WEB DEFACEMENT

Oscar A. Pulido Rodríguez
Director: Juan Carlos Martínez Santos

Universidad Tecnológica de Bolívar
Facultad de Ingenierías
Programa de Ingeniería de Sistemas
Cartagena

Enero de 2016

WEB DEFACEMENT

Oscar A. Pulido Rodríguez

Trabajo de grado para optar al título de

Ingeniero de Sistemas

Director: Juan Carlos Martínez Santos

Universidad Tecnológica de Bolívar
Facultad de Ingenierías
Cartagena

Enero de 2016

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍAS

Título: Web Defacement

Autor: Oscar Pulido Rodríguez

Jurado

Jurado

Director:

Cartagena, Enero de 2016

Resumen

En el siguiente proyecto investigativo encontraremos un seguimiento a la página principal de la Universidad Tecnológica de Bolívar (www.unitecnologica.edu.co). El seguimiento fue de dos meses, donde en el primer mes se monitorearon los ataques que le hicieron a ésta. Posterior a esto, en el segundo mes se concentró en verificar el cambio de contenido, donde se monitorearon los cambios efectuados en la página, es decir, se quiso saber si se le hizo algún cambio a la página, éste haya sido de parte del *web master* u otra persona autorizada para hacer dicho cambio. Se utilizaron diversas herramientas para comparar su trabajo y para saber así, cual según las necesidades de la universidad le es más conveniente. Dichas herramientas son algunas totalmente gratuitas, otras son pagas pero ofrecen 30 días de prueba. Los resultados se encuentran tabulados de manera de fácil comprensión. Al final se arrojará una conclusión, la cual será dada a criterio propio y así saber si habrá un siguiente paso o determinar si la universidad no necesita de estas herramientas. Se presentaron problemas con algunas herramientas que serán detallados más adelante, a medida que se entregue información de cada una de estas.

Agradecimientos

Se debe hacer una mención al webmaster de la Universidad Tecnológica de Bolívar (Richard Velasquez), quien fue la persona encargada de decir que tan acertados fueron los reportes de las distintas aplicaciones.

Contents

List of Figures

List of Tables

Capítulo 1.
Introducción

Conforme al crecimiento de la internet, crecen los riesgos de las páginas web y más si son de tráfico alto, esto debido a que existen personas malintencionadas con diferentes propósitos, unos por demostrar su sabiduría y otros por hacer daño y ganar fama dentro del mundo de la internet. Ante esta situación, cada web master debe preocuparse por que su página esté siempre en linea, a demás que mantenga siempre el contenido que él le proporcione y califique como adecuado para su página.

En el siguiente estudio que se realizó en dos meses, se mostrarán los resultados de que tanto es atacada la página de la universidad y se presentarán diferentes servicios que ayudarán a identificar cuales son las características que suplen las necesidades de la ésta.

1.1 Planteamiento del problema.

El aumento de la publicación de sitios web en el mundo como medio de comunicación e información por aprte de las organizaciones ha generado el aumento proporcional de ataques informáticos a estos sitios que buscan afectar la confidencialidad, integridad y disponibilidad de la información. Es el caso de los denominados "Defacers" los cuales

buscan identificar y explotar vulnerabilidades de los sitios web y sus servidores para lograr afectar la integridad de los archivos y contenidos funcionales de los sitios.

La existencia de comunidades virtuales (como Anonymous) que está realizando ataques dirigidos contra organizaciones gubernamentales, militares y empresas privadas por diferencias políticas, religiosas, ideológicas, ambientales, ciberguerra, sociales o simplemente por diversión [8] evidencia el crecimiento del problema y el conjunto de riesgos al que están sometidos sitios web públicos en la red. Posteriormente, se mostrarán datos estadísticos que demostrarán que existe la necesidad de desarrollar controles de seguridad informática que prevengan, detecten o bloqueen los ataques; mediante un modelo que realice la contención, informe al responsable del sitio web y el equipo de respuesta a incidentes informáticos interno o del proveedor tecnológico y finalmente permita dar tiempo a una corrección por parte de los administradores antes de que se genere un impacto reputacional o económico por pérdidas de la integridad de los sitios web.

1.2 Objetivos.

El principal objetivo de este estudio realizado en dos meses, es determinar si es necesario o no usar una herramienta de monitoreo para las páginas de la Universidad Tecnológica de Bolívar.

Para lograr el anterior objetivo se proponen los siguientes objetivos específicos:

- Identificar las vulnerabilidades y riesgos que permiten el éxito de los ataques

informáticos tipo Defacement en sitios Web en la Universidad Tecnológica de Bolívar.

- Establecer estrategias para brindar protección a los riesgos identificados en el objetivo anterior.

- En caso de ser necesario el uso de una de estas herramientas, y verificar si una de las implementadas en el periodo de prueba cumpla con todos los requerimientos que la UTB presenta.

- En caso de ser necesario el uso de una de estas herramientas, y que al verificar que ninguna de las implementadas en el periodo de prueba cumpla con la totalidad de los requerimientos que la UTB presenta, determinar cuáles son los fuertes que tienen unos, que otros no tienen. Esto para determinar si es viable desarrollar una herramienta propia que atienda a las necesidades específicas de la Universidad Tecnológica de Bolívar.

1.3 Justificación.

La Universidad Tecnológica de Bolívar como empresa, no debe permitir que su ventana ante el mundo no esté en optimas condiciones o tenga contenidos inapropiados introducidos por maliciosos. Por esto debe tomar una decisión, seguir vulnerable a la no fácil detección de anomalías en sus páginas, o buscar una herramienta que le permita alertar rápidamente ante algún evento no normal de éstas.

Para lograr observar la importancia y la relevancia que tiene el ataque web en la actualidad, a continuación mostraremos estadísticas de años anteriores que nos harán reflexionar sobre lo anteriormente dicho:

En la siguiente gráfica vemos las 10 técnicas más usadas de ciberataques en 2014 (ver figura 1.1). Podemos observar que el web defacement más común de los ataques conocidos (con un porcentaje de 16,4), esto nos lleva a darle una justificación a esta investigación.

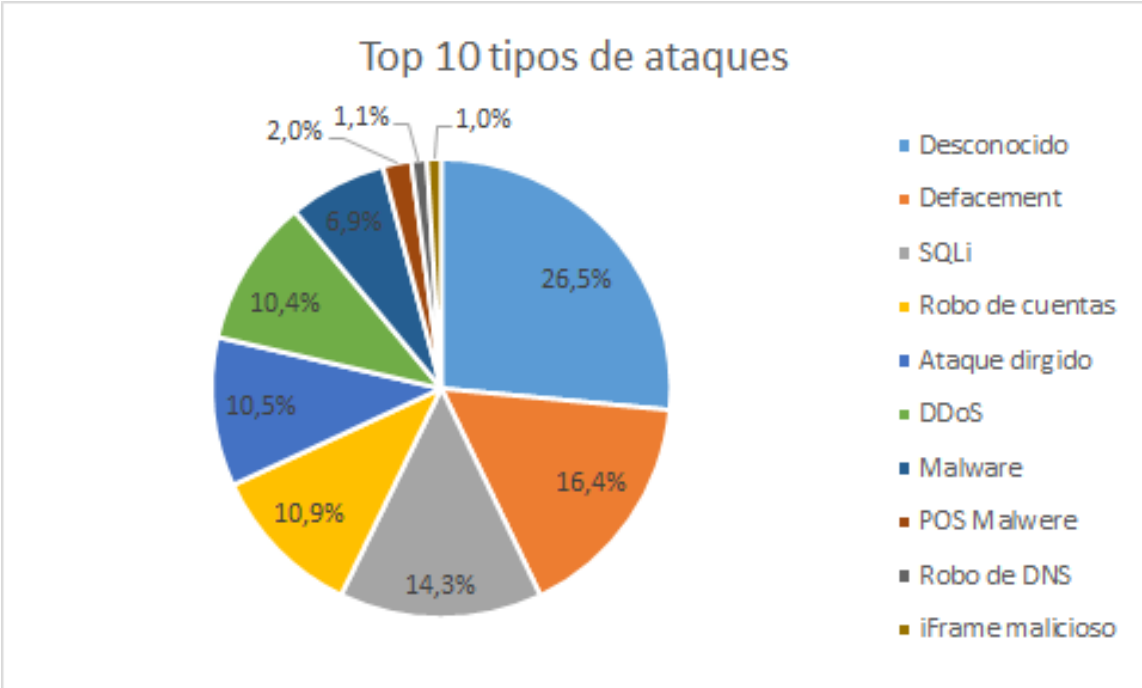

Figure 1.1: 10 Técnicas de ataques más comunes [17].

Mientras en la Figura 1.2 observamos las instituciones más atacadas durante el mismo año en estudio (2014), podemos observar que nuestro caso (educación) se encuentra de sexto lugar entre los más atacados (con un porcentaje de 5.5), un número considerable donde la próxima víctima podría ser la página de la UTB.

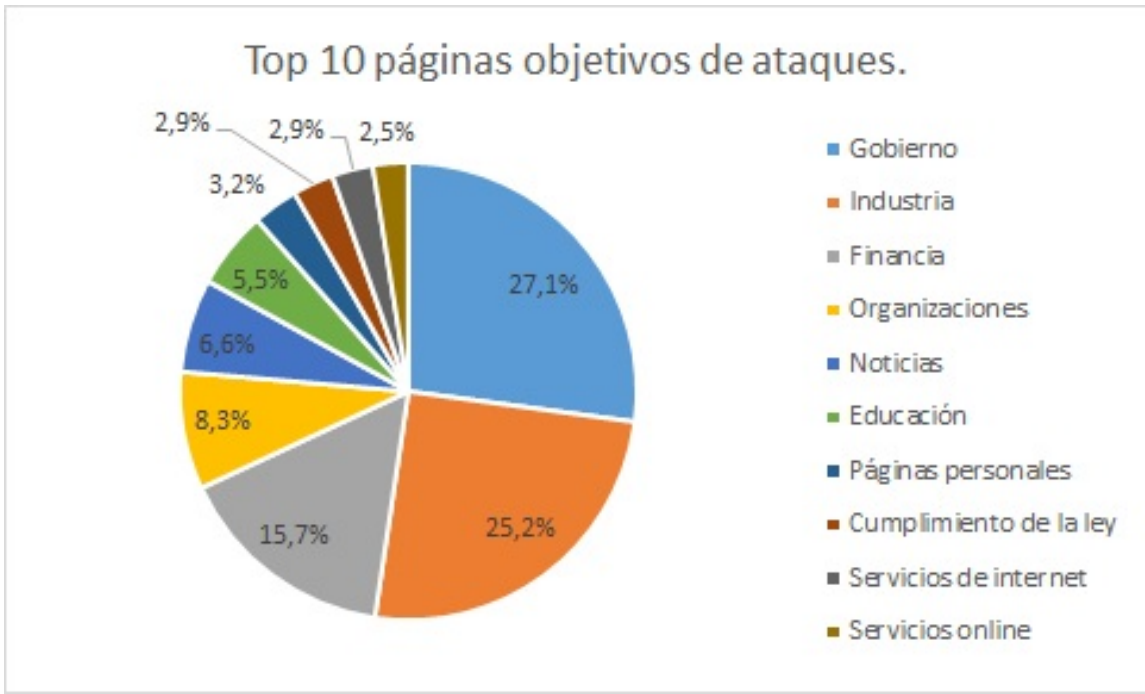

Figure 1.2: Top 10 de páginas objetivos en 2014 [17].

Capítulo 2.
Marco teórico.

2.1 Marco teórico.

El termino website defacement hace referencia a un cambio no autorizado hecho a la apariencia de simplemente página web o un sitio entero. En ciertos casos un sitio web es completamente derribado y reemplazado por una nueva página web. En otras ocasiones un hacker puede inyectar código al punto de añadir imágenes, popups, o texto a una página que anterior mente no tenia. A demás, otra manera de deformar websites puede ser introducir código malicioso con el intento de infectar las computadoras de los visitantes, así hacerlos vulnerables a ataques de virus y otros problemas. [12]

2.1.1 Hacker

Un hacker es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador.[3]

Existen dos tipos de hackers que son los siguientes:

- Hackers de sombrero blanco (White hat hackers): Hacker blanco o white hacker

es un término inventado a finales de los 90 para definir a los hackers que se dedicaban profesionalmente a la seguridad informática y practicaban el hacking desde motivaciones éticas o económica. Surgió como contrapunto a los black hackers o hackers de sombrero negro, criminales informáticos. [14]

- Hackers de sombrero negro (Black hat hackers): Un hacker de sombrero negro es un hacker que viola la seguridad informática por razones más allá de la malicia o para beneficio personal. Los hackers de sombrero negro son la personificación de todo lo que el público teme de un criminal informático. Los hackers de sombrero negro entran a redes seguras para destruir los datos o hacerlas inutilizables para aquellos que tengan acceso autorizado. [24]

2.1.2 Website Monitoring.

Website monitoring es el proceso de prueba y registro de tiempo de estado de una o más páginas web. Estas herramientas de monitoreo, aseguran que el sitio web está accesible para todos los usuarios y es usada por negocios, organizaciones e instituciones para asegurar que el sitio web esté en linea, funcionando y el rendimiento sea siempre el optimo.

2.1.3 Servidor web.

Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información. A modo de ejemplo, imaginemos

que estamos en nuestra casa, y tenemos una despensa. Pues bien a la hora de comer necesitamos unos ingredientes por lo cual vamos a la despensa, los cogemos y nos lo llevamos a la cocina para cocinarlos. [11] Existen distintos tipos de servidores web:

- Servidor DNS: Son centros de datos situados en distintas ubicaciones geográficas que poseen computadoras con bases de datos, en las que están registradas las direcciones que corresponden a los millones de sitios web de internet existentes. Tienen registrada la relación que existe entre cada nombre de dominio y su dirección IP correspondiente.[16]

- Servidor FTP: Uno de los servicios más antiguos de Internet, es el File Transfer Protocol (FTP), este permite mover uno o más archivos con seguridad entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia, los Servidores FTP comunicaban con los clientes "en abierto," es decir, que la información de la conexión y de la contraseña eran vulnerables a la interceptación, de ahí la importancia y uso de los mismos.[9]

- Servidor SMTP: El acrónimo SMTP proviene de Simple Mail Transfer Protocol (Protocolo de Transferencia de Correo Simple), es decir, el procedimiento que permite el transporte del email en la Internet. Qué sucede cuando usted envía un email? El proceso de entrega del email es en realidad muy similar al correo clásico: un sistema organizado se encarga de transportar su mensaje a lo largo

de una serie de pasos y deposita el mismo en su destinatario. En este proceso, el servidor SMTP es simplemente una computadora que ofrece un servicio de SMTP, la cual actúa más o menos como un cartero electrónico. Una vez que el mensaje ha sido entregado al servidor, este se encarga de concretar la entrega a sus destinatarios.[18]

- Servidor Proxy: Un servidor proxy es un equipo que actúa de intermediario entre un explorador web e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor proxy, el servidor proxy la proporciona, lo que resulta más rápido que consultar la Web. Los servidores proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado.[29]

2.1.4 Hash.

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).[1]

En la tabla 2.1 se listarán los diferentes tipos de hash:

Tipo	Ejemplo	Usado en	Longitud
DES (Unix)	lvS7aeT4NzQPM	Usado en Linux y sistemas similares	13 caracteres
Domain Cached Credentials	Admin:b474d48cdfc4974d86ef4d24904cdd91	Se utiliza para almacenar en caché las contraseñas de dominio de Windows	16 bytes
MD5 (Unix)	$1$12345678$XM4P3PrKBgKNnTaqG9P0T/	Usado en Linux y sistemas similares	34 caracteres
MD5 (APR)	$apr1$12345678$auQSX8Mvzt.tdBi4y6Xgj.	Usado en Linux y sistemas similares	37 caracteres
MD5 (phpBB3)	H9123456785DAERgALpsri.D9z3ht120	Usado en phpBB 3.x.x	34 caracteres
MD5 (WordPress)	PB123456780BhGFYSlUqGvE6ErKErL01	Usado en WordPress	34 caracteres
RAdmin 2.x	5e32cceaafed5cc80866737dfb212d7f	Usado en la aplicación Remote Administrator v2.x	16 bytes
MD5	c4ca4238a0b923820dcc509a6f75849b	Usado en phpBB 2.x, Joomla >= 1.0.13 y otros sistemas CMS	16 bytes
SHA-1	356a192b7913b04c54574d18c28d46e6395428ab	Usado en varios foros y CMS	20 bytes
SHA-256 (Unix)	$5$12345678$jBWLgeYZbSvREnuBr5s3gp13vqi	Usado en Linux y sistemas similares	55 caracteres
SHA-1 (Django)	sha1$12345678$90fbbcf2b72b5973ae42cd3a19ab4ae8a1bd210b	Usado en Linux y sistemas similares	54 caracteres
SHA-256 (Django)	sha256$12345678$154c4c511cbb166a317c247a839e46...	Usado en Linux y sistemas similares	90 caracteres

Figure 2.1: Tipos de hash [13].

2.1.5 Ejecución en hilos (threads).

En sistemas operativos, un hilo de ejecución, hebra o subproceso es la unidad de procesamiento más pequeña que puede ser planificada por un sistema operativo.

La creación de un nuevo hilo es una característica que permite a una aplicación realizar varias tareas a la vez (concurrentemente). Los distintos hilos de ejecución comparten una serie de recursos tales como el espacio de memoria, los archivos abiertos, situación de autenticación, etc. Esta técnica permite simplificar el diseño de una aplicación que debe llevar a cabo distintas funciones simultáneamente.

Un hilo es simplemente una tarea que puede ser ejecutada al mismo tiempo con otra tarea.[28]

2.1.6 Protocolos de comunicación.

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física.[25]

Existen distintos tipos de protocolos de comunicación, entre esos el protocolo HTTP (Hypertext Transfer Protocol o en español Protocolo de Transferencia de Hipertexto)el cual es, dicho de forma sencilla, el lenguaje de comunicación que se utiliza en la Web para que los clientes y los servidores puedan entenderse entre sí. [6]

Cada transacción HTTP es una comunicación distinta. En cada una de ellas se intercambian mensajes. Según la especificación del protocolo, un mensaje es "la unidad básica de la comunicación HTTP y consiste de una secuencia estructurada de octetos ordenados con formato válido y transmitidos por la conexión". Existen dos tipos de mensajes, petición (*request*) y respuesta (*response*). [5]

La petición es un mensaje de texto creado por un cliente (por ejemplo un navegador, una aplicación para el celulares, etc.) en un formato especial conocido como HTTP. El cliente envía la petición a un servidor, y luego espera la respuesta. [22]

Para hacer estas peticiones se necesita un método que son quienes definen lo que se quiere hacer con los recursos. En la Tabla 2.1, se verán los distintos métodos

existentes y una breve descripción.

Método	Descripción
Get	Devuelve el recurso identificado en la URL pedida
Post	Indica al servidor que se prepare para recibir información del cliente. Suele usarse para enviar información desde formularios.
Put	Envía el recurso identificado en la URL desde el cliente hacia el servidor.
Options	Pide información sobre las características de comunicación proporcionadas por el servidor. Le permite al cliente negociar los parámetros de comunicación.
Trace	Inicia un ciclo de mensajes de petición. Se usa para depuración y permite al cliente ver lo que el servidor recibe en el otro lado.
Delete	Solicita al servidor que borre el recurso identificado con el URL.
Conect	Este método se reserva para uso con proxys. Permitirá que un proxy pueda dinámicamente convertirse en un túnel. Por ejemplo para comunicaciones con SSL.
Head	Funciona como el GET, pero sin que el servidor devuelva el cuerpo del mensaje. Es decir, sólo se devuelve la información de cabecera.

Table 2.1: Tipos de verbos HTTP [7].

Una vez que un servidor ha recibido la petición, sabe exactamente qué recursos necesita el cliente (a través de la URI) y lo que el cliente quiere hacer con ese recurso (a través del método). Por ejemplo, en el caso de una petición GET, el servidor prepara el recurso y lo devuelve en una respuesta HTTP. [22]

Capítulo 3.
Estado del arte.

Existen tres tipos de herramientas para monitorear páginas web: herramientas de escritorio, herramientas en la nube y extensiones del navegador.[2]

Para el presente estudio, se utilizaron solo herramientas en la nube, las cuales se detallarán a continuación y posteriormente se expondrán los resultados.

A continuación se detallaran algunas investigaciones referente a la problemática planteada. (Tomado de propuesta presentada a consejo académico)

3.1 Mecanismo avanzado para reducir falsas tasas de alarma en detecciones de web page defacement.

Contiene un mecanismo para la detección desde un sitio remoto de sitios web que han sido afectadas por el ataque tipo Defacement y un método de ajuste de umbral. Para un mecanismo de detección, se genera un vector de características para cada página web mediante el uso de indice de frecuencia, que calcula la similitud entre el vector de características actual y el vector de características anterior y decide si la página ha sido alterada o no, comparando la similitud del umbral actual con el

umbral de la página anterior. Antes de iniciar un proceso de detección, se corre un proceso inicial de generación de umbral durante un determinado periodo de tiempo.

3.2 Disminución de deformamiento web utilizando estrategia solo lectura.

Esta técnica se centra en el uso de CDs en vivo personalizado con el contenido del sistema y del sitio web. Un CD en vivo es una instalación completamente funcional de un sistema operativo que se ejecuta directamente desde un CD o DVD, en lugar de un disco duro. Una de las dificultades es el reinicio del servidor a un estado de confianza, pues al reiniciar habrá un impacto en la disponibilidad de los contenidos web.

El sistema se basa en tres premisas:

- Si un servidor web es un sistema de solo lectura, éste será significativamente más difícil de modificar que cuando no lo es.
- Es un sistema sencillo de implementar.
- es una estrategia usada por muchos servidores web.

Basados en la primera premisa, será significativamente más difícil que se realice un Deface.

3.3 Implementar un navegador web con técnicas de detección de Defacement.

Esta técnica propone un algoritmo para la detección de modificaciones de sitios web implementando un navegador web con técnicas de detección de Defacement incorporadas. Se realiza un cálculo periódico de la suma de comprobación del sitio web. La frecuencia de detección se basa en el código hash guardado o suma de comprobación para cada página web. El prototipo incluye actualmente una aplicación C(sharp) y .Net de un navegador web. El administrador del servidor tendrá que utilizar el navegador web para abrir las páginas web. En caso de que la modificación sea detectada, el administrador es notificado y se dan consejos para recuperar la página.

El algoritmo propuesto para la detección y la recuperación por modificación de sitios web es el siguiente:

- Sobre la base de relevancia de la página web y su modificación, validar la página web.
- Calcular el hash actualizado de la página web elegida en el paso 1, usando algoritmos MD5 o SHA1.
- Comparar el código reciente del hash actualizado (NCI) de la página web con el códig del hash almacenado en la base de datos.

  Si el resultado de la comparación es verdadero, entonces la página no ha sido borrada y el porceso se detendrá.

Si el resultado de la comparación es falsa, la página web ha sido borrada o el contenido de la página ha sido modificado, así que vaya al siguiente paso.

- Informar al administrador sobre la posible modificación del sitio web y recomendar corrección.

3.4 Soluciones comerciales

En el mercado existen múltiples aplicaciones que brindan el servicio que buscamos, para nuestro estudio, utilizamos los siguientes servicios:

Aplicaciones de monitoreo de caídas.

3.4.1 Monitor.us

Este servicio es la versión gratis de Monitis, y tiene las siguientes características:

- Monitoreo de sitio web: Seguimiento del tiempo de respuesta del sitio y rendimiento de éste desde distintos puntos de locación en el mundo.
- Monitoreo de redes: Tiene herramientas para seguir el estado de la red en cualquier momento.
- API de monitoreo abierta: Se puede personalizar fácilmente sus herramientas de monitoreo para las necesidades especiales del cliente.
- Monitoreo de servidores: Desde una consola, detecta problema de cuellos de botella y se puede prevenir problemas antes que surjan en el servidor o en el sistema operativo.

- Monitoreo móvil: Se envían alertas a los dispositivos Android o iOS vía texto o emails.

[15]

3.4.2 FreeSiteStatus

Este servicio contiene las siguientes características:

- Monitorización permanente: Se encargan de monitorizar el sitio o servidor las 24 horas de los 7 días a la semana y los 365 días del año.

- Informes de disponibilidad y rendimiento: Ofrecen toda la información necesaria sobre el tiempo útil y el rendimiento de los sitios web y servidores en informes y gráficos fáciles de entender.

- Ventanas de mantenimiento: Se pueden definir ventanas de mantenimiento puntual y recurrente para pausar las comprobaciones. No se enviarán alertas durante paradas programadas.

- Dependencias: En un centro de datos, los dispositivos dependen unos de otros. Por ejemplo, diez servidores están conectados a un mismo switch. Se pueden definir las dependencias entre los servidores y el switch, así en caso de una caída del switch, se recibirá solo un aviso “Para el switch” en lugar de recibir un aviso por cada uno de los servidores que están detrás.

- Soporte Multi-Protocolo: Soporta ping, HTTP, HTTPS, FTP, SSH, SWTP, DNS, POP3, IMAP, MySQL y cualquier otro servicio que corra sobre TCP/IP.
- Monitorización mundial: Monitorean los sitios web y servidores desde una red mundial con 34 nodos de monitorización.
- Aviso de tiempo de caída: Notifican vía email, SMS.
- Envíe solicitudes de reinicio al proveedor cuando se detecte una caída.
- Reducción de falsas alarmas: Utilizan avanzadas tecnología de comprobación para evitar falsas alarmas. También se pueden aumentar o reducir la sensibilidad de la monitorización basándose en timeouts, tiempo de espera y ubicaciones geográficas.

[10]

3.4.3 ServiceUpTime

Las características de este servicio son las siguientes:

- Frecuencia de monitoreo: Se puede elegir entre 1, 2, 3, 5, 10, 15, 30 y 60 minutos como la cantidad de tiempo que se verificará el sitio web.
- Soporte de contacto: Se puede ser notificado vía email y sms. Los emails contienen detalles del servicio estando abajo y el error que retorna. Las alertas SMS es una breve notificación enviada a tu celular con el estado del servicio

monitoreado. También se pueden utilizar herramientas propias del servicio para crear una aplicación propia y alerta.

- Contenido: Se verifica que la página tiene un contenido apropiado. Si una letra no está presente en la página web, se envía una alerta ya sea válido o no dicho cambio.

- Ping: Envía comandos echo al dispositivos/host destino, ayudando a verificar el nivel de conectividad IP, provechoso tanto para host como para dispositivos como routers y firewalls.

- Servidores Web: HTTP (Puerto 80) y HTTPS (puerto fuente 443) protocolos. Monitorea el rendimiento y el estado del sitio web.

- Verificación de link: Se puede monitorear el intercambio de links de los sitios web padres y estar alerta una vez sean removidos.

- Distintos tipos de protocolos de servidores: Está seguro que tus protocolos funcionan correctamente (POP3, MySQL, SMTP, IMAP, DNS, FTP) también se pueden añadir puertos personalizados para monitorear en tu host para estar seguro que un servicio especial está corriendo.

[19]

3.4.4 Site24x7

Las características de este servicio son las siguientes:

- Monitoreo de rendimiento de páginas web: controla la el rendimiento y la disponibilidad de sitios web desde múltiples ubicaciones globalmente y sé notificado de inmediato cuando se produzca una caída.

- Analizador de páginas web: obtén visibilidad a fondo de como tus páginas web se están cargando para los clientes alrededor del mundo. Sigue el rendimiento de componentes HTML como JavaScript, CSS e imágenes. También ver el rendimiento de servidores web corriendo los principales dominios y subdominios.

- Servicio de monitoreo: Monitorea la disponibilidad de servicios críticos. Soportan monitoreo de protocolos HTTP(S), FTP(S), DNS, PING, TCP, SSL, SMTP, POP, etc.

- Monitoreo real del usuario: obtén la comprensión de problemas a fondo que afecta a usuarios reales, accediendo a sitios web y aplicaciones. Analiza el rendimiento de aplicaciones desde todas las perspectivas como browser, plataformas, geográficas, ISP y más.

- Monitoreo de la nube: Proporciona métricas de rendimiento comprensivas de Amazon EC2, instancias RDS y Bucket. Garantizar el máximo rendimiento de las aplicaciones y servicios críticos de negocio alojados en sus plataformas de Amazon. Obtenga información sobre la utilización de recursos de instancias de EC2 y RDS y las aplicaciones que se ejecutan en ellos.

- Monitoreo de VMware: Adquirir una visión integral de su infraestructura VMware. Monitorear hosts VMware vSphere y máquinas virtuales (VM). Obtener vistas gráficas, alarmas y umbrales, informes fuera de la caja, la gestión integral de fallas y el máximo tiempo de actividad del servidor ESX. Servidores vCenter Site24x7 le permiten tomar el control de sus recursos virtuales e infraestructura VMware.

- Monitoreo de Servidor: Monitorear indicadores críticos del servidor, tales como CPU, disco, memoria, procesos, servicios y uso de la red de Linux y servidores Windows que ejecutan aplicaciones críticas. Asegúrese de costos mínimos generales y de mantenimiento.

- Controla la red interna via On-premise poller: Supervisar portales de intranet, sistemas ERP, aplicaciones de nómina, dispositivos de red de ping, servidores de aplicaciones, servidores de bases de datos y garantizar otras aplicaciones personalizadas están arriba y un rendimiento óptimo. On-Premise Poller le ayuda a controlar los recursos internos y empuja a la información de rendimiento y tiempo de actividad para Site24x7 usando una arquitectura amigable nube (ida HTTPS).

- Monitorea desde redes móviles, WiFi interno y dispositivos móviles: Compruebe el rendimiento y disponibilidad de sus aplicaciones móviles, sitios web y otros servicios en línea a través de operadores de telefonía móvil (3G, 4G) y

redes Wi-Fi de la empresa.

- Monitoreo de redes: Monitoreo integral para dispositivo de red críticos tales como routers, switches y firewalls. Ayudar a los equipos de la red a obtener visibilidad del rendimiento de profundidad necesaria para gestionar redes complejas.

- Monitoreo de servidor DNS: Site24x7 puede asegurar DNS que los lookup-ups están funcionando y el servidor DNS está resolviendo nombres de dominio correctamente. También puede controlar el tiempo de respuesta para la resolución DNS y DNS look-ups.

- Monitoreo de certificados SSL: establezca alertas para que le notifique antes de que caduque el certificado SSL de su sitio web. Asegúrese de que tiene un certificado SSL válido para mantener la confianza de los clientes en su presencia en línea.

- Monitoreo FTP RTT: compruebe el tiempo de respuesta para subir y descargar archivos importantes a través de su servidor FTP. Garantizar un rendimiento óptimo marcando el tiempo de ida y vuelta de su servicio FTP.

- Monitoreo de servidores de correo: Monitoreo de servidor de correo desde Site24x7 hace un chequeo completo de circulación de tiempo correo y garantiza un rendimiento óptimo. Hace cosas como tu cliente de correo electrónico (Outlook o Thunderbird) y se puede controlar el tiempo de respuesta y el

rendimiento de los servidores de correo, tanto SMTP saliente y entrante POP / IMAP.

- Alertas y notificaciones: sé notificado acerca de los problemas de rendimiento o el tiempo de inactividad en cualquier lugar, en cualquier momento con mecanismos de alerta que soportan SMS, Email, Push Notifications, Twitter y RSS feeds.

- Administradores SLA: Definir los acuerdos de nivel de servicio y un seguimiento de su cumplimiento.

- Acceso desde móvil: Cuenta con aplicaciones para celulares con SO Android e iOS.

- Gestión de usuarios: proporciona acceso basado en roles para ver los informes, páginas de estado y los datos sobre el monitor a su empleados, gerente o su proveedor de hosting propio.

[20]

3.4.5 SiteUpTime

Las características de este servicio son las siguientes:

- 6 páginas para monitoear
- Chequeo cada 2 minutos
- Alertas por SMS/llamadas
- DNS monitoreo
- Estadísticas de descarga
- Acceso a la API
- 20 créditos para SMS/llamadas
- Alertas por email
- Cuenta para subusuario

[21]

3.4.6 Costo de las aplicaciones

El costo de los servicios se ve en la tabla 3.1, donde se ven los diferentes precios de los servicios utilizados para la fase de monitoreo de caídas. Como podemos observar, la mayoría de las empresas tiene una manera distinta de cobrar. Unas cobran según sus diferentes planes, es decir, ofrecen distintos servicios dependiendo el plan que

se escoja (ServiceUptime, Site24x7, SiteUptime). Otras cobran según la frecuencia de monitoreo, es decir, dependiendo de la frecuencia que se escoja (1, 2, 3, 5, 10 o 15 min), será el costo de dicho servicio (FreeSiteStatus). Y otras tienen un costo estándar (Monitis, es la versión paga de monitor.us). Se observa que el servicio más barato sería FreeSiteStatus) con una frecuencia de monitoreo de 15 minutos sería un costo de 2 dolares. Pero este servicio no suple las necesidades de la universidad, esto será explicado más adelante:

Servicios	Costos
Monitis	Se monitorea cada 1 minuto 34.80USD / mes ——— 334.08USD / año
FreeSiteStatus	Depende de la frecuencia de monitoreo. 1 min - 12.00USD / mes 2 min - 7.00USD / mes 3 min - 5.00USD / mes 5 min - 3.00USD / mes 10 min - 2.50USD / mes 15 min - 2.0USD / mes
ServiceUptime	Estandar - 4.95USD / mes Avanzada - 9.95USD / mes Profesional - 52.95USD / mes
Site24x7	Avanzada - 89.10USD / mes Empresa - 35.10USD / mes Estándar 9.00USD / mes Básico 4.50USD / mes
SiteUptime	Estándar - 10.0USD / mes Pro plan - 20.0USD / plan

Table 3.1: Costo de aplicaciones. [15, 21, 20, 19, 10]

Aplicaciones de monitoreo de contenido.

Existen múltiples aplicaciones para monitorear el contenido de un sitio web, a continuación se listarán tres de estas donde una (Distill alert) es del tipo, "Herramientas extensiones del navegador".:

- Follow That Page
- Change detection
- Distill alert

Estos dos primeros servicios, hacen una captura del código HTML que está presente en un determinado momento, diaria mente dicho servicio vuelve a inspeccionar la página y hace la comparativa, en caso de encontrar algún cambio lo notifica dependiendo de qué tan grande sea y la manera como el usuario configure las condiciones de notificación. Esto quiere decir, en caso de ser un cambio pequeño y el usuario configure el servicio para que le avise solo cuando sean cambios mayores, dicho cambio mínimo no será notificado. Distill alert, no funciona diferente en cierto modo, pero para nuestro test no fue de gran ayuda pues en su versión gratis tiene un límite de emails. Luego de superar este límite, la aplicación cancela sus servicios. En la hoja de cálculo de reportes podremos observar el registro de cambios. Hubo cientos de alertas, esto debido a que la página de la universidad tiene por seguridad un cache el cual cambia cada hora aproximadamente, y se configuraron las aplicaciones para que

reporten el mínimo cambio. Dentro del reporte se omitieron estos cambios de caché y solo se registraron los cambios que podrían ser producto de presuntos ataques.

3.5 Resultados del estudio.

Reportes de caídas.

En la tabla 3.2 se listarán los resultados arrojados por los distintos servicios durante los distintos meses:

Fecha	Aplicaciones				
	Monitor.us	FreeSiteStatus	ServiceUpTime	Site 24x7	SiteUpTime
12/09/2015	4:10 / 1 min				
17/09/2015	9:08:57 / 30 min	8:50 / 42 min	9:00:04 / 30 min 38 seg	8:55:10 / 37 min 50 seg	9:13:41 / 30 min
19/09/2015		3:45 / 1 min		3:45:03 / 1 min 12 seg	
25/09/2015				4:05:10 / 1 min 13 seg	

Table 3.2: Resultados de seguimiento de caídas.

En la figura 3.1 Observamos en la primera columna la fecha donde se reportó la caída, en las siguientes, se observa como cabecera el nombre de las aplicaciones usadas en el mes de testeo, y como contenido la hora en que cada una de estas aplicaciones lo reportó seguido de la cantidad de minutos que según cada una de éstas duro caída la página de la universidad. Como se puede ver en la tabla se registró un total de 9 reportes de caídas. Donde 4 de éstas no fueron registradas por todos los servicios. Estos reportes que no fueron reportados por todas los servicios se le llaman falsos positivos, y se reconocen pues la cantidad de minutos que dura

caída la página de la universidad según el reporte de cada aplicación es muy ínfima. La única caída comprobada fue la que se registró el día 17 de Septiembre de 2015, donde duró la página caída durante aproximados 32 minutos. Cada servicio tiene un número de tiempo de caída distinto, esto se debe a que la frecuencia de monitoreo no es la misma. Se supo por medio de una consulta al web master, que la caída se presentó pues se hicieron varios intentos de logueo al panel de administración de la universidad, esto con algún presunto fin malicioso. Hubo una caída no reportada por ninguno de estos servicios pero esto debido a que cuando ocurrió el ataque, el mes de testeo de caídas había expirado al igual que las licencias de prueba por un mes de cada uno de los mismos dicho día fue el 28 de octubre de 2015.

Reportes de cambio de contenido.

Ahora listaremos el reporte de los cambios detectados por los servicios descritos en el capítulo pasado.

	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg
Aplicación	Oct 5		Oct 7		Oct 8		Oct 9		Oct 10	
Follow that page	4		2		2		2		1	
Change detection	4		2		2		2		1	
Distill Alert							1			
	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg
Aplicación	Oct 13		Oct 14		Oct 19		Oct 20		Oct 22	
Follow that page	1		1		1		1		1	
Change detection	1		1		1		1		1	
Distill Alert										
	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg	Reg	Irreg
Aplicación	Oct 23		Oct 28		Nov 2		Nov 3		Nov 4	
Follow that page	1				1		1		2	
Change detection	1		1		1		1		2	
Distill Alert										

Figure 3.1: Reportes de cambio de contenido obtenido de las aplicaciones

En las anteriores tablas, se ven los cambios detectados por los distintos servicios, en la primera columna se muestra una lista de los servicios, y en las siguientes como cabecera se discrimina por cambios regulares e irregulares y se da la fecha donde se reportó el cambio. Se consideraron un total de reportes de 15 días de cambios, algunos con dos cambios por día. En realidad fueron cientos de reportes que llegaron, pues la página de la universidad como control tiene un captcha el cual es cambiante, y ninguno de estos servicios está en la capacidad de ignorar dichos cambios de captcha.

Los resultados que arrojaron estos estudios fueron buenos, pero no hubo una

herramienta que cumpliera con todos los requisitos de la universidad, por esto, en el siguiente capitulo de hará una propuesta que busca solucionar ésta problemática de manera personalizada para la Universidad Tecnológica de Bolívar.

Capítulo 4.
Propuesta

Basados en el estudio realizado en dos meses de seguimiento del comportamiento de la página web institucional, se llegó a la conclusión que se necesita utilizar un software que realice esta acción. Las aplicaciones que se utilizaron en el estudio brindaron buenos resultados, pero ninguno de estas cumple con la totalidad de las necesidades de la universidad, por esto, se propone la creación de un software que supla con todos los requerimientos que la universidad tiene. A continuación se hará una lista de las necesidades específicas de la Universidad Tecnológica de Bolívar:

- Se necesita hacer seguimiento al estado de las páginas (online u offline)
- Se necesita hacer seguimiento al estado del contenido de las páginas.
- Se necesita darle a la persona encargada de una página la facilidad para hacerle seguimiento a dicha página.

Básicamente no se deben usar las aplicaciones de cambio de contenido usadas en el test pues dichas aplicaciones hacen reportes cada día, algo que para la universidad es algo inutilizable, pues en caso de un ataque, la persona maliciosa tendría

mucho tiempo de "fama" antes que la aplicación lo detecte. A continuación, se presentará una manera más eficaz de como chequear el contenido de las páginas web monitoreadas.

4.1 Metodología del chequeo de cambio de contenido.

- Indexar las páginas de la universidad, revisar la cantidad de links para saber las subpáginas que tiene ésta. Se dividirá el trabajo en hilos, asignandole a cada hilo un número de páginas a revisar. Estos hilos se encargaran de verificar las subpáginas a su cargo y comparar el contenido con las referencias que ya tienen. Basta con encontrar un cambio para que la aplicación envíe un mensaje de alerta al administrador.

  Actualmente existen distintas maneras de hacer esto, la técnica de scrapping es una de éstas, que nos ayuda a obtener el contenido de las páginas y hacer el rastreo de las mismas.

- No basta con revisar el contenido HTM, pues un atacante puede sobre escribir el nombre de una imagen y cambiarla por otra con contenido de su preferencia. Por esto, se verificará el contenido de las imágenes una vez comparados sus nombres por medio del hash único que estas tienen al ser descargadas. Al igual que el contenido HTML, bastará con que un hash no concuerde con el de referencia que la aplicación tiene para enviar un mensaje de alerta al administrador.

  se recomienda el uso de MD5 o SHA-1, pues son los algoritmos de hash menos probabilidades de repetición debido a su cantidad de caracteres.

- Las referencias con las que los robots comparan los cambios, se actualizarán

conforme a que se reporte un cambio legítimo. Esto es, Una vez se reporte una alerta, se debe clasificar que sea legítimo o que sea un ataque. En caso que el administrador lo reporte como legítimo, este cambio será la nueva referencia para hacer las comparaciones futuras. En caso de ser un cambio "ataque", el administrador tomará la decisión que él crea pertinente.

A en la figura 4.1 se muestra un diagrama de flujo que explica gráficamente lo dicho con anterioridad.

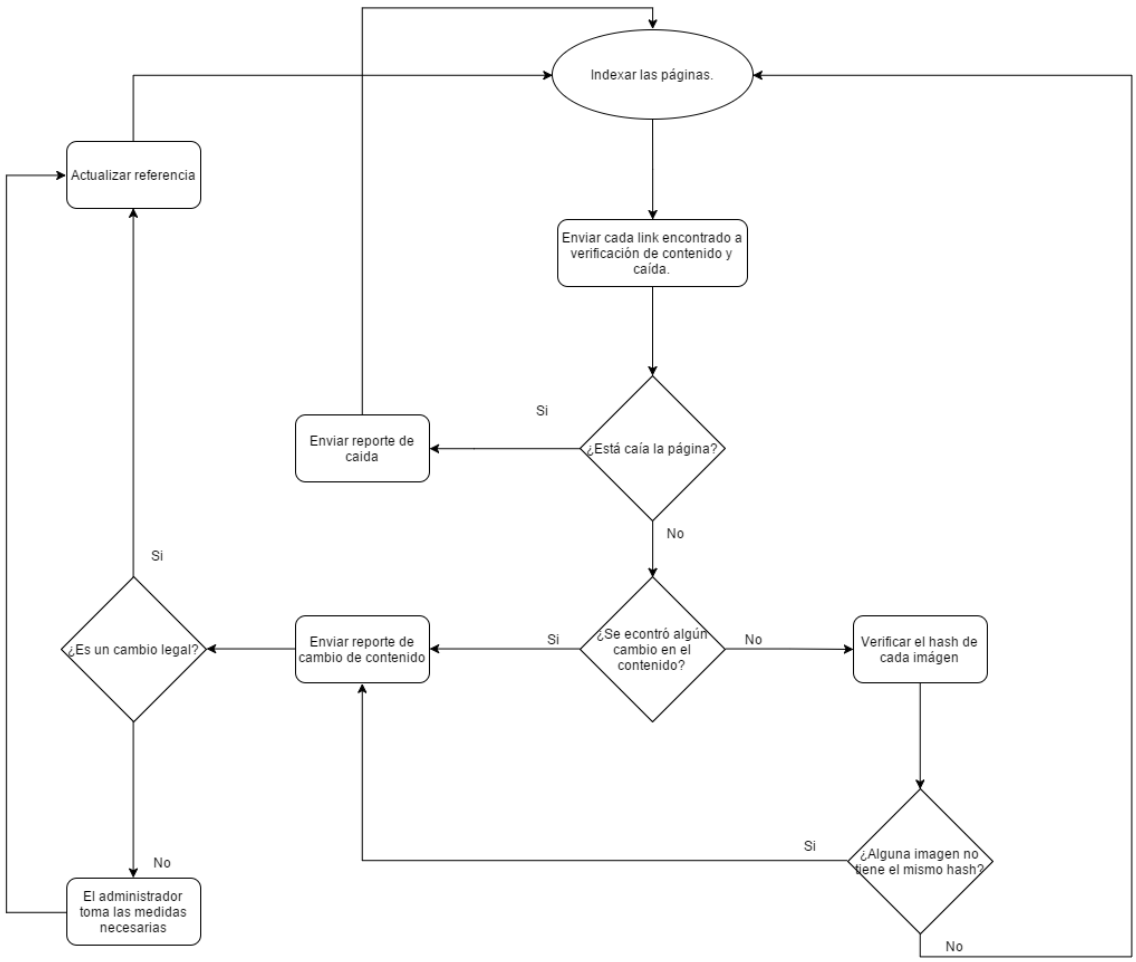

Figure 4.1: Diagrama de flujo.

Capítulo 5.
Web Security Alert.

Software de monitoreo de páginas web.

A continuación veremos el modelamiento del software propuesto en el capitulo anterior. Para esto se utilizaron diagramas de clase, base de datos y casos de uso; también se detallaron los requerimientos funcionales y no funcionales así como los casos de uso de la aplicación.

5.1 Requerimientos funcionales.

Un requerimiento funcional define una función del sistema de software o sus componentes. Una función es descrita como un conjunto de entradas, comportamientos y salidas. Los requisitos funcionales pueden ser: cálculos, detalles técnicos, manipulación de datos y otras funcionalidades específicas que se supone, un sistema debe cumplir. [26]

Los requerimientos funcionales de nuestro caso son los siguientes:

- La aplicación debe enviar periódicamente peticiones HTTP a las páginas que se desean monitorear. En caso que el servidor responda con algún error tipo 404,

500 entre otros, la aplicación debe alertar a la persona encargada por medio de un correo el tipo de error que se presentó.

- La aplicación debe escanear las páginas cada vez que la persona encargada reporte un cambio. Tendrá este escáner como referencia para luego compararlo con otros que se tomarán periódicamente. En caso que en una de estas comparaciones se note un cambio, la aplicación deberá notificar el mismo a los usuarios asociados a dicha página. (Se verificará el código HTML, por lo que no será necesario la descarga de ninguna imagen o vídeo presente en la página).

- El tiempo por defecto de verificación de contenido e intervalo de envío de peticiones será de 1h. Este tiempo será fácilmente modificable.

- Los cambios de captcha no serán reportados, la aplicación deberá estar en las condiciones de identificar cuando el cambio sea de este tipo.

- La aplicación debe permitir crear, modificar y eliminar usuarios. Serán estos a quienes se les enviarán las alertas.

- La aplicación debe permitir agregar, eliminar y modificar páginas para ser monitoreadas, estas páginas estarán asociadas a uno o varios usuarios.

- La aplicación debe mostrar un listado de las páginas a monitorear asociadas al usuario logueado, con el estado de las páginas (online u offline) y la fecha de la última modificación realizada sobre ella.

- Estas páginas pueden ser seguidas por usuarios invitados siempre y cuando el usuario administrador de dicha página le de permisos. Los usuarios invitados también serán notificados vía email sobre los eventos anteriormente descritos (caídas y cambio de contenido).

- La aplicación debe alertar cada vez que se intente ingresar al panel de administración de la página y se hagan más de 4 intentos errados.

5.1.1 Requerimientos no funcionales.

Los requerimientos no funcionales es, en la ingeniería de sistemas y la ingeniería de software, un requisito que especifica criterios que pueden usarse para juzgar la operación de un sistema en lugar de sus comportamientos específicos, ya que éstos corresponden a los requisitos funcionales. Por tanto, se refieren a todos los requisitos que no describen información a guardar, ni funciones a realizar, sino características de funcionamiento. [27]

Los requerimientos no funcionales de nuestra aplicación son los siguientes:

- Se podrá acceder al sistema vía web.

- Los tiempos de escaneo y número de peticiones enviadas al servidor serán fácilmente modificables.

- Debe haber una aplicación desarrollada para dispositivos móviles donde también se pueda acceder a la información.

5.2 Diagrama de clases.

En ingeniería de software, un diagrama de clases en Lenguaje Unificado de Modelado (UML) es un tipo de diagrama de estructura estática que describe la estructura de un sistema mostrando las clases del sistema, sus atributos, operaciones (o métodos), y las relaciones entre los objetos. [23]

La figura 5.1 muestra el diagrama de clases propuesta para nuestra aplicación:

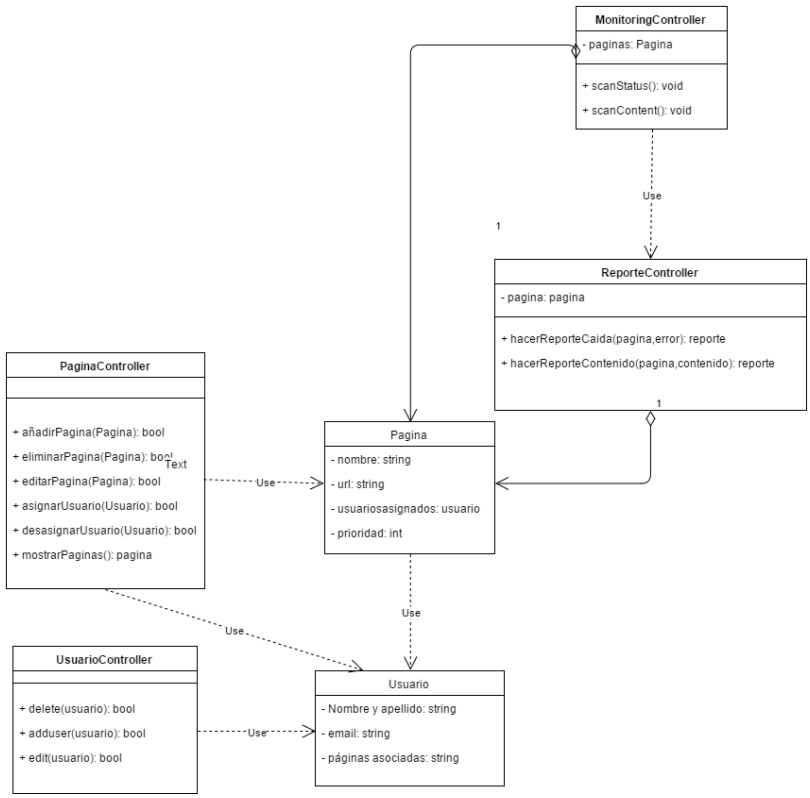

Figure 5.1: Diagrama de base de clases.

5.3 Casos de uso.

Los casos de uso son una técnica para especificar el comportamiento de un sistema: "Un caso de uso es una secuencia de interacciones entre un sistema y alguien o algo que sua alguno de los servicios. [4]"

Encontraremos a continuación los casos de uso de nuestra aplicación:

Especificaciones del caso de uso: Recibir reportes de caídas			
Código	Caso1		
Nombre	Monitorear caídas		
Descripción	La aplicación debe enviar peticiones HTTP constantemente a las páginas a monitorear con el fin de analizar la respuesta del servidor, en caso de éste retornar un error 500 o 400 debe alertar automáticamente al administrador de dicha página sobre lo sucedido		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Administrador, invitado, Súper administrador		
Precondición	El servidor retorna un error 500 o 400		
Postcondición	Se enviará un email en caso que el servidor retorne un error 500 o 400 informando dicho error.		
Flujo normal	- La aplicación envía una petición HTTP. - El servidor retorna con un error. - La aplicación envía un email alertando dicho error.		

Table 5.1: Caso de uso 1.

Especificaciones del caso de uso: Recibir reportes de cambio de contenido de las páginas			
Código	Caso2		
Nombre	Escaner de contenido de las páginas		
Descripción	La aplicación debe monitorear el contenido de las páginas incluyendo sus imágenes, vídeos etc. En caso de encontrar algún cambio (regular o irregular), la aplicación debe alertar automáticamente al administrador.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Administrador, invitado, Súper administrador		
Precondición	Se encontró un cambio en el contenido de la página.		
Postcondición	Se envía un email alertando que se ha hecho un cambio y el contenido que se ha cambiado.		
Flujo normal	- La aplicación hace la verificación de contenido de la manera , anteriormente descrita. - Se detecta un cambio en el contenido (ya sea en el código HTML o en el contenido de alguna imagen). - La aplicación envía un email de alerta al administrador de la página		

Table 5.2: Caso de uso 2.

Especificaciones del caso de uso: Modificación de tiempo de monitoreo			
Código	Caso3		
Nombre	Modificación de frecuencia de monitoreo		
Descripción	La aplicación debe permitir fácilmente modificar la frecuencia de número de peticiones por día hacia una página determinada.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Administrador, Súper administrador		
Precondición			
Postcondición	Se alterará la frecuencia de cantidad de peticiones envíadas.		
Flujo normal	- El usuario se loguea. - Busca la página a su cargo que desea modificar la frecuencia de monitoreo. - Modifica la frecuencia.		

Table 5.3: Caso de uso 3.

Especificaciones del caso de uso: Crear usuarios			
Código	Caso4		
Nombre	Panel de usuario		
Descripción	La aplicación debe permitir crear usuarios a los que se asignará una página web para que sean notificados en caso de alguna anomalía en éstas.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Súper administrador		
Precondición	El usuario a crear debe tener permisos de edición de por lo menos una página web de la universidad.		
Postcondición	La aplicación tendrá nuevos usuarios en su base de datos.		
Flujo normal	- El usuario se loguea. - Va al panel de registro de usuario. - Llena el formulario con la información del nuevo usuario. - Se le asigna una página web.		

Table 5.4: Caso de uso 4.

Especificaciones del caso de uso: Modificar y eliminar usuarios			
Código	Caso5		
Nombre	Actualización de usuarios.		
Descripción	La aplicación debe permitir modificar y eliminar usuarios.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Súper administrador		
Precondición	Debe existir el usuario a modificar o eliminar en la base de datos de la app.		
Postcondición	Se actualizará la tabla de usuarios en la base de datos de la app.		
Flujo normal	- El usuario se loguea. - Va al panel de registro de usuario. - Elige la opción de eliminar o modificar su usuario según sea el caso. - Se realiza la opción que el administrador seleccionó.		

Table 5.5: Caso de uso 5.

Especificaciones del caso de uso: Listado de páginas.			
Código	Caso6		
Nombre	Listado de páginas.		
Descripción	La aplicación debe ofrecer un listado de las páginas asociadas al usuario una vez logueado con el estado de la página y última modificación.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Administrador, invitado, Súper administrador		
Precondición	Debe estar logueado el usuario.		
Postcondición			
Flujo normal	- El usuario se loguea. - Va al panel de páginas.		

Table 5.6: Caso de uso 6.

Especificaciones del caso de uso: Inscribir usuarios invitados.			
Código	Caso7		
Nombre	Listado de páginas.		
Descripción	La aplicación debe permitir al usuario administrador de una página invitar a otro a seguir una página y ser notificado ante las anomalías que ésta presente.		
Autores	Oscar Pulido		
Fecha de creación	Diciembre – 2015	Fecha de modificación	Diciembre 2015
Actores	Administrador, Súper administrador		
Precondición	Debe estar logueado el usuario.		
Postcondición			
Flujo normal			

Table 5.7: Caso de uso 7.

5.4 Diagramas de casos de uso.

La figura 5.2 muestra el diagrama de caso de uso y en él las funcionalidades que tiene cada actor, en nuestro caso, el "Súper administrador", "Invitado" y "Administrador".

El súper administrador está habilitado para tener las siguientes funcionalidades:

- Recibir reporte de caídas.
- Recibir reporte de cambio de contenido.
- Modificación de tiempo de monitoreo.
- Crear usuarios.
- Modificar, eliminar usuarios.
- Ver listado de páginas.

El administrador está habilitado para las siguientes funcionalidades:

- Recibir reporte de caídas.
- Recibir reporte de cambio de contenido.
- Modificación de tiempo de monitoreo.
- inscribir usuarios invitados.
- Modificar, eliminar usuarios.
- Ver listado de páginas.

Mientras que el invitado, solo esta habilitado para las siguientes funcionalidades:

- Recibir reporte de caídas.
- Recibir reporte de cambios.
- Ver listado de páginas.

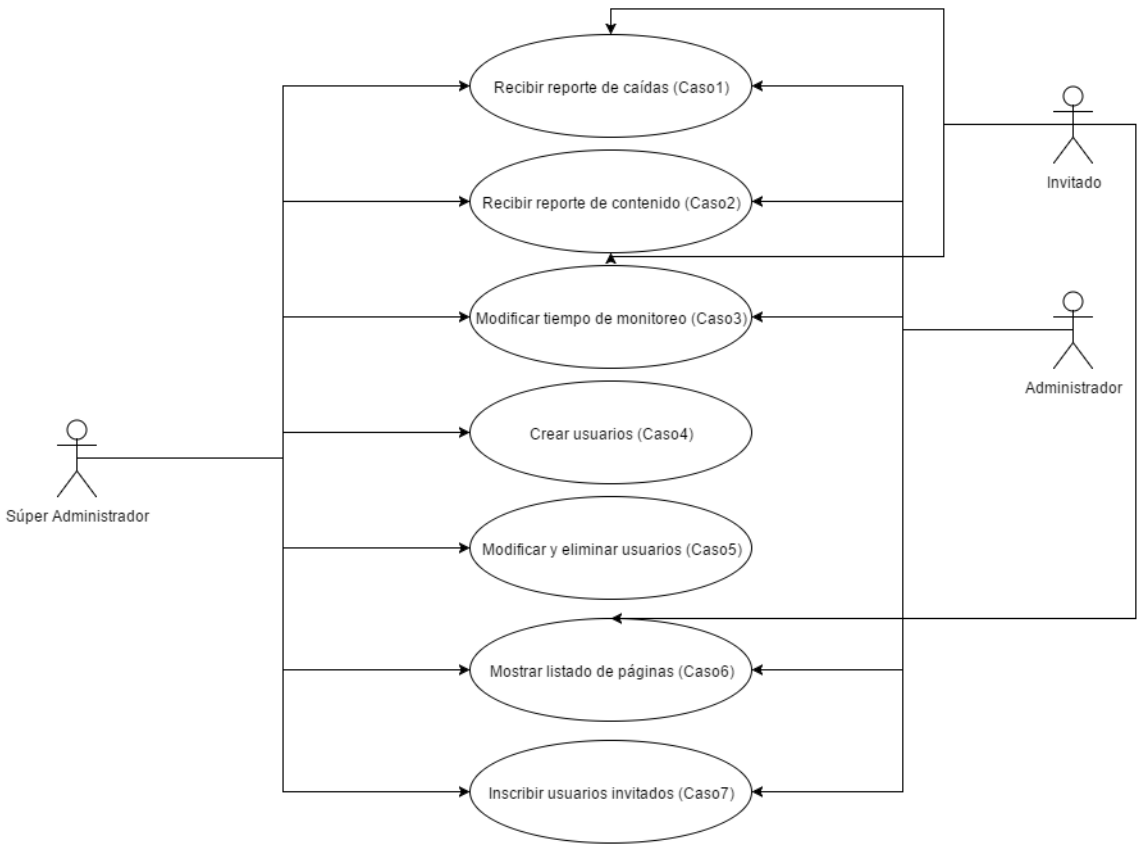

Figure 5.2: Diagrama de casos de uso. Los casos de uso mostrados en esta figura se presentaron en la subsección anterior.

5.5 Diagrama de base de datos.

En la figura 5.3, muestra un modelo de base de datos con tres tablas (reportes, páginas y usuarios) donde nos enfrentamos con una relación de muchos a muchos entre la tabla usuarios y la tabla páginas, esto debido a que un usuario puede tener a su cargo muchas páginas así como una página puede estar siendo seguida por muchos usuarios. También encontramos una relación de uno a muchos entre la tabla Reportes y la tabla páginas, esto debido a que un reporte solo puede ser una página pero una página puede tener varios reportes asociados a ella.

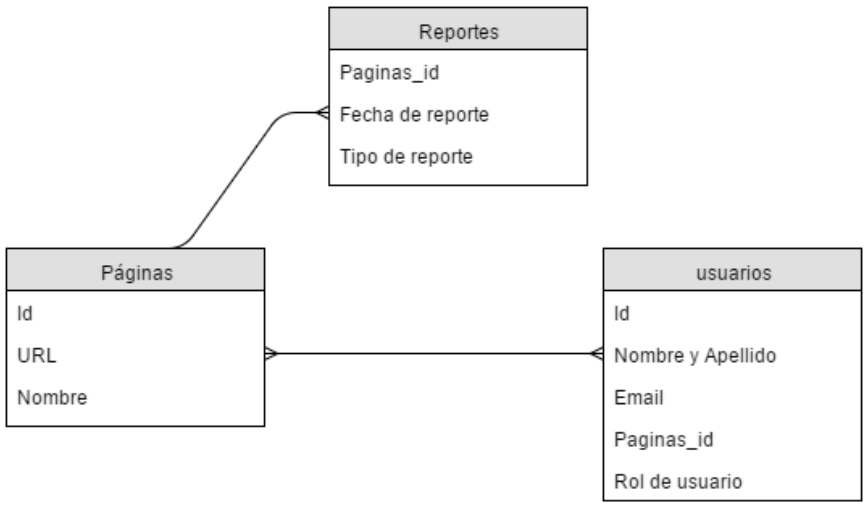

Figure 5.3: Diagrama de base de datos.

Capítulo 6.
Conclusiones y recomendaciones.

6.1 Conclusiones.

Con base a los estudios que se realizaron en los dos meses de seguimiento podemos concluir que la principal debilidad de los sitios web de la Universidad Tecnológica de Bolívar, es que el administrador no se da cuenta que están atacando la página si no hasta cuando está caída o (en caso de lograr el ingreso indebido) observar un cambio no regular.

Del mismo modo, concluimos que aunque existen múltiples herramientas en el mercado, ninguna está completa y para lograr todas las necesidades se necesitaría del uso de varias de estas herramientas, lo que sería algo costoso tanto para la Universidad Tecnológica de Bolívar como para cualquier empresa que pretenda proteger sus sitios web.

6.2 Recomendaciones.

Se recomienda hacer una aplicación móvil, esto con el fin de que se haga más rápido el proceso de alerta al usuario ante una anomalía que presente alguna de las páginas a su cargo. Dicha aplicación solo se encargará de recibir datos y alertar en caso que

sea necesario, la lógica del negocio debe estar toda hecha en el backend.

Se recomienda el uso de patrones de diseño en la implementación del software, esto con el fin de su fácil mantenimiento y optimización. Al igual el uso de inteligencia artificial como método para determinar cuando un cambio es capcha o no y así disminuir los falsos positivos.

Bibliography

[1] Que son y para que sirven los hash.

[2] P. Archanco. ¿cómo monitorizar una página web sin gastar un solo peso? 2014.

[3] Batanga. ¿qué es un hacker? http://www.batanga.com/tech/13182/que-es-un-hacker.

[4] S. Ceria. Casos de uso, un método práctico para explorar requerimientos.

[5] U. de Vigo. Mensajes http. http://trevinca.ei.uvigo.es/ txapi/espanol/proyecto/superior/memoria/node45.html.

[6] U. de Vigo. Protocolo http. http://trevinca.ei.uvigo.es/ txapi/espanol/proyecto/superior/memoria/node41.html.

[7] U. de Vigo. Tipos de verbos http. http://trevinca.ei.uvigo.es/ txapi/espanol/proyecto/superior/memoria/node46.html.

[8] G. R. Domínguez. "hacktivismo: hackers y redes sociales." jovenes, globalización y moviminetos altermundistas. 2007.

[9] Ecured. Servidores ftp. http://www.ecured.cu/Servidores-FTP.

[10] FreeSiteStatus. Características.

[11] M. S. Garcíaa. ¿qué es un servidor y cuales son los diferentes tipos de servidores? (proxy, dns, web, ftp, smtp, etc.) (dv00408a). 2006.

[12] L. Grozeva. What is website defacement? 2013.

[13] E. Hacking. Different types of hash codes-how to find which hash types? 2011.

[14] Hackstory. Hacker de sombrero blanco. http://hackstory.net/Hacker-blanco.

[15] Monitor.us. Características. http://www.monitor.us/free-monitoring-features/features-overview.

[16] Norfipc. Los servidores dns, usos, características y configuración. https://norfipc.com/internet/servidores-dns.html.

[17] P. Passeri. 2014 cyber attacks statistics (aggregated). 2015.

[18] Serversmtp. ¿qué es un servidor smtp? http://www.serversmtp.com/es/que-es-servidor-smtp.

[19] ServiceUpTime. Características.

[20] site24x7. Características. https://www.site24x7.com/features.html.

[21] SiteUpTime. Características. https://www.siteuptime.com/.

[22] L. Web. Http es simple. http://librosweb.es/libro/symfony-2-x/capitulo-1/http-es-simple.html.

[23] Wikipedia. Diagrama de clases. https://es.wikipedia.org/wiki/Diagrama-de-clases.

[24] Wikipedia. Hacker. https://es.wikipedia.org/wiki/Hacker-(seguridad-informatica)Sombrero-negro.

[25] Wikipedia. Protocolo de comunicación. https://es.wikipedia.org/wiki/Protocolo-de-comunicaciones.

[26] Wikipedia. Requisito funcional. https://es.wikipedia.org/wiki/Requisito-funcional.

[27] Wikipedia. Requisito funcional. https://es.wikipedia.org/wiki/Requisito-no-funcional.

[28] Wikipedia. Hilos. https://es.wikipedia.org/wiki/hilo-de-ejecucion, 2015.

[29] M. Windows. ¿qué es un servidor proxy? http://windows.microsoft.com/es-co/windows-vista/what-is-a-proxy-server.