

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”



PROYECTO - *botGIT*
Versión 1.0
Septiembre, 2016

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

1 RESUMEN EJECUTIVO

1.1 Descripción del requerimiento

Se estima que el 7% de la población mundial de usuarios con acceso a internet son venezolanos, que en números demográficos se traduce en 16.728.894 personas, de las cuales gran parte se beneficia con los servicios en línea que ofrece el estado. En el marco de facilitar trámites, el Estado Venezolano ha impulsado el— Gobierno Electrónico, disminuyendo la distancia entre los servicios gubernamentales y el pueblo venezolano a un solo click de distancia.

Pero no todo es una panacea, los esfuerzos del Gobierno por mejorar la calidad de vida del venezolano se ve mermada con frecuencia con acciones vandálicas, adversas a la política de mejora social que cuyas acciones perjudican a la población.. Muchos de estos grupos poseen como objetivo el lucro y reconocimiento.

Entre los tipos de incidentes telemáticos, se hallan los *Defacements* (Desfiguraciones de portales Web) los cuales representan la increíble cifra del 65% de los ataques ciberneticos anuales que tienen lugar en el espacio virtual venezolano. Los *Defacers* (Autores del ataque) se valen de vulnerabilidades encontradas en los portales Web, explotandolas.

Generalmente, los ataques son propiciado por individuos que apenas se inician en el crimen informático lo que resulta en un indicador que responde a la pregunta del por qué las cifras de ataques tipo *defacement* son tan numerosas y rutinarias, también implica que dichos ataques sean pasivos y ocasionen daños ligeros, pretenden llamar la atención. Afortunadamente la gran mayoría son pasados por alto y los medios de comunicación con más prestigio no hacen eco de ellos, con excepción de ataques a gran escala que afecten organizaciones o entes importantes.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Sin embargo, restar relevancia a estos ataques sería un error, ya que sigue siendo un delito informático tipificado en la Ley Especial contra Delitos Informáticos (Artículos 6, 7 y 8), sobra decir que para ahorrar molestias se recomienda con ímpetu la actualización y mantenimiento habitual de un portal Web.

Otro de los incidentes informáticos de mención especial en este proyecto, son los ataque *DDOS* (Ataque distribuido de denegación de servicios), estos inhabilitan el acceso a los servicios prestados por los portales y representa el 10 % de los ataques de ciberguerra en contra de Venezuela, un ataque de este tipo tiene lugar cuando un grupo de computadoras infectadas conocidas como *Botnet* o computadores zombies que generan un importante flujo de datos , satura el ancho de banda, deshabilitan los portales e impiden el acceso de los usuarios.

Con el tiempo, los atacantes han evolucionado, sus métodos cada dia son mas sofisticados, numerosos, para tener una respuesta proactiva ante estos incidentes es necesario promover nuevas formas de defensa, recurriendo a soluciones-innovadoras, que tomen por sorpresa a los ciberdelincuentes.

Actualmente, garantizar la integridad, disponibilidad de los portales Web es tarea del- departamento-Gestión de Incidentes Telemáticos (GIT) que monitorea la Web activamente, las 24 horas del día, los 7 días de la semana, cumpliendo su trabajo con total eficiencia y tenacidad; no obstante a largo plazo para un ser humano esta faena resulta bastante agotadora, repetitiva y tediosa al final de cuentas no son robots o máquinas que pueden realizar sin descanso la importantísima labor de vigilar la red, y así asegurar la periferia como centinelas durante un plazo de tiempo indeterminado, manteniendo siempre un buen desempeño y constante rendimiento sin claudicar.

En tal sentido, El equipo de respuesta del Departamento de Gestión de Incidentes Telemáticos (GIT), nos-solicitó-programar una aplicación que cubra

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

todas sus necesidades y simplifique en gran medida el cumplimiento de sus tareas.

La solución propuesta es desarrollar una entidad virtual automatizada, independiente,-que podemos definir como un *Bot* (Robot cibernético) imita que el comportamiento de un humano, en concreto simulará las acciones de un usuario que navega metódicamente la web.

En tal sentido, se propone el desarrollo de una Araña Web con acceso a internet y que visite secuencialmente y de manera periódica los portales de los enlaces registrados y predeterminados.

Este *Bot* explora los portales de los enlaces que encuentre teniendo sumo cuidado de no guardar aquellos que salten fuera de los dominios de portales gubernamentales. Seguidamente, procederá a hacer una copia de cada página además de almacenar la fecha, la hora, el nombre del portal, código del estado HTML para que luego, al momento de visitar nuevamente los enlaces, el *Bot* realice una comparación minuciosa con la página almacenada, detectar cambios y emitir una alerta.

En caso de que sea un cambio autorizado de la página se deberá actualizar la copia de los portales y almacenar debidamente.

1.2 Productos a obtener

Para cumplir a cabalidad con todos los requisitos identificados en el “PROYECTO SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT” ” se pretende elaborar los siguientes artefactos

- Bot de monitoreo periódico para los portales de los entes del poder público nacional que tendrá como objetivo analizar de forma cíclica las ocurrencias (cambios, no respuesta) de páginas en los los portales Web.
- Generador automático de reportes indicando cambios y disponibilidad de la página y estadísticos con información relacionada al monitoreo.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"	Septiembre -2016
---	------------------

- Bot de alerta de incidentes telemáticos para enviar alertas vía sms y e-mail.
- Interfaz de usuario agradable, intuitiva y ergonómica, de calidad teniendo como principal objetivo su usabilidad.
- Documento final que contendrá diagrama de casos de uso, diagrama de modelo del dominio, diagrama de clases, diagrama de secuencia, diagrama de colaboración, diagrama de flujo, visión del negocio, modelo relacional.
- Manual del usuario.

1.3 Resultado e impacto esperado

En el corto plazo: Facilitar la tarea de monitorear activamente la web sirviendo con prontitud al departamento de gestión de incidente telemáticos alertando oportunamente sobre arremetidas informáticas.

En el largo plazo: Disminuir el promedio en tiempo de detección de incidentes telemáticos asociados con *defacements* y *DDOS*, demostrar el desempeño de una Araña Web al obtener información denotar la flexibilidad para incorporar mejoras a futuro.

Confidencial	SUSCERTE, 2017	Página 5/38
--------------	----------------	-------------

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

2 DESCRIPCIÓN TÉCNICA:

El enfoque sistemático para el desarrollo de software usado en este Sistema es el paradigma *Orientado a Objeto (OO)*.

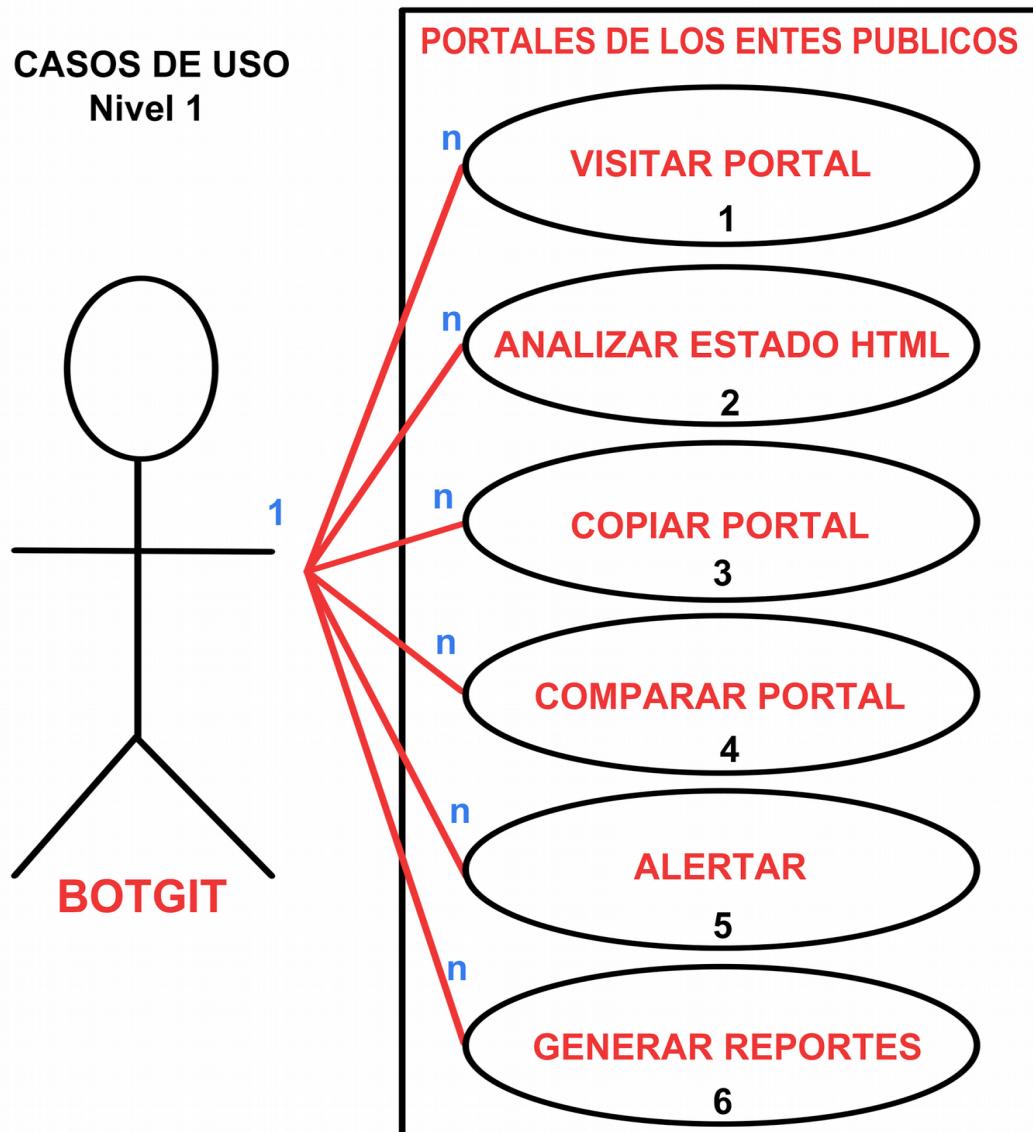
El Sistema será codificado en base a la suma de varios lenguajes de programación los prototipos se harán con *php*, *javascript* haciendo uso de *AJAX* necesarios para culminar con éxito ciertas aplicaciones interactivas el *lenguaje de marcado de hipertexto (HTML)* y *css* como base para la interfaz preliminar.

El uso de *JSON* de texto ligero para los *log* y una base de datos usando *MariaDB* como gestor de esta, todo esto dentro del entorno de software libre que para el Estado Venezolano y nuestra Universidad (Universidad Bolivariana de Venezuela) es de política prioritaria tal y como es mencionado en el Artículo 3, numeral 10 de la Ley de Infogobierno, donde el estado es el responsable de “Promover la adquisición, desarrollo, investigación, creación, diseño, formación, socialización, uso e implementación de las tecnologías de información libres a los sujetos sometidos a la aplicación de esta Ley”.

La metodología usada el desarrollo de este proyecto es el “Proceso Unificado” (PU) guiado por [casos de uso](#), centrado en la arquitectura y se caracteriza por ser **iterativo e incremental**.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

CASOS DE USOS DEL SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”**Descripción de escenario formato breve - Nivel 1**

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Una Araña Web visita un número determinado de portales, luego analiza el estado html y determina si el portal está o no está en línea, si no lo está, lo notifica. Después de copiar el portal la Araña Web en el momento exacto en el que retorna al mismo portal compara el *md5* con el almacenado en la base de datos, en caso de que difieran, indica que existe una modificación así que procede a comparar con la copia que antes hecha para establecer cuáles fueron las modificaciones, para almacenar luego el cambio en el log para entonces alertar y generar el reporte pertinente.

CASOS DE USO

Nivel 2

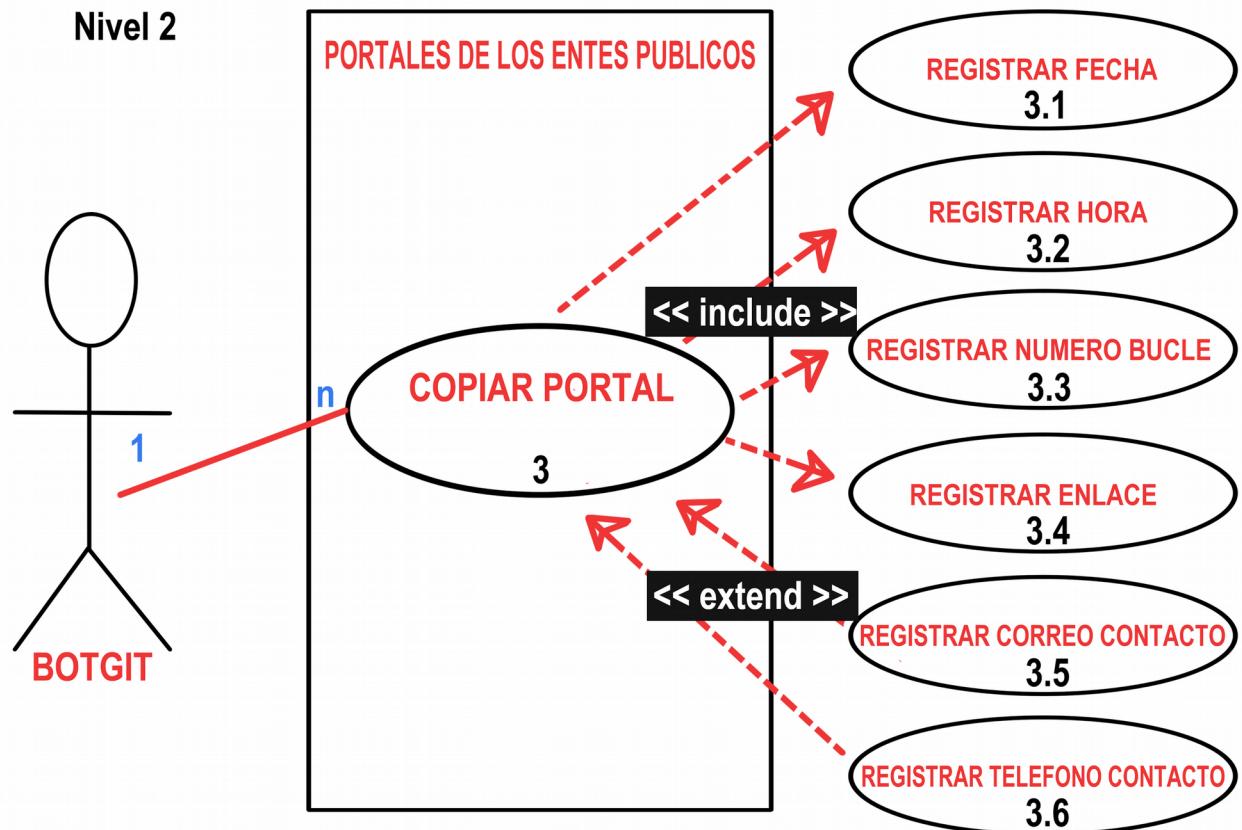


SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Descripción de escenario formato breve - Nivel 2 Analizar Estado HTML

La Araña analiza el código de estado html del portal y verifica que la página se encuentra en línea, de lo contrario, notifica que no funciona.

CASOS DE USO**Nivel 2****Descripción de escenario formato breve - Nivel 2 Copiar Portal**

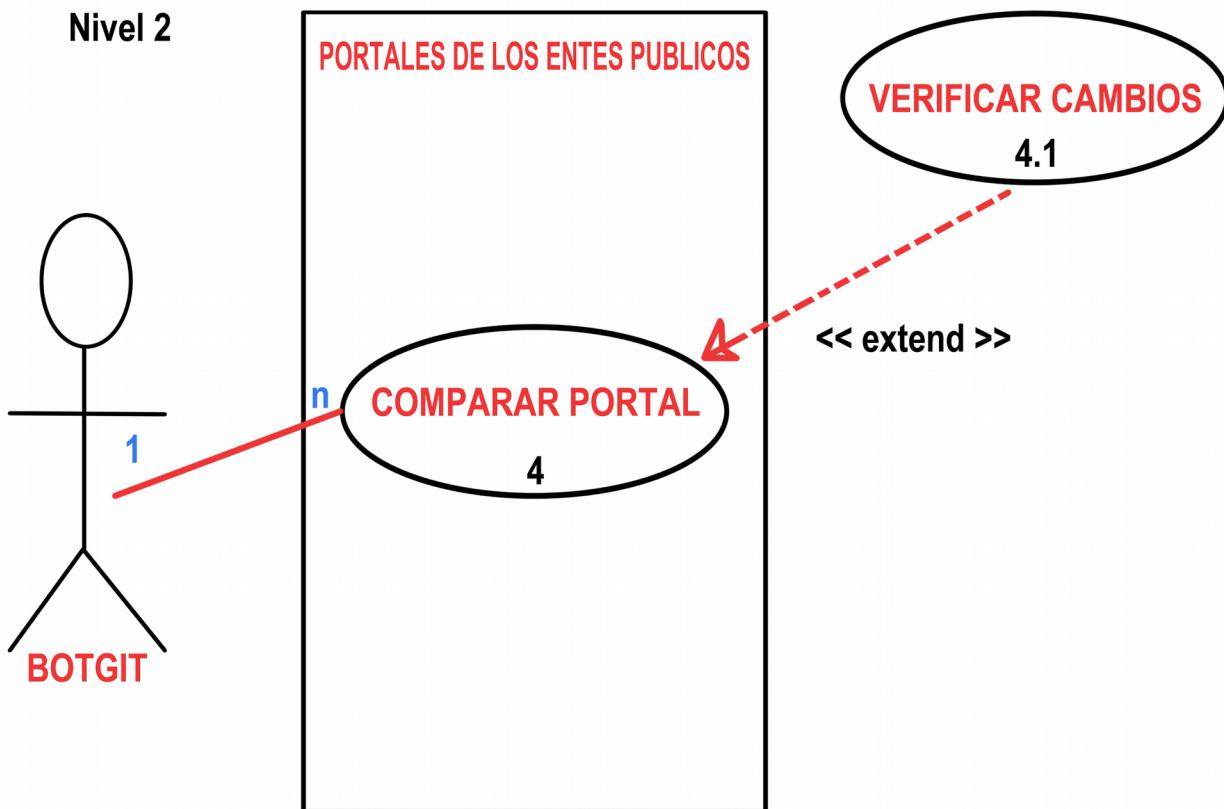
La Araña Web copia el portal y registra la fecha, la hora en la que almacenó el HTML de una determinada página en la base de datos.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

CASOS DE USO

Nivel 2

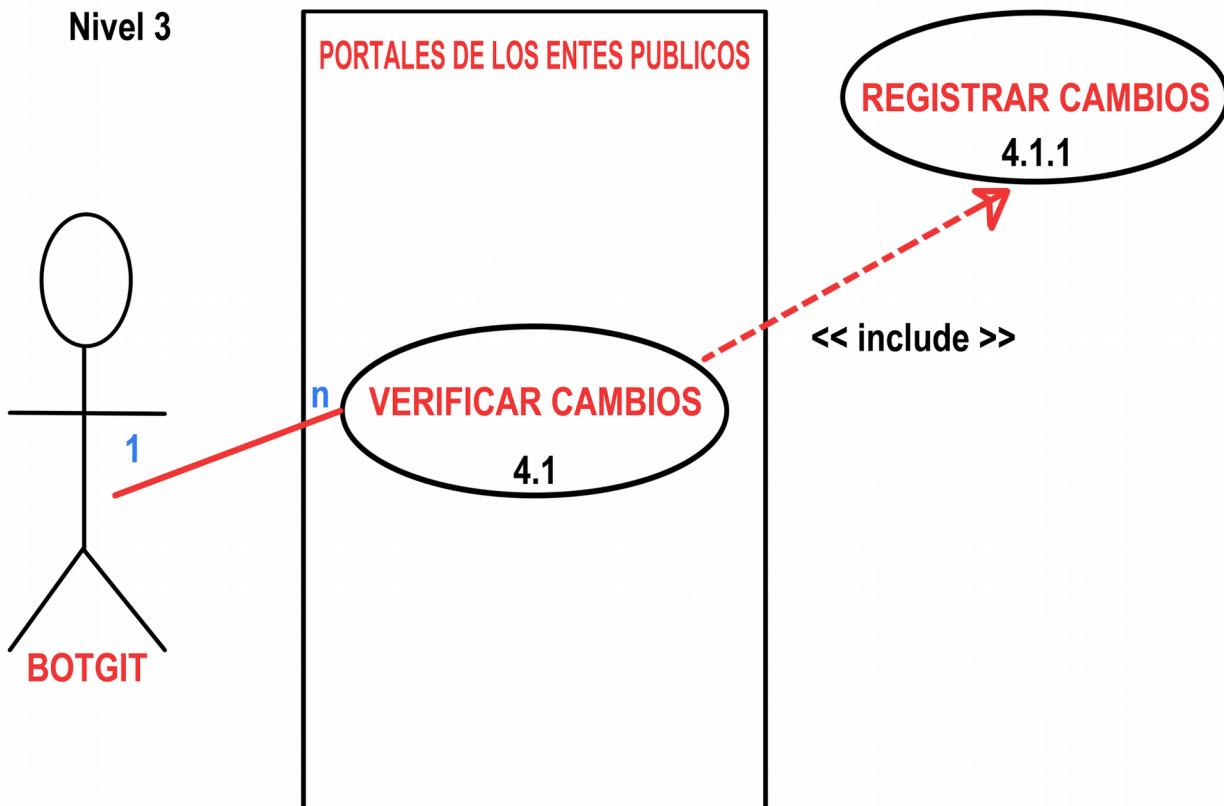


SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Descripción de escenario formato breve - Nivel 2 Comparar Portal

El Bot compara el portal actual con el *md5* almacenado en la base de datos, de ser diferentes, realizará la comparación más extensiva de el código HTML usando el programa *diff* disponible en distribuciones de GNU Linux.

CASOS DE USO**Nivel 3****Descripción de escenario formato breve - Nivel 3 Verificar Cambios**

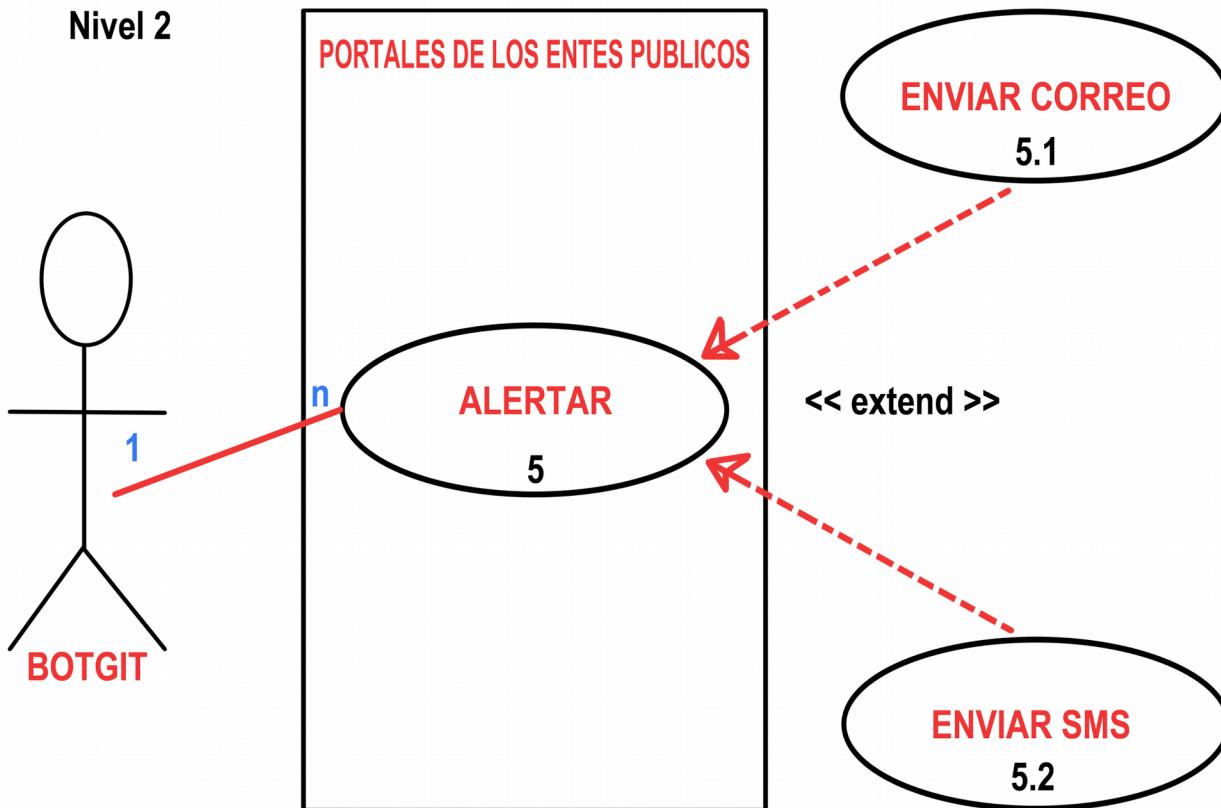
Si la Araña Web encuentra un cambio inmediatamente lo registra en el log de cambios.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

CASOS DE USO

Nivel 2



Descripción de escenario formato breve - Nivel 2 Alertar

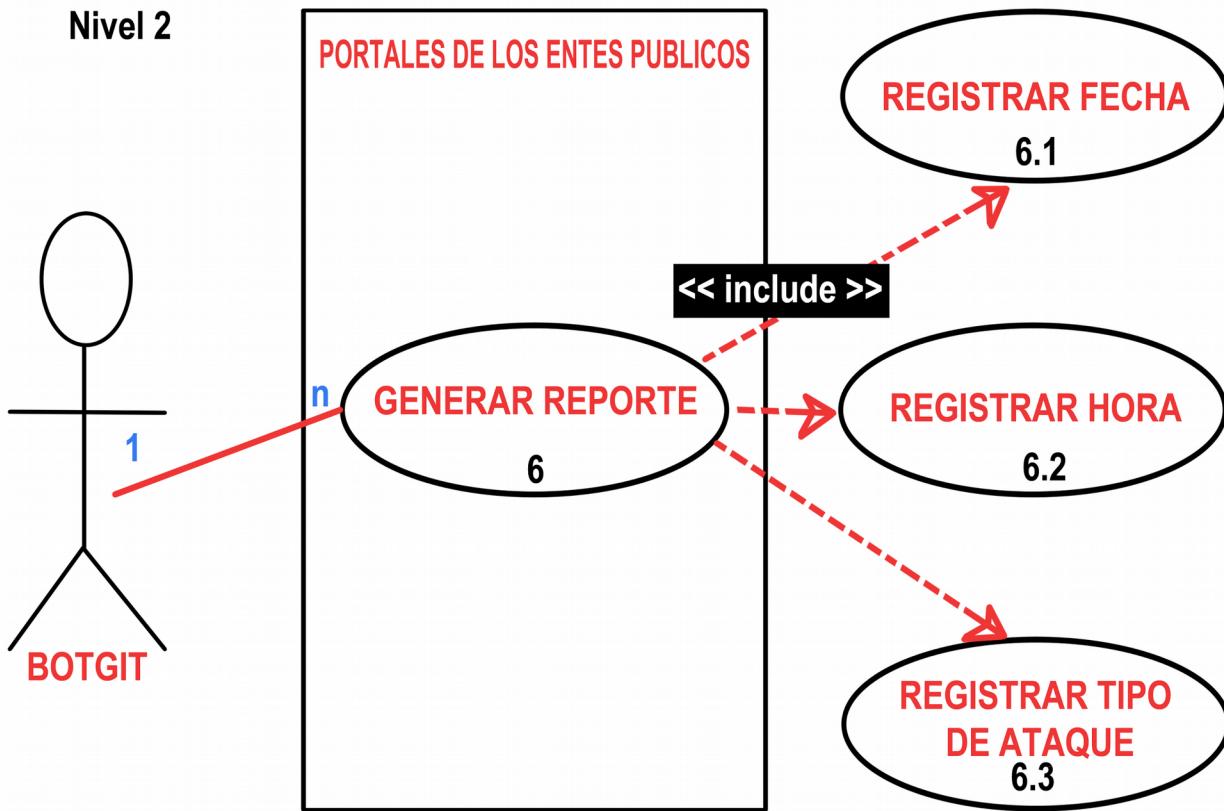
El Bot alertara de una ocurrencia mediante el envío de un correo electrónico o un mensaje sms al teléfono celular determinado.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

CASOS DE USO

Nivel 2



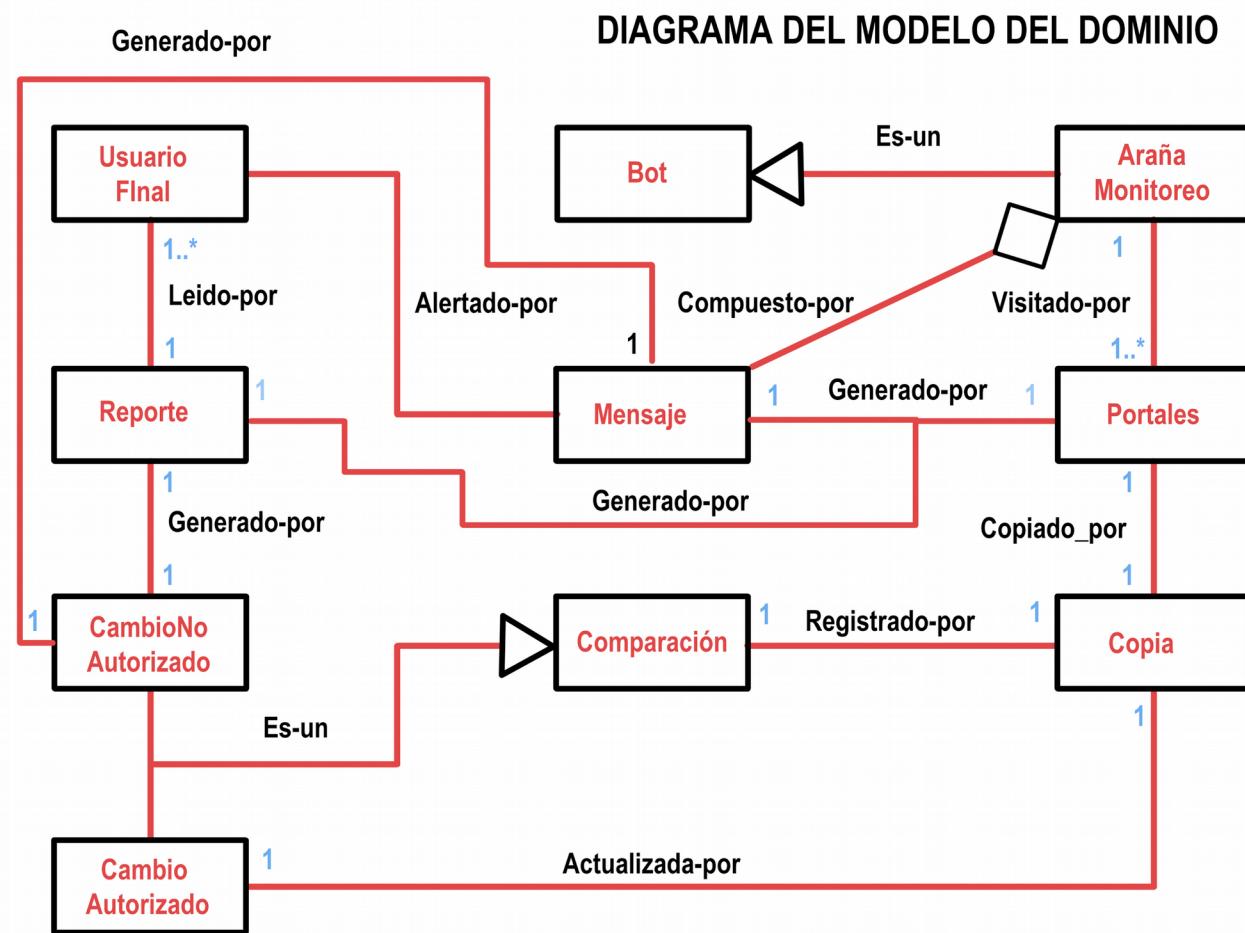
Descripción de escenario formato breve - Nivel 2 Generar Reporte

El Bot genera reporte y en el registrará la fecha, hora y cambios en la página Web (de existir) o si esta se encuentra fuera de línea.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Modelo del Dominio



SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

Arañas Web

Son *Bots* especializados que definen su destino descargando múltiples páginas Webs recorriendo cada enlace que encuentran. El uso más frecuente que se les da es el de copiar todas las páginas Web visitadas para posteriormente anexarlas a un motor de búsqueda.

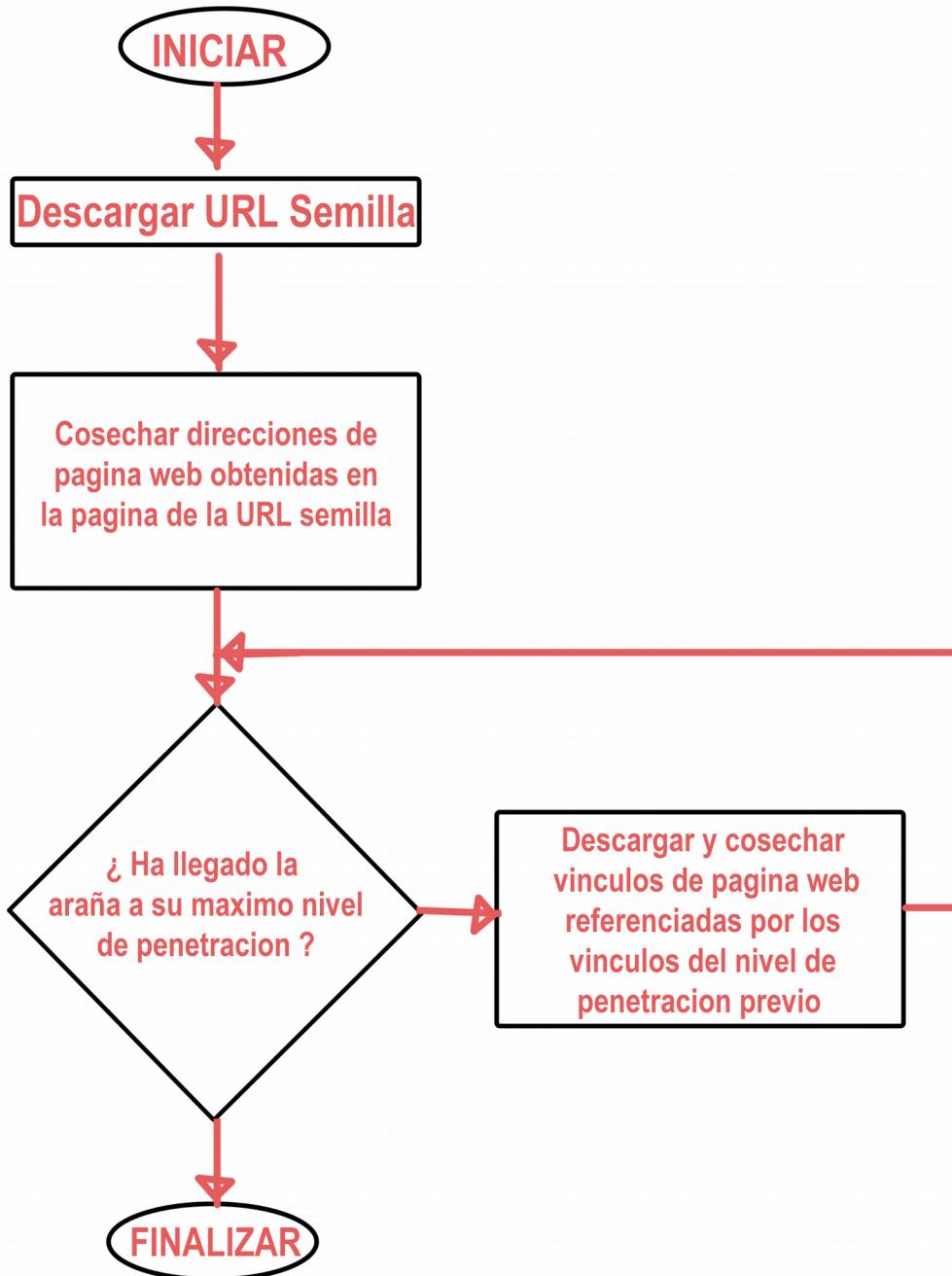
Sin embargo, el potencial de las Arañas va mucho más allá, pueden ser usadas para cometer actos antiéticos y a veces destructivos, en forma de spam, botnets, hijacking, entre otros, razones por lo que se estableció un convenio que limita a las Arañas en su penetración de los sitios Web. El uso como estándar de facto de un archivo de texto llamado “robots .txt ” en el directorio raíz de todo portal Web que especifica a donde no debería de acceder una Arañas Web.

Funcionamiento de una Araña

Las Arañas Web, constan de una lista inicial de URLs o direcciones web llamada “semillas” que usarán como inicio visitando, recolectando cada hipervínculo que identifican, luego, las arañas usan estos enlaces como nuevo objetivo para analizar y entonces visitar nuevamente todos los enlaces de ésta, hasta no encontrar más o son limitadas por un nivel de penetración.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016



3 ANTECEDENTES PROPÓSITO Y JUSTIFICACIÓN:

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

3.1 Antecedentes

Los robots son de las herramientas más poderosas que se ha creado, cualquier dramaturgo diría que en su afán de desempeñar el papel de un dios, el hombre ha querido diseñarlos a su imagen y semejanza aunque al hacerlo se ha venido generando en parte ciertas contradicciones con la naturaleza biológica de la psiquis humana y los paradigmas sociales un buen ejemplo sería el fenómeno psicológico conocido como "el valle inquietante" otro ejemplo conocido es la ansiedad que surge con respecto a la usurpación de los autómatas en las funciones laborales del género humano la sustitución de trabajadores especializados en un área que podría cubrir con eficiencia una máquina derivaría en la marginalización del profesional de los que podría prescindir cualquier corporación que menosprecie sus derechos abaratando costos e incrementando ganancias despojándose de la responsabilidad de cumplir con el salario y a largo plazo una crisis de desempleo.

Afortunadamente, dichos fenómenos son parte de un escenario ficticio de un futuro distópico por otra parte ha de señalarse que hoy día muchas empresas y organizaciones modernas ya implementan estos sistemas autónomos que se fusionan de manera simbiótica, creando un beneficio más que un problema , el futuro inmediato aparenta ser más utópico de lo esperado.

Casos conocidos son Amazon y su flota de robots kiva que se encargan de elegir y trasladar los productos que procesan en su venta simplifican la tarea de sus empleados. Otro caso los robots meseros que llevan comida a los comensales de "Taste and Aroma en Guiyang" un restaurante chino ubicado en la provincia de Guizhou; o los robots reposteros de "Hen na resutoran ROBOT" de Nagasaki, Japón, que preparan platillos apetitosos previamente programados mediante complejos algoritmos de cocina ejemplos de entidades mecánicas.

Este proyecto se basa en una entidad virtual es un robot sí pero un robot cibernético también llamado Bot (aféresis de robot). La computadora es una especie de analogía metafórica funcional y artificial de un cerebro el órgano que se encarga de asociar todos

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

los estímulos generados de la interacción perceptible con el universo el cerebro hasta ahora es el artefacto más complejo del universo y la computadora la herramienta más sofisticada de la civilización humana como en el cerebro la computadora emula los objetos del mundo real y los robots no se libran de ese efecto.

El robot tkwww

El robot tkwww fue una de las primeras arañas web y bot basado en tkwww (un navegador web libre de 1992 para distribuciones linux). Se desarrolló en 1994, con financiación de la Fuerza Aérea de EEUU, para construir índices HTML, compilar estadísticas WWW, recolectar imágenes, etc. La principal ventaja del robot tkwww era su flexibilidad para adaptarse a prácticamente cualquier criterio.

Los Bots pueden gozar de una enorme diversidad y tener distintos objetivos dependiendo de la tarea desempeñada para la que se hayan creado

Bots conversacionales: simulan mantener un diálogo con una persona ejemplos son ELIZA del MIT (instituto de tecnología de Massachusetts), SimSimi para android, CleverBot al que se puede acceder desde un navegador, y el tristemente célebre Bot de microsoft, Tay.

Bots de juego o Borgs son capaces de jugar por sí mismos el juego ejemplos son MegaBot para tibia , WRobot para World of Warcraft, Bot of Legends para League of Legends, y un sin fin más que se escapan de ser mencionados.

Botopedia asistente en la creación de artículos para la wikipedia.

Bots para redes sociales son de varios tipos: Testing Bots, Following Bots, Traffic Bots, Trending Bots, Crisis Bots.

Sistemas Expertos emulan el razonamiento de un experto en un dominio concreto.

Araña Web también llamados rastreadores, hormigas, Google y Yahoo se valen de esta

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

tecnología para crear sus buscadores. GoogleBot es el robot creado por la empresa Google que colecciona documentos con el fin de construir una base de datos para su motor de búsqueda y [Yahoo! Slurp](#) el de la corporación del mismo nombre

Propósito y alcance

El sistema automatizado centinela para órganos y entes del poder público nacional “botGIT”, previene los daños ocasionados por ofensivas ciberneticas de tipo defacement y ataque DDOS este documento de requerimiento describe una visión temprana del proyecto y el documento mismo es un prototipo no finalizado.

Justificación:**Descripción del requerimiento**

Nombre Del Requerimiento F o NF	Visitar Portal
--	----------------

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

ID	RF - 1
Objetivos Asociados	Obj. - 1.1
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez
Fuentes	Director de VenCERT
Descripción	Visitar portales periódicamente para de manera automática filtrar y almacenar sus enlaces
Importancia	Vital

Nombre Del Requerimiento F o NF	Analizar Estado HTML
ID	RF - 2
Objetivos Asociados	Obj. - 1.2
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Fuentes	Departamento de Gestión de Incidentes Telemáticos
Descripción	Usar los códigos de estados HTML notificar si una página se encuentra funcional o no
Importancia	Vital

Nombre Del Requerimiento F o NF	Copiar Portal
ID	RF - 3
Objetivos Asociados	Obj. - 1.1
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez
Fuentes	Departamento de Gestión de Incidentes Telemáticos

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Descripción	Almacenar el portal original considerando el espacio en memoria
Importancia	Vital

Nombre Del Requerimiento F o NF	Comparar Portal
ID	RF - 4
Objetivos Asociados	Obj. - 1.2, Obj. - 1.4
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez
Fuentes	Director de VenCERT
Descripción	Comparar la copia almacenada en memoria con la página actual con la finalidad de encontrar cambios importantes
Importancia	Vital

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Nombre Del Requerimiento F o NF	Alertar
ID	RF-5
Objetivos Asociados	Obj. - 1.5
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez
Fuentes	Superintendente de Servicios de Certificación Electrónica
Descripción	Enviar mensaje por correo electrónico y sms a los usuarios finales alertando sobre las ocurrencias
Importancia	Vital

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Nombre Del Requerimiento F o NF	Generar Reporte
ID	RF - 6
Objetivos Asociados	Obj. - 1.3, Obj. - 1.4
Versión	1.0
Autores	Leonel Becerra, Miguel Márquez
Fuentes	Departamento de Gestión de Incidentes Telemáticos
Descripción	Generar reportes mostrando cambios encontrados y estado HTML con enfoque estadístico
Importancia	Vital

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Situación actual

Actualmente se desarrolla del *Proceso Unificado (PU)*, la fase de inicio (Análisis diseño implementación y prueba) en la que se da luz verde a la factibilidad y alcance del proyecto quedan plenamente identificados los requerimientos funcionales o la mayor parte de ellos y se hace entrega del documento de requerimientos preliminar para subsecuentemente seguir con la fase de elaboración (análisis diseño implementación y prueba) cumpliendo con iteración del PU.

* Se experimenta los métodos necesarios de codificación para atacar la problemática desde la perspectiva de dos ángulos en el desarrollo del software por un lado se usan los métodos ya elaborados de librerías por defecto de forma provisional (como md5 y diff) que responde a la construcción de prototipos de manera rápida ideal para conocer el alcance y factibilidad alternativamente se escribe código funcional con métodos propios especializados en el proyecto esto asegura la portabilidad integridad correctitud y eficiencia la finalidad última es la de ampliar el espectro de resolución del problema y contar con opciones varias que aseguran la terminación exitosa del proyecto

* Se planea la elaboración de la interfaz usuario a través de bocetos y prototipos reconocimiento de restricciones iconos para las acciones metáforas contrastes etc.

Situación deseada

Culminación del proyecto plenamente funcional e instalado

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

4 INDIQUE SOBRE EL CUMPLIMIENTO DE LOS CRITERIOS GENERALES DE CALIFICACIÓN

El Proyecto “ SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “BOTGIT” ” contiene, cumple y refleja íntegramente los seis (06) criterios generales de calificación establecidos en el artículo 6 del Reglamento Parcial de la Ley Orgánica de Telecomunicaciones, a saber:

4.1 De la capacidad creativa e investigación de utilidad proyectada para el desarrollo de las telecomunicaciones

No solamente se encargará de prestar apoyo a venCert para preservar la disponibilidad de los portales Web de la administración pública nacional, pues, además, sentará las bases para el uso de Arañas Web por parte de la administración pública nacional para la obtención de información de sus Web.

4.2 De la acción para el desarrollo del sector de las telecomunicaciones

Servirá de apoyo a el SMAT (Sistema de Monitoreo de Alertas Tempranas), emitiendo avisos en caso de detectar modificaciones en portales Web de la administración pública nacional para luego determinar si estos pudieran ser asociados con defacements o, ataques DDOS (significado....), de esta forma los entes adheridos a venCert reciben alertas con mayor prontitud sobre los ataques junto con recomendaciones para re establecer el servicio lo antes posible.

4.3 De la acción social y económica

La detección y rápida acción para contrarrestar los ataques a portales Web de la administración pública nacional, ayudan a preservar la disponibilidad continua de servicios de gobierno electrónico, que cuando fallan no solamente generan disgusto e incluso retraso, además de pérdidas monetarias muchas veces no mesurables.

4.4 Del capital humano para el desarrollo del sector de las telecomunicaciones

Este es un proyecto que se maneja con estándares abiertos, cualquiera persona con conocimientos técnicos interesado en el desarrollo de Arañas Web podrá tener acceso a información, pruebas, y código fuente tras su creación. Permitiendo de fomentar el su uso

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL “botGIT”

Septiembre -2016

no solo como una herramienta para venCert, si no, como un prototipo para el uso de esta tecnología en la recopilación de información, permitiendo sentar las bases para proyectos similares, no solo en el ámbito de la educación superior, si no para cualquiera que esté interesado en el tema.

4.5 De la articulación de redes de innovación

El proyecto, al ser liberado con estándares abiertos, busca propiciar un intercambio de ideas entre todos los interesados en el tema de seguridad Web, de esta forma es posible considerar añadir funcionalidades, mejorarlas o implementar ciertos elementos de este proyecto en otros.

4.6 De la articulación con las tendencias internacionales

La puesta en marcha e implementación del proyecto implica, la posibilidad de contactar con personas y entes internacionales interesados en la implementación de proyectos similares, que permitan compartir ideas y propuestas de entes o personas extranjeras para de esta manera, a entender cuales son las tendencias mundiales con respecto al monitoreo de portales Web.

En consecuencia, a través de venCert, establecer un conjunto de estrategias articuladas para el desarrollo de conocimiento y para compartir las experiencias y lecciones aprendidas en torno al tema.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

5 OBJETIVOS:**5.1 General:**

1. Crear un sistema que permita monitorear portales Web de la administración pública nacional, que permita detectar e informar modificaciones benignas o malignas asociadas con defacements, para atender con la premura del caso la situación problemática presentada en los portales monitoreados.

5.2 Específicos:

- 1.1 Crear una Araña Web para explorar una lista de portales de la administración pública nacional a una determinada profundidad, almacenar una copia de los archivos de hipertexto de estos para ser usados como comparación en la detección de cambios maliciosos.
- 1.2 Desarrollar un centinela Web encargado de monitorear y detectar cambios en los portales Web almacenados por la Araña Web.
- 1.3 Mostrar información estadística con el número y frecuencia de los cambios detectados por el centinela.
- 1.4 Desarrollar un archivo log de cambios para almacenar de forma automática los cambios detectados en los portales Web, contendrá información relacionada con la fecha de detección de la modificación y la modificación como tal.
- 1.5 Crear un sistema de mensajería por correo electrónico y sms asociados a los teléfonos celulares de los **Responsables de atender las alertas con urgencia del caso**
- 1.6 Desarrollar de una interfaz gráfica que permita controlar todos los elementos mencionados anteriormente así como mostrar información sobre el estatus de los portales y del sistema como tal.

6 ESTRUCTURA:

Confidencial	SUSCERTE, 2017	Página 28/38
--------------	----------------	--------------

**SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"**

Septiembre -2016

6.1 Estructura y Segmentación del Proyecto:

El presente proyecto se ejecutará en seis (06) fases que se distribuirán a lo largo del tiempo de ejecución:

FASE I: Elicitación preliminar de requerimientos

En esta fase, mediante entrevista guiada, y tormenta de ideas, se obtiene información del proceso usado por venCert para la detección de ataques, las necesidades que debe satisfacer el nuevo sistema, los puntos débiles a fortalecer a través del nuevo sistema, además del alcance del proyecto.

Esta fase tiene un tiempo estimado de ejecución de dos (02) días

Actividades:

- 1.- Entrevista a el personal encargado de detectar y reportar incidentes telemáticos en venCert.
- 2.- Estudio del proceso usado por venCert para detectar y gestionar incidentes telemáticos.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

FASE II: Investigación del estado del arte

Investigar tecnologías actuales en lo referente a Webbots, Arañas Web y herramientas de control de versiones, necesarias para la creación de un proyecto con las tecnologías actuales. Se elaborarán una serie de prototipos de módulos no aptos para entrar en producción con el uso de las tecnologías investigadas para de esta forma, corroborar su correcto funcionamiento.

Esta fase tiene un tiempo estimado de ejecución de seis (06) semanas.

Actividades:

- 1.- Investigación de Arañas Web.
- 2.- Investigación de WebBots.
- 3.- Investigación de herramientas para el control de versiones.
- 4.- Creación de prototipos no aptos para producción.

FASE III: Ingeniería de requerimientos.

Tras la investigación del estado del arte, es posible determinar con exactitud los requerimientos de venCert, analizarlos y verificar las formas en las que estos pueden cumplirse usando las tecnologías actuales antes investigadas. Una nueva serie de entrevistas es realizada para verificar los requerimientos y proponer nuevas funcionalidades.

Tiempo de ejecución estimado de una (1) semana.

Actividades:

- 1.- Entrevista a el personal encargado de detectar y reportar incidentes telemáticos en venCert.
- 2.- Definición y documentación de requerimientos funcionales.
- 3.- Definición y documentación de requerimientos no funcionales.

FASE IV: Desarrollo y prueba de módulos a través desarrollo iterativo incremental.

En esta fase se crearán prototipos de cada módulo para verificar su funcionamiento

Confidencial	SUSCERTE, 2017	Página 30/38
--------------	----------------	--------------

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

individual usando cargas de trabajo real, es decir; usando información obtenida de portales Web de la administración pública nacional se obtiene data de tiempos de ejecución y se eliminan posibles bugs, se aumenta la robustez de cada módulo con cada iteración.

Actividades:

- 1.- Desarrollo de módulos.
- 2.- Prueba de módulos analizando sus tiempos de ejecución o encontrar errores para buscar mejoras en los algoritmos.

Tiempo estimado ejecución de siete (7) semanas e iteraciones para la creación y prueba de módulos cada semana.

FASE V: Desarrollo de Ambiente de Prueba de prototipos a través desarrollo iterativo incremental.

En esta fase, se busca preparar el ambiente en el que funcionará el sistema, preferiblemente un servidor capaz de manejar un gran número de peticiones. Se ensamblan los módulos para crear los prototipos a probar en conjunto con el personal de venCert. Se verifica que se cumplan los requerimientos y el correcto funcionamiento de los prototipos.

Actividades:

- 1.- Preparación de ambiente de sistema.
- 2.- Prueba de prototipos.
- 3.- Ajustes a prototipos.

Tiempo estimado de ejecución de cuatro (4) semanas e iteraciones para la creación y prueba de prototipos cada semana.

FASE VI: Entrega y aceptación.

Se procede a documentar el proyecto para que el personal de venCert sea capaz de entender su funcionamiento y mantener adecuadamente el sistema, abriendo la posibilidad

**SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"**

Septiembre -2016

de su futura modificación o adaptación a otros proyectos. El proyecto es presentado y se procede a su aceptación y entrega final.

Actividades:

- 1.- Documentación del producto.
- 2.- Presentación del producto.
- 3.- Aceptación y entrega final.

Tiempo estimado de ejecución de tres (3) a cuatro (4) semanas.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

6.2 Cronograma del proyecto

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

Actividad	Duración	Desde	Hasta
1.- Elicitación preliminar de requerimientos:	2 días	28/07/2016	29/07/2016
2.- Investigación del Estado del Arte:	6 semanas	01/08/2016	16/09/2016
2.1.- Webbots			
2.2.- WebSpiders			
2.3.- Herramientas para control de versiones			
2.4.- Otros, etc			
3.Ingeniería de requerimientos:	1 semana	19/09/2016	23/09/2016
3.1.- Definición de Requerimientos Funcionales			
3.2.- Definición de Requerimientos No Funcionales			
4.- Desarrollo y prueba de modulos a través desarrollo iterativo incremental:	7 semanas	26/09/2016	11/11/2016
4.1.- Desarrollo de Modulos			
4.2.- Prueba de Modulos			
5.- Desarrollo de Ambiente de Prueba de prototipos a través desarrollo iterativo incremental:	4 semanas	14/11/2016	15/01/2017
5.1.- Preparación de ambiente de sistema			
5.2.- Prueba de prototipos			
5.3.- Ajustes a prototipos			
6.- Entrega y Aceptación:	3 a 4 semanas	16/01/2017	15/02/20107
6.1.- Documentación del Producto	2 semanas		
6.2.- Presentación de Producto	1 semana		
6.3.- Aceptación y Entrega Final	1 semana		

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

8 GLOSARIO

AJAX	AJAX es el acrónimo de JavaScript y XML asíncrono (por sus siglas en inglés Asynchronous JavaScript and XML). Siendo la palabra clave "asíncrono", AJAX permite a una aplicación web realizar una o más llamadas al servidor en segundo plano via JavaScript, obtener información de este y presentarla al usuario sin la necesidad de tener que recargar la página web donde funciona una aplicación.
Araña Web	Son Webbots especializados que -a diferencia de webbots tradicionales que tienen objetivos bien definidos- descargan múltiples páginas web. Una araña construye su propio camino a través del internet, es difícil anticipar a dónde irán o que encontrarán en muchos casos, simplemente siguen los vínculos de las páginas web que van descargando. Aun así es posible controlarlas estableciendo ciertas condiciones.
Arquitectura	Conjunto de decisiones significativas acerca de la organización de un sistema de software, la selección de los elementos estructurales a partir de los cuales se compone el sistema, las interfaces entre ellos, su comportamiento, sus colaboraciones, y su composición.
Caso de Uso	Un caso de uso es un fragmento de funcionalidad del sistema que proporciona un resultado de valor a un usuario. Los casos de uso modelan los requerimientos funcionales del sistema.
DDOS, Distributed Denial of Service (Denegación de servicio distribuida)	En un ataque DDOS, un atacante planta programas("zombies") en varias computadoras que crean un ataque de Denegación de servicio (por ejemplo, enviando un gran volumen de paquetes dentro de una red cuando reciban la señal de una máquina especializada llamada el "manejador").
DOS	Un ataque DOS es aquel que busca interrumpir o cortar por un tiempo prolongado el acceso a un servicio computacional. Existen varias formas de ejecutar un ataque DOS, entre ellas están el sabotaje de software o hardware, ataques de "inundación" (flooding) que usan un programa para enviar muchos paquetes a un sistema sobrecargandolo, ataques de fragmentación de paquetes que abusan de este

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

	<p>proceso de fragmentación de paquetes de una forma u otra para que el sistema que los reciba y deba procesarlos se "cuelgue".</p>
Defacement, Desfiguramiento	<p>Un defacement, o desfiguramiento, ocurre cuando un perpetrador accesa un sitio web y lo cambia. Es un problema para el sitio web pues este no puede ser usado para lo que fue planeado, además existe un factor de "vergüenza", y el impacto que esto genera a los usuarios.</p>
Desarrollo iterativo incremental	<p>Consiste en dividir el esfuerzo de desarrollo de un proyecto de software en partes más pequeñas o mini proyectos. Cada mini proyecto es una iteración que resulta en un incremento. Las iteraciones hacen referencia a pasos en el flujo de trabajo, y los incrementos a crecimientos en el producto.</p>
JSON	<p>Usualmente la comunicación usada por las aplicaciones que hacen uso de AJAX está en formato de XML o en JSON (JavaScript Object Notation). Json, al igual que XML es usado para el intercambio de datos en aplicaciones web con la diferencia que usa la misma notación que los objetos de javascript, ayudando a reducir el tamaño de los documentos para intercambiar data si lo comparamos con XML.</p>
MariaDB	<p>MariaDB es uno de los servidores de bases de datos más populares del mundo. Hecho por los desarrolladores originales de MySQL y garantiza que se mantendrá como un proyecto con estándares libres.</p>
Portal Web	<p>En términos no relacionados a la World Wide Web, el diccionario Macquarie define un portal como "una puerta, o entrada" (Macquarie Library, 1981). De forma más específica, un portal web es visto como un sitio en internet diseñado para funcionar como entrada para dar acceso a otros sitios. Un portal combina información de múltiples fuentes y la hace disponible a varios usuarios. En otras palabras, un portal web es un sitio web "todo el uno" usado para encontrar y ganar acceso a otros sitios web.</p>
Proceso Unificado	<p>El proceso unificado es un proceso de desarrollo de software: "conjunto de actividades necesarias para transformar los requisitos del usuario en un sistema de software". El proceso unificado está dirigido por los casos de uso, centrado en la</p>

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

	arquitectura y es iterativo incremental.
Programación orientada a objetos (POO)	Como su nombre lo sugiere, la POO pone a los objetos en el centro de el modelo de programación. Un objeto es el concepto más importante en el mundo de la POO - una entidad autónoma que posee una estado y un comportamiento, igual que un objeto de la vida real-.
Webbot	Programa especializado en automatizar procesos usando recursos e información de la web.
HTML	El lenguaje de Marcas de Hipertexto (por sus siglas en inglés HyperText Markup Language) es un lenguaje basado en etiquetas que dictamina el formato de un documento web y su diseño en lo referente a texto e imágenes estáticas.
JavaScript	JavaScript es un lenguaje de scripting diseñado ejecutado del lado del cliente diseñado para crear una experiencia más amigable a los usuarios de internet.
PHP	PHP es un lenguaje de programación diseñado para generar páginas web de forma interactiva en la computadoras que las sirve, es decir, el servidor web.
XML	Son documentos similares a los de HTML en el sentido de que usan etiquetas, es usado para intercambiar datos en aplicaciones web.

SISTEMA AUTOMATIZADO CENTINELA PARA ÓRGANOS Y ENTES DEL
PODER PÚBLICO NACIONAL "botGIT"

Septiembre -2016

9 BIBLIOGRAFÍA

BIDGOLI, H: **Handbook Of Information Security**, (Threats, Vulnerabilities, Prevention, Detection, and Management), United States of America, John Wiley & Sons, Inc.,2006.

BOGDAN, Brizanrea-lamandi, Cristian Darie y Audra Hendrix, **AJAX AND PHP Building modern web applications** (Build user-friendly Web 2.0 Applications with JavaScript and PHP), 2nd Edition, Reino Unido, PACKT Publishing, 2009.

DAVIS, Michele E. y Jon A.Phillips, **Learning PHP and MySQL**, (A step-by-step guide to creating dynamic, database-driven web sites), 2nd Edition, United States of America, O'Reilly Media, Inc., 2007.

SCHRENK, M: **WEBBOTS, SPIDERS AND SCREEN SCRAPERS**, (A guide to developing internet agents with PHP/CURL),2nd Edition, United States of America, No Starch Press, Inc, 2012.

TATNALL, A.: **Web Portals**, (The new gateways to internet information and services), United States of America, Idea Group Publishing, 2005.

TOROSSI, G.: **El Proceso Unificado de Desarrollo de Software**, Instituto Tecnológico de Morelia, <http://dsc.itmorelia.edu.mx/~jcolivares/courses/pm10a/rup.pdf>

+