado utilizado por el aplicativo para su protección.
  Finalmente, se realiza un ataque de fuerza bruta para poder obtener un ID de sesión válido.

- Session Sniffing: Dentro de esta variante, el atacante hace uso de un sniffer (herramienta que permite obtener los datos transmitidos a través de una red), para de esta manera obtener el token de sesión válido dentro de la comunicación entre el usuario y el servidor, para obtener acceso al mismo.

- Ataques del lado del cliente (XSS, ejecución de código JavaScipt malicioso): Dentro de esta clasificación, el atacante obtiene el ID de sesión mediante el envío de código malicioso, regularmente creado en Javascript. Esto se realiza mediante la creación de un enlace falso que espera ser ejecutado por la víctima, para que el código Javascript genere las instrucciones necesarias para la obtención del ID de sesión.

- Man in the middle attack: En esta variante el atacante busca interceptar la comunicación entre el usuario y el sitio web, este tipo de ataques es muy efectivo debido a que el atacante tiene la posibilidad de actuar como un proxy entre el cliente y el servidor, con la posibilidad de leer, insertar y modificar los datos transmitidos entre ambos, de esta manera el atacante puede ver toda la información dentro de esta comunicación.

2.6.12. APT (Advanced Persistent Threat).

Este tipo de ataque informático es muy distinto a los listados anteriormente, debido a que se desarrolla a largo plazo, esto, debido a que va escalando entre los equipos del personal de la organización a través de la explotación de las vulnerabilidades.

El APT contiene un conjunto de herramientas para poder realizar estas acciones, entre ellas pueden ser:

- Keyloggers.
- Backdoors.
- Exploits.

Además, el APT se mantiene oculto para el usuario, en espera de encontrar información que pueda permitirle moverse entre los equipos de la organización.

Este tipo de ataques es muy complicado de detectar debido a la gran cantidad de herramientas que contiene, además, no se propaga de forma tan rápida como un malware y finalmente al ser un ataque dirigido, esto genera una gran dificultad para erradicación.

2.7.- Malware.

En esta sección se van a definir los distintos tipos de malware asociados a los sitios web y aplicaciones móviles, se describirá su funcionamiento, posibles medios de transmisión, cual es la finalidad del atacante al enviar este tipo de malware y las posibles afectaciones que podrían realizar.

2.7.1.- ¿Qué es el malware?

Antes de comenzar con la descripción de los distintos tipos de malware, es importante conocer que es un malware.

Es la abreviación de software malicioso y se refiere a cualquier aplicación o programa cuya finalidad sea la de dañar algún equipo de cómputo o modificar, sin el conocimiento del usuario la funcionalidad del sistema.[5]

[5] UNAM-CERT, 2017. *Definición de Malware.* Recuperado de: falta título https://www.seguridad.unam.mx/taxonomy/term/1159

2.7.2.- Virus Informático.

Los virus informáticos son programas informáticos que suelen esconderse dentro de otra aplicación, es decir, se adhiere a archivos ejecutables, su finalidad es dejar que el sistema quede inoperable o realizar un daño menor como el borrado y corrupción de ciertos archivos del sistema, una de las desventajas de este tipo de malware es que requieren de la intervención del usuario u otro proceso del sistema para propagarse dentro del sistema y poder realizar acciones maliciosas, su forma de propagación entre distintos equipos se realiza mediante la copia de los archivos.

Finalmente, los virus informáticos realizan estas acciones maliciosas a través del payload o carga útil contenida en su código.

2.7.3.- Gusano

Son aplicaciones informáticas con la capacidad de auto replicarse e invadir equipos de cómputo dentro de una red, esto lo realiza mediante la explotación de alguna vulnerabilidad en los servicios de los equipos para poder trasladarse de un host a otro con la finalidad de realizar acciones maliciosas.

Los gusanos comúnmente se a través de la red de una organización por medio de correos electrónicos, mensajería instantánea o dispositivos extraíbles, por lo que no requiere la intervención del usuario para su ejecución.

Uno de los gusanos más conocidos es Stuxnet, el cual se aprovechaba de las vulnerabilidades que existen en los sistemas SCADA, con la finalidad de obtener el control de los sistemas industriales iraníes.

2.7.4.- Troyano.

Los troyanos son programas maliciosos que se hacen pasar por un software legítimo, pero realizan más actividades que las que dicen hacer, regularmente estas actividades buscan realizar afectaciones al sistema del usuario.

El principal medio de transmisión de este malware es a través de internet desde sitios poco confiables, por esa razón requieren de la intervención del usuario u otro proceso del sistema para ejecutarse.

2.7.5.- Spyware.

Son aplicaciones cuya finalidad es la de recolectar la información de un usuario sin su consentimiento, muchas de estas son utilizadas por distintos medios como redes sociales o aplicaciones de comercio electrónico para poder mostrar al usuario información relacionada a sus intereses.

Esta recolección se realiza a partir de los hábitos de navegación, este tipo de malware se instala con ayuda de otro tipo de malware como los gusanos informáticos, troyanos o adware.

La información obtenida puede ser utilizada para fines de negocios como los descritos anteriormente, pero además puede dar información relevante al atacante, el cual puede utilizarla para poder realizar otros tipos de ataques como el phishing o pharming y poder realizar una mayor afectación al usuario.

2.7.6.- Adware.

Acrónimo de **advertisement y software**, son programas maliciosos cuya finalidad es la de mostrar anuncios publicitarios en la pantalla de la víctima mientras esta navega por un sitio web, los anuncios se pueden mostrar como ventanas emergentes en el navegador o modificar las páginas de los buscadores.

Este tipo de malware se puede generar gracias a la información recopilada por un spyware y tiene la finalidad de enviar ataques dirigidos a un objetivo para la obtención de información sensible.

2.7.7.- Ransomware.

Uno de los malware más conocidos, el cual tiene como finalidad el cifrar la información de la víctima, esta información pueden ser solamente algunos archivos o carpetas hasta el disco duro, dejando inoperable el sistema operativo.

Este tipo de malware se puede replicar a través de la red dentro de equipos que se encuentren infectados o con la intervención del usuario para su ejecución, la finalidad del atacante es la obtención de dinero a cambio de la liberación de la información de la víctima.

Hay muchas variantes de este tipo de malware, aunque se considera uno de los más dañinos, debido a que el hecho de pagar por el rescate de la información no asegura que el atacante realmente devuelva a la víctima el control de su sistema, aunque existen muchas variantes que, gracias a la investigación de analistas de malware, ya se encontró un método de descifrado sin necesidad de realizar un pago a cambio al atacante.

2.7.8.- Botnet.

Son programas maliciosos que, al ser ejecutados por el usuario funcionan como un equipo zombie, es decir, permiten realizar una serie de acciones dentro del sistema afectado, estas instrucciones o comandos son enviadas por el BotMaster a través del Centro de Control (C&C).

El atacante utiliza estos equipos zombies comúnmente para realizar ataques de Denegación de Servicio, aunque también puede utilizarlos para el envío de correos spam o malware dentro de una organización, entre otros.

Como ya se explicó anteriormente, el BotMaster hace uso de un C&C, de los cuales existen dos tipos:

- C&C Centralizado: Dentro de esta clasificación existen a su vez dos tipos:
    - *Tipo PUSH*: Usa el protocolo IRC (Internet Relay Chat), en este tipo, la botnet espera a que el C&C le envíe las instrucciones, las cuales son publicadas dentro de los canales IRC.
    - *Tipo PULL*: Usa el protocolo HTTP/HTTPS (Hypertext Transfer Protocol), a diferencia del tipo PUSH, el bot consulta periódicamente al servidor web donde se encuentran los comandos para saber si hay alguna acción nueva a realizar.

- C&C Distribuido: Este tipo de C&C hace uso del protocolo P2P (Peer to Peer), dentro de esta clasificación, existen múltiples C&C y múltiples botnet, por esa razón una bot puede recibir comandos de cualquiera de los C&C, con lo cual no existiría problema si alguno de los C&C se da de baja o deja de funcionar.

2.8.- Vulnerabilidades.

En esta sección se van a describir las vulnerabilidades más comunes dentro de los sitios web de acuerdo con el OWASP (Open Web Application Security Project), el cual, como su nombre lo menciona es un proyecto sin fines de lucro, cuya finalidad es mejorar la seguridad en el software, dentro de este proyecto existen herramientas para el análisis y explotación de vulnerabilidades en sitios web, para este trabajo, se tomaron las bases del top Ten del 2013.

2.8.1.- Inyección de Código.

Este tipo de vulnerabilidad es aprovechada por los atacantes cuando se realiza el envío de datos no confiables hacia el aplicativo como parte de un comando o una consulta, estos datos buscan engañar al intérprete con el fin de obtener más información que la solicitada o acceder a datos no autorizados, el ataque más común utilizado para este tipo de vulnerabilidad es el de SQL Injection, en el cual se busca obtener información de la base de datos del sitio web.

2.8.2.- Pérdida de Autenticación y Gestión de Sesiones.

Algunas de las funciones utilizadas por los sitios web relacionadas a la autenticación del usuario y la gestión de las sesiones son uno de los objetivos que más buscan aprovechar los atacantes, debido a que, pueden obtener las contraseñas y cuentas de un usuario, así como también el token de sesión del mismo, con la finalidad de obtener acceso al aplicativo.

Uno de los ataques más utilizados para la explotación de esta vulnerabilidad es el de Hijacking.

2.8.3.- Secuencia de Comandos en Sitios Cruzados (XSS).

Este tipo de vulnerabilidad sucede cuando una aplicación permite como entrada código JavaScript sin una validación del mismo, con lo cual, el atacante puede ejecutar dicho código en la máquina de la víctima y realizar distintas actividades maliciosas, como el secuestro del token de sesión del usuario, la destrucción del sitio web o inclusive redirigir al usuario hacia un sitio web malicioso.

2.8.4.- Referencia Directa Insegura a Objetos.

Esto ocurre cuando el desarrollador del aplicativo expone la referencia hacia un objeto de implementación interno, este objeto puede ser un archivo, directorio o base de datos, sin la debida protección o control de acceso hacia estos objetos, por lo que el atacante puede consultarlos o manipularlos sin tener los privilegios necesarios.

2.8.5.- Configuración de Seguridad Incorrecta.

Esta vulnerabilidad es una de las más comunes dentro de las organizaciones, debido a que no se tiene la cultura de mantener actualizados los sistemas utilizados dentro de la misma.

Su importancia radica en que día a día se descubren vulnerabilidades en los sistemas, ya sean sitios web, bases de datos, sistemas operativos, etcétera., los cuales buscan ser solucionados por los especialistas de seguridad dentro de las actualizaciones.

2.8.6.- Exposición de Datos Sensibles

Muchas aplicaciones web no realizan una protección adecuada de los datos sensibles de los usuarios, estos datos pueden ser desde el nombre del usuario, dirección de correo electrónica, domicilio, datos de tarjetas de crédito, números telefónicos, entre otros.

Estos datos pueden ser utilizados por los atacantes para realizar fraudes o suplantación de identidad, por esa razón es importante que los desarrolladores realicen una adecuada protección de estos datos haciendo uso de métodos de cifrado y usando protocolos seguros para el intercambio de datos.

2.8.7.- Ausencia de Control de Acceso a las Funciones

La mayoría de las aplicaciones web verifican los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando este acede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada.

2.8.8.- Falsificación de Peticiones en Sitios Cruzados (CSRF).

Este tipo de vulnerabilidad obliga al navegador de un usuario autenticado a enviar peticiones HTTP falsas, las cuales incluyen la sesión del usuario y toda la información necesaria para la autenticación de este dentro del sitio web, pero esta es enviada a un aplicativo vulnerable.

El atacante puede aprovechar esta vulnerabilidad para que el navegador genere peticiones a una aplicación vulnerable, la cual pensará que son peticiones legitimas del usuario.

2.8.9.- Uso de componentes con vulnerabilidades conocidas

Esta vulnerabilidad sucede cuando el sitio web o aplicativo hace uso de extensiones para mejorar la interacción con el usuario o para hacer más atractivo el sitio.

Algunos de estos componentes podrían ser explotados por el atacante con la finalidad de obtener acceso a los archivos o directorios en los cuales se encuentra almacenado ese componente.

Por esa razón es importante que antes de agregar algún plugin al sitio web, se verifique si este no es vulnerable, debido a que eso podría ser un hueco de seguridad en las defensas de la organización.

2.8.10.- Redirecciones y reenvíos no validados

Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, esto, en ocasiones lo realizan sin una correcta validación o envío de los datos de manera segura, por lo que, un atacante puede aprovechar esta falta de seguridad para realizar redirecciones hacia sitios phishing o que contengan malware.

.

Capítulo 3

Estándares de Seguridad

Dentro de este capítulo se describirá el estándar ISO/IEC 27001:2013, se describirá su importancia dentro de la organización, ventajas competitivas en el ámbito de seguridad y elementos a considerar para realizar una correcta implementación dentro de cualquier organización.

3.1.- Estándares de Seguridad.

Un estándar de acuerdo con el Instituto de Gestión de Proyectos (PMI) es:

"*Un documento establecido por consenso, aprobado por un cuerpo reconocido, que ofrece reglas, guías o características para que se use de forma repetida."*[6]

Lo estándares permiten a la organización replicar de forma similar los procesos, esto, mediante la correcta gestión de recursos, dentro del área de la seguridad de la información estos recursos se enfocan principalmente al tratamiento seguro de los activos e información de los clientes.

Un punto importante que tomar en cuenta dentro de los estándares es, que no existe uno que se adapte completamente a una organización, debido a que cada uno proporciona bases y ventajas competitivas que deben de ser adoptados de acuerdo con las necesidades de cada empresa, la mayoría buscan una mejora basada en la implementación y retroalimentación.

3.2.- ISO 27000

ISO, organización internacional, no gubernamental encargada de proporcionar estándares para cualquier ámbito de la industria, los cuales proporcionan las bases para la implementación de Sistemas de Gestión y permiten a las organizaciones certificarse en la norma que mejor se adapte a su modelo de negocio.

En el área de Seguridad de la Información, la familia de las ISO 2700 es la que permite implementar y gestionar un Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo que toda la información utilizada dentro de la organización se maneje de manera segura.

[6]PMI, 2018. *¿Qué es un estándar?.* Recuperado de: http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Dentro de estas normas las principales que permiten implementar y mantener un SGSI son:

- ISO 27001.
- ISO 27002.
- ISO 27003.
- ISO 27004.
- ISO 27005.

ISO 27001, es la única certificable del listado, debido a que contempla todo lo que conlleva un SGSI, compuesta de 10 cláusulas y 3 anexos.

De las cláusulas, 7 son las que integran el Sistema de Gestión, mientras que el Anexo A, contiene los 114 controles que permiten disminuir los riesgos que podrían afectar a los activos de la organización.

ISO 27002, es un compendio de consejos sobre implementación de controles, debido a que, como se mencionó previamente, los estándares dicen el qué hacer, no el cómo, por lo que, está norma puede servir como guía para la implementación de controles listados en la norma ISO 27001.

ISO 27003, de manera similar a la norma ISO 27002, sirve como guía para la implementación, la diferencia es que esta norma proporciona algunos consejos para la implementación del SGSI desde la planeación inicial para poder comenzar con un sistema y la aprobación por parte de la Alta Dirección, hasta la certificación.

ISO 27004, contiene una serie de mejores prácticas para medir el desempeño del SGSI, es decir, el cumplimiento o resultados obtenidos que permitan llegar a los objetivos planteados del sistema permite establecer que parámetros son los que se desean medir, cómo medirlos y cuándo.

ISO 27005, proporciona las directrices para la gestión de los riesgos que podrían afectar a los activos de información de la organización, es un apoyo muy importante para las cláusulas 6 y 8 de la norma ISO 27001.

Cómo se mencionó anteriormente, la norma certificable es la ISO 27001, por esa razón, a continuación, se describirá de forma detallada cómo se compone la norma, significado de cada cláusula, descripción de los controles, planes de contingencia y metodologías de análisis de riesgos.

3.2.1.- Ciclo de Deming

Para comenzar, es importante mencionar que los Sistemas de Gestión están basados en el ciclo de Deming, utilizado para mejora continua y el cuál se compone de 4 fases:

- Plan.
- Do.
- Check.
- Act.

Plan, el primer paso consiste en determinar que procesos o actividades son necesarias mejorar para el crecimiento de la organización, estás pueden involucrar personal, equipo, materia prima, documentación, etcéteraétera.

Do, en esta etapa se realizan los cambios dentro de los procesos a mejorar, estos cambios pueden realizarse en un entorno de prueba para evitar afectaciones dentro de los procesos reales de la organización.

Check, una vez realizados los cambios y superado un período de prueba, se deben de revisar que estos hayan sido efectivos, para determinarlo se debe realizar una comparación de los resultados obtenidos con los esperados.

Act, si los resultados obtenidos cumplen con los objetivos esperados se deben de realizar los cambios, de forma contraria, se deberán implementar nuevas medidas y comenzar el ciclo de nuevo para verificar que estas hayan sido efectivas.

3.2.2.- ISO 27001

Las 10 cláusulas que componen la norma son las siguientes:

0. Introducción.
1. Alcance y campo de aplicación.
2. Referencias normativas.
3. Términos y definiciones.
4. Contexto organizacional.
5. Liderazgo.
6. Planificación.
7. Apoyo.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

Cláusula 0, no se contempla dentro de SGSI, debido a que solamente proporciona una introducción al contenido de la norma.

Cláusula 1, define el campo de aplicación de la norma dentro de la organización.

Cláusula 2, proporciona una breve descripción de la familia de las normas 27000.

Cláusula 3, es un listado de términos utilizados dentro de la norma, que permiten tener un vocabulario en común para todos aquellos que tengan alguna relación con la implementación, gestión, mantenimiento o mejora del SGSI.

Cláusula 4, a partir de este punto y hasta el número 10, se contemplarán dentro del SGSI y serán auditados; se compone de 4 sub-cláusulas:

> *4.1. Comprender la organización y su contexto.*
> Para este punto se debe identificar cual es el rol de la organización, dónde se encuentra ubicada, que aspectos internos y externos podrían afectar los objetivos de la organización.

4.2. Comprender las necesidades y expectativas de las partes interesadas. Consiste en definir quiénes tendrán alguna relación con el proceso que funcionará como base del SGSI, los cuales pueden ser proveedores, personal encargado de realizar las actividades, clientes, etcéteraétera.

4.3.- Determinar el alcance del Sistema de Gestión de la Seguridad de la Información.
Se debe definir cuál o cuáles serán los procesos que se certificarán dentro de la organización, para definirlo de forma correcta, se debe analizar cuál de ellos proporcionaría mayor valor a la organización (ventaja competitiva, solicitud de alguno de los clientes, prestigio, etcétera.), es recomendable que, si el SGSI aún no está implementado, solamente se certifique un proceso.

4.4 Sistema de Gestión de la Seguridad de la Información.

Consiste en implementar cada una de las cláusulas siguientes listadas dentro de la norma.

Cláusula 5, contiene a su vez las siguientes 3 sub-cláusulas:

5.1. Liderazgo y compromiso.

Dentro de este apartado, la Alta Dirección debe de proveer todo lo necesario para el cumplimiento de los objetivos propuestos en la cláusula 4, esto mediante el compromiso de esta con el SGSI, comunicando y apoyando al personal involucrado en el proceso certificado, realizando revisiones constantes de los controles implementados para proveer mejoras al sistema.

5.2. Política.

Se debe establecer como mínimo una política de seguridad de la información, en la cual se deben de detallar los objetivos del sistema, los cuales, a su vez, deben de permitir lograr los objetivos de la organización, además, esta política debe ser conocida por todo el personal que tenga alguna relación con el proceso y debe encontrarse disponible en todo momento para su consulta.

5.3. Roles organizacionales, responsabilidades y autoridades.

Para este punto, deben de asignarse roles dentro de la organización, relacionados a la seguridad de la información, es decir, segregar tareas para evitar accesos no autorizados o fuga de información.

Cláusula 6, compuesta de 2 sub-cláusulas:

6.1 Acciones para abordar los riesgos y las oportunidades.

De acuerdo al análisis realizado en la Cláusula 4, se obtendrá la información necesaria para comprender el entorno de la organización, a partir del cual se podrán identificar los riesgos que podrían afectar a los activos de información, dentro de este punto, se deben determinar cuáles son esos riesgos, tanto internos como externos, que aceptación del riesgo está dispuesta la organización a gestionar, quiénes son los encargados de proporcionar alguna solución en caso de que el riesgo se presente y finalmente determinar que controles del Anexo A, serán utilizados para disminuir estos riesgos, para establecer de forma detallada que controles se utilizarán se hace uso de una Declaración de Aplicabilidad (SoA), que contiene un listado de los 114 controles y se debe definir:

- Controles implementados y referencias a los mismos.
- En caso de no implementarse, describir porque no aplica para la organización.
- Si se encuentra en proceso de implementación, se debe describir en que punto de la implementación se encuentra.

6.2 Objetivos de seguridad de la información y planificación para lograrlos.

Se deben definir los objetivos que se desean lograr con el SGSI, los cuales es recomendable que sean basados en la metodología SMART (específico, medible, alcanzable, relevante y con un tiempo determinado), ya que de esta forma se podrán generar objetivos reales y planificados de forma correcta.

Además, se debe describir quien es el responsable de realizar las acciones necesarias para el cumplimiento de los objetivos, en cuanto tiempo, recursos necesarios y que resultados se esperan obtener.

Cláusula 7, contiene 5 sub-cláusulas:

7.1 Recursos.

Se deben definir los recursos tanto materiales, tecnológicos, humanos, etcétera., que serán necesarios para que el SGSI pueda implementarse, mantenerse y retroalimentarse de forma continua.

7.2 Competencias.

La Alta Dirección debe determinar que competencias debe tener el personal que se encuentra dentro del proceso certificado y en caso de no tenerlas realizar las acciones necesarias para la obtención de estas, esto puede ser mediante capacitaciones o generando una documentación detallada de que tareas se deben de realizar para llevar a cabo correctamente una tarea en específico.

7.3 Conocimiento.

Como se mencionó anteriormente, todo el personal involucrado con los procesos que se encuentren certificados por la norma, deben conocer las políticas de seguridad que formen parte del SGSI, a su vez, deben comprender la importancia de su apoyo para el crecimiento del SGSI y finalmente, que consecuencias conlleva el no seguir las políticas y lineamientos implementados.

7.4 Comunicación.

Debe definirse qué información será comunicada, cuándo y quién será el encargado de comunicarla, es decir, que cambios o mejoras al sistema, deben de ser informados a las personas involucradas, para de esta manera poder determinar si afecta de alguna manera a la realización de sus procesos.

7.5 Información documentada.

Toda la información que componga al SGSI debe de encontrarse disponible, legible y actualizada, además debe de contarse con un control que permita diferenciar el contenido de los documentos, esto mediante identificadores, clasificación de la información, versionado, etcéteraétera.

Además, debe definirse en que medios será almacenada la información, de qué forma será su tratamiento en caso de ser necesaria su eliminación y finalmente, de acuerdo con la clasificación que se tenga, que tipo de protección debe otorgarse a la información que se encuentre clasificada como confidencial.

Cláusula 8, se definen las siguientes 3 sub-cláusulas:

8.1 Control y planificación operacional.

Comprende la planificación, implementación y control de los procesos que se encuentran certificados dentro del SGSI, consiste en determinar en qué tiempo se llevarán a cabo las acciones definidas en el punto 6.1.

8.2 Evaluación de riesgo de la seguridad de la información.

Se deben realizar evaluaciones potenciales riesgos, siempre que la Alta Dirección lo considere necesario o cuando se realice alguna modificación a los activos o infraestructura de los procesos.

8.3 Tratamiento de riesgo de la seguridad de la información.

Se debe implementar un plan de tratamiento de riesgos, en el cual se debe definir qué controles se implementarán y de qué manera.

Cláusula 9, divida en 3 sub-cláusulas:

9.1 Monitoreo, medición, análisis y evaluación.

La Alta Dirección debe definir qué procesos deben de ser monitoreados, en que intervalos de tiempo y de qué forma, a su vez, los controles implementados a partir del tratamiento de riesgos también deben de ser monitoreados, para determinar su efectividad y decidir si estos redujeron los riesgos encontrados dentro del análisis.

9.2 Auditoría Interna.

Es un proceso en el cual se realiza una revisión de la información generada por el SGSI y el cumplimiento de la misma con la norma, se deben realizar a un intervalo planificado, además el auditor interno, debe de ser ajeno a los procesos de la organización, para que la auditoría se lleve de la manera más imparcial posible y pueda proporcionar algún beneficio al SGSI.

9.3 Revisión de gestión.

Se debe realizar una revisión planificada del SGSI, en donde se analicen los resultados obtenidos a partir de alguna de las siguientes fuentes:

- Auditorías Internas.
- Monitoreo.
- Comentarios de las partes interesadas.

A partir del análisis de esta información, se deberán tomar las medidas que permitan mejorar al sistema.

Cláusula 10, se compone de 2 sub-cláusulas:

10.1 No conformidades y acciones correctivas.

Se deben determinar las acciones a realizar para la solución de no conformidades derivadas tanto de auditorías internas como externas, para evitar que estas vuelvan a suceder, para ello se debe de realizar su implementación y seguimiento, para verificar que las acciones tomadas, proporcionan algún cambio positivo.

10.2 Mejora continua.

Finalmente, una vez terminado el ciclo, se debe comenzar nuevamente, basándose en las oportunidades de mejora detectadas durante todo el proceso.

3.2.2.1.- Controles

Como se menciona en la cláusula 6, existen controles que proporciona la norma para poder reducir los riesgos que podrían afectar a los procesos de la organización, esos controles se encuentran divididos en 14 objetivos de control:

A. 5. Políticas de seguridad de la información.

A. 6. Organización de la seguridad de la información.

A. 7. Seguridad ligada a los recursos humanos.

A. 8. Administración de activos.

A. 9. Control de acceso.

A. 10. Criptografía.

A. 11. Seguridad física y del ambiente.

A. 12. Seguridad de las operaciones.

A .13. Seguridad de las comunicaciones.

A. 14. Adquisición, desarrollo y mantenimiento del sistema.

A. 15. Relaciones con el proveedor.

A. 16. Gestión de incidentes de seguridad de la información.

A. 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

A. 18. Cumplimiento.

Los controles contenidos dentro de los objetivos de control son solamente una guía de medidas a implementar, pero no contiene una descripción detallada de cómo realizar esa actividad.

A.5 Políticas de seguridad de la información, dentro de este objetivo, se encuentran dos controles:

A.5.1 Orientación de la dirección para la seguridad de la información.

A.5.1.1 Políticas para la seguridad de la información, este control se encuentra ligado a la cláusula 4, en la cual como su nombre lo dice, se debe definir una política de seguridad de la información que considere a todas las partes interesadas del SGSI.

A. 5.1.2 Revisión de las políticas de seguridad de la información, una vez generada la política, esta debe de ser revisada por la Alta Dirección a intervalos planificados, esto con la finalidad de determinar si es necesaria su actualización.

A.6 Organización de la seguridad de la información, contiene 7 controles, divididos en dos apartados:

A.6.1 Organización interna.

A.6.1.1 Roles y responsabilidades de la seguridad de la información, se deben designar que actividades relacionadas a la protección de la información y de los activos que debe de realizar el personal dentro de la organización.

A.6.1.2 Segregación de funciones, permite asignar distintas jerarquías o niveles necesarios para la protección de la información y evitar accesos no autorizados debido a errores de configuración.

A.6.1.3 Contacto con autoridades, se deben de contemplar todas las entidades que permitan a la organización llevar a cabo las actividades necesarias, estas pueden ser desde los proveedores, bomberos, protección civil, etcéteraétera.

A.6.1.4 Contacto con grupos especiales de interés, se deben establecer relaciones con otros grupos especializados en el área de seguridad de la información, especialmente con Equipos de Respuesta a Incidentes (CERT), para poder obtener una ventaja competitiva y mayor conocimiento en el campo de la seguridad.

A.6.1.5 Seguridad de la información en la gestión de proyecto, se deben establecer las medidas de seguridad mínimas para la realización de los proyectos, sin importar que estos no estén relacionados con el área de seguridad de la información.

A.6.2 Dispositivos móviles y trabajo remoto.

A.6.2.1 Política de dispositivos móviles, esta política debe de contemplar los requerimientos mínimos en seguridad que deben de cumplir los dispositivos inteligentes personales utilizados por parte de los empleados de la organización, esto, para evitar la relación de información personal con información laboral.

A.6.2.2 Trabajo remoto, se deben de establecer medidas que permitan al personal laboral desde su hogar, para poder seguir realizando sus actividades en caso de alguna contingencia, una de las medidas más utilizadas para este control es el uso de una VPN.

A.7 Seguridad ligada a los recursos humanos, contiene 6 controles, divididos en 3 apartados:

A.7.1 Previo al empleo.

A.7.1.1 Selección, se debe determinar cuáles son las competencias y conocimientos con los que deben de contar los candidatos a laboral dentro de la organización, para que el ingreso de este sea de una manera más sencilla y no se vean afectados los procesos.

A.7.1.2 Términos y condiciones de la relación laboral, una vez realizada la selección, se debe dar a conocer al empleado que actividades va a realizar, quiénes son sus responsables, cuál es el personal a su cargo, etcéteraétera.

A.7.2 Durante el empleo.

A.7.2.1 Responsabilidad de la dirección, todas las actividades realizadas deben de hacerse tomando en cuenta la seguridad de la información utilizada, por esa razón la Alta Dirección, debe solicitar a todos los empleados que apliquen la misma dentro de sus labores.

A.7.2.2 Concientización, educación y formación en seguridad de la información, se debe capacitar a los empleados de recién ingreso en las medidas utilizadas para la seguridad de la información dentro de la organización.

A.7.2.3 Proceso disciplinario, se deben determinar un conjunto de sanciones que se llevarán a cabo en caso de incumplimiento en alguno de los aspectos que contemplan el SGSI.

A.7.3 Desvinculación y cambio de empleo.

A.7.3.1 Responsabilidades en la desvinculación o cambio de empleo, debe existir un procedimiento formal para la baja de personal, esto debe implicar, devolución de la información y activos a su cargo, revocación de los derechos de acceso a los sistemas, etcéteraétera.

A.8 Administración de activos, contiene 10 controles, divididos en 3 apartados:

A.8.1 Responsabilidades por los activos.

A.8.1.1 Inventario de activos, todos los activos utilizados dentro de los procesos certificados de la norma deberán de ser identificados dentro de un inventario, el cual deberá de ser revisado a intervalos constantes de tiempo.

A.8.1.2 Propiedad de los activos, además del inventario, debe de ser de conocimiento de todo el personal, quiénes son los encargados de gestionar esos activos y tomar las medidas necesarias para la solución y respuesta en caso de afectación de estos.

A.8.1.3 Uso aceptable de los activos, una vez definidos los dueños de los activos, se deben establecer los lineamientos de uso de estos, para evitar daños o afectaciones a estos.

A.8.1.4 Devolución de activos, cuando finalice la relación laboral, el empleado deberá devolver los activos a su responsabilidad en las mismas condiciones en que le fueron entregados al iniciar sus labores.

A.8.2 Clasificación de la información.

A.8.2.1 Clasificación de la información, se deben establecer parámetros para clasificar la información, de acuerdo con el valor de la misma, la afectación que podría causarse en caso de acceso o modificación no autorizada.

A.8.2.2 Etiquetado de la información, se deben generar los identificadores necesarios que permitan organizar la información de acuerdo con los parámetros generados a partir del control anterior.

A.8.2.3 Manejo de activos, adicionalmente, los activos deberán de ser gestionados de acuerdo con la misma clasificación de información generada del control A.8.2.1.

A.8.3 Manejo de los medios.

A.8.3.1 Gestión de los medios removibles, se deben implementar las medidas para el uso de dispositivos removibles, basándose en la clasificación de la información.

A.8.3.2 Eliminación de los medios, se deben establecer las reglas de borrado seguro de la información contenida en los medios removibles una vez que esta ya no es necesaria.

A.8.3.3 Transferencia física de medios, la información que así lo requiera deberá de ser protegida durante el transporte de está fuera de la organización.

A.9 Control de acceso, contiene 14 controles, los cuales se encuentran divididos en 4 apartados:

A.9.1 Requisitos de negocio para el control de acceso.

A.9.1.1 Política de control de acceso, dentro de esta deberá especificarse quiénes tienen acceso a la organización tanto física como lógicamente y a través de qué medios.

A.9.1.2 Acceso a las redes y a los servicios de red, basándose en los roles y responsabilidades de cada puesto, se deberán generar los accesos necesarios para cada usuario dentro de los sistemas de la organización.

A.9.2 Gestión de acceso al usuario.

A.9.2.1 Registro y cancelación de registro de usuario, para este control se deberá establecer un procedimiento formal de alta y baja de usuarios a los sistemas.

A.9.2.2 Asignación de acceso de usuario, adicionalmente deberá existir un procedimiento para la solicitud de accesos por parte de los responsables de los procesos hacía los administradores de sistemas.

A.9.2.3 Gestión de derechos de acceso privilegiados, a partir de la segregación de tareas, solamente los administradores de los sistemas deberán tener la capacidad de proporcionar los derechos de acceso.

A.9.2.4. Gestión de información secreta de autenticación de usuarios, deberán implementarse los mecanismos necesarios para proteger las credenciales de acceso de los usuarios.

A.9.2.5 Revisión de los derechos de acceso de usuario, deberán realizarse revisiones periódicas de los accesos, para verificar su validez de acuerdo con los procesos de la organización.

A.9.2.6 Eliminación o ajuste de los derechos de acceso, debe existir un procedimiento formal para la baja de los privilegios, desde la notificación hasta la eliminación o suspensión de una cuenta, en caso de requerirlo, deberán contemplarse las modificaciones de las funciones de la cuenta.

A.9.3 Responsabilidades del usuario.

A.9.3.1 Uso de información de autenticación secreta, se deben establecer las medidas de seguridad y de uso de la información de acceso a los sistemas, las cuales deben de ser comunicadas a todo el personal para evitar fuga de información y accesos no autorizados.

A.9.4 Control de acceso al sistema y aplicaciones.

A.9.4.1 Restricción de acceso a la información, a partir de la política de control de acceso y a las funciones de cada puesto, será la información a la que tendrá acceso la cuenta de cada usuario.

A.9.4.2 Procedimiento de inicio de sesión seguro, se deberán implementar las medidas necesarias que permitan el acceso de manera segura a los sistemas de la organización.

A.9.4.3. Sistema de gestión de contraseñas, se deben establecer los lineamientos que permitan generar contraseñas robustas y seguras, solicitando un cambio constante de las mismas.

A.9.4.4 Uso de programas utilitarios privilegiados, de acuerdo con las funciones de cada puesto, deberán gestionarse los comandos y programas que podrá ejecutar el usuario.

A.9.4.5 Control de acceso al código fuente de los programas, solamente el personal autorizado y que lo requiera, podrá tener acceso al código fuente de los programas.

A.10 Criptografía, contiene 2 controles de la norma:

A.10.1 Controles criptográficos.

A.10.1.1 Política sobre el uso de controles criptográficos, se deberá establecer una política que defina el uso de controles criptográficos y se especifique para que tipo de información deberán de ser utilizados.

A.10.1.2. Gestión de claves, deberán establecerse los parámetros a utilizar para los controles criptográficos, tiempo de vida de las llaves y cómo protegerán la información.

A.11 Seguridad física y del ambiente, contiene 15 controles divididos en 2 apartados:

A.11.1 Áreas seguras

A.11.1.1 Perímetro de seguridad física, deberá establecerse un área segura que permita la protección de la información crítica para la organización y a su vez se garantice la seguridad física de los empleados y activos.

A.11.1.2 Controles de acceso físico, estos controles contemplan el uso de biométricos para personal autorizado y bitácoras para personal ajeno a la organización, esto con la finalidad de llevar un registro de quién tuvo acceso a qué área de la organización.

A.11.1.3 Seguridad de oficinas, salas e instalaciones, deben establecerse las medidas de seguridad físicas necesarias dentro de la organización, es decir, todas aquellas que permitan evitar accesos no autorizados o afectaciones a los activos.

A.11.1.4 Protección contra amenazas externas y del ambiente, deberán establecerse controles para la protección de los activos contra desastres naturales, ataques dirigidos o accidentes.

A.11.1.5 Trabajo en áreas seguras, deberán proporcionarse procedimientos que aseguren que las labores se realizan en áreas seguras tanto para el personal, como para los activos de seguridad.

A.11.1.6 Áreas de entrega y carga, se deben establecer áreas para entrega y carga por parte de proveedores, con la finalidad de evitar accesos físicos no autorizados y fuga de información.

A.11.2 Equipamiento.

A.11.2.1 Ubicación y protección del equipamiento, todos los activos como servidores, equipos de cómputo, equipos de red, deberán ubicarse en puntos estratégicos que permitan evitar las afectaciones que podrían suceder por desastres naturales o perpetrados por el hombre y accesos no autorizados.

A.11.2.2 Elementos de soporte, se deben contemplar las medidas de seguridad contra cambios de suministro de energía que podrían afectar a los activos.

A.11.2.3 Seguridad en el cableado, se deberá proteger el cableado eléctrico y de telecomunicaciones que podrían afectar la disponibilidad de los activos utilizados dentro de los procesos de la organización.

A.11.2.4. Mantenimiento del equipamiento, deberá realizarse el correcto mantenimiento de los equipos, a intervalos planificados para mantenerlos en un correcto funcionamiento y actualizados.

A.11.2.5. Retiro de activos, debe llevarse un registro de los activos retirados, los cuales no podrán salir de la organización sin una autorización previa.

A.11.2.6 Seguridad del equipamiento y los activos fuera de las instalaciones, deberán generarse medidas de seguridad que permitan proporcionar el mismo nivel de seguridad a los activos tanto dentro como fuera de la organización.

A.11.2.7 Seguridad en la reutilización o descarte de equipos, previo a la eliminación de algún activo, deberá validarse que no contiene información sensible de la organización.

A.11.2.8 Equipo de usuario desatendido, deberán establecerse los procedimientos necesarios, para evitar la fuga de información que podría suceder a través de los equipos de cómputo.

A.11.2.9 Política de escritorio y pantalla limpios, implica mantener la pantalla del equipo de cómputo sin ningún documento que contenga información sensible de la organización, así como el escritorio del personal sin papeles que puedan revelar información confidencial.

A.12 Seguridad de las operaciones, contiene 14 controles, divididos en 7 secciones:

A.12.1 Procedimientos operacionales y responsabilidades.

A.12.1.1 Procedimientos de operación documentados, se deben documentar los procesos importantes dentro de la organización y estar disponibles para todo el personal que así lo requiera.

A.12.1.2 Gestión de cambios, todos los cambios que se realicen dentro de la organización, ya sea información, infraestructura o personal deberán ser registrados.

A.12.1.3 Gestión de la capacidad, se deben validar que los recursos con los que cuenta la organización serán suficientes para las actividades que se realizan dentro de la mismas, para que, en caso de no cumplirlas, tomar las medidas necesarias para la mejora de esos recursos.

A.12.1.4 Separación de los ambientes de desarrollo, prueba y operacionales, para evitar accesos no autorizados a la información a entornos de desarrollo y propagación de malware en entornos operacionales.

A.12.2 Protección contra código malicioso.

A.12.2.1 Controles contra código malicioso, se deben establecer las medidas de protección necesarias contra código malicioso, estas medidas deberán contemplar la detección, prevención, eliminación y recuperación ante esos ataques.

A.12.3 Respaldo.

A.12.3.1 Respaldo de la información, se deberán generar respaldos de la información crítica de la organización, realizándose y verificándolos a intervalos planificados.

A.12.4 Registro y monitoreo.

A.12.4.1 Registro de evento, se deberá tener un registro de todas las personas que se encuentren dentro de la organización, para que de esta manera exista la posibilidad de realizar una conexión entre un incidente de seguridad y una persona involucrada en el mismo.

A.12.4.2 Protección de la información de registros, la información obtenida de estos registros deberá almacenarse y protegerse contra accesos no autorizados y alteraciones.

A.12.4.3 Registros del administrador y el operador, todas las acciones realizadas por los administradores de sistemas deberán quedar registradas dentro de las bitácoras de estos.

.

A.12.4.4 Sincronización de relojes, se deben de sincronizar los relojes a una sola fuente horaria.

A.12.5 Control del software de operación.

A.12.5.1 Instalación del software en sistemas operacionales, se deben establecer los procedimientos que permitan controlar la instalación de software sobre los sistemas de la organización.

A.12.6 Gestión de la vulnerabilidad técnica.

A.12.6.1 Gestión de las vulnerabilidades técnicas, se deben realizar pruebas para determinar que vulnerabilidades existen sobre los sistemas y proporcionar soluciones a estos.

A.12.6.2 Restricciones sobre la instalación de software, se deben establecer las reglas y software permitido dentro de los equipos de los usuarios.

A.12.7 Consideraciones de la auditoría de los sistemas de información.

A.12.7.1 Controles de auditoría de sistemas de información, se deben realizar a intervalos planificados revisiones de los sistemas operativos de los usuarios y de los sistemas que forman parte de la infraestructura crítica de la organización.

A.13 Seguridad de las comunicaciones, contiene 7 controles divididos en 2 apartados:

A.13.1 Gestión de la seguridad de red.

A.13.1.1 Controles de red, se deben gestionar y controlar las redes que permiten los accesos a los sistemas de información.

A.13.1.2 Seguridad de los servicios de red, se deben establecer los niveles de servicio mínimos, requerimientos de seguridad y recursos necesarios para la implementación de las redes, esto, ya sea proporcionado por la organización o por terceros.

A.13.1.3 Separación en las redes, se deben segregar las redes de acuerdo con los grupos de servicio y a los roles pertinentes de cada usuario.

A.13.2 Transferencia de información.

A.13.2.1 Políticas y procedimientos de transferencia de información, se debe implantar una política que establezca los procedimientos y controles necesarios para la transferencia de información.

A.13.2.2 Acuerdos sobre transferencia de información, deben establecerse los procedimientos necesarios para la transferencia de la información, tanto dentro como fuera de la organización.

A.13.2.3 Mensajería electrónica, la información enviada a través de este medio y considerada como sensible, deberá de protegerse con los controles necesarios, como por ejemplo el uso de criptografía.

A.13.2.4 Acuerdos de confidencialidad o no divulgación, se deben establecer requisitos de confidencialidad y no divulgación tanto para el personal que labora en la organización, como para terceras partes.

A.14 Adquisición, desarrollo y mantenimiento del sistema, compuesto de 13 controles, divididos en 3 secciones:

A.14.1 Requisitos de seguridad de los sistemas de información.

A.14.1.1 Análisis y especificación de requisitos de seguridad de la información, se deben establecer los requerimientos mínimos de seguridad para todos los sistemas de información que se implementen dentro de la organización.

A.14.1.2 Aseguramiento de servicios de aplicación en redes públicas, se deben proteger los servicios que se encuentren públicos contra todos los posibles ataques que podrían afectarlos.

A.14.1.3 Protección de las transacciones de servicios de aplicación, todos los intercambios de información sensible que sucedan a través de los sistemas de la organización deberán realizarse sobre un canal de información cifrado, con el fin de evitar el robo de esa información.

A.14.2 Seguridad en procesos de desarrollo y soporte.

A.14.2.1 Política de desarrollo seguro, se deben establecer los procedimientos y metodologías para el desarrollo seguro de sistemas.

A.14.2.2 Procedimientos de control de cambios del sistema, todos los cambios o actualizaciones realizadas en los sistemas deberán de ser registrados para determinar las mejoras o posibles vulnerabilidades que estos pudieran tener.

A.14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación, se deben realizar revisiones a los sistemas para determinar posibles vulnerabilidades a partir de los cambios realizados.

A.14.2.4 Restricciones en los cambios a los paquetes de software, se deben establecer las reglas necesarias para las modificaciones que se realizan sobre los sistemas, para evitar cambios no necesarios sobre estos.

A.14.2.5 Principios de ingeniería de sistema seguro, se deben determinar e implementar principios de desarrollo seguro para los sistemas.

A.14.2.6 Entorno de desarrollo seguro, se deben implementar las medidas necesarias para proteger los entornos de desarrollo, esto implica, privilegios de acceso a las diferentes áreas del entorno.

A.14.2.7 Desarrollo tercerizado, en caso de que el desarrollo del sistema sea realizado por terceras partes, deberá solicitarse el cumplimiento de los requerimientos mínimos de seguridad que se esperan por parte de la organización.

A.14.2.8 Pruebas de seguridad del sistema, se deben realizar pruebas de funcionalidad del sistema, antes de la implementación a la operación de cualquier sistema.

A.14.2.9 Pruebas de aprobación del sistema, se deben definir los criterios mínimos de aceptación de los sistemas y realizar las revisiones y aprobaciones pertinentes de los mismos.

A.14.3 Datos de prueba.

A.14.3.1 Protección de datos de prueba, los datos utilizados para las pruebas de los sistemas no deberán tener ninguna relación con información de la organización, esto para evitar la fuga de esta.

A.15 Relaciones con el proveedor, contiene 5 controles divididos en 2 secciones:

A.15.1 Seguridad de la información en las relaciones con el proveedor.

A.15.1.1 Política de seguridad de la información para las relaciones con el proveedor, se deben establecer los requisitos de seguridad necesarios con los que deben de cumplir los proveedores.

A.15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor, los requisitos de seguridad de la información deberán de ser aclarados con los proveedores, con la finalidad de permitir su cumplimiento.

A.15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones, se deben establecer los requisitos de seguridad durante todo el proceso realizado por los proveedores donde se involucre la información de la organización.

A.15.2 Gestión de entrega del servicio del proveedor.

A.15.2.1 Supervisión y revisión de los servicios del proveedor, se deben establecer los requerimientos mínimos de servicio que se esperan por parte del proveedor, para verificar su cumplimiento, es recomendable realizar auditorías a estos.

A.15.2.2 Gestión de cambios a los servicios del proveedor, en caso de cambios en los procesos, infraestructura o cualquier ámbito de la organización, se deberán reestructurar los requerimientos que se deben cumplir con el proveedor, los cuales deberán quedar registrados.

A.16 Gestión de incidentes de seguridad de la información, contiene los siguientes 7 controles:

A.16.1 Gestión de incidentes de seguridad de la información y mejoras.

A.16.1.1 Responsabilidades y procedimientos, se deben tener registrados los procedimientos para el tratamiento de incidentes de seguridad dentro de la organización, quiénes son los responsables de atenderlos y darles seguimiento para una solución eficiente.

A.16.1.2 Informe de eventos de seguridad de la información, se deben informar a los involucrados sobre el incidente, para su pronta solución.

A.16.1.3 Informe de debilidades de seguridad de la información, se debe impulsar al personal a notificar cualquier vulnerabilidad detectada dentro de los sistemas que están a su cargo.

A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información, se deben analizar los incidentes, para determinar si se deben de atender de acuerdo con las políticas implementadas dentro del SGSI, procesos y criticidad de los activos de información que se tengan en la organización.

A.16.1.5 Respuesta ante incidentes de seguridad de la información, los incidentes se deben de atender de acuerdo con los procedimientos que se tengan documentados dentro de la organización.

A.16.1.6 Aprendizaje de los incidentes de seguridad de la información, se debe determinar que mejoras se pueden realizar al SGSI a partir de la solución de los incidentes.

A.16.1.7 Recolección de evidencia, se debe guardar un registro sobre el incidente de seguridad de la información, la causa que originó ese incidente y qué medidas se tomaron para su solución.

A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio, contempla 4 controles, dentro de 2 secciones:

A.17.1 Continuidad de la seguridad de la información.

A.17.1.1 Planificación de la continuidad de la seguridad de la información, se deben establecer planes que permitan a la organización seguir operando ante cualquier contingencia.

A.17.1.2 Implementación de la continuidad de la seguridad de la información, se deben realizar pruebas de los planes para verificar su utilidad.

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información, se deben revisar los planes y mejorar de acuerdo con los cambios que sufra la organización.

A.17.2 Redundancias.

A.17.2.1 Disponibilidad de las instalaciones de procesamiento de la información, se deben replicar todos los sistemas de información que sean considerados como críticos para la operación.

A.18 Cumplimiento, contiene los últimos 8 controles, divididos en 2 apartados:

A.18.1 Cumplimiento con los requisitos legales y contractuales.

A.18.1.1 Identificación de la legislación vigente y los requisitos contractuales, se deben identificar las leyes tanto nacionales como internacionales en materia de seguridad que sean aplicables al entorno de negocio de la organización.

A.18.1.2 Derechos de propiedad intelectual, se deben proteger, en caso de ser necesario, los desarrollos o patentes propias de la organización.

A.18.1.3 Protección de los registros, los registros de eventos, es decir, bitácoras, registros de incidentes de seguridad de la información, entre otros, deberán de ser resguardados y almacenados durante el tiempo que se considere pertinente.

A.18.1.4 Privacidad y protección de la información de identificación personal, toda la información de los empleados, clientes y proveedores deberá de contar con los mecanismos de protección necesarios para evitar accesos no autorizados a ella.

A.18.1.5 Regulación de los controles criptográficos, los controles criptográficos utilizados por la organización deberán cumplir con la legislación y regulaciones pertinentes.

A.18.2 Revisiones de seguridad de la información.

A.18.2.1 Revisión independiente de la seguridad de la información, se deben establecer revisiones del sistema a intervalos planificados, con el fin de mejorar las posibles fallas que existan.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad, cada responsable del proceso deberá revisar que el personal a su cargo, la infraestructura y procedimientos cumplan con las políticas y normatividad establecida dentro de la organización.

A.18.2.3 Verificación del cumplimiento técnico, se deben revisar los sistemas de información para validar su cumplimiento con los requisitos mínimos solicitados por la organización.

3.3.- Metodologías de análisis de riesgos.

El punto medular de la norma ISO/IEC 27001:2013 es el análisis de riesgos, como se puede observar en las cláusulas 6 y 8 de la misma, este análisis nos permite identificar, cuantificar y valorar distintas acciones o elementos que podrían causar algún daño a los activos de información de la organización.

Existen diversas metodologías, dentro de este trabajo se describirán 2 de las metodologías más conocidas, las cuales se listan a continuación:

- Octava Allegro.
- Mehari.

Aunque es importante destacar que cada organización puede generar su propia metodología para análisis de riesgos siempre y cuando esta sea entendible y fácilmente replicable.

3.3.1.- Octave Allegro.

Esta metodología fue desarrollada por la Universidad de Carnegie Mellon, se encuentra dividido en 3 categorías:

- Octave puro.
- Octave S.
- Octave Allegro.

Se utilizan de acuerdo con la cantidad de personal con el que cuente la organización, por lo que, cada uno es más complejo que el anterior.

Octave Allegro es el más simple dentro de la metodología, se compone de 8 fases divida en 10 hojas de trabajo, en las cuales se deberá introducir la información de acuerdo con los parámetros de la organización.

Fase 1, establecimiento de los criterios de medición del riesgo: La metodología provee 5 áreas de impacto o criterios de medición del riesgo, que son:

- Financiero.
- Productividad.
- Seguridad y Salud.
- Multas y Penas Legales.
- Reputación y Confianza del cliente.

Adicionalmente, se puede agregar otras áreas que sean consideradas importantes para el logro de los objetivos de la organización.

Estas áreas deben de clasificarse con valores del 1 al 5 (en caso de que no se agregue otra área), donde el número mayor corresponderá al área que sea de mayor importancia para la organización y el 1, el de menor importancia.

Además, se deben de establecer 3 tipos de impacto (Alto, Medio y Bajo) donde se deberán de describir qué consecuencias o afectaciones sucederán si ese criterio de medición se ve afectado.

De acuerdo con los criterios que se establezcan, se deberá generar una matriz, en la cual se determine hasta qué puntuación y qué probabilidad de ocurrencia, está dispuesta la organización a aceptar.

Esta información deberá escribirse en las hojas de trabajo de la 1 a la 6 de Octave Allegro, la priorización de estas deberá verse reflejada en la hoja de trabajo número 7.

Fase 2, desarrollo del perfil de los activos: Se deben identificar cuáles son los activos que forman parte del proceso certificado dentro del SGSI, es decir, todos los activos técnicos, físicos y humanos que permiten realizar las actividades que dan vida al proceso.

Además, se deben definir quiénes son los responsables y custodios encargados de gestionar el desarrollo y protección de los activos, la descripción que se desarrolle de cada activo debe establecer claramente cuáles son los requisitos de seguridad fundamentales para la protección de este.

Fase 3, identificación de los contenedores de los activos: Se deben describir los repositorios en los cuales almacena la información de los activos descritos en la fase anterior, estos pueden ser físicos, técnicos o humanos, a su vez, se deben identificar a los responsables de la protección de estos.

Fase 4, identificación de las áreas de preocupación: Se determinan las actividades que podrían causar algún daño a los activos, las áreas deben detallarse de la manera más clara posible en un solo enunciado, además se debe describir quién podría realizar esa acción, a través de qué medios y por qué motivo.

Fase 5, identificación de los escenarios de amenaza: Una vez determinadas las áreas de preocupación, se deben extender a escenarios de amenaza, a través de los cuales se detalla más a fondo cada uno de los puntos descritos anteriormente, para el caso de los actores, existen distintas clasificaciones, como lo son:

- Actor humano utilizando medios técnicos: Dentro de esta categoría se encuentran todos los ataques informáticos, es decir, todos aquellos que sean realizados por el hombre a través de un equipo de cómputo.
- Actor humano utilizando medios físicos: Dentro de esta clasificación se encuentran todas las afectaciones que podrían suceder por parte de accesos físicos no autorizados, es decir, daños físicos a los servidores, equipos de cómputo o infraestructura en general de la organización.
- Terceros: Son aquellas afectaciones que podrían suceder por parte de los proveedores de servicio con los que cuenta la organización.
- Otros: Finalmente, dentro de esta clasificación se encuentran los desastres naturales, malware, incendios, huelgas y todo aquello que forme parte del entorno de la organización y del cual no puede tener control.

Posteriormente, se debe determinar si el actor es interno o externo a la organización, así como su motivo o razón, los cuales pueden ser accidentales o deliberados y cuál sería el requisito de seguridad que se vería afectado en caso de que esa área de preocupación sucediera.

Para esta fase se pueden utilizar dos herramientas, la primera son los cuestionarios de amenazas proporcionados por la metodología, los cuales permiten definir qué tipos de actores son los que podrían afectar a los activos, es importante recalcar que estos cuestionarios deben de ser realizados por el personal que tiene alguna relación con los activos.

La otra herramienta son los árboles de amenaza, en los cuales se establecerán distintos escenarios a través de distintas combinaciones, para poder determinar otros escenarios que previamente no se habían pensado, aunque también existirán muchos que podrían no causar ninguna afectación a los activos.

Fase 6, identificación de los riegos, los cuales se calculan a través de la suma de la amenaza más el impacto causado, la amenaza se obtiene a partir de las áreas de preocupación definidas en las fases 4 y 5, mientras que el impacto será determinado por las áreas definidas en la fase 1, adicionalmente, para obtener un valor más realista, se puede agregar la probabilidad de ocurrencia de esa amenaza, a partir de 3 posibles valores:

- Probabilidad baja de ocurrencia, con un valor de 1.
- Probabilidad media de ocurrencia, con un valor de 2.
- Probabilidad alta de ocurrencia, con un valor de 3.

Fase 7, análisis de riesgos: Por cada área realista, se deberán realizar los cálculos correspondientes para cada criterio de medición, es decir, se multiplica la probabilidad de ocurrencia por el valor del criterio de medición, finalmente se deberán sumar todos los criterios, obteniendo el valor real del riesgo.

Fase 8, selección del enfoque de mitigación: De acuerdo con la calificación total del riesgo y a la matriz de calor generada en la Fase 1, se determinará qué acción se debe realizar con el riesgo, las cuales pueden ser:

- Aceptar.
- Mitigar.
- Transferir.

Aceptar, el riesgo y las afectaciones causadas por este, son aceptadas por la organización.

Mitigar, los riesgos que se encuentren dentro de los valores que componen esta área, deben de mitigarse a través de controles.

Transferir, son aquellos riesgos a los cuales, la organización no puede realizar ninguna acción para disminuir sus afectaciones.

3.3.2.- Mehari.

Fue desarrollada por el Club de la Seguridad de la Información de Francia (CLUSIF), el proceso de análisis de riesgos con esta metodología se divide en 3 fases de la manera siguiente:

Fase 1: De preparación.

1. Evaluación del contexto.
    a. Contexto estratégico.
    b. Contexto técnico.
    c. Contexto estructural.
2. Determinación del alcance y límites del análisis de riesgos y el tratamiento operacional.
    a. Perímetro técnico de análisis y tratamiento de riesgos.
    b. Perímetro organizacional del análisis y tratamiento de riesgos.
    c. Supervisión de la estructura operacional.
3. Establecer los parámetros técnicos del análisis de riesgos.
    a. Tabla del riesgo aceptable.
    b. Tabla de exposición natural.
    c. Tabla de evaluación de potencialidades residuales e impactos.

Fase 2: Operacional (Análisis de riesgos).

1. Análisis de puntos clave y clasificación de los activos.
    a. Escala de valores relacionados al mal funcionamiento.
    b. Clasificación de los activos.
    c. Tabla de impacto intrínseco.
2. Evaluación de la calidad en los servicios de seguridad.
    a. Establecimiento de un esquema de auditoría.
    b. Valoración de la calidad en los servicios de seguridad.
3. Evaluación del riesgo.
    a. Selección de los escenarios de riesgo para el análisis.
    b. Valoración de los escenarios de riesgo.

Fase 3: Planeación para el tratamiento de riesgos.

1. Planeación de las medidas inmediatas.
    a. Selección de los riesgos a tratar de forma inmediata.
    b. Selección de las medidas para la implementación inmediata.
2. Planeación de las medidas específicas para el contexto.
    a. Tratamiento y prioridad de la estrategia.
    b. Selección de las medidas y planeación.
3. Implementación de la supervisión del tratamiento de riesgos.
    a. Planificación de la supervisión.
    b. Indicadores, tablero de mando, graficación.

Dentro de la primera fase se debe establecer bajo que contexto se encuentra la organización, es decir, que tipo de dependencia es, ya sea privada, de gobierno o educativa, a partir de ese punto, se deben determinar los siguientes:

- Leyes o mandatos regulatorios a los que se debe de apegar la organización.
- Objetivos o metas del SGSI.
- Objetivos o metas de la organización.
- Normatividad interna, en caso de contar con una.

Adicionalmente, se debe tener información documental de alguno de los siguientes aspectos técnicos:

- Arquitectura de red.
- Arquitectura de los sistemas utilizados dentro de la organización.
- Arquitectura de las aplicaciones.
- Cartografía general.
- Planes de mejora a mediano y largo plazo.
- Proveedores de servicios estructurales.
- Proveedores de software.
- Proveedores ocasionales (Mantenimiento).

Dentro del contexto organizacional se debe establecer un organigrama de la organización, el cual debe contener las jerarquías y relaciones entre los distintos puestos, así como la descripción de las actividades a realizar dentro de los mismos, a partir de la cual se deberán determinar los responsables de los activos de la organización.

Una vez generada esa información, se pueden determinar el alcance y límites que tendrá el análisis de riesgos, el alcance se puede definir dentro de 3 clasificaciones:

1. Perímetro geográfico: Relacionado a una zona o lugar en particular.
2. Información relacionada a los sistemas: Cuáles son los sistemas o aplicaciones que forman parte del proceso certificado.
3. Tipo de información a considerar: Digital, impresa o escrita, audio o vídeo.

Una vez definido el alcance, se deben establecer los activos críticos del proceso y los posibles riesgos que afecten a los mismos.

Para poder realizar el análisis de riesgos de manera adecuada, se deben determinar los dueños de cada activo, los cuales permitirán definir de mejor manera si el riesgo puede suceder realmente o no.

Para la Fase 2 y el inicio del análisis de riesgos, se debe hacer uso de la base de conocimientos que proporciona la metodología, la cual se divide en 30 hojas, las cuales se describen a continuación:

- Hojas T1, T2, T3: Dentro de estas se deben describir los activos de información y el requisito de seguridad que se vería afectado.
- Classif: Muestra un resumen de los activos de información a partir de las definiciones realizadas de las hojas anteriores, donde se muestra el requisito de seguridad que se vería afectado.
- Expo: Describe de manera detallada los eventos que pueden originar que una amenaza surja.

- Las siguientes 14 hojas están relacionadas a las categorías que contempla Mehari, las cuales permiten determinar que controles o medidas se tienen para la protección de los activos de información dentro de la organización.
    - 01 organización: Contempla todas las medidas de seguridad relacionadas a la segregación de funciones y accesos lógicos.
    - 02 sitio: Se establecen las medidas de seguridad necesarias para las medidas de accesos físicos.
    - 03 instalaciones: Medidas de protección y uso de las instalaciones.
    - 04 WAN: Medidas necesarias para la protección de redes tipo WAN, dentro de la metodología se ve una red WAN, como la interconexión de la red interna de la organización con cualquier otra red externa a la misma.
    - 05 LAN: Protección en la red interna de la organización y los equipos conectados a la misma.
    - 06 operaciones de red: Medidas de seguridad utilizadas para la protección de las redes operativas de la organización y el software utilizado.
    - 07 arquitectura de Sistemas: Medidas de seguridad utilizadas para determinar los distintos privilegios de acceso a la información y sistemas de la organización.
    - 08 entornos de producción: Medidas y controles establecidos dentro de los procesos y procedimientos operativos de la organización.
    - 09 aplicación: Medidas de seguridad implementadas para las aplicaciones utilizadas por parte del personal de la organización.
    - 10 proyectos y desarrollo de aplicaciones: Medidas de seguridad que se tienen dentro de la organización para la gestión de proyectos y el desarrollo de nuevos sistemas de información.
    - 11 protección de los equipos: Medidas de seguridad encaminadas a la protección física y lógica de los equipos utilizados por el personal de la organización.
    - 12 telecomunicaciones: Medidas de seguridad utilizadas en las redes dentro y fuera de la organización, donde se deben proteger principalmente los canales de comunicación.
    - 13 gestión de los procesos: Políticas y procedimientos para manejar de manera segura la información a lo largo de los procesos de la organización.
    - 14 gestión de la Seguridad de la Información: Todos los elementos que se deben de tomar en cuenta para la implementación de un SGSI.

- Servicios: Hace referencia a todas las categorías listadas anteriormente, adicionalmente, permite determinar el nivel de riesgos de acuerdo con las respuestas proporcionadas por el analista, a partir de las cuáles se establece que medidas de seguridad tiene la organización y cuáles son las necesarias para el cumplimiento con la norma.
- Temas: Muestra una relación entre los Servicios y las categorías, es decir, que categorías pertenecen a cierto servicio.
- ISO 27002: Proporciona una guía sobre que controles de la norma ISO 27002 pueden implementarse para proteger a los activos de información de cada categoría.
- Escenarios: Muestra los distintos escenarios de amenaza que podría afectar a los activos de información y la puntuación obtenida a partir de las respuestas proporcionadas por los analistas.
- Riesgo % Activo: Muestra la calificación del riesgo a alguno de los pilares de la seguridad, en caso de que alguna de las amenazas se materialice.
- Riesgo % Evento: Resumen de las distintas amenazas y escenarios que podrían suceder, mostrando el nivel de impacto.
- Planes de acción: A partir de las calificaciones obtenidas, la metodología muestra los escenarios que podrían ocurrir y las afectaciones que podrían causar, para que, a partir de los mismos, la organización tome las medidas pertinentes para mitigar los riesgos.
- Obj_PA: A partir de los Planes de Acción elegidos, se mostrará la efectividad de estos ante los distintos escenarios.
- Obj_Projects: Permite generar distintos Planes de Acción de manera simultánea.
- Vulnerabilidades: Muestra una clasificación de las distintas vulnerabilidades consideradas dentro de la metodología.
- Gravedad: Muestra un mapa de calor donde se establece el nivel de impacto y la probabilidad de ocurrencia.

IP_Grids: De cada categoría, se determinan que riesgos hay que mitigar a partir de las vulnerabilidades y gravedad de estos.

De esta manera, la organización podrá establecer que riesgos se deben de mitigar, para lograr evitar la materialización de este.

3.4.- Planes de contingencia

Otro aspecto fundamental de la ISO/IEC 27001:2013 son los planes de contingencia, los cuales permitirán a la organización continuar con sus actividades cuando suceda algún imprevisto o situación fuera del control de la empresa.

Se pueden identificar dos planes principales:

- BCP: Bussiness Continuity Planning.
- DRP: Disaster Recovery Planning.

BCP, tiene como finalidad establecer las actividades que debe de realizar la organización para poder continuar con las operaciones, es decir, se puede contemplar una sede alterna a la organización, en la cual puedan seguir desarrollándose los procesos, esta sede alterna debe de contar con las medidas mínimas de seguridad e infraestructura necesarias para la operación.

Dentro de este plan se debe especificar como mínimo:

- Los encargados de ejecutar el plan, es decir, las personas que decidirán si una situación provoca que se dé inicio al BCP.
- Identificación de los procesos críticos para la organización, los cuales deben de restablecerse de la manera más rápida y efectiva posible.
- Encargados de restablecer los servicios, el personal involucrado con los activos y que tiene un conocimiento claro sobre cómo gestionarlos en caso de alguna emergencia.
- Determinar los equipos que formarán parte del plan, dentro de este punto, se pueden establecer equipos que desarrollen distintas actividades, como puede ser, toma de decisiones para ejecutar el BCP, encargados de proporcionar la infraestructura mínima dentro de la sede alterna, encargados de validar que la infraestructura cumple con los requisitos mínimos.
- Establecer una sede alterna, en la cual se desarrollarán las actividades necesarias para la continuidad del negocio.
- Árbol de llamadas, donde se especifica quien es el encargado de notificar a todos los jefes de cada área y ellos a su vez, al personal a su cargo sobre la contingencia.
- Tiempos de recuperación, tiempo necesario para restablecer los servicios de la organización.

- Actividades que se realizarán para volver a la normalidad.

DRP, dentro de este plan, se deben considerar distintas contingencias que podrían afectar a la organización, estas pueden ser derivadas por desastres naturales, huelgas, afectaciones causadas en la electricidad o red, entre otras.

Dentro de este plan, se deben contemplar las mismas medidas que dentro del BCP.

La principal diferencia entre ambos planes deriva en que un DRP puede estar compuesto por diversos planes, uno de ellos el BCP, es decir, el DRP tiene un plan de acción para cada posible contingencia que podría afectar a la organización.

Capítulo 4

Metodologías para el desarrollo seguro de software

Dentro de este capítulo se describirán distintas metodologías de desarrollo seguro utilizadas dentro del ámbito de seguridad de la información, entre las cuales se pueden destacar:

- SDL (Secure Development Lifecycle), desarrollada por Microsoft.
- CLASP (Comprehesive, Lightweight Application Security Process), desarrollada por OWASP.
- C by C (Correctness by Construction), desarrollada por Praxis High Integrity Systems.
- SAMM (Software Assurance Maturity Model), desarrollada por OWASP.
- SSF (Software Security Framework), desarrollada por Citigal y Fortify.
- CMMI (Capability Maturity Model Integration), desarrollada por el SEI (Software Engineering Institute).
- TSP (Team Software Process), desarrollada por el SEI (Software Engineering Institute).

Del listado anterior se tomarán como base las primeras 3 (SDL, CLASP y C by C), debido a que contemplan partes tanto de desarrollo como de seguridad, permitiendo que la implementación se realice de manera más sencilla en ambas áreas.

4.1.- Metodologías de desarrollo seguro

Permiten a las organizaciones estructurar, planear y controlar el desarrollo de sistemas computacionales, es decir, establecer los pasos para que los sistemas cumplan con los requisitos solicitados y en el tiempo establecido.

Adicionalmente, se han establecido algunas metodologías en las cuales el punto principal es la seguridad de la información que será tratada dentro de dichos sistemas, debido a que existe una diversa variedad de estas, se listarán las más conocidas.

4.2.- SDL (Secure Development Lifecycle)

Ciclo de Vida de Desarrollo Seguro, es una metodología propuesta por Microsoft, para el desarrollo de software de manera más segura, permitiendo el cumplimiento de estas medidas y reduciendo los costos de implementación y desarrollo.

Se encuentra compuesta de 6 etapas:

1. Capacitación.
2. Requerimientos.
3. Diseño.
4. Implementación.
5. Verificación.
6. Publicación.
7. Respuesta.

1.- Capacitación: Está etapa es previa a la implementación del SDL, se deben de tomar en cuenta los conocimientos previos para el desarrollo, es decir, que lenguaje de programación es el que se utilizará, para que a partir del mismo se puedan identificar las distintas vulnerabilidades conocidas en las diferentes versiones de este, así como también se deben establecer las buenas prácticas de desarrollo y pruebas para validar la seguridad del software.

Adicionalmente, se deben establecer los roles dentro del proyecto, es decir, quienes son los encargados de realizar el sistema, los encargados de validar y dar seguimiento junto con el cliente sobre el cumplimiento de este y finalmente, los encargados de realizar las pruebas de seguridad de los sistemas.

El equipo encargado de todas las actividades descritas anteriormente debe de contar con conocimientos técnicos tanto en el área de desarrollo, como en el área de seguridad en sistemas, para que su trabajo proporcione algún valor al proyecto.

2.- Requerimientos: Dentro de esta fase, se deben determinar los requerimientos que necesita el cliente para el sistema, dentro de la metodología se dividen en 3 grandes ramas:

- Requerimientos de Seguridad y Privacidad.
- Niveles mínimos de calidad.
- Medición de los riesgos de seguridad y privacidad.

Requerimientos de Seguridad y Privacidad, se deben determinar qué puntos de entrada o salida podrían verse afectados por alguna vulnerabilidad, adicionalmente, establecer los privilegios de acceso de usuarios a los elementos que componen el sistema, con esto, se evitan retrasos en el desarrollo del proyecto y en los entregables, para lograrlo, se debe de contar con un grupo de expertos en seguridad de la información, que puedan definir puntos vulnerables.

Niveles mínimos de calidad, establecer los niveles mínimos de seguridad con los que deba de contar la aplicación, la metodología recomienda el análisis e investigación de distintas vulnerabilidades conocidas para sistemas o desarrollos similares a la aplicación, para que de esta manera, puedan identificarse posibles puntos críticos que podrían verse afectados, adicionalmente, las vulnerabilidades identificadas, deberán solucionarse de manera inmediata para no continuar con esa falla durante todo el desarrollo.

Medición de los riesgos de seguridad y privacidad, se debe calcular dentro del costo del diseño los requerimientos regulatorios que serán necesarios para la realización del proyecto, es decir, el costo de implementar ciertas partes del sistema y las posibles implicaciones en seguridad y privacidad que podrían generar un gasto adicional dentro del desarrollo.

3.- Diseño: De manera similar al paso anterior, está fase se divide en las siguientes 3 ramas:

- Establecimiento de los Requerimientos del Diseño.
- Análisis y reducción de la superficie de ataque.
- Modelo de Amenazas.

Establecimiento de los Requerimientos del Diseño, permite identificar los elementos que contendrá el software, con lo cual se pueden reducir costos de desarrollo, adicionalmente, permite establecer las medidas de seguridad mínimas que contendrán estos elementos.

Análisis y reducción de la superficie de ataque, para reducir la posible explotación de una vulnerabilidad del sistema, se debe de realizar un análisis detallado de cada componente del mismo, para que, de esta manera, se restringa o deshabilite el acceso a los elementos del sistema si no es necesario, todo esto, basándose en el principio del mínimo privilegio, para que, de esta manera, se pueda tener una mayor certeza de que el sistema no cuenta con ninguna vulnerabilidad visible.

Modelo de Amenazas, al determinar las amenazas que podrían explotar las vulnerabilidades de los sistemas, permite a los desarrolladores realizar las medidas de seguridad de manera previa, es decir, se reducen los costos de desarrollo, debido a que las medidas no son correctivas, adicionalmente, se pueden identificar los riesgos asociados a esas amenazas y establecer los planes de mitigación.

4.- Implementación, una vez desarrollado el sistema, la metodología contempla 3 aspectos principales a tomar en cuenta durante la etapa de implementación:

- Uso de herramientas.
- Evitar funciones no seguras.
- Análisis estático.

Uso de herramientas, las cuales permitirán identificar distintas vulnerabilidades que hayan sido pasadas por alto dentro de las fases anteriores, estas herramientas permitirán reducir los costos de implementar medidas correctivas una vez que el sistema ya se encuentre en funcionamiento.

Evitar funciones no seguras, consiste en realizar un análisis a fondo del código fuente del sistema, para identificar posibles funciones que podrían ser explotadas por algún atacante y adicionalmente, podrían afectar de manera importante una corrección posterior, para identificarlas, la metodología recomienda el uso de listados o herramientas que analicen el código y proporcionen alternativas a esas funciones.

Análisis estático, permite generar políticas de uso del sistema, para evitar que sean explotadas posibles vulnerabilidades no identificadas, adicionalmente, permite generar una revisión del sistema en aspectos de seguridad de la información.

5.- Verificación, como en las fases anteriores, está se divide en 3 aspectos principales:

- Análisis Dinámico.
- Fuzzing.
- Revisión de la superficie de ataque.

Análisis Dinámico, a diferencia del análisis realizado en la fase anterior, en este punto se contemplan las posibles vulnerabilidades del sistema una vez que este se encuentra en ejecución, es decir, afectaciones que puedan causar accesos no autorizados, consumo de los recursos del sistema, entre otros que provoquen la pérdida de la disponibilidad, confidencialidad o integridad de la información contenida en el sistema.

Fuzzing, consiste en realizar pruebas sobre el sistema enviándole información aleatoria y paquetes mal formados, para poder analizar el comportamiento de este y arreglar cualquier actividad que permita obtener información adicional a cualquier atacante.

Revisión de la superficie de ataque, permite validar que las vulnerabilidades y amenazas encontradas en las fases anteriores han sido mitigadas, con lo cual se puede establecer un nuevo análisis para determinar si la implementación de las medidas tomadas no ha provocado nuevas vulnerabilidades dentro de los sistemas.

6.- Publicación, se compone de las siguientes 3 etapas:

- Creación de un Plan de Respuesta a Incidentes.
- Revisión final de seguridad.
- Certificar lanzamiento.

Creación de un Plan de Respuesta a Incidentes, consiste en establecer los puntos en los cuales la organización intervendrá en caso de que alguna vulnerabilidad haya sido explotada por algún atacante, o en su defecto, haya sido descubierta por la misma organización y se hayan desarrollado los parches de seguridad necesarios para mitigarla, se deben contemplar quienes serán los encargados de implementar dichas medidas, así como los contactos de emergencia que tienen la capacidad de responder ante alguna contingencia de seguridad de la información.

Revisión final de seguridad, también conocido como FSR (Final Security Review), consiste en validar que el sistema cumple con los requerimientos mínimos de seguridad establecidos en la Fase 2, cumpliendo con los planes de mitigación de amenazas y riesgos, existen 3 FSR dentro de este punto:

1. FSR aprobado.
2. FSR aprobado con excepciones.
3. FSR con escalación.

Donde, el primero se considera como el establecimiento de las medidas de seguridad mínimas, el segundo contempla los fallos que no afectan ningún elemento del funcionamiento del sistema y el tercero contempla medidas de seguridad que quedan a cargo de terceros.

Certificar el lanzamiento, una vez aceptado el software, se deben de almacenar todos aquellos datos que serán importantes para el conocimiento de los líderes de proyecto, esto incluye el código fuente de la aplicación, documentación de uso, planes de emergencia, licencia y todo aquello que permita a la organización respaldarse sobre la información utilizada para el desarrollo del sistema, en caso de que alguna vulnerabilidad afecte al mismo.

7.- Respuesta, consiste en realizar las actividades listadas dentro del Plan de Respuesta a Incidentes generado en la fase anterior, las cuales podrán ser solicitadas por el cliente siempre que este lo considere necesario.

4.3.- CLASP (Comprehensive, Lightweight Application Security Process).

Metodología desarrollada por OWASP, organización internacional sin fines de lucro, cuya finalidad es reducir las causas que provocan un desarrollo inseguro de software, dentro de CLASP se proporciona una guía basada en los procesos de la organización, para el establecimiento de la seguridad en las distintas etapas del desarrollo de software, para que este se realice de forma estructurada, repetible y medible.

CLASP se basa en el desglose de los recursos proporcionados a los desarrolladores durante cada etapa del ciclo de vida del desarrollo, dando como resultado vulnerabilidades contenidas en el sistema, las cuales al ser explotadas podrían afectar alguno de los requisitos de seguridad de la información.

Los componentes con los que cuenta la metodología son los siguientes:

- Vistas.
- Buenas Prácticas
- Actividades.
- Recursos.
- Taxonomía.

Vistas, el proceso se desglosa en 5 etapas, las cuales permiten a los desarrolladores implementarlo de manera muy sencilla, dentro de estas etapas se describe cómo interactúan los componentes entre sí y como agregarlos al ciclo de vida del desarrollo, las vistas son las siguientes:

- *Conceptos*: Establece una introducción detallada sobre la metodología.
- *Basada en Roles*: Establece los roles dentro de la metodología.
- *Evaluación de las actividades*: Permite evaluar las 24 actividades proporcionadas por la metodología y su aplicabilidad dentro de la organización.
- *Implementación de las actividades*: Describe las actividades de la vista anterior a fondo.
- Vulnerabilidades: Contiene un catálogo de 104 tipos de vulnerabilidades identificadas dentro de CLASP, las cuales se dividen en 5 categorías.

Buenas prácticas, proporciona las bases para distintas etapas del desarrollo como lo son la planeación, codificación e implementación, incluyendo el uso de herramientas y técnicas, dentro de la metodología se contemplan las siguientes 7 buenas prácticas:

1. *Programas de conocimiento*: Para un correcto establecimiento de medidas de seguridad dentro de los sistemas, el personal a cargo del desarrollo de este debe de encontrarse capacitado tanto en las funciones que realiza dentro de la organización como en el ámbito de seguridad de la información.

2. *Evaluación del entorno de la aplicación*: Debido a la dificultad que representa el identificar vulnerabilidades mediante el análisis del código, la metodología recomienda implementar el sistema y realizar pruebas de este en producción.

3. *Requerimientos de seguridad:* Adicional al establecimiento de los requerimientos necesarios para el correcto funcionamiento del sistema, se deben determinar aquellos que permitan mantener la seguridad de la información contenida en el mismo, para ello se debe considerar cuál será su funcionamiento, los activos o servicios que proporcionará, el tipo de arquitectura utilizada y que tipos de vulnerabilidades existentes.

4. *Implementación de prácticas de desarrollo seguras*: Consiste en proporcionar todo el entorno necesario para el desarrollo del sistema, esto debe de contemplar toda la infraestructura y software, así como los controles de seguridad para los mismos.

5. *Ejecución de procedimientos de remediación de vulnerabilidades*: Se debe tener un procedimiento en el cual se identifiquen, evalúen, prioricen y solucionen las vulnerabilidades encontradas en el sistema, así como los roles y responsabilidades para realizar dichas actividades.

6. *Definición y monitoreo de métricas*: Se deben establecer valores mínimos a evaluar cuando una vulnerabilidad sea detectada, esto, para determinar qué tan efectivas son las medidas de mitigación implementadas.

7. *Publicación de guías de seguridad operacional:* Se debe comunicar a todos los involucrados en el desarrollo sobre los procedimientos que se hayan planteado en los pasos anteriores.

Actividades, de acuerdo con las buenas prácticas descritas anteriormente, la metodología proporciona un conjunto de actividades a realizar para que estas se puedan cumplir de manera correcta, las actividades son las siguientes:

- Implementar un programa de capacitación.
- Análisis de requerimientos y diseño.
- Análisis de los requisitos de seguridad.
- Identificar, implementar y evaluar revisiones de seguridad.

- Verificar los requerimientos de seguridad de los recursos que se utilizarán para el desarrollo del sistema.
- Investigar y evaluar herramientas de soluciones de seguridad.
- Generar una política de seguridad.
- Identificar los recursos y límites de los mismos.
- Establecer roles de usuarios.
- Especificar el entorno de desarrollo.
- Detallar casos de fallos.
- Identificar el vector de ataque.
- Documentar elementos de seguridad relevantes.
- Aplicar principios de seguridad de diseño.
- Establecer parámetros de seguridad durante el desarrollo del sistema.
- Implementar políticas y tecnologías en seguridad de la información.
- Implementar contratos de intercambio.
- Realizar análisis de seguridad durante el proceso de desarrollo.
- Perfeccionar la codificación de inicio de sesión.
- Gestionar las afectaciones causadas por divulgación de la información.
- Gestionar el manejo de reportes de seguridad de la información.
- Monitoreo de las métricas.
- Especificar las configuraciones de seguridad en bases de datos.
- Generar una guía de seguridad en el desarrollo de sistemas.

Recursos, proporcionan apoyo para la planeación, implementación y desarrollo de las actividades listadas en el inciso anterior.

Taxonomía, proporciona una clasificación dividida en clases para una correcta evaluación y resolución de las vulnerabilidades contenidas dentro del código fuente, las cuáles se listan a continuación:

- *Problemas*: Son las vulnerabilidades identificadas dentro de los sistemas.

- *Categorías*: Los problemas detectados se clasifican dentro de alguna de las siguientes categorías:
    - Errores en el tipo de dato.
    - Problemas en la infraestructura.
    - Sincronización y errores de tiempo.
    - Errores en los protocolos.
    - Errores de lógica en la aplicación.

- *Períodos de exposición*: Contempla el tiempo en el que la vulnerabilidad se encuentra dentro del sistema y no se ha mitigado o solucionado.

- *Consecuencias*: Aquellas que pueden ocurrir en caso de que la vulnerabilidad sea explotada por algún atacante.

- *Recursos*: Aquellos utilizados por el atacante para explotar las vulnerabilidades.

- *Evaluación del riesgo*: La metodología recomienda evaluarlo a partir del resultado de las vulnerabilidades detectadas entre las vulnerabilidades explotadas.

- *Período de mitigación*: Medidas implementadas para reducir la vulnerabilidad del sistema.

4.4.- C by C (Correctness by Construction)

Desarrollada por la organización Praxis High Security Systems, es una metodología que permite realizar software de manera segura, tomando las ventajas que proporcionan las metodologías de desarrollo ágil, se basa en tres principios:

1. Un desarrollo complejo producirá errores difíciles de detectar.
2. Asegurarse que los errores han sido corregidos hasta tal punto que pueden realizarse mejoras en el sistema tomando como premisa el punto número 1.
3. Generar evidencia de las acciones realizadas para la mejora del producto final.

De esta manera, la metodología nos permite generar un sistema funcional en una primera entrega, para que en posteriores revisiones el software se vuelva más robusto y seguro.

4.4.1.- Técnicas

Adicionalmente a los principios, la metodología proporciona las siguientes técnicas para lograr los objetivos:

- Especificaciones claras.
- Correcta validación de los datos.
- Desarrollo incremental.
- Evitar la repetición.
- Mantenerlo simple.
- Gestión de los riesgos.
- Thinking hard.

Especificaciones claras, está técnica permite establecer todos los requerimientos que solicita el cliente de forma clara, es decir, todos los elementos que compondrán el sistema, así como la adaptación de estos al lenguaje de programación que se desea utilizar para su desarrollo.

Dentro de la metodología uno de los puntos importantes es tener todos los elementos claros, para evitar de esta manera desarrollos que contengan componentes no utilizados que podrían provocar la explotación de alguna vulnerabilidad, adicionalmente, toda la información sobre el uso del sistema debe de ser clara para evitar que de manera accidental algún usuario pueda acceder a apartados del sistema de manera no autorizada.

Correcta validación de los datos, todas las entradas al sistema, es decir, formularios que requieran alguna interacción con el usuario final, deben de ser sanitizadas para evitar la inyección de código o información que pueda afectar la seguridad de la información contenida en el sistema.

Desarrollo incremental, dentro de este apartado se toman en cuenta dos aspectos, el primero es relacionado a la infraestructura proporcionada para el desarrollo, la cual, en ocasiones provoca retrasos en el proyecto, debido a que no cuenta con los requerimientos mínimos, el segundo aspecto contempla la adición de nuevas funcionalidades al sistema, las cuales deben de ser revisadas previo a la puesta en producción de este.

Evitar la repetición, la principal causa de errores en los sistemas es debido a la falta de detalle de los requerimientos del cliente, la segunda causa es la reutilización de código, debido a que se pueden utilizar funciones vulnerables o una incorrecta validación de la información.

Mantenerlo simple, para realizar una validación ágil dentro del sistema, este, debe ser desarrollado de la manera más simple posible, para que, además, permita la solución del mismo de manera más sencilla, en caso de detectar errores.

Gestión del riesgo, dentro de esta metodología, los riesgos no se deben de gestionar a partir de las fortalezas o conocimientos que se tengan para resolver una tarea, es decir, primero se deben de realizar las actividades de las cuales no se tiene ningún conocimiento para que de esta manera se puedan identificar distintas vulnerabilidades no detectadas previamente.

Thinking Hard!, es un concepto utilizado dentro de la metodología, el cual se puede describir como: "*realizar el sistema pensando en la manera más viable y sencilla de realizarlo.*"

4.4.2.- Etapas

Las etapas para el desarrollo e implementación de la metodología son las siguientes:

- Requerimientos.
- Especificaciones de software.
- Desarrollo de alto nivel.
- Detalle del diseño.
- Especificaciones de modularidad.
- Codificación.
- Especificaciones de prueba.
- Construcción del software.
- Instalación del software.

Requerimientos, deben tenerse de manera clara y detallada las razones del porque se va a desarrollar el sistema, así como cuáles serán las funcionalidades que va a tener el mismo, para que, de esta manera se puedan determinar las medidas de seguridad que deben de considerarse durante el desarrollo.

Descripción del software, en esta etapa se describe todo el funcionamiento del sistema de manera detallada, inclusive se deben describir los errores que podría contener el sistema y como responder a los mismos, junto con la etapa anterior permiten a los desarrolladores obtener la información necesaria para determinar cómo deberá de operar el sistema.

Diseño de alto nivel, describe la arquitectura del sistema, considerando los elementos funcionales y no funcionales, dentro de los segundos se contempla la seguridad de la información. A diferencia de otras metodologías, dentro de CbyC cualquier error debe de solventarse a través de un desarrollo más complejo.

Detalle del diseño, describe el tiempo que se tomará entre la planeación del desarrollo y la codificación del sistema, es decir, desde el establecimiento de los requerimientos y funcionalidades hasta la implementación del sistema.

Especificaciones de modularidad, como muchas otras metodologías de desarrollo, dentro de CbyC se recomienda que el sistema se desarrolle en módulos separados para que finalmente, al juntarlos todos se tenga un software completamente funcional, adicionalmente, se recomienda que se determine la prioridad de implementación, es decir, realizar los módulos en base al flujo de información, desde los datos introducidos por el usuario final, hasta el resultado del procesamiento de estos.

Codificación, consiste en el desarrollo de los módulos que compondrán al sistema, el código debe desarrollarse de manera cuidadosa y revisarse de forma continua para evitar cualquier tipo de error, para ello se deben tomar en cuenta los siguientes puntos:

- Correcto establecimiento de los requerimientos del sistema.
- Evitar ambigüedades.
- Análisis exhaustivo del código.

Especificaciones de prueba, se deben de realizar pruebas tanto de los elementos funcionales descritos dentro de los requerimientos, como de los elementos no funcionales que se encuentren documentados.

Construcción del software, las versiones finales del sistema serán aquellos que hayan pasado las etapas anteriores de la metodología, comúnmente, las primeras versiones contendrán solamente la estructura del sistema y alguna funcionalidad principal del mismo, posteriormente, éste irá creciendo de acuerdo a los avances incrementales.

En caso de encontrarse algún error en el sistema, la metodología contempla 3 posibles escenarios:

Usualmente se debe a algún elemento no funcional del sistema, por lo cual se realizan revisiones y modificaciones a esa parte del código.

- En caso de que el código no sea necesario, eliminarlo.
- Si la funcionalidad es primordial para el funcionamiento del sistema, se debe de documentar la existencia del error.

Instalación del software, finalmente se debe de instalar en el ambiente de producción el sistema funcional y seguro desarrollado a lo largo de las etapas listadas anteriormente.

4.4.3.- Paralelismo.

Aunque el desarrollo del sistema se ve como una secuencia de actividades, éstas se pueden realizar de forma paralela desde 3 diferentes aspectos:

- Dos actividades distintas pueden realizar de manera simultánea, actividades que no dependan de manera directa entre sí.
- El desarrollo de los módulos puede realizarse al mismo tiempo.
- Finalmente, la revisión de seguridad de los módulos y el desarrollo de nuevos, son actividades que pueden realizarse a la par.

4.4.4.- Recomendaciones.

Debido a todos los elementos listados anteriormente, la metodología proporciona las siguientes recomendaciones para su implementación:

- Retroalimentación.
- Análisis de causa raíz.
- Mejora del proceso.
- Flexibilidad.

Retroalimentación, a pesar de que en cada etapa se tratan de disminuir los errores de la mejor manera posible, éstos son inevitables, por esa razón, una vez que se han identificado, se deben de documentar y establecer las medidas necesarias para su corrección después de haber realizado un análisis de este, para evitar causar una afectación mayor al sistema.

Análisis causa raíz, una vez identificado algún error, se debe de regresar al inicio de la etapa en la que se encontraba el desarrollador, posteriormente, se debe de solucionar el error encontrado y reorganizar la planeación del trabajo en caso de que ésta se haya visto afectada por el fallo, debido a la naturaleza de la metodología, la reorganización de la planeación no debe verse afectada de sobremanera, adicionalmente se debe de modificar la documentación en caso de ser necesario.

Proceso de mejora, además de corregir la vulnerabilidad, se debe entender cómo es que esta sucedió, para de esta manera poder implementar las medidas de seguridad dentro del sistema.

Flexibilidad, CbyC plantea ser una metodología aplicable a cualquier entorno de desarrollo de sistemas, por esa razón dentro de la misma se contemplan los siguientes aspectos:

- *Nivel de rigor*, de forma indiferente del tipo de proyecto que se esté desarrollando, mientras exista un nivel mínimo de aceptación, se deben de establecer las medidas de seguridad necesarias para el mismo.

- *Técnicas*, se deben documentar todas las técnicas y elementos utilizados dentro de cada sistema.

- *Subconjunto de actividades*, tareas o requerimientos adicionales al sistema.

- *Contenido del diseño*, el nivel de detalle en el diseño dependerá siempre del tamaño del sistema y la complejidad de este.

- *Evaluación formal*, se debe generar evidencia de todos los elementos que contenga el sistema y el grado de interacción con el usuario, para poder determinar de manera más precisa las vulnerabilidades que podrían afectarlo.

Capítulo 5

Prácticas seguras de desarrollo

Dentro de este capítulo se describirán buenas prácticas de desarrollo para sitios web y aplicaciones móviles proporcionadas por OWASP, esto con la finalidad de proporcionar una guía que permita reducir las vulnerabilidades producidas en las etapas de desarrollo de los sistemas.

5.1.- OWASP.

Open Web Application Security Project, es una comunidad cuya finalidad es proporcionar herramientas, documentos, foros y capítulos relacionados a la correcta implementación de la seguridad de la información dentro de los aplicativos de las organizaciones.

Dentro de sus principales contribuciones a la comunidad se encuentra el *Top Ten de las vulnerabilidades para sitios web y aplicaciones móviles*, así como el listado de buenas prácticas para evitar la aparición de dichas vulnerabilidades, a continuación, se describirán cada una de ellas para que la implementación de las mismas dentro de las organizaciones se realice de forma transparente.

5.2.- Prácticas seguras de desarrollo para sitios web

Dentro de esta clasificación, OWASP considera las siguientes prácticas seguras:

- Autenticación del usuario.
- Complejidad de la contraseña
- Gestión de sesiones.
- Control de Acceso.
- Validación de la información de entrada.
- Transmisión segura de información.
- Carga de archivos.
- Bitácoras.
- Criptografía.
- Gestión de las Cookies de sesión.
- Redirecciones inválidas.
- SQL Injection.
- Cross Site Scripting.
- Cross Site Request Forgery.
- Referencia insegura a objetos.

Autenticación del usuario: Se deben gestionar los distintos usuarios dentro de los sistemas de la organización, para ello, es recomendable el uso de identificadores únicos para cada uno de ellos, adicionalmente, los identificadores deben de ser case sensitive, esto, para evitar duplicidad en las cuentas, para ello pueden utilizarse correos electrónicos con la debida sanitización y validación de la entrada de información.

Adicionalmente, se debe gestionar un correcto manejo de errores, para evitar respuestas que permitan determinar al usuario el tipo de servicios utilizados por los sistemas.

Para evitar ataques de fuerza bruta, una recomendación es establecer un período de tiempo de espera entre cada intento de inicio de sesión, así como la implementación de la autenticación de doble factor.

Complejidad de la contraseña, se debe implementar una política o medidas en las cuales se describa que es una contraseña segura para la organización, además, estas medidas deben de ser comunicadas a los usuarios.

Algunas de las recomendaciones para establecer contraseñas seguras son las siguientes:

1. Longitud: Una contraseña de longitud menor a 10 caracteres es considerada como no segura.
2. Complejidad: La contraseña debe de estar compuesta por al menos una mayúscula, una minúscula, un número, un caracter especial.
3. No utilizar palabras que se encuentren en diccionarios, debido a que esto facilita los ataques de fuerza bruta.

Dentro de la implementación del sistema deben agregarse estas medidas, para que, si algún usuario no cumple con las mismas se muestre un mensaje de error.

Adicionalmente, se debe de implementar un mecanismo de recuperación de contraseñas seguro, el cual permita asegurar en la medida de lo posible que el usuario que solicita el cambio de contraseña sea realmente ese usuario.

Gestión de sesiones, la mayoría de los sitios web hacen uso de un identificador de sesión para gestionar, identificar y diferenciar entre los usuarios que han iniciado sesión dentro del aplicativo, por esa razón es importante implementar las correctas medidas de seguridad para evitar el robo de sesión, por esa razón se considera que el identificador debe de contar con las siguientes características:

- *Nombre:* No debe de ser bastante descriptivo para evitar proporcionar información sobre el propósito y significado del identificador, algunos de los más comunes son **PHPSESSID, JSESSIONID, CFID & CFTOKEN, ASP.NET_SessionId**, los cuales vienen por defecto dentro de los lenguajes de programación utilizados para el desarrollo de sitios web, por lo cual adicionalmente se recomienda modificar esos nombres.
- *Longitud:* El valor del identificador debe tener una longitud de al menos 128 caracteres, esto, con la finalidad de reducir la probabilidad de éxito de un ataque de fuerza bruta.
- *Entropía:* El identificador debe de contener al menos 64 caracteres aleatorios, esto para prevenir que un atacante pueda determinar la lógica de funcionamiento al momento de generarlos, es decir, si el aplicativo genera identificadores secuenciales, un atacante puede enviar una petición con un identificador válido que le permita iniciar sesión dentro del sistema.
- *Contenido:* El valor del identificador nunca debe de contener información sensible como el nombre de usuario o contraseña, debido a que solamente debe de permitir la identificación de este en el sistema, en caso de contener información sensible es importante mantenerla protegida bajo algún algoritmo criptográfico.

Control de Acceso, permite gestionar los permisos dentro del aplicativo, es decir, que acciones puede realizar el usuario dentro del sistema, para poder llevar a cabo este punto, se recomienda generar una política o listado de usuarios en el cual se describa que privilegios tendrá cada uno de ellos, para posteriormente implementarlos dentro del sistema y evitar accesos no autorizados.

Validación de la información de entrada, las metas que se buscan lograr con esta recomendación es validar que realmente la información introducida al aplicativo no contiene caracteres maliciosos que podrían afectar el funcionamiento de este o proporcionar información sensible.

Para evitarlo, algunas buenas prácticas a implementar de acuerdo al OWASP son las siguientes:

- Validar el tipo de datos permitidos por parte del aplicativo.
- Establecer un máximo número de caracteres permitidos en los campos que permitan la introducción de información.
- Generación de listas blancas y listas negras, esto quiere decir, que las primeras son los caracteres que se encuentran permitidos dentro del aplicativo, mientras que las listas negras, son todos aquellos caracteres no soportados por el sistema y que podrían causar una afectación al mismo en caso de introducirse.
- Expresiones regulares, de manera similar al punto anterior, con las expresiones regulares es posible que el sistema determine qué valores están permitidos y cuáles no.
- Validación en la conversión del tipo de datos.

Transmisión segura de información, dentro de esta recomendación se determina la forma en que la información viajará desde el aplicativo hasta el usuario, el principal error cometido por los desarrolladores es la falta de implementación de un canal de comunicación seguro, es decir, toda la información viaja en claro, permitiendo que cualquier atacante que se encuentre monitoreando la red pueda capturar esos paquetes.

Una medida de mitigación es la implementación de protocolos seguros como SSL y TLS, aunque dentro de los mismos existen versiones vulnerables a ataques como heartbleed o poodle.

Algunas reglas que permiten la disminuir este vector de ataque son:

- Utilizar TLS o algún protocolo más robusto de transporte en todos los elementos que permitan el inicio de sesión al sistema.
- No permitir la existencia de páginas no seguras, es decir, si se tienen implementados protocolos seguros dentro de la página, conocido como *HTTPS,* no debe existir dentro del mismo servidor un sitio web no seguro, como en este ejemplo sería un sitio que contenga *HTTP*, debido que de manera errónea un usuario podría acceder al sitio no seguro y su información viajaría en claro.

- Evitar que los encabezados realicen más saltos de los permitidos, es decir, si el atacante está utilizando un proxy, realizar las configuraciones necesarias para que, la información que llega al usuario final no contenga datos sobre el aplicativo.
- Para los certificados de servidor:
    - Utilizar llaves con longitudes mayores a 2048 bits, esto, como medida de prevención para evitar que algún atacante pueda obtener las llaves que permiten firmar los certificados.
    - Realizar los certificados con CA´s de confianza, es decir, Entidades Certificadoras que aseguren o proporcionen el uso de protocolos seguros de comunicación.

Carga de archivos, adicional a la validación de entrada, se deben verificar los archivos que están permitidos subir al aplicativo, ya que estos en muchas ocasiones pueden contener algún payload que permita la ejecución de código remoto.

Algunas medidas para prevenir este tipo de acciones son las siguientes:

- Validar la extensión del archivo y verificar que se encuentre dentro del listado permitido por el sistema.
- Modificar el nombre del archivo dentro de la base de datos donde se almacena, para esta medida es recomendable generar un nombre aleatorio, para evitar que algún atacante pueda acceder a los directorios del sistema.
- Realizar un análisis de los archivos subidos para evitar que estos tengan algún contenido malicioso.
- La ruta de almacenamiento debe de ser determinada por el servidor no por el cliente.
- No permitir la carga de archivos ejecutables, es decir, con extensión como .css, .swf, .xhtml,. rhtml, .shtml, jsp, .js, .pl, .php, .cgi.

Bitácoras, una buena práctica es llevar un registro de todas las acciones que han sucedido dentro del servidor, las cuáles nos pueden permitir realizar modificaciones en caso de encontrar alguna vulnerabilidad que no había sido encontrada previamente.

Algunas de las actividades que se recomiendan monitorear son las siguientes:

- Intentos de inicio de sesión.
- Errores en la información de entrada.
- Respuestas del aplicativo.
- Modificaciones de la Cookie de Sesión.
- Reinició o apagado del sistema.
- Gestión de los usuarios (alta, baja o modificación).
- Uso excesivo del aplicativo.
- Intentos de fraude o actividad criminal.
- Comportamiento extraño de algún usuario.
- Modificaciones de configuración.

Adicionalmente, de cada uno de los eventos listados anteriormente, se debe tener un registro de la siguiente información:

- Día y hora en que sucedió el evento.
- Identificador del usuario que realizó la acción.
- Componente del sistema donde se realizó la acción.
- Dirección URL.
- Código de respuesta del aplicativo.

Criptografía, existen una gran cantidad de herramientas para el cifrado de la información, estás dependerán del punto en el que se implementen y la información que se desee proteger, los requerimientos mínimos recomendados son los siguientes:

- Llave de intercambio: Es preferible el uso del algoritmo Diffie-Hellman con una llave de 2048 bits.
- Integridad del mensaje: Algoritmo HMAC-SHA2.
- Hash del mensaje: Algoritmo SHA2 con longitud mínima de 256 bits.
- Cifrado asimétrico: Algoritmo RSA con longitud mínima de 2048 bits.
- Cifrado simétrico: Algoritmo AES con longitud de la llave mínimo de 128 bits.
- Algoritmos para la contraseña: PBKDF2, Scrypt, Bcrypt.

Adicionalmente, las recomendaciones para el uso de algoritmos de cifrado son las siguientes:

- Almacenar solamente la información que sea considerada como sensible, este tipo de información puede estar relacionada a tarjetas bancarias de los usuarios.
- Uso de algoritmos de cifrados conocidos y comprobados, no es recomendable realizar una implementación propia para la protección de la información, debido a que puede no proporcionar los niveles de seguridad mínimos.
- Evitar el uso de algoritmos de cifrado simétrico, debido a que son más sencillos de predecir que los asimétricos.
- Asegurar que se usa la suficiente entropía para generar números aleatorios.
- Asegurar que las medidas de cifrado implementadas apoyan a las otras medidas de seguridad implementadas.
- Definir el tiempo de vida de las llaves.
- Protección de las llaves dentro de un llavero.
- Tener documentados los procedimientos utilizados para el cifrado de información y la generación de las llaves.

Gestión de las Cookies de sesión, como se comentó en la recomendación de "Gestión de Sesiones", otro tipo de identificador de sesión adicional son la Cookies, las cuales guardan información de los datos consultados por el usuario y comúnmente permiten que una página previamente visitada cargue de forma más rápida, otra de las ventajas que proporciona este tipo de identificador es que permiten evitar los ataques Man in the Middle.

Entre los atributos más importantes contenidos dentro de la Cookie de sesión se encuentran:

- *Secure,* permite una doble validación en caso de que el identificador de sesión sea obtenido por algún atacante, si este intenta iniciar sesión sin la Cookie, el servidor cerrará la sesión debido a la falta de ese valor.
- *HttpOnly,* no permite la ejecución de ningún tipo de script, evitando de esa manera la ejecución de código dentro del sistema.

- *Domain and Path,* la Cookie de sesión solamente se enviará a través de los sitios web que contengan el mismo nombre de dominio o subdominios derivados de este, adicionalmente el parámetro **Path**, permite validar la ruta de instalación de este, obtenida a través del identificador de sesión.
- *Expire and Max-Age,* es el tiempo de duración de la Cookie dentro del servidor, si se encuentran configurados, la Cookie dejará de existir dentro del servidor una vez que se haya cerrado el navegador del usuario.

Redirecciones inválidas, este tipo de vulnerabilidades son causadas cuando un sitio web permite la entrada de parámetros que realizan la redirección a sitios web maliciosos, los cuales comúnmente buscan realizar ataques de phishing, para mitigar este tipo de vulnerabilidades es importante sanitizar las entradas al sistema, para evitar la introducción de caracteres no válidos o no permitidos dentro de los campos del aplicativo.

SQL Injection, a pesar de que es uno de los ataques más comunes realizados contra los sitios web, es uno de los más sencillos de mitigar, debido a que se puede prevenir desde las primeras etapas del desarrollo de software.

Regularmente, este tipo de ataques suceden debido a la interacción que tiene el sitio web con la base de datos, para prevenirlos, de manera general se pueden realizar alguna de las siguientes acciones:

- Evitar la consulta dinámica hacia la base de datos.
- No permitir al usuario la introducción de caracteres similares a una consulta en base de datos.

Algunas técnicas que permiten realizar alguna de las acciones mencionadas anteriormente son:

- *Declaraciones bien definidas:* Consiste en dividir el entorno de desarrollo del aplicativo y el entorno de la base de datos, es decir, establecer parámetros previos entre la interacción del sistema y la base de datos, para que de esta manera si algún atacante introduce alguna inyección SQL, no reciba ninguna respuesta por parte de la base de datos.
- *Uso de procedimientos almacenados:* Permiten evitar la ejecución dinámica de código dentro de la base de datos, aunque pueden ser utilizados como otro vector de ataque si algún atacante descubre los mismos.

- *Uso de listas blancas:* Consiste en establecer los caracteres permitidos dentro de los campos que utilizará el usuario para introducir información, evitando así el uso de caracteres que permitan realizar una consulta a la base de datos.
- *Validación de entrada,* la mejor opción para evitar ser afectados por un ataque de inyección de código es validar todas las entradas que envía el usuario.

Cross Site Scripting, algunas de las recomendaciones para evitar las afectaciones causadas por este tipo de ataques son:

- *Nunca permitir la inserción de información no confiable:* Dentro de este principio, se debe entender que toda la información es no confiable, hasta que se realice una validación de la misma.
- *Validación de código JavaScript:* Consiste en sanitizar los campos de entrada para verificar que dentro de la información no contiene código JavaScript que pueda ejecutarse.
- *Validación de direcciones URL:* De manera similar a la recomendación anterior, se debe sanitizar la entrada para verificar que no contenga una dirección URL, la cuál puede ser utilizada para realizar una redirección a algún sitio malicioso.

Cross Site Request Forgery, debido a que este tipo de ataques son diferentes a **XSS,** las medidas de mitigación son las siguientes:

- Verificar los encabezados, para esta recomendación es importante verificar los encabezados **Origin** y **Referer,** con el fin de identificar que es el mismo usuario que realizó las peticiones previas.
- Gestión de la sesión mediante doble factor, es decir, no solamente manejar la sesión de un usuario con el identificador de sesión, si no, implementar medidas adicionales como una Cookie de Sesión, para mitigar el robo de sesión por parte de los atacantes.
- Uso de Token de sesión cifrado, para esta técnica, el sistema genera un token con el cual inicia sesión el usuario, una vez dentro del sistema, se genera un nuevo Token de sesión con un algoritmo distinto al anterior.
- Uso de autenticación de doble factor (Captcha), para las transacciones bancarias realizadas dentro del aplicativo.

Referencia insegura a objetos, a pesar de que este tipo de ataques no causa una afectación tan grave hacia los sitios web, es importante tomar las medidas necesarias de mitigación, debido a que puede proporcionar información sobre las herramientas utilizadas para la creación del sitio web, las cuales permitirían al atacante explotar distintas vulnerabilidades.

La única recomendación existente para este punto, de manera similar a las buenas prácticas de programación, es realizar un correcto manejo de errores, para evitar proporcionar información sobre el desarrollo del sistema.

5.3.- Prácticas seguras de desarrollo para aplicaciones móviles

Para la descripción de las prácticas seguras en el desarrollo de dispositivos móviles, se listarán a continuación las vulnerabilidades más comunes proporcionadas por OWASP dentro de esta categoría, para posteriormente desarrollar las medidas de mitigación recomendadas:

- M1 Uso inadecuado de la plataforma.
- M2 Almacenamiento inseguro de la información.
- M3 Comunicación insegura.
- M4 Autenticación insegura.
- M5 Cifrado.
- M6 Autorización insegura.
- M7 Calidad del desarrollo del lado del cliente.
- M8 Manipulación de código.
- M9 Ingeniería Inversa.
- M10 Funcionalidad inadecuada.

Uso inadecuado de la plataforma, la principal recomendación proporcionada en este punto es mantener actualizados los sistemas operativos en los cuales se encuentran alojadas las aplicaciones móviles, adicionalmente, se deben establecer las medidas de protección de la información sensible por parte de los desarrolladores.

Almacenamiento inseguro de la información, en algunas aplicaciones toda la información es enviada en claro a través del método GET, con lo cual un atacante podría capturar los paquetes y obtener información sensible del usuario, por esa razón una medida para disminuir esta afectación es, realizar las transacciones mediante el método POST, cuando la información sea sensible (contraseñas, nombres de usuario, números de tarjetas bancarias, etcétera.).

Adicionalmente, la información utilizada por las aplicaciones no se almacena de manera segura dentro de los dispositivos móviles, por esa razón es importante considerar el uso de algoritmos de cifrado para la información utilizada por parte de la aplicación, otra medida de mitigación es almacenar la información en la memoria RAM, debido a que, al ser una memoria volátil, no quedarán registros de la misma una vez que se acabe de ejecutar la aplicación.

Comunicación insegura, de manera similar a las recomendaciones proporcionadas para sitios web, esta práctica de seguridad contempla el uso de protocolos de comunicación seguros para evitar la fuga de información a través de la captura de los paquetes de tráfico.

Autenticación insegura, la mayoría de las aplicaciones no implementan las medidas necesarias para la generación de usuarios y contraseñas seguros, provocando que cualquier atacante obtenga credenciales válidas al momento de realizar un ataque de fuerza bruta.

Otra recomendación para la solución de esta vulnerabilidad es el uso de autenticación de doble factor, la cual puede ser a través del envío de mensajes de texto al usuario, preguntas de seguridad, o Captcha, algunas aplicaciones bancarias, hacen uso de un token físico para realizar el proceso de doble autenticación.

Cifrado insuficiente, la principal recomendación proporcionada para este punto es el uso de cifrado para la información almacenada tanto dentro del dispositivo móvil del usuario, como para la que se encuentra almacenada por parte de los desarrolladores.

Adicionalmente, algunas aplicaciones hacen uso del cifrado de la información, pero no de manera correcta, esto es, al momento de realizar el análisis de código de la aplicación, se puede determinar la función que realiza el cifrado de la misma, permitiendo al atacante realizar el proceso inverso, por esa razón es recomendable usar algoritmos de cifrado seguro.

Autorización insegura, se apoya de las medidas implementadas en la recomendación de **Autenticación insegura,** debido a que una vez que el usuario ha iniciado sesión, se deben gestionar los privilegios que este último tendrá dentro de la aplicación, para evitar modificaciones a la misma.

Calidad del desarrollo del lado del cliente, esta práctica de seguridad contempla las medidas necesarias para evitar vulnerabilidades como *Buffer Overflow*, debido a que plantea las siguientes medidas de mitigación:

- *Evitar el uso de lógica simple,* es decir, no realizar validaciones sencillas, que comprendan igualdades de numéricas o de caracteres, debido a que un atacante podría modificar el número válido y afectar la aplicación, para esta recomendación es importante el establecimiento de paradigmas de desarrollo más complejos.
- *Revisión de las bibliotecas de terceros,* en ocasiones el desarrollo del código propio es correcto, pero las bibliotecas utilizadas para proporcionar funcionalidades al mismo pueden contener vulnerabilidades, por esa razón es importante realizar una revisión constante de las funciones de terceros utilizadas dentro de la aplicación.
- *Validación de la información de entrada del cliente,* de manera similar a las prácticas seguras descritas para sitios web, todas las entradas a la aplicación deben de entenderse como maliciosas, hasta que hayan pasado por un proceso de validación previo.

Manipulación del código, la principal vulnerabilidad en esta clasificación es la instalación de algún backdoor dentro del código de la aplicación, para evitar este tipo de afectaciones, una de las medidas más sencillas y efectivas es el uso de checksum o sumas de verificación, para verificar la integridad de la aplicación.

Ingeniería inversa, como se describió en medidas de mitigación anteriores, existen herramientas que permiten revisar el funcionamiento del código fuente de la aplicación, de esta manera, un atacante podría modificar los valores recibidos por la misma para ver si es posible causar alguna afectación.

Para evitar este tipo de vulnerabilidades las principales recomendaciones son:

- Realizar código más complejo, mediante paradigmas de programación avanzados.
- Ofuscar el código para evitar que el análisis del mismo sea sencillo.
- En algunas plataformas es posible habilitar la función *Anti- debug,* la cual no permite realizar el análisis de código, excepto que sea por parte de los desarrolladores del mismo.
- Realizar actualizaciones constantes de la aplicación.
- Dividir los binarios que componen la aplicación, para evitar que un atacante pueda realizar un análisis de la misma de forma sencilla.

Funcionalidad inadecuada, los desarrolladores en ocasiones colocan elementos que permiten el funcionamiento de la aplicación, los cuales, si no son eliminados antes de poner en producción la aplicación, pueden ser aprovechados por los atacantes para explotar vulnerabilidades dentro de la aplicación.

Para mitigar esta afectación, es recomendable eliminar todo aquello que no sea necesario para el funcionamiento de la aplicación, realizar revisiones previas a la puesta en producción de la aplicación, en caso de que un componente sea necesario para el funcionamiento de la aplicación, en la medida de lo posible, ocultarlo.

Capítulo 6

Uso de herramientas para comprobar la seguridad de sitios web y aplicaciones móviles

Dentro de este capítulo se describirán y ejemplificarán las herramientas más utilizadas en el ramo de la seguridad de la información para la revisión de vulnerabilidades dentro de los sitios web y aplicaciones móviles.

Todas las herramientas utilizadas para el desarrollo de este capítulo se pueden encontrar dentro de la distribución *Kali Linux*, perteneciente a la familia de sistemas operativos *Unix.*

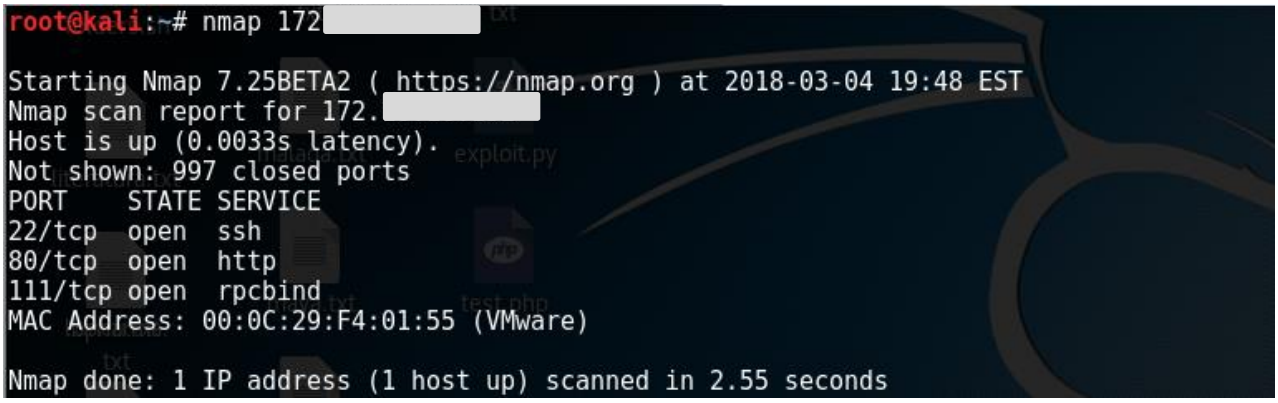
A continuación, se proporcionará una breve descripción de cada herramienta y se describirán las opciones mínimas de uso.

6.1.- Nmap.

Network Mapper, herramienta de código abierto utilizada para la detección y auditoría de red, permite identificar a través de peticiones puertos, servicios, sistema operativo, entre otros de equipos de cómputo o servidores.

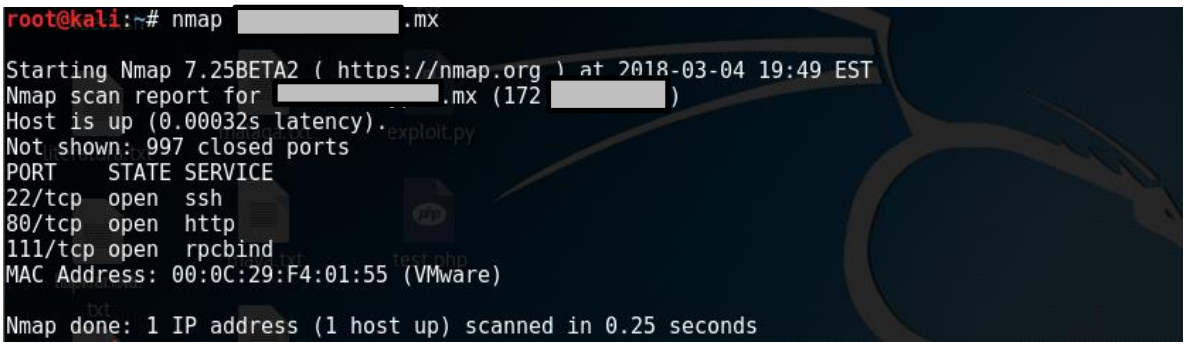
1.- Para ejecutar la herramienta sobre una dirección IP, el comando es:

nmap dirección_IP.



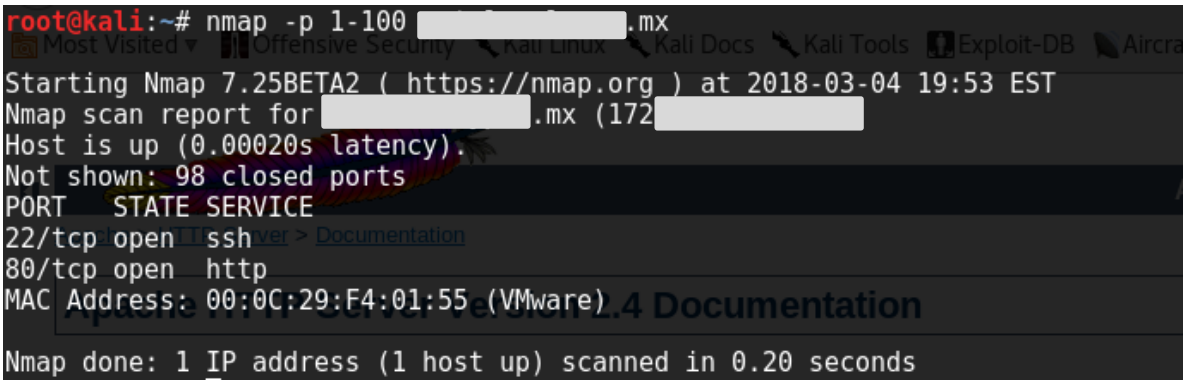
2.- Para ejecutar la herramienta sobre un nombre de dominio.

nmap Dominio



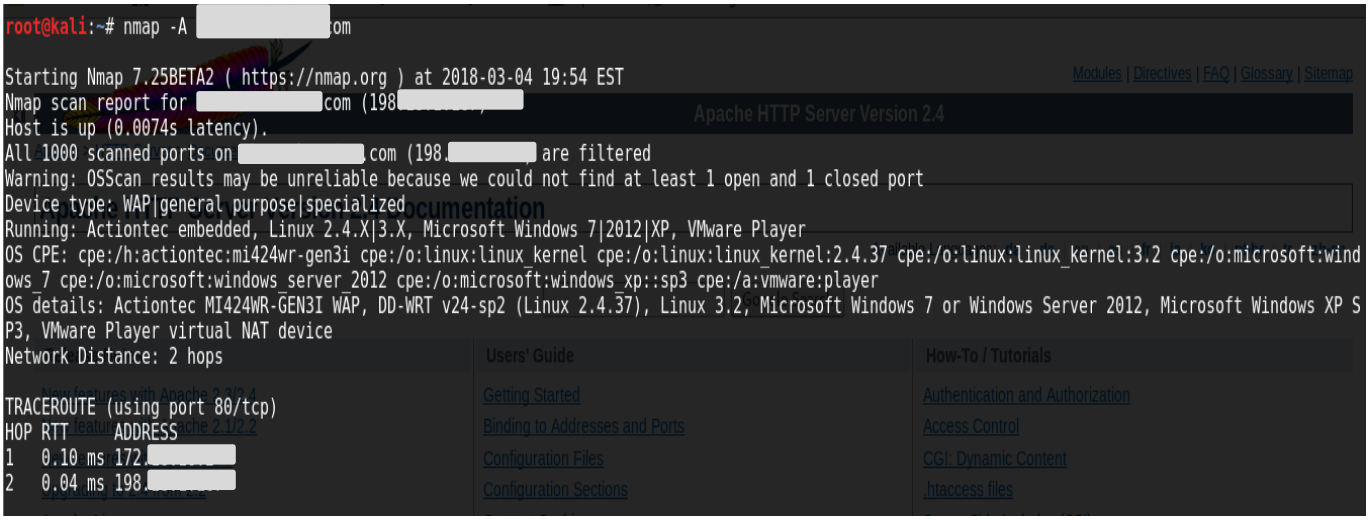
3.- Para escanear un rango de puertos.

nmap –p [0-65535] dominio/dirección_IP



4.- Para determinar el sistema operativo utilizado por el sitio.

nmap –A dominio/dirección_IP



5.- Ejecución de scripts.

nmap –script='Nombre_de_script' dominio/dirección_IP

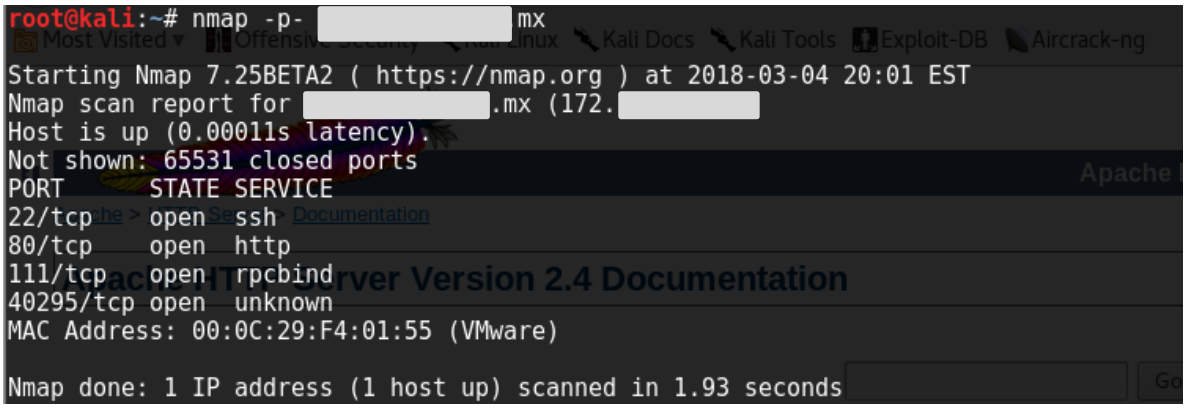
```
root@kali:~# nmap --script=http-title [redacted].mx

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2018-03-04 19:56 EST
Nmap scan report for [redacted].mx (172.[redacted])
Host is up (0.00022s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-title: Apache2 Debian Default Page: It works
111/tcp open  rpcbind
MAC Address: 00:0C:29:F4:01:55 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

El contenido del script mostrado anteriormente es el siguiente:

```
local http = require "http"
local nmap = require "nmap"
local shortport = require "shortport"
local stdnse = require "stdnse"
local string = require "string"
description = [[
Shows the title of the default page of a web server.
The script will follow up to 5 HTTP redirects, using the default rules in the
http library.
]]
---
--@args http-title.url The url to fetch. Default: /
--@output
-- Nmap scan report for scanme.nmap.org (74.207.244.221)
-- PORT   STATE SERVICE
-- 80/tcp open  http
-- |_http-title: Go ahead and ScanMe!
--
-- @xmloutput
-- <elem key="title">Go ahead and ScanMe!</elem>
-- @xmloutput
-- <elem key="title">Wikipedia, the free encyclopedia</elem>
-- <elem key="redirect_url">http://en.wikipedia.org/wiki/Main_Page</elem>
author = "Diman Todorov"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
portrule = shortport.http
action = function(host, port)
  local resp, redirect_url, title
  resp = http.get( host, port, stdnse.get_script_args(SCRIPT_NAME..".url") or "/" )
  -- check for a redirect
  if resp.location then
    redirect_url = resp.location[#resp.location]
    if resp.status and tostring( resp.status ):match( "30%d" ) then
      return {redirect_url = redirect_url}, ("Did not follow redirect to %s"):format( redirect_url )
    end
  end
  if ( not(resp.body) ) then
    return
  end
-- try and match title tags
title = string.match(resp.body, "<[Tt][Ii][Tt][Ll][Ee][^>]*>([^<]*)</[Tt][Ii][Tt][Ll][Ee]>")
local display_title = title
if display_title and display_title ~= "" then
  display_title = string.gsub(display_title , "[\n\r\t]", "")
  if #display_title > 65 then
    display_title = string.sub(display_title, 1, 62) .. "..."
  end
else
  display_title = "Site doesn't have a title"
  if ( resp.header and resp.header["content-type"] ) then
    display_title = display_title .. (" (%s)."):format( resp.header["content-type"] )
  else
    display_title = display_title .. "."
  end
end
local output_tab = stdnse.output_table()
output_tab.title = title
output_tab.redirect_url = redirect_url
local output_str = display_title
if redirect_url then
  output_str = output_str .. "\n" .. ("Requested resource was %s"):format( redirect_url )
end
return output_tab, output_str
nd
```

6.- Para realizar el escaneo por todos los puertos

nmap –p- dominio/dirección_IP

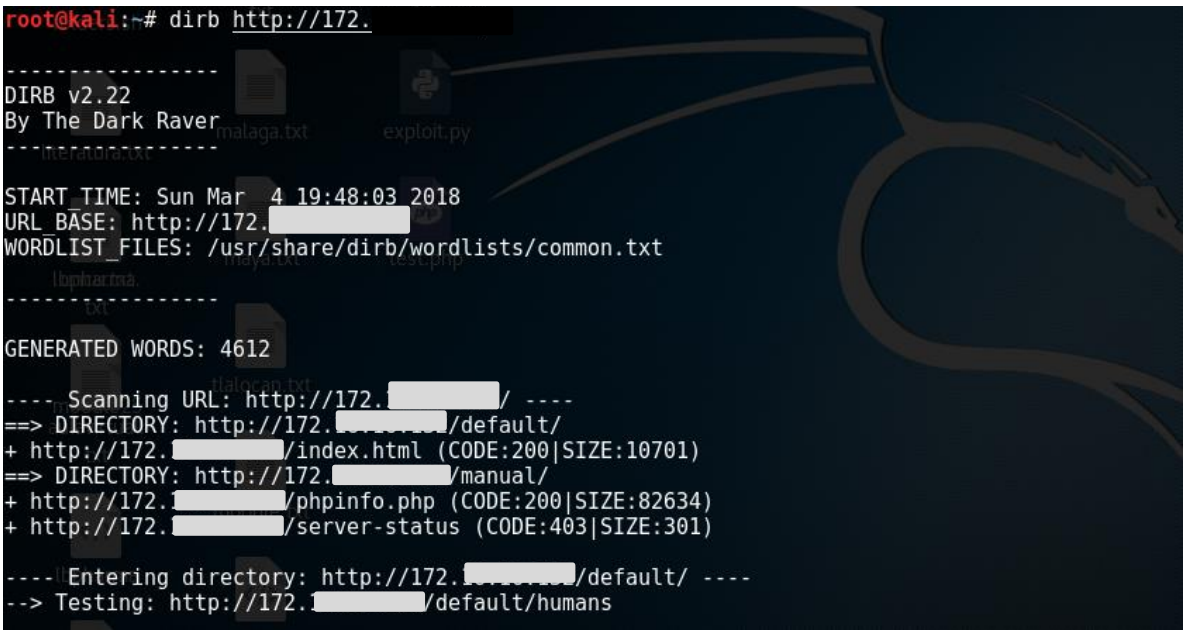


6.2.- Dirb.

Escáner de sitios web utilizado para encontrar recursos o directorios haciendo uso de diccionarios.

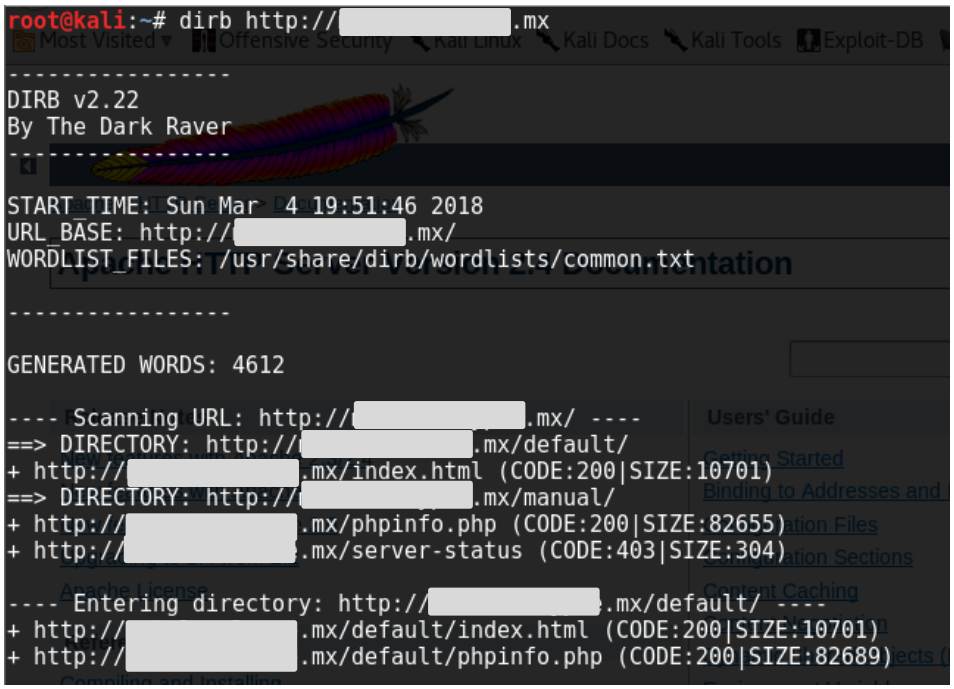
1.- Ejecución básica de la herramienta con dirección IP.

dirb http(s)://IP



2.- Ejecución básica de la herramienta con nombre del dominio.

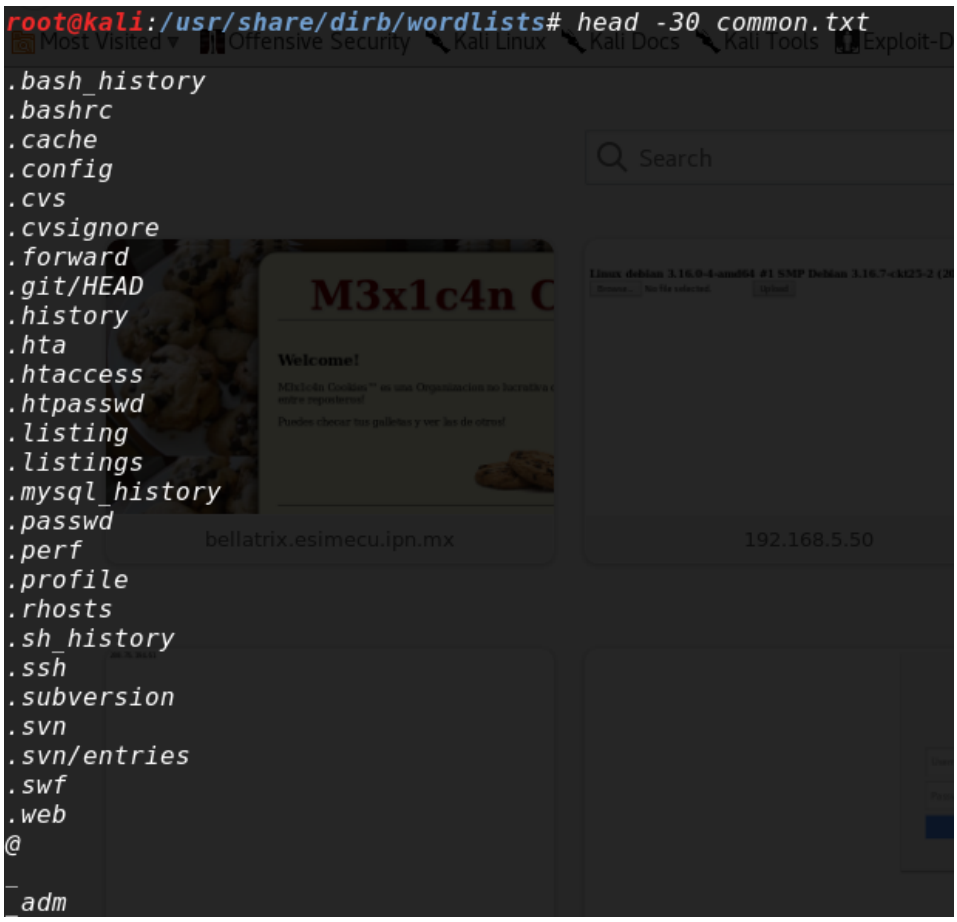
dirb http(s)://dominio



3.- Seleccionando un diccionario propio

dirb dominio/ip ruta_del_diccionario

Algunas de los directorios contenidos dentro del diccionario mostrado anteriormente son los siguientes:

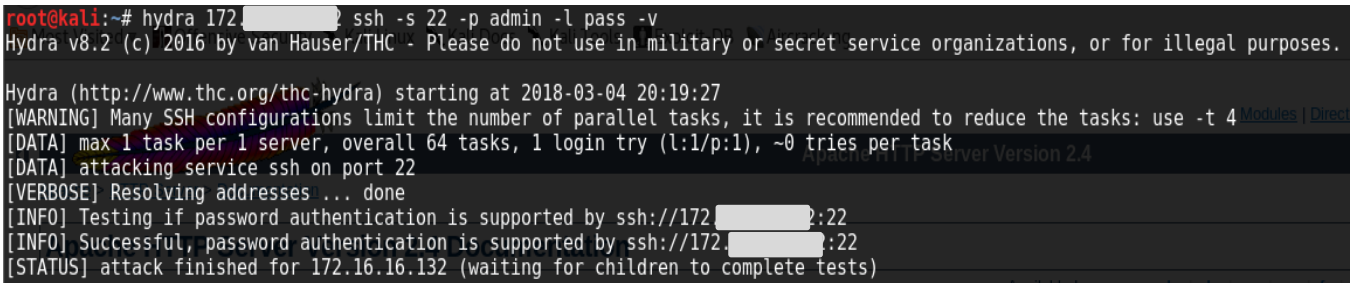


6.3.- THC-Hydra

Herramienta que permite realizar ataques de fuerza bruta a servicios y aplicativos haciendo uso de hilos.

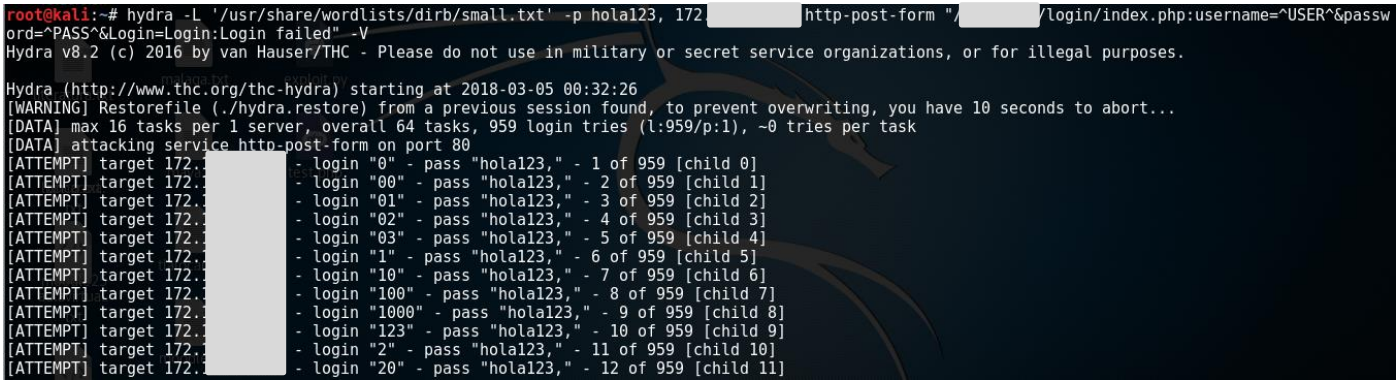
1.- Ataque a un servicio en particular (SSH).

hydra dirección_IP servicio –s puerto –p usuario –l password -v



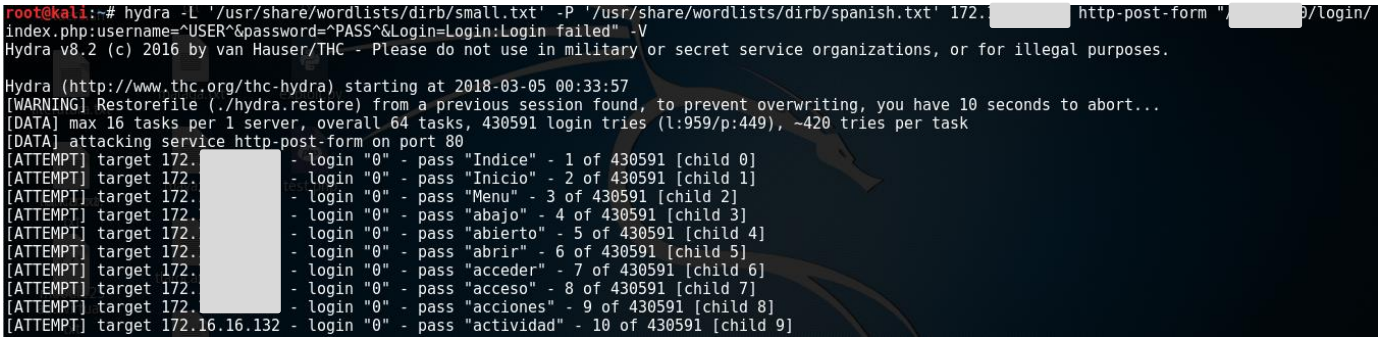
2.- Ataque a un formulario web, especificando el diccionario de usuarios.

hydra –L 'diccionario_usuarios' –p password dirección_IP/dominio http-post-form "dirección_URL:username=campo_para_ingreso_de_usuario&password=campo_para_ingreso_de_password:Mensaje_de_error" -v



3.- Ataque a formulario web haciendo uso de diccionarios para el nombre de usuario y contraseña

hydra –L 'diccionario_usuarios' –P 'diccionario_passwords' dirección_IP/dominio http-post-form "dirección_URL:username=campo_para_ingreso_de_usuario&password=campo_para_ingreso_de_password:Mensaje_de_error" -v

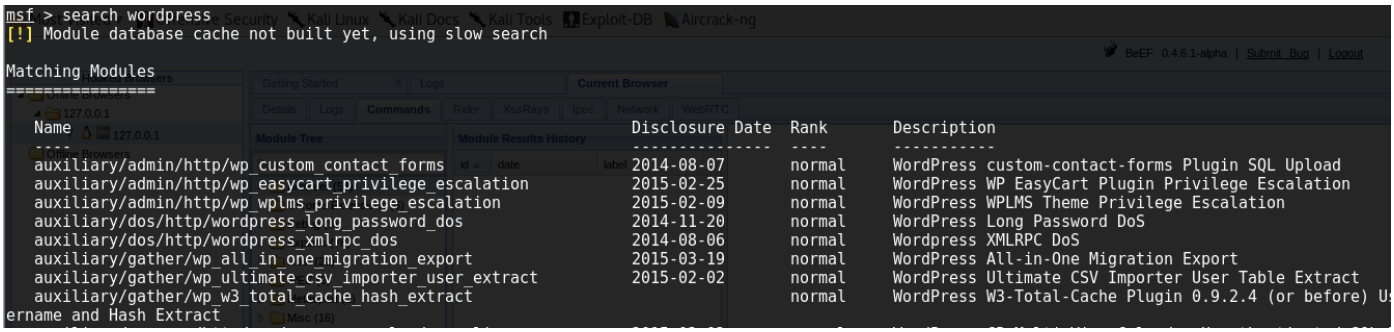


6.4.- Metasploit

Framework de explotación que contiene una biblioteca de exploits validados, los cuales pueden ser utilizados para verificar vulnerabilidades dentro de los sistemas o sitios web.

1.- Para ejecutar la herramienta se debe de escribir el siguiente comando dentro de la terminal

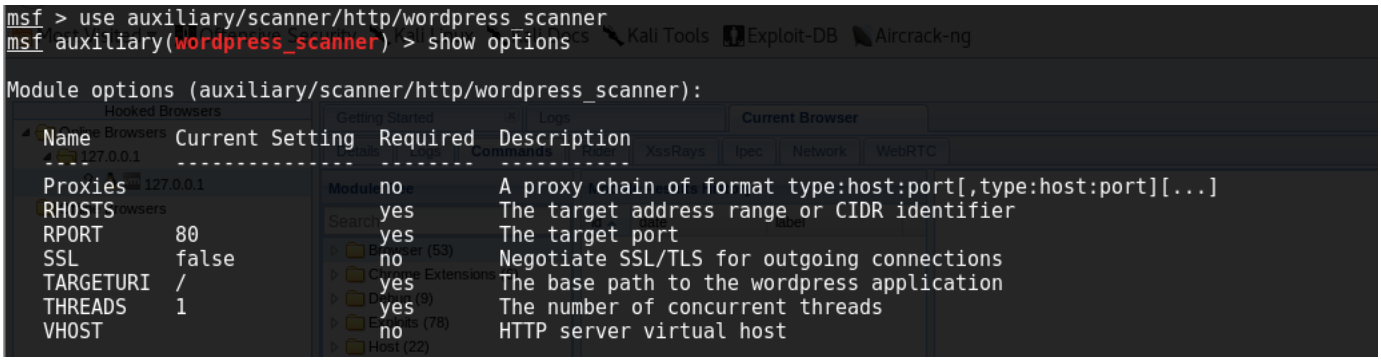
2.- Para buscar una categoría en particular se hace uso de la palabra ***search***



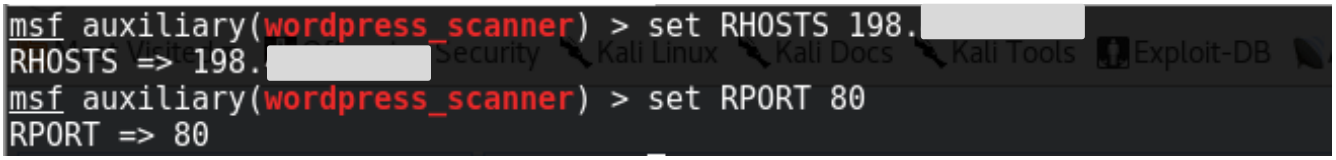
3.- Para seleccionar un exploit en particular.

use 'ruta_del_exploit'

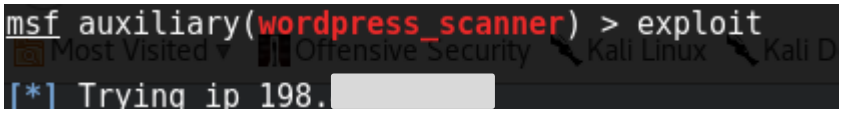
Para ver los requisitos necesarios para ejecutar el exploit, se hace uso del comando *show options*



4.- Para configurar los requisitos del exploit, se hace uso de la palabra *set* seguido de la información solicitada.



5.- Para realizar el ataque, se hace uso de la palabra ***exploit.***

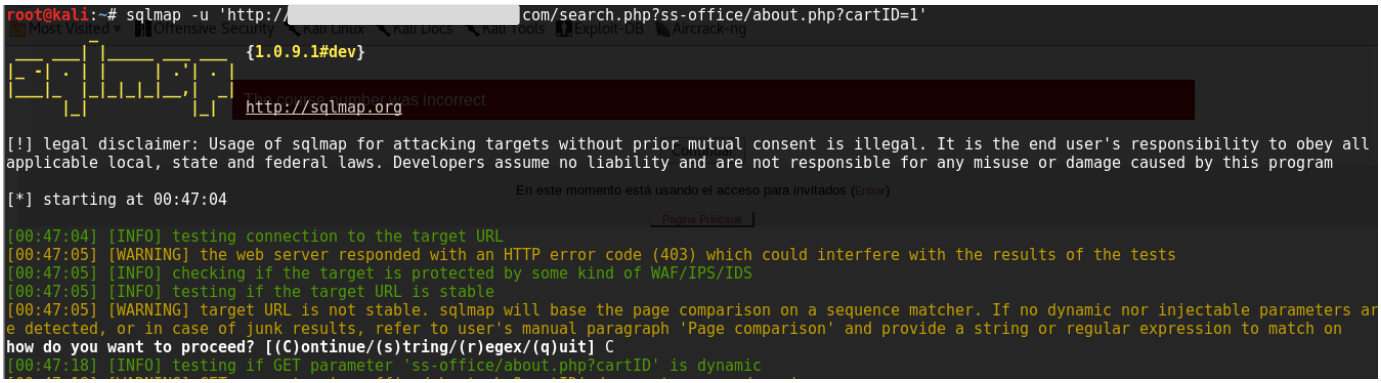


6.5.- Sqlmap

Herramienta de código abierto que permite identificar ataques de inyección SQL dentro de los sitios web.

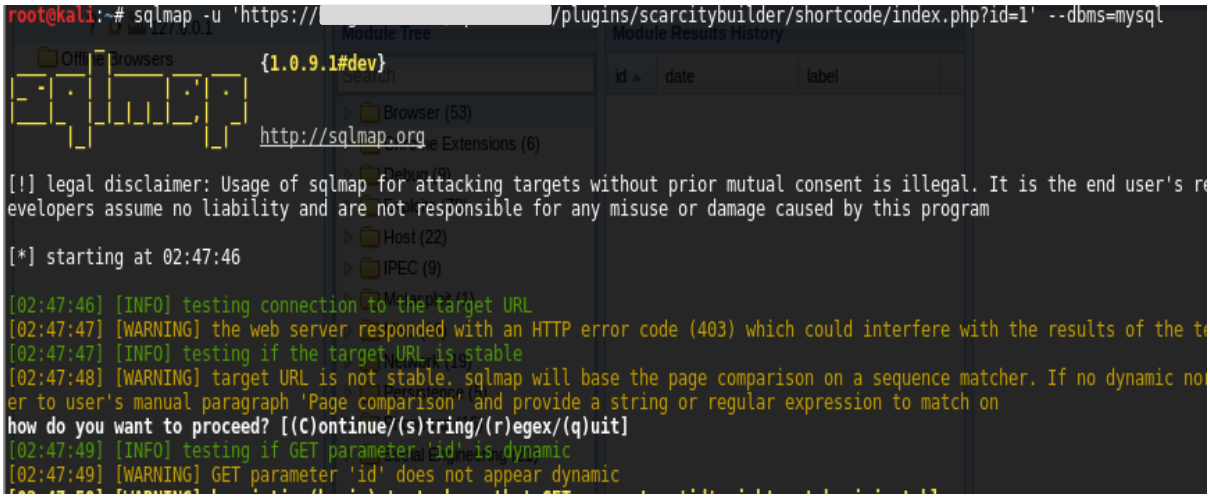
1.- Funcionamiento básico de la herramienta.

sqlmap -u 'dirección_url_con_parámetro_vulnerable'



2.- Para realizar el ataque haciendo uso de parámetros de un manejador de base de datos en particular.

sqlmap –u 'dirección_url_con_parámetro_vulnerable' --dbms=manejador_de_base_de_datos



3.- Para realizar un ataque más detallado:

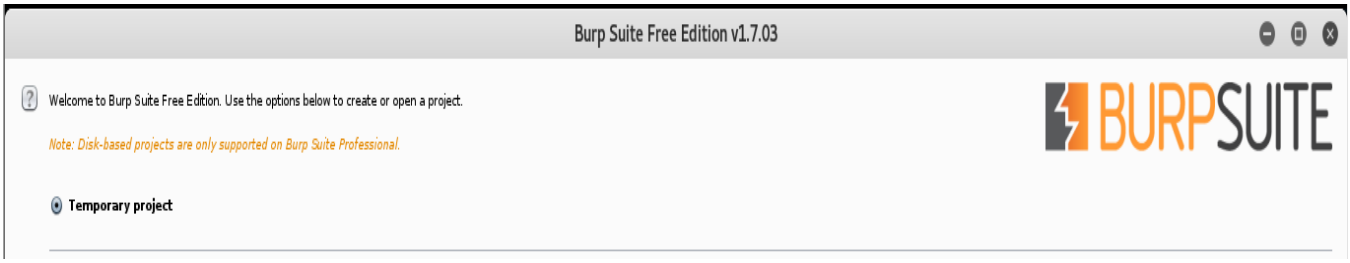
sqlmap –u 'direccion_url_con_parametro_vulnerable' --dbms=manejador_de_base_de_datos --level=[1-3]

```
sqlmap -u 'https://[redacted]/plugins/scarcitybuilder/shortcode/index.php?id=1' --dbms=mysql --level=3
```

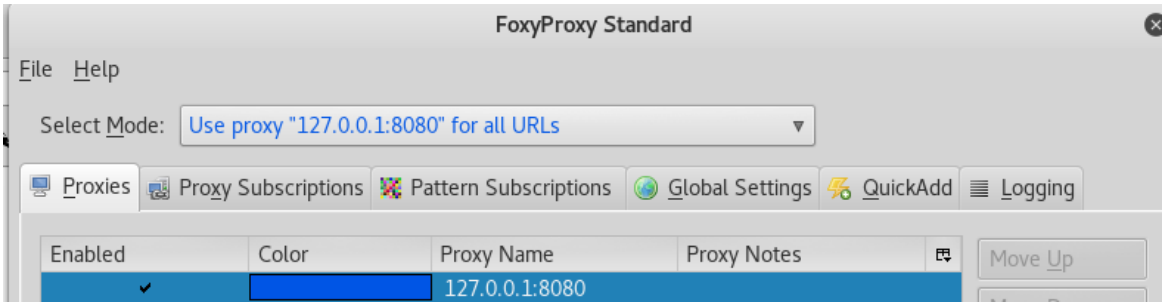
6.6.- Burpsuite

Herramienta utilizada para auditoria de sitios web, su utilidad principal es la funcionalidad de proxy, en la cual permite interceptar las peticiones realizadas entre el usuario y el sitio web, para realizar la modificación de estas, adicionalmente permite realizar ataques de fuerza bruta, entre otros.

1.- Para ejecutar la herramienta se debe de seleccionar la opción ***Temporary Project***.

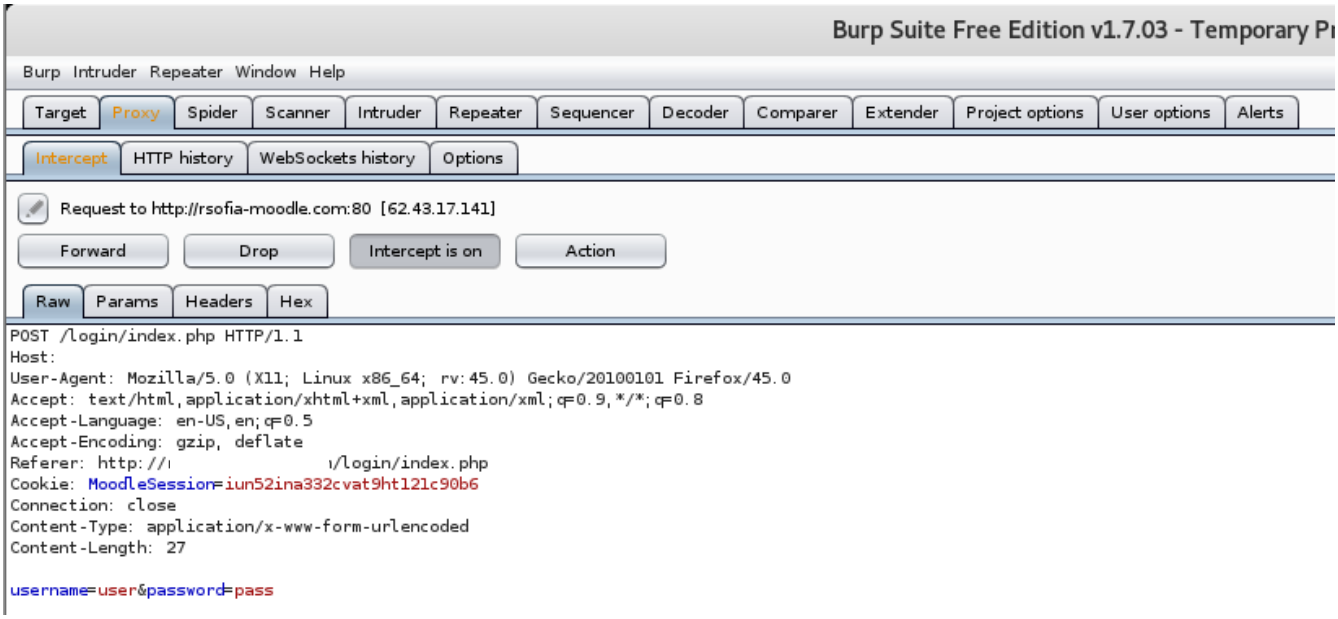


2.- Adicionalmente se debe de hacer uso de un proxy dentro del navegador del equipo de cómputo, para este ejercicio se usó la extensión proporcionada por el navegador **Firefox,** llamada ***FoxyProxy***, dentro de la cual se debe de configurar la dirección IP del localhost como proxy.



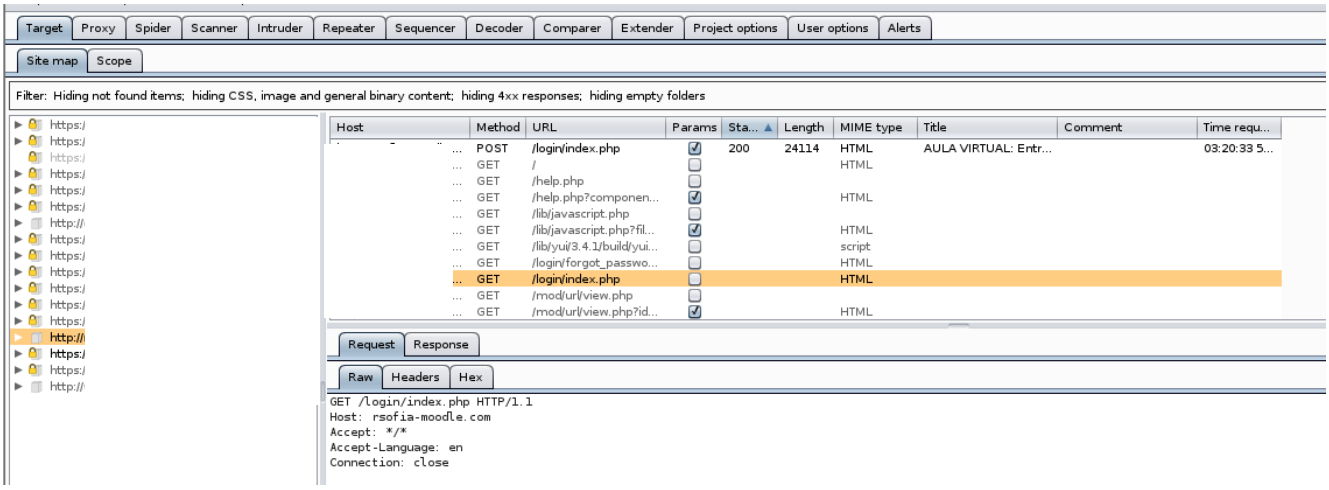
3.- Posteriormente, se debe de acceder al sitio web que se desea e interactuar con el mismo.

4.- Dentro de **BurpSuite,** se puede ver como se realizan las peticiones hacia el sitio web.



5.- Se puede modificar la información que será enviada hacia el sitio web, para ver su comportamiento, en este ejercicio se modificó el nombre de usuario y contraseña.

6.- Como se puede observar se lleva un registro de todas las peticiones realizadas.



6.7.- Nikto

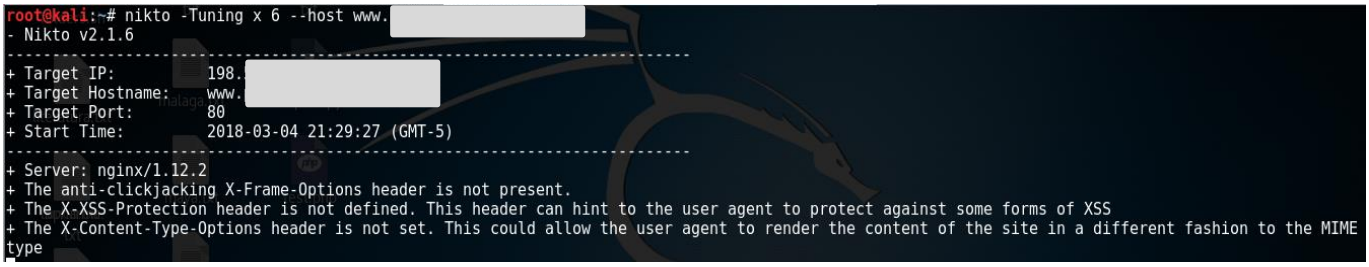
Escáner de vulnerabilidades de sitios web de código abierto, contiene dentro de su repositorio información relacionada a archivos, rutas de configuración, plugins instalados, entre otros.

1.- Funcionamiento básico de la herramienta.

nikto --host nombre_de_dominio

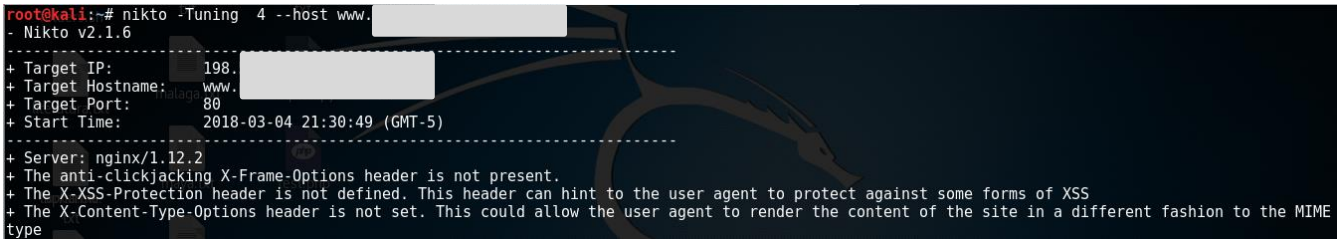
2.- Para realizar el escaneo de todos los componentes, excepto aquellos que permitan determinar un ataque de *Denegación de Servicio*, la opción es:

nikto –Tuning x 6 --host nombre_de_dominio



3.- Para realizar un escaneo solamente de componentes que permitan obtener información de ataques de *XSS*, la opción es:

nikto –Tuning 4 --host nombre_de_dominio

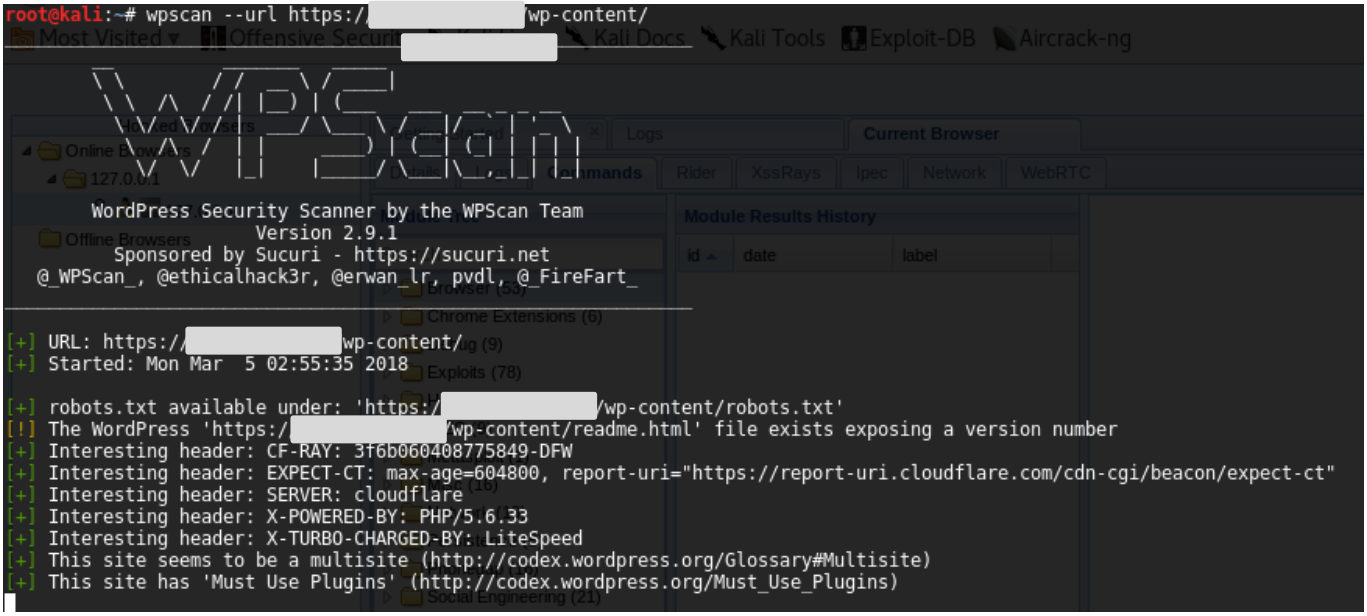


6.8.- Wpscan

Escáner de vulnerabilidades para gestores de contenido *Wordpress*.

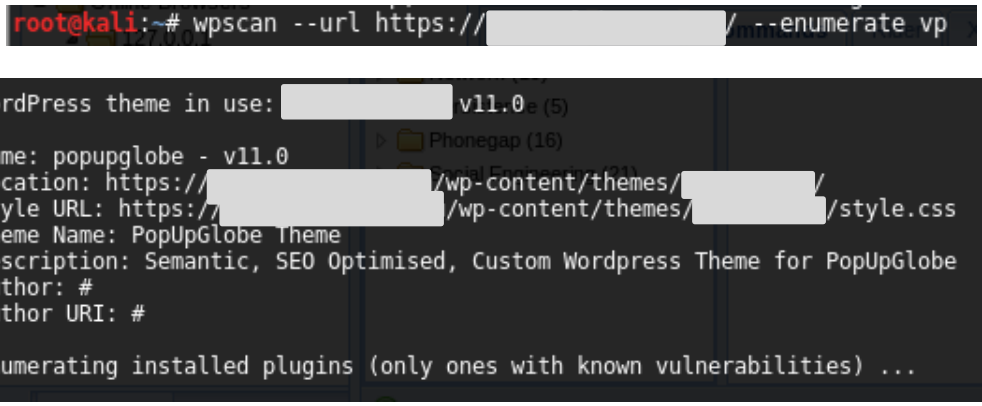
1.- Funcionamiento básico de la herramienta.

wpscan --url dirección_url_del_sitio



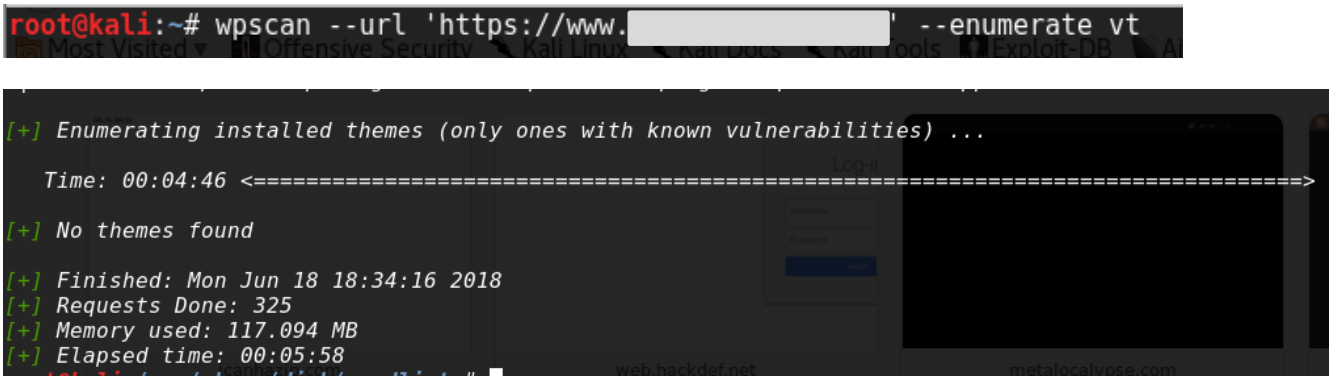
2.- Para listar los plugins que tiene el sitio web

wpscan --url dirección_url_del_sitio --enumerate vp



3.- Para lista los temas instalados en el sitio web.

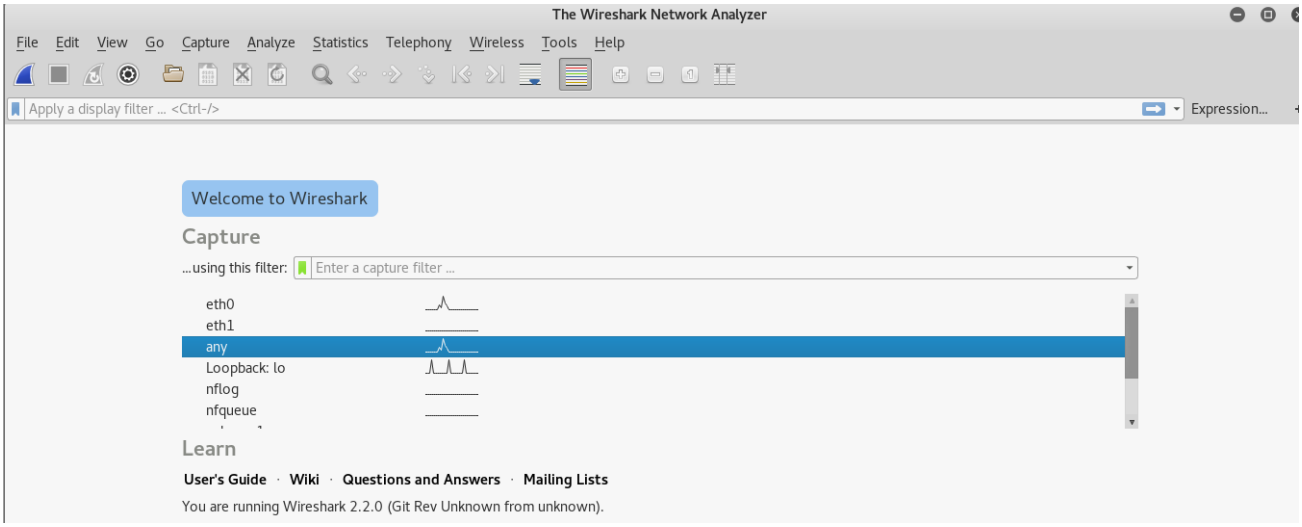
wpscan --url dirección_url_del_sitio --enumerate vt



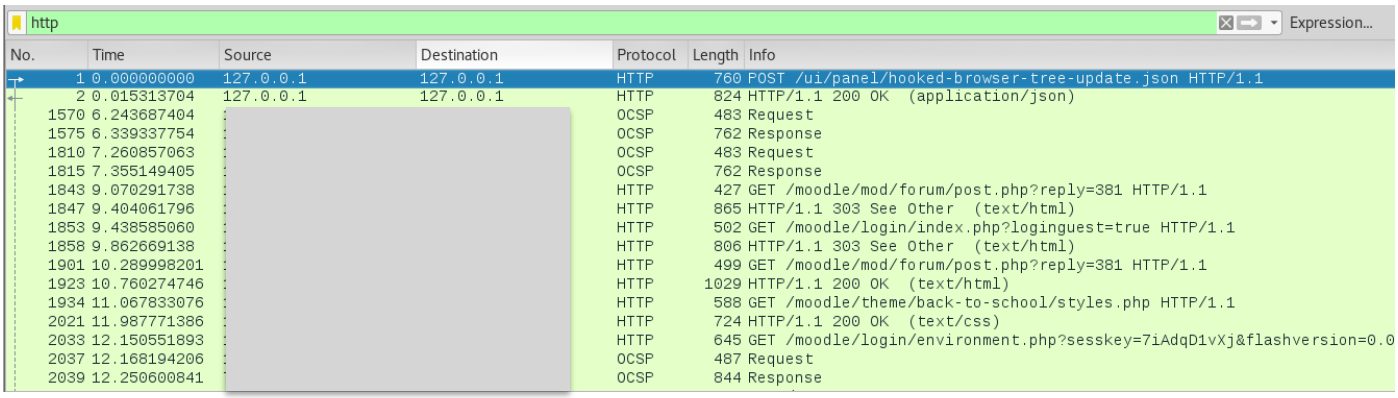
6.9.- Wireshark

Herramienta que permite capturar y analizar los paquetes transmitidos dentro de la red.

1.- Una vez ejecutada la herramienta se debe seleccionar la interfaz por la cual se va a capturar el tráfico.

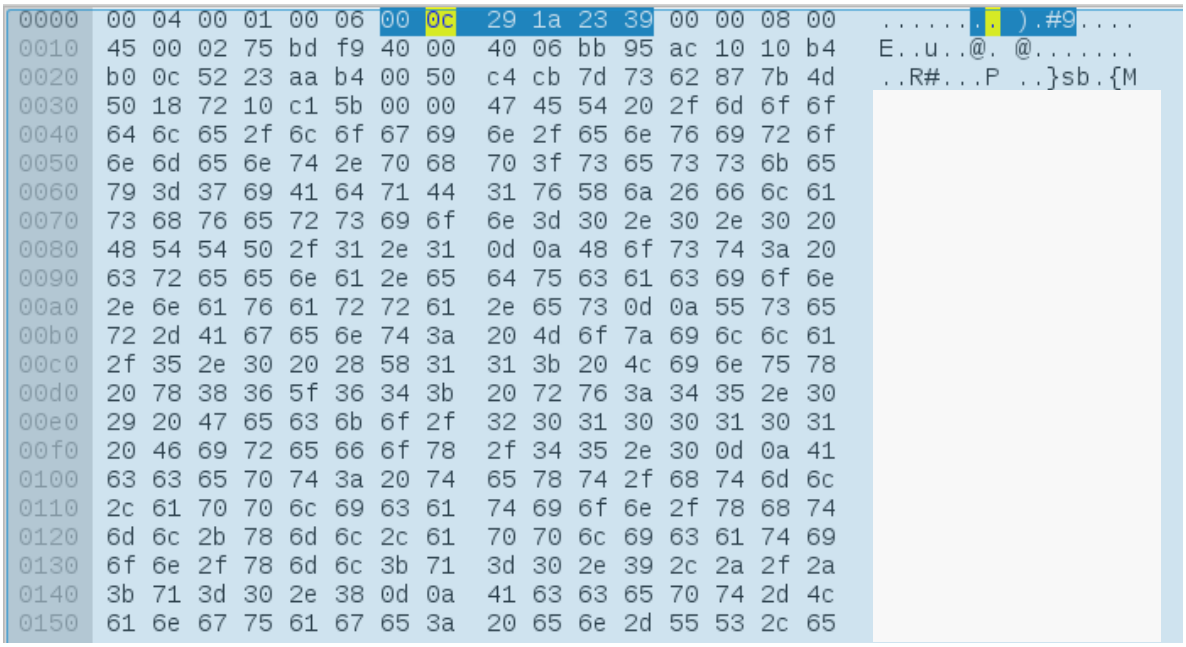


2.- Otro de los beneficios que proporciona **Wireshark** es la realización de filtros de la información, para ver todos los paquetes que van hacia sitios web, se puede hacer uso del filtro *http* o *https.*



3.- Al seleccionar un paquete, se puede ver la información que contiene.

4.- Adicionalmente se puede observar la información en claro enviada hacia el sitio web.



6.10.- Dzulum

Herramienta de desarrollo propio utilizada como escáner de vulnerabilidades para OJS (Open Journal System) y Moodle, adicionalmente, permite realizar ataques de fuerza bruta, crawling y explotación de vulnerabilidades.

1.- Para la instalación de la herramienta:

git clone https://github.com/rockrubio666/Dzulum.git

```
root@kali:~# git clone https://github.com/rockrubio666/Dzulum.git
```

2.- Para realizar escanear vulnerabilidades en sistemas que contengan OJS.

./scanner –o dirección_del_sitio

```
root@kali:~/ProyectoFinal# ./scanner.py -o http://[redacted].mx/ojs248/
```

```
Do yo want to update the databases? [y/N]
No updated :(

Beginning OJS scanner
Site Version: Open Journal Systems 2.4.8.0
Plugin Name: Resolver Gateway Plugin
Plugin Name: resolver
Plugin Name: Subscriptions Report Plugin
Plugin Name: subscriptions
Plugin Name: OJS TinyMCE Editor Plugin
Plugin Name: tinymce
Plugin Name: OJS Static Pages Plugin
Plugin Name: staticPages
Plugin Name: OJS Custom Block Manager Plugin
Plugin Name: customBlockManager
Plugin Name: pdf.js Viewer Plugin
Plugin Name: pdfJsViewer
Plugin Name: OJS CrossRef Export Plugin
Plugin Name: crossref
Plugin Name: OJS mEDRA Export Plugin
Plugin Name: medra
Plugin Name: OJS PubMed Export Plugin
Plugin Name: pubmed
Plugin Name: OJS Web Feeds Plugin
Plugin Name: webFeed
There are some exploits in our DB that could be used in thi site, Do you want to try them? [Y/n]
Sorry there aren't any exploit available in the database
```

3.- Para realizar el escaneo de vulnerabilidades en Moodle:

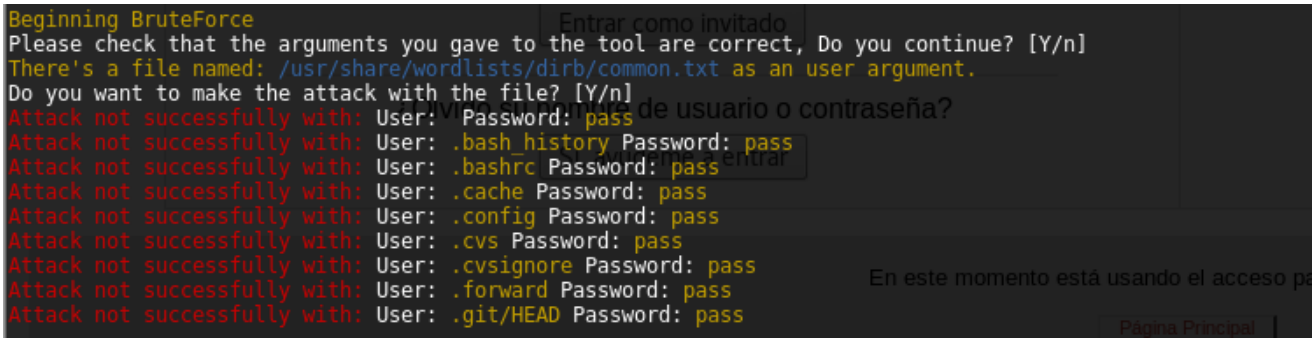
./scanner.py –m dirección_del_sitio

```
root@kali:~/ProyectoFinal# ./scanner.py -m http://[redacted].mx/moodle24
```

```
Do yo want to update the databases? [y/N]
No updated :(

Beginning moodle scanner
Version site:  2.4
Plugin Name: auth
Plugin Name: backup
Plugin Name: blocks
Plugin Name: cache
Plugin Name: calendar
Plugin Name: enrol
Plugin Name: filter
Plugin Name: lib
Plugin Name: message
Plugin Name: mod
Plugin Name: portfolio
Plugin Name: report
Plugin Name: tag
Plugin Name: theme
Plugin Name: repository
Theme Name: formal_white
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-9060/'
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-9059/'
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-7848/'
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-7846/'
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-7845/'
Vulnerability Link: https://www.cvedetails.com/cve/CVE-2014-7838/'
```

4.- Para realizar ataques de fuerza bruta:

./scanner.py –m sitio –B direccion_del_login, campo_del_usuario, campo_del_password, usuario, password, 'mensaje_de_error'



5.- Para realizar crawling a los directorios del sitio web:

./scanner.py –o sitio –d ruta_del_diccionario

Conclusiones

Como resultado del presente trabajo de tesis se puede concluir:

- La seguridad de la información no solamente se enfoca en proteger los datos, sino todo el entorno de estos, dentro de los cuales se contemplan: Bases de Datos, equipos de cómputo y usuarios que tienen algún conocimiento de dichos activos.

- La seguridad de la información continuará vigente mientras la tecnología siga evolucionando, debido a que día a día se encuentran nuevas vulnerabilidades en los sistemas.

- No existe un sistema de información completamente seguro, es decir, todos los sistemas son vulnerables en mayor o menor grado, por esa razón, es importante mantenerlos actualizados y realizar revisiones de seguridad periódicas con la finalidad de reducir las vulnerabilidades que podrían afectar a la organización.

- Las buenas prácticas de desarrollo seguro permiten a las organizaciones evitar la implementación de código que podría contener vulnerabilidades desde las primeras etapas del desarrollo de sistemas.

- La familia de las normas ISO 27000, proporcionan las bases necesarias para la implementación de un Sistema de Gestión de la Seguridad de la Información que permitirá a la organización realizar sus procesos sin afectar la funcionalidad de estos tomando en cuenta las medidas de seguridad necesarias para la protección de la información, adicionalmente, la adopción de planes de contingencia permite continuar con la operación cuando sucede cualquier situación no esperada.

Finalmente, en mi experiencia laboral en el campo de la seguridad de la información dentro del UNAM-CERT, puedo decir que la mayoría de las vulnerabilidades explotadas dentro de los sistemas son debido a errores de configuración o malas prácticas de seguridad, esto, debido a que no se tiene una cultura de seguridad de la información dentro de las organizaciones, la cual permita mostrar a los desarrolladores y administradores de sistemas que la protección de la información de los clientes es igual de importante que el funcionamiento del sistema.

Glosario

Concepto	Definición
ARPANET	Acrónimo de Advanced Research Project Agency Network, fue un Proyecto realizado por el departamento de defensa de los Estados Unidos, el cual dio paso a lo que hoy se conoce como Internet.
Backdoor	Concepto empleado en seguridad de la información para describir el acceso que tiene un atacante a un sistema, equipo, base de datos, etcétera., sin el conocimiento del usuario al que pertenece dicho activo.
Base de Datos	Colección de datos organizados y estructurados, en la cual se refleja la información de estos y su relación.
Cookie	Son utilizadas en los sitios web para llevar un registro de las actividades que realiza un usuario dentro de este, con la finalidad de que el funcionamiento del sitio sea más rápido.
Command & Control	Es el servidor que envía la información a los equipos que forman parte de una red de botnets.
Dot Dot Slash	En sistemas operativos Linux, permite saltar entre directorios sin la necesidad de conocer el nombre.
Exploit	Código que permite obtener acceso o privilegios a un sistema, servidor, etcétera.
Firewall	Dispositivo de seguridad de red que monitorea el tráfico de que recibe y envía un equipo de cómputo o servidor.
Framework	Esquema para el desarrollo o implementación de una aplicación.
FTP	Acrónimo de File Transfer Protocol, protocolo de red utilizado para la transferencia de archivos entre sistemas.
Honeypot	Equipo señuelo utilizado por los Equipos de Respuesta a Incidentes de Seguridad en Cómputo con la finalidad de que sea vulnerado por los atacantes informáticos y así obtener información sobre como realizan estos ataques.
IDS	Acrónimo de Intrusion Detection System, es un dispositivo de seguridad utilizado para la generar alertas cuando una organización detecta un ataque informático.
IoT	Acrónimo de Internet Of Things, son todos aquellos dispositivos de uso cotidiano (refrigeradores, televisiones, lámparas) que se encuentran conectadas a internet.
IPS	Acrónimo de Intrusion Prevention System, dispositivo de seguridad que provee un control de acceso a los activos de una organización.
Keylogger	Software que permite registrar las pulsaciones generadas en un teclado con la finalidad de obtener información sensible de una persona.
MBR	Acrónimo de Master Boot Record, identifica en que partición de un disco duro se encuentra el sector de arranque de un sistema

	operativo.
Moodle	Moodle es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. *
OJS	Acrónimo de Open Journal System, es un gestor de contenidos que permite la publicación de revistas de contenido científico.
Plugin	Complemento de un sistema o aplicación que proporciona funcionalidades adicionales.
POP3	Acrónimo de Post Office Protocol, protocolo que permite el envío de correos electrónicos.
Proxy	Es un intermediario entre el sitio web y el usuario, utilizado para el anonimato.
SSH	Acrónimo de Secure Shell, protocolo que permite establecer comunicaciones seguras entre dos sistemas.
VPN	Acrónimo de Virtual Private Network, es un canal utilizado para el anonimato o acceso a redes restringidas.
Wordpress	Gestor de contenidos enfocado en la creación de páginas web.

Bibliografía

Alejandro Reyes Plata. (2017). *UNAM-CERT: ¿Qué es y cómo funciona un ataque DDOS?*. Recuperado de: http://revista.seguridad.unam.mx/numero-12/que-es-y-como-funciona-un-ataque-ddos

Álvaro Gómez Vieites. (2017). *Edisa: Tipos de ataques e intrusos en las redes informáticas.* Recuperado de: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Applecoding (2015). *AppleCoding: Curso de Apps (I): estructura básica y primera app*. Recuperado: https://applecoding.com/cursos/curso-apps-estructura-basica

Argentina Code Dimension. (2007). Code Dimension: *¿Qué es y para que sirve un sitio web?.* Recuperado de: http://www.citethisforme.com/es/cite/website/autocite

Burp Suite (2014). *Kali: Burp Suite Package Description*. Recuperado de: https://tools.kali.org/web-applications/burpsuite

Buyto (2016) Buyto: *Páginas web Estáticas – Que son y para queé sirven.* Recuperado de: http://www.buyto.es/general-diseno-web/que-es-una-pagina-web-estatica-para-que-sirve-una-pagina-web-estatica

Buyto (2016). Buyto: *Páginas web Dinámicas – Que son y para quequé sirven*. Recuperado de: http://www.buyto.es/general-diseno-web/que-es-una-pagina-web-dinamica-para-que-sirve-una-pagina-web-dinamica

Charit Mishra. (2016). *Mastering Wireshark (308).* UK: Packt Publishing.

DIRB (2014). *Kali: DIRB Package Description*. Recuperado de: https://tools.kali.org/web-applitacions/dirb

EstudioSeijo (2015). *EstuioSeijo: Web 1.0, Web 2.0 y Web 3.0*. Recuperado de: http://www.estudioseijo.com/noticias/web-10-web-20-y-web-30.htm

EstudioSeijo (2017). *EstudioSeijo: Tipos de sitios web*. Recuperado de: http://www.estudioseijo.com/noticias/tipos-de-sitios-web.htm

Paola CasasFES Acatlán. (2015), Paola Casas: *El triángulo de la Seguridad*. FES Acatlán. Recuperado de: http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/

Gonzalo Suez (2013) *Joomla Community Magazine: Estructuta y Composición de un Sitio Web*. Recuperado de: https://magazine.joomla.org/es/ediciones-anteriores/julio-2013/item/1398-estructura-y-composicion-de-un-sitio-web

David López. (2018). David López: *Grupo Control:. Evolución de la Seguridad Informática*. Recuperado de: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

Ignacio Pérez (2015). *We live security: Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web*. Recuperado de: https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/

Ignacio Pérez. (2015). *We live security: ¿En qué consiste la vulnerabilidad Cross Site Request Forgery (CSRF)?.* Recuperado de: https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/

Inf-fu. (2017). Inf-fu: The Making of thw World Wide Web. Recuperado de: http://www.inf.fu-berlin.de/lehre/SS01/hc/www/www2.html

InformaticaHoy (2017). *Informatica Hoy: Qué es una Intranet y para qué sirve?.* Recuperado de: https://www.informatica-hoy.com.ar/aprender-informatica/Que-es-una-Intranet.php

ISO (2018). *ISO: About ISO*. Recuperado de: https://www.iso.org/about-us.html

Jason Deckard. (2005). *Buffer Overflow Attacks (304).* USA: Syngress.

Jorge Jimeno Bernal (2013). *PDCA Home: Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua*. Recuperado de: https://www.pdcahome.com/5202/ciclo-pdca/

Juan (2016). *We live security: 5 cosas que debes saber sobre la Ingeniería Social.* Recuperado de: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

Justin Seitz. (2014). Black Hat Python: Python Programming for Hackers and Pentesters (192). USA: No Strach Press.

Kali (2018). *Kali: Our Most Advanced Penetration Testing Distribution, Ever.* Recuperado de: https://www.kali.org/

Kaspersky Labs. (2017). *Kaspersky Labs: Más información sobre el malware y cómo proteger todos tus dispositivos.* Recuperado de: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

María de Jesús Lapuente. (2013). *Hipertext: Bases de Datos*. Recuperado de: http://www.hipertexto.info/documentos/b_datos.htm

Metasploit (2014). *Kali: metasploit-framework Package Description*. Recuperado de: https://tools.kali.org/explotation-tools/metasploit-framework

Microsoft. (2018), *Microsoft: What is the Security Development Lifecycle?.* Recuperado de: https://www.microsoft.com/en-us/sdl

Milenium. (2017). *Milenium*: Sitio Web. Recuperado de: http://www.informaticamilenium.com.mx/es/temas/que-son-los-sitios-web.html

MindTools (2018). *MindTools: SMART Goals*. Recuperado de: https://www.mindtools.com/pages/article/smart-goals.htm

Moodle (2018). *Moodle: Acerca de Moodle*. Recuperado de: https://docs.moodle.org/all/es/Acerca_de_Moodle

Netsparker (2018). *CIRT: Nikto2*. Recuperado de: https://www.cirt.net/Nikto2

Nipul Jawsal. (2014). *Mastering Metasploit (378).* UK: Packt Publishing.

Nmap (2014). *Kali: Nmap Package Description*. Recuperado de: https://tools.kali.org/information-gathering/nmap

OWASP. (2011). *OWASP: Session Prediction*. Recuperado de: https://www.owasp.org/index.php/Session_Prediction

OWASP. (2013). *OWASP: Top 10 2013.* Recuperado de: https://www.owasp.org/index.php/Top_10_2013-Top_10

OWASP. (2013). US-CERT: *Introduction to the CLASP Process.* Recuperado de: https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/introduction-to-the-clasp-process

OWASP. (2014). *OWASP: Hijacking Attack*. Recuperado de: https://www.owasp.org/index.php/Session_hijacking_attack

OWASP. (2015). *OWASP: Man in the middle attack*. Recuperado de: https://www.owasp.org/index.php/Man-in-the-middle_attack

OWASP. (2016). OWASP: Man in the browser attack. Recuperado de: https://www.owasp.org/index.php/Man-in-the-browser_attack

Panda Security. (2017). *Panda Security: Phishing.* Recuperado de: https://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/

Panda. (2018). *Panda: Classic Malware: su historia, su evolución*. Recuperado de: https://www.pandasecurity.com/peru/homeusers/security-info/classic-malware/

Pedro Pimienta (2017). *Zenva: Tipos de aplicaciones móviles y sus características*. Recuperado de: https://deideaaapp.org/tipos-de-aplicaciones-moviles-y-sus-caracteristicas/

Peter Arntz. (2016). *Malwarebytes: Explained: Advanced Persistent Threat (APT*). Recuperado de: https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/

Praxis High Integrity Systems Ltd. (2013). *US-CERT: Correctness by Construction.* Recuperado de: https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/correctness-by-construction

Project Management Institute. (2018), *Project Management Institute: ¿Qué es un estándar?*. Recuperado de: http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Rockrubio666 (2018). *Github: Dzulum*. Recuperado de: https://github.com/rockrubio666/Dzulum

Sgoliver. (2010). *Sgoliver.net: Componentes de una aplicación Android*. Recuperado de: http://www.sgoliver.net/blog/componentes-de-una-aplicacion-android/

Software Engineering Institute. (2007). *Software Engineering Institute: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Proce*ss. Recuperado de: ftp://ftp.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf#page32

Sqlmap (2014). *Kali: sqlmap Package Description*. Recuperado de: https://tools.kali.org/vulnerbaility-analysis/sqlmap

T. J. O'Connor. (2012). *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers (262).* USA: Syngress Media Inc.

Tajinder Kalsi. (2016). *Practical Linux Security Cookbook* (277). UK: Packt Publishing.

THC-Hydra (2014). *Kali: Hydra Package Description*. Recuperado de: https://tools.kali.org/password-attacks/hydra

UNAM-CERT (2015). *UNAM-CERT: ¿Qué es y cómo opera un ataque Cross-Site-Scripting* (XSS)?. Recuperado de: https://www.seguridad.unam.mx/historico/documento/index.html-id=35

UNAM-CERT. (2017). *UNAM-CERT: DDOS*. Recuperado de: https://www.seguridad.unam.mx/historico/usuario-casero/?txtbusq=ddos

UNAM-CERT. (2018), UNAM-CERT: *Usuario Casero*. Recuperado de: https://www.seguridad.unam.mx/historico/usuario-casero/

US Norton. (2017). *US Norton: What is malware and how can prevent it?.* Recuperado de: https://us.norton.com/internetsecurity-malware.html

US-CERT. (2013), *US-CERT: Secure Software Development Life Cycle Processes.* Recuperado de: https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes#tsp

Vivek Ramachadran, Cameron Buchanan. (2015). *Kali Linux Wireless Penetration Testing (214)*. UK: Packt Publishing.

Wireshark (2014). *Kali: Wireshark Package Description*. Recuperado de: https://tools.kali.org/information-gathering/wireshark

Wolf Halton. (2016). *Kali Linux 2: Windows Penetration Testing (422).* UK: Packt Publishing.

WPscan (2014). *Kali: WPScan Package Description*. Recuperado de: https://tools.kali.org/web-applications/wpscan