ANALISIS DE RIEGOS Y PROTOTIPO DE UNA PAGINA WEB MEDIANTE AUTENTICACION CAPTCHA

TRABAJO DE GRADO

PARTICIPANTES

MAURE KATERINE MUÑOZ LUNA.
LUIS FERNANDO GARCIA RODRIGUEZ

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

ANALISIS DE RIEGOS Y PROTOTIPO DE UNA PAGINA WEB MEDIANTE AUTENTICACION CAPTCHA

TRABAJO DE GRADO

PARTICIPANTES

MAURE KATERINE MUÑOZ LUNA.
LUIS FERNANDO GARCIA RODRIGUEZ.

Asesor(es)
ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

AGRADECIMIENTOS

Gracias a Dios por la oportunidad de crecer cada día en todos los niveles de nuestra vida.

Agradecemos a los docentes de la especialización de seguridad de la información del politécnico Grancolombiano, que nos han brindado su tiempo y conocimientos para guiarnos en el desarrollo de nuestro proyecto de grado.

Igualmente queremos agradecer a nuestras familias por su constante apoyo y motivación, que a pesar de las adversidades nos apoyan para que continuemos en el logro de nuestras metas profesionales.

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, junio de 2017

INTRODUCCIÓN

El presente documento describe la propuesta para resolver la necesidad de contar una página web segura para el acceso a los clientes de una empresa privada relacionada con el sector financiero, la cual se ha visto enfrentada a una serie de eventos y ataques cibernéticos que han generado la indisponibilidad de los servicios en sus canales virtuales y que han puesto en compromiso la confidencialidad de la información de sus clientes y proyectos organizacionales, debido a las pérdidas financieras que implica para la empresa la materialización de los riesgos asociados a las vulnerabilidades y amenazas de sus sistemas, es preciso gestionar estos de manera proactiva.

La participación de las empresas en internet conlleva a estar preparados contra las amenazas externas y vulnerabilidades internas, la gestión del riesgo de seguridad de la información nos permite lo expresado anteriormente y lleva a que las empresas pongan en práctica los estándares y controles necesarios para asegurar la seguridad de la información en todos los medios y canales de comunicación en que se encuentren.

1. RESUMEN EJECUTIVO

El presente proyecto tiene como finalidad identificar y proponer solución a falencias especificas en cuanto a seguridad informática para una empresa localizada en la ciudad de Bogotá, dedicada a prestar los servicios de recuperación de cartera, recaudo y crédito para entidades financieras. La empresa cuenta con una sola página web para el acceso a los servicios virtuales, sin embargo se han identificado algunas limitaciones para atender todos los diferentes clientes, se tienen por un lado los clientes reales y por otro lado los futuros clientes de la empresa que están solicitando un servicio y que aún no tienen ningún producto matriculado a su nombre, pero tienen creados usuarios en las bases de datos con credenciales y de la misma manera que un cliente con producto matriculado, dado que no todos los solicitantes recibirán la aprobación de la solicitud y en algunos casos, los solicitantes no vuelven a realizar otras solicitudes, con lo cual se estarían creando usuarios que después de un corto periodo de tiempo no se utilizarían y que podría estar usando espacio en base de datos de manera innecesaria dado que no se realiza depuración de los usuarios en las bases datos. Adicionalmente se podría estar creándose acceso a personas que no se han validado sus datos completamente o con datos falsos por causa a posibles ataques cibernéticos con bots y crawlers que pueden poner en riesgo la seguridad de la plataforma informática y su información.

De igual manera se evidencia que no están conscientes de los riesgos a los que está expuesta la plataforma web dado que no se han gestionado los mismos y han sido precarias las acciones tomadas para evitar, minimizar o enfrentar las vulnerabilidades asociadas al desarrollo de las aplicaciones web debido a la falta de concientización en la gestión de riesgos y seguridad de la información.

El objetivo general es diseñar un prototipo de una página web que permita a los clientes potenciales de la empresa tener acceso, con verificación a través de captcha a partir del análisis preliminar de los riesgos asociados a esta. Entre los objetivos específicos tenemos:

- Analizar la arquitectura de la página web actual con el fin de identificar mejoras en la seguridad de esta, de acuerdo a las mejores prácticas de desarrollo seguro de la guía OWASP.
- Identificar los riesgos a los que está expuesta la información contenida en la página web de la empresa para su gestión y tratamiento.
- Capacitar y concientizar en todas las áreas de la empresa en temas de riesgos y de desarrollo seguro.

En este proyecto aplica el análisis y diseño del prototipo de una página web para los futuros clientes de la empresa que permita el reconocimiento si es una persona la que está solicitando el acceso y conseguir el cumplimiento de los objetivos propuestos sin exponer su información confidencial, no se incluye dentro del alcance la creación e implementación de la página web con captcha. También se

incluye el análisis y tratamiento de los riesgos de seguridad de la información asociados a la página web.

Las metodologías empleadas para solucionar el problema de desarrollo seguro presentado son basadas en la guía OWASP y la norma NTC-ISO 31000 para la gestión del riesgo, a partir de la identificación y análisis de los riesgos de seguridad de información de la página web de la empresa se busca priorizar la atención de aquellos riesgos que pongan en compromiso los objetivos de la empresa.

Palabras clave:
Seguridad, Informática, Análisis, Riesgo, Captcha, Bots, OWASP, Prototipo, Autenticación

2. JUSTIFICACIÓN

Seleccionamos una empresa privada ubicada en la ciudad de Bogotá, que actualmente cuenta con 7 sedes ubicadas en su área metropolitana y municipios aledaños, es una empresa dedicada a brindar a sus clientes productos y servicios de carácter financiero, cuenta con los servicios de recuperación de cartera, recaudo y crédito para entidades financieras.

La empresa realizó un análisis de riesgos para detectar las causas raíz del porque se presenta indisponibilidad de la página web para el acceso a los servicios que presta, sin embargo en los últimos años debido a ataques cibernéticos se ha generado la denegación de servicios e intermitencias en su plataforma web por largos periodos de tiempo, esta página ha sido blanco constante de ataques de bots, llenando la base de datos de información basura y malware. Lo cual da como resultado lentitud en los servidores, y en las tablas donde se almacenan los registros de solicitud de contacto se evidencia la generación diaria de más registros de lo usual, se concluyó que la página está siendo atacada por bots por la falta de protocolos para el desarrollo seguro y la poco frecuencia de actualización de los frameworks.

Entre los principales ataques cibernéticos a los que está expuesto la página web principal de la empresa tenemos “Bots”, los cuales realizan una saturación de los servicios web de la organización mediante el envío de peticiones masivas y que han generado que algunas páginas expuestas generen información basura en las bases de datos de la organización y que por el aumento del volumen de información, las bases de datos han tendido a aumentar el tiempo de respuesta a las peticiones y se han presentado negaciones de servicios por bloqueo en algunos servidores.

También se presentan ataques por inyección SQL, el cual consiste en el envío de sentencias SQL con el fin de obtener información de las bases de datos, como el caso de información de los esquemas de base de datos, identificación de las tablas de las bases de datos y posteriormente usar esta información para obtener información contenida en las tablas de las bases de datos. El área de TI afirma que aún que se han presentado varios eventos de este tipo, los atacantes no han logrado acceder a información confidencial de los clientes y se han implementado más controles a las transacciones actuales y filtros de seguridad en los servidores, además que se proyecta con las directivas de la organización mayor presupuesto para la actualización de las aplicaciones, y de los dispositivos informáticos.

En cuanto al personal se evidencia que no está conscientes de los riesgos a los que está expuesta la plataforma web dado que no se han tomado las acciones a tiempo para evitar, minimizar o enfrentar las vulnerabilidades asociadas al desarrollo de las aplicaciones web debido a la falta de definición de una política de desarrollo seguro y la concientización en la gestión de seguridad de la información.

La empresa ha identificado algunas limitaciones para atender algunas necesidades específicas de sus clientes y que puede generar una pérdida en el terreno competitivo frente a otras entidades de similar tamaño y servicios. La empresa cuenta solo con una página web para atender todos los diferentes clientes, se tienen por un lado los clientes y por otro lado los futuros clientes de la empresa que están solicitando un servicio y que aún no tienen ningún producto matriculado a su nombre tienen creados usuarios en las bases de datos con credenciales y de la misma manera que un cliente con producto matriculado, dado que no todos los solicitantes recibirán la aprobación de la solicitud y en algunos casos, los solicitantes no vuelven a realizar otras solicitudes, con lo cual se estarían creando usuarios que después de un corto periodo de tiempo no se utilizarían y que podría estar usando espacio en base de datos de manera innecesaria dado que no se realiza depuración de los usuarios en las bases datos. Adicionalmente que podría estar creándose acceso a personas que no se han validado sus datos completamente o con datos falsos y podrían ser posibles atacantes que pueden poner en riesgo la seguridad de la plataforma informática y su información.

El acceso a este tipo de clientes requiere de una solución que no ponga en riesgo la seguridad de la plataforma, que cumpla con estándares internacionales en cuanto desarrollo, y seguridad de aplicaciones, y que no sea vulnerable al ataque mediante peticiones masivas con botnets.

En la siguiente figura podemos ver la distribución de solicitudes no aprobadas por periodo de tiempo para las 7 sucursales.

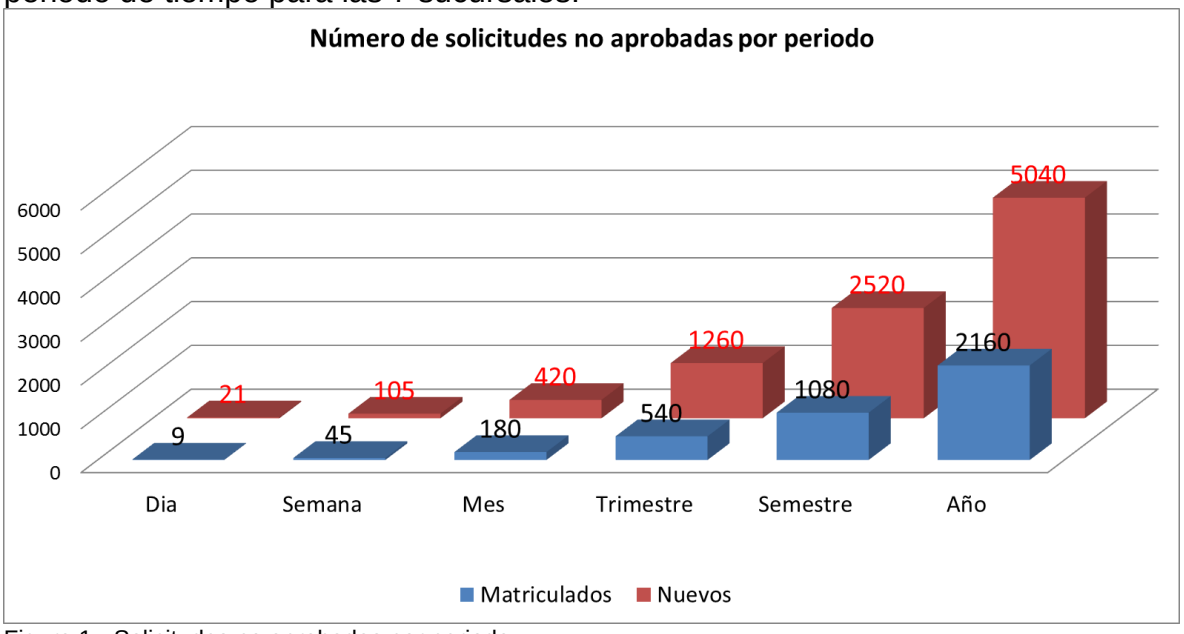

Figura 1 - Solicitudes no aprobadas por periodo

De acuerdo a la anterior figura podemos concluir que si creamos un usuario con credenciales en la plataforma por cada solicitante nuevo (sin productos

matriculados), por año la empresa estaría creando 5040 usuarios a los cuales no se aprobará su solicitud. Por esta razón se hace necesario tener una página web diferente de consulta para estos usuarios a los cuales no se les creerían credenciales de autenticación y no se almacenarían en las bases de datos de clientes matriculados, se propone diseñar un CAPTCHA que verifique que el usuario no es un bot o robot para permitirle el acceso a la página web. Con lo cual se puede pensar en tener una arquitectura de base de datos separada de la principal plataforma en la cual en caso que se presente un ataque o vulneración no se ponga en riesgo información clasificada de los clientes, mejorando la capacidad y veracidad de las bases de datos de clientes potenciales y la toma de decisiones al tener datos reales de la cantidad de estos usuarios.

3. MARCO TEÓRICO Y REFERENTES

3.1 ISO 31000:2009

Para la gestión de riesgos se requiere acoger la norma ISO 31000:2009 que "proporciona principios y directrices genéricas sobre la gestión de riesgos, la cual puede ser utilizada por cualquier empresa, asociación, grupo o individuo público, privado o comunitario.

La ISO 31000: 2009 puede aplicarse a lo largo de toda la vida de una organización ya una amplia gama de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos. Esta puede aplicarse a cualquier tipo de riesgo, cualquiera que sea su naturaleza, con consecuencias positivas o negativas.

Aunque ISO 31000: 2009 proporciona directrices genéricas, no pretende fomentar la uniformidad de la gestión del riesgo entre las organizaciones. El diseño e implementación de los planes y marcos de gestión de riesgos deberán tener en cuenta las diferentes necesidades de una organización específica, sus objetivos particulares, contexto, estructura, operaciones, procesos, funciones, proyectos, productos, servicios o activos y prácticas específicas empleadas.

La ISO 31000: 2009 nos permite armonizar los procesos de gestión de riesgos en los estándares existentes y futuros. Proporciona un enfoque común en apoyo de normas que se ocupan de riesgos y / o sectores específicos, y no sustituye esas normas". [1]

Es por ello que a partir de la identificación de los riesgos asociados a la exposición de la página web a ataques cibernéticos se propone el diseño de un Captcha que valide si el usuario es un humano para poder autorizar el acceso a los servicios web de solicitudes.

3.2. ATAQUE INFORMATICO

Como parte del proceso de análisis debemos entender como tal que es un ataque informático, como puede afectar a la organización y de esta manera tendremos las herramientas necesarias para evitar, contener y mitigar futuros eventos de ataques informáticos en las organizaciones.

Primero que todo debemos entender que un ataque informático es un método que tiene como objetivo acceder de manera no autorizada a un sistema informático (programa, servidor, maquina o dispositivo), con el fin tomar el control, eliminar, cambiar o acceder información a la cual no se tiene permiso e incluso con el fin de divulgar dicha información de manera no autorizada.

El impacto de los ataques varia del objetivo o meta del atacante, por ejemplo, si el atacante tiene un objetivo claro como obtener información confidencial (historias clínicas, datos financieros, informes bancarios, prototipos, planes de mercadeo futuro, entre otros) con el fin de lucrarse, es muy seguro que el ataque sea discreto y cuidadoso de manera que la víctima le tome lo mayormente posible darse por enterarse que fue atacado y esto le permite al atacante tiempo valioso para su cometido. Pero por el contrario si el ataque busca desestabilizar a una organización y poner en entredicho su seguridad, lo más seguro es que el ataque sea algo que afecte en gran medida a los sistemas informáticos, como por ejemplo que se produzcan negaciones de servicio, que se robe información confidencial y se le informe a los medios, o que se vendan datos de tarjetas de crédito en sitios del mercado negro informático, algo que en poco tiempo será de interés publico y lo que repercutiría directamente en la reputación de la organización afectada, viéndose envuelta en situaciones de carácter legal (demandas de los clientes), y económicas (si la empresa está en el mercado de valores, generaría que sus acciones caigan), incluso se han dado intentos de ataques a dispositivos de hardware en instalaciones nucleares con el fin de generar una falla en los dispositivos que pudieron terminar en tragedia de no ser por la oportuna intervención de expertos en seguridad.

Entre los principales tipos de ataques informáticos tenemos:

- **Trashing**: Consiste en el robo de credenciales de autenticación que fueron desechadas de manera descuidada por la víctima en algún medio físico o informático y obtenidas por el atacante, como por ejemplo: claves en papeles que se arrojaron a la basura, o claves anotadas en comentarios de las aplicaciones por los desarrolladores con el fin de poder probar más rápidamente y que no fueron removidas.
- **Monitorización**: Es un ataque que consiste en hacer una vigilancia a la víctima a la espera que revele información de interés (Credenciales de autenticación, tokens de seguridad, entre otros). Este tipo de ataque es muy común al hacer uso de redes wifi públicas que no cuentan con los requisitos de seguridad mínimos y que mediante proxies el atacante puede filtrar y re direccionar información de las víctimas, de igual manera el uso de equipos públicos con programas de monitorización como keyloggers o proxies, como es el caso de cibercafés.
- **Negación del servicio (DoS)**: Busca saturar los servicios informáticos de la víctima de manera que no puedan estar disponibles para los clientes o usuarios de esta. Por ejemplo, atacar una página web mediante bots, que lo que hacen es que la pagina deje de estar disponible para el público.
- **Ataques de Autenticación**: Es una manera que engañar a la víctima mediante correos con falsas identidades de personas o empresas, con el fin que el usuario ingrese sus credenciales en una web falsa y luego sea redirigida a la real, después que la víctima ingresa sus credenciales en la página falsa esta información es almacenada para futuros ataques, algunos casos de este tipo se conocen como pishing.

Teniendo un panorama más claro relacionado a los ataques informáticos y sus tipos, ahora es necesario de comprender mejor los eventos específicos a los que se ha visto enfrentada la organización y por los que se generó esta investigación.

- **Bots y botnets**: Son programas informáticos que tienen como objetivo tomar el control de otras máquinas remotamente con el fin de usarlas para otros propósitos malintencionados, cuando se tiene un grupo de estos bots se conocen como botnets.
  Estas máquinas infectadas tienen como función el envió de spam, virus y de software espía a otras máquinas. Lo cual puede conllevar a que las victimas pierdan información confidencial, e incluso que presenten en sus plataformas informáticas eventos de denegación de servicio.
- **Inyección SQL**: Es un ataque informático que consiste en adicionar código SQL en campos de la aplicación o a través de las peticiones rest, con el fin que este código se ejecute y/o almacene en el servidor de base de datos con el fin obtener información confidencial o del sistema que pongan en riesgo la integridad de la aplicación, y en algunos casos que pueda permitirle al atacante modificar información directamente en la base de datos.

Algunos consejos que se tienen para reducir y mitigar los ataques informáticos son los siguientes:

- Usar programas legales con sus respectivas licencias.
- Actualizar constantemente el hardware y software de la organización.
- Implementar controles de seguridad tanto desde el punto de vista lógico como físico.
- Si la empresa desarrolla algunas de sus aplicaciones, que los desarrolladores sigan una metodología de desarrollo de código seguro, tales como CbyC, SDL, CLASP, o OWASP.
- Implementar controles de verificación de que quien realiza consultas de información sensible sea un humano (Captcha o reCaptcha).
- Implementar controles de acceso por roles y con una correcta especificación de acceso por rol a los recursos.
- Implementar políticas de seguridad de la información en la organización.
- Realizar campañas de capacitación y concientización de los efectos de los ataques informáticos a las compañías.
- Implementar controles de navegación a los usuarios de las plataformas informáticas.
- Contar con antivirus debidamente actualizados para asegurar el control de archivos descargados por correo o desde la web.
- Implementar protocolos seguros de comunicación https
- Asegurar las comunicaciones de la organización con algoritmos RSA

Como podemos observar en las organizaciones el aseguramiento de los sistemas de información no es solo una labor del área de las tecnologías de la información (TI), es también parte de la gerencia y las directivas que deben garantizar

presupuestos para la actualización de equipos y software, para la obtención de las licencias informáticas. Adicional a esto el equipo de trabajo de las organizaciones debe estar capacitado en cuanto a conceptos básicos enfocados en la seguridad informática de manera que no se agreguen más brechas de seguridad desde el interior de la organización.

3.3. CAPTCHA

“Captcha son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos). Este test es controlado por una máquina, en lugar de por un humano como en la prueba de Turing. Por ello, consiste en una prueba de Turing inversa. Consiste en que el usuario introduzca correctamente un conjunto de caracteres que se muestran en una imagen distorsionada que aparece en pantalla. Se supone que una máquina no es capaz de comprender e introducir la secuencia de forma correcta, por lo que solamente el humano podría hacerlo”. [2]

Esta herramienta permite identificar si quien hace uso de la página es un humano y no un robot, minimizando así los eventos de ataques informáticos con el fin de colapsar los servicios web, bloqueo de servidores, o inserción de basura en bases de datos.

Algunas ventajas de usar captcha en las páginas web con interaccione de usuarios en sesiones no seguras son las siguientes:

- Evita que un sitio web sea dañado o vulnerado
- Evita el acceso a información privada
- Evita el spam en blog y foros.

Aunque no todo es beneficio, el captcha también tiene desventajas, como por ejemplo:

- Puede ser molesto para usuarios principiantes o sin mucha experiencia en sistemas.
- En ocasiones los números, letras o imágenes que hay que resolver no son lo suficientemente claros para solucionar el captcha.

Hoy en día existen muchas opciones en el mercado, de pago y gratuitas que permiten agregarle seguridad a las páginas web mediante este tipo de herramientas, donde dependiendo de la herramienta, se utiliza una estrategia diferente para identificar a quien usa el recurso, por ejemplo a través de preguntas, presentándole palabras distorsionadas al usuario que sería difícil a una maquina comprender, o preguntándole acerca de una imagen que la aplicación le

presente al usuario o permitiéndole elegir entre diferente imágenes las que corresponden a una categoría.

A continuación se mostrarán algunos ejemplos de captchas.

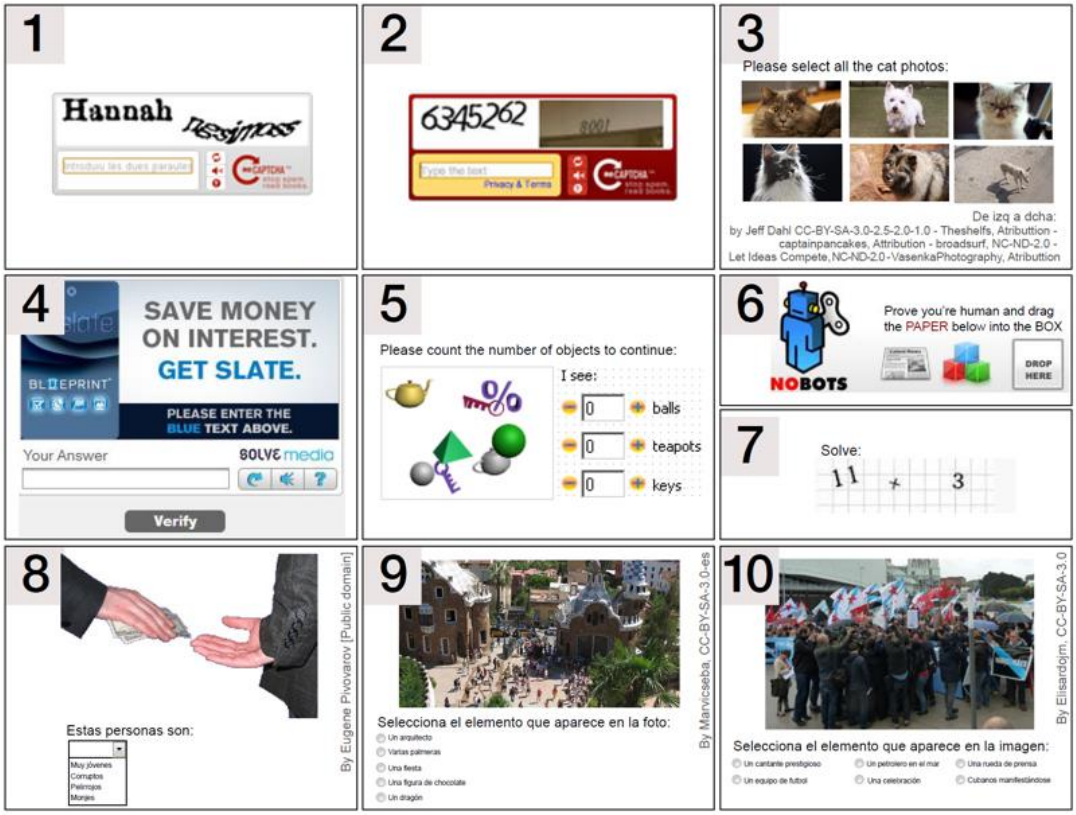

Figura 2 - Ejemplos de captchas [3]

3.4 OWASP

El desarrollo seguro de la aplicación web se basa en el estándar OWASP "(acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera". [4]

4. METODOLOGÍA

Entre las diferentes metodologías para la realización del presente trabajo tenemos:

4.1 Metodología de valoración de riesgos

La metodología para la valoración de riesgos se fundamenta en la norma NTC-ISO 31000 [5], explicada a continuación:

4.1.1 Definir contexto y alcance de la gestión del riesgo

Es necesario conocer el contexto de la organización, la interrelación de los procesos y las actividades ejecutadas con el fin de identificar posibles falencias o vulnerabilidades de los procesos que puedan poner en riesgo la información. Para ello se deberá realizar un entendimiento de la información contenida en la página web, así como entrevistas con los dueños de los procesos para profundizar en el contexto interno y externo de la empresa.

4.1.2 Identificar los riesgos

Evaluar todas aquellas situaciones que puedan poder en riesgo el cumplimiento de los objetivos de la empresa, se deberán tener en cuenta los riesgos de origen interno y externo, en esta etapa se requiere identificar las vulnerabilidades, amenazas, consecuencias y factores de riesgo.

Consecuencias

Para evaluar las consecuencias se deberá seleccionar entre:

- Pérdidas financieras
- Pérdidas reputacionales
- Pérdidas legales

Fuentes generadoras de riesgo

Entre las fuentes generadoras de riesgo tendremos en cuenta:

- Recursos humanos
- Tecnología
- Externos
- Ambiental
- Infraestructura
- Operativo

4.1.3 Analizar los riesgos

En esta etapa de acuerdo a las causas, consecuencias positivas o negativas, fuentes de riesgo, se determina la probabilidad de ocurrencia del riesgo y el impacto, variables que nos permiten establecer el nivel de riesgo.

Probabilidad
Se define como la posibilidad de ocurrencia en el tiempo del riesgo:

Valor	Probabilidad de ocurrencia
1	Esporádico, puede suceder una (1) vez en una (1) década
2	Ocasional, puede suceder una (1) vez en un (1) año
3	Posible, puede suceder una (1) vez en un (1) mes
4	Frecuente, puede suceder una (1) vez en una (1) semana
5	Muy frecuente, puede suceder una (1) vez en un (1) día

Tabla 1- Probabilidad de ocurrencia

Impacto
Se define de acuerdo a la afectación que puede tener el cumplimiento de los objetivos del proceso, por la materialización del riesgo.

Valor	Grado de impacto
1	Insignificante, no hay afectación significativa en los objetivos del proceso
2	Bajo, puede haber afectación baja en los objetivos del proceso
3	Moderado, puede haber afectación significativa en los objetivos del proceso
4	Crítico, puede haber afectación grave de los objetivos del proceso
5	Catastrófico, puede haber afectación desastrosa de los objetivos del proceso

Tabla 2 - Grado de impacto

Nivel del riesgo

De acuerdo al resultado entre la intersección entre la probabilidad y el impacto se establece el nivel del riesgo, el cual se determinará basado en la siguiente tabla:

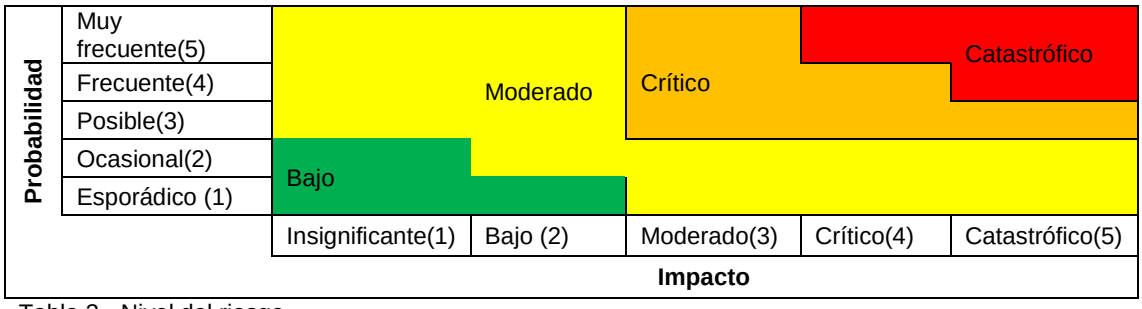

Tabla 3 - Nivel del riesgo

Una vez finalizado esta etapa se realiza un resumen de los riesgos con mayor criticidad de atención para su presentación a la alta gerencia en donde justifica la necesidad de tratar los riesgos que pueden poner en riesgo el cumplimiento de los objetivos de la empresa.

4.1.4 Tratamiento del riesgo

Se deberán determinar acciones de tratamiento para reducir el nivel de riesgo a un nivel aceptable. Las acciones para el tratamiento de los riesgos se determinarán de acuerdo al nivel del riesgo, a excepción del Nivel Bajo para todos los demás niveles se deberá tomar uno de los siguientes tratamientos:

- Transferir el riesgo a un tercero
- Evitar el riesgo
- Reducir el nivel de riesgo

De acuerdo a la criticidad del riesgo se definieron las siguientes acciones de tratamiento:

Criticidad del riesgo	Acciones a tomar
Bajo	Aceptar y monitorear el riesgo
Moderado	Transferir, evitar o reducir el nivel riesgo
Crítico	Transferir, evitar o reducir el nivel riesgo
Catastrófico	Transferir, evitar o reducir el nivel riesgo

Tabla 4 - Tratamiento del riesgo

En esta etapa se construye el plan de acción de riesgos, en donde se determina el dueño del riesgo, quien será el responsable de la ejecución de las actividades necesarias para reducir los niveles de riesgo.

4.2 Estándares de desarrollo seguro

Para minimizar los incidentes de seguridad en cuanto a la plataforma de la organización y para diseñar de la página web segura se deberán tener en cuenta la guía OWASP, la cual busca que se construyan aplicaciones seguras.

La idea es que se identifiquen claramente los riesgos, las vulnerabilidades y el impacto sobre el negocio de manera que podamos controlar o disminuir dicho riesgo. Las siguientes debilidades son las más comunes y que de acuerdo al análisis previo realizamos son las más críticas en este momentos para la organización

- A1: Inyección
- A2: Cross-Site Scripting (XSS)
- A3: Autenticación y gestión de sesiones

Respecto a los lineamientos a implementar en la guía de seguridad informática tomaremos como base las fases propuestas por la metodología OWASP, las cuales son:

Fase 1. Antes de empezar el desarrollo.
Para esta fase se contempla la ejecución de las siguientes actividades:

- Comprobación del ciclo de desarrollo del software
- Comprobación de los estándares y políticas de seguridad
- Desarrollo de los criterios de medición y métricas

Fase 2. Durante el diseño y la definición
Para esta fase se contempla la ejecución de las siguientes actividades:

- Revisar los requerimientos de seguridad (gestión de usuarios, autenticación, roles, sesiones, confidencialidad de los datos, integridad de los datos).
- Revisar el diseño de la arquitectura (asegurar que los documentos de arquitectura existan, modelos, entre otros).
- Creación y revisión de los modelos UML.
- Creación y revisión de los modelos de amenaza.

5. RESULTADOS Y DISCUSIÓN

5.1 Análisis de riesgos

Mediante el análisis de riesgo podemos identificar los principales riesgos y vulnerabilidades a las cuales estaría expuesta la aplicación web (**Ver Anexo 1 MATRIZ DE ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**), de este ejercicio resulto la priorización de los riesgos de la siguiente manera:

- **Catastróficos**:
  - Pérdida de disponibilidad de la página web por ataques externos

- **Críticos**:
  - Pérdida de la integridad de las bases de datos y/o el rendimiento de los servidores de aplicación
  - Acceso lógico no autorizado por asignación errónea de permisos a aplicaciones web del negocio
  - Explotación de vulnerabilidades técnicas por atacantes externos
  - Pérdida de confidencialidad por robo de información confidencial de las bases de datos

Adicionalmente podemos concluir que de no mitigar los riegos representarían pérdidas financieras y reputacionales para la organización, que podrían conllevar a gastos mayores si no se tratan proactivamente.

5.2 Identificación de Requerimientos

El documento de identificación de requerimientos permitió conocer las necesidades de la organización en cuanto a la página web para la consulta de solicitudes (**Ver Anexo 2 IDENTIFICACIÓN DE REQUERIMIENTOS**), adicional en dicho documento se hizo el análisis de los casos de uso y los casos de abuso. Permitiéndonos así proponer la implementación de un prototipo de la página web de la herramienta reCaptcha de google para asegurar que quien realiza la consulta es un humano y de esta manera evitar los ataques por bots o crawlers, que vulneran la seguridad de la página web, llenan formularios con información falsa generando spam.

Entre los beneficios de reCaptcha vs otras aplicaciones de captcha tenemos:

- Es soportado por google
- Es más fácil de usar por los humanos
- Tiene diferentes tipos de pruebas lo que genera que no sea fácilmente solucionada por bots, mediante el uso de patrones.
- Está en constante evolución
- Es gratuito

En la siguiente figura podemos ver el diagrama de la API de recaptcha para hacer la verificación de usuarios en las aplicaciones.

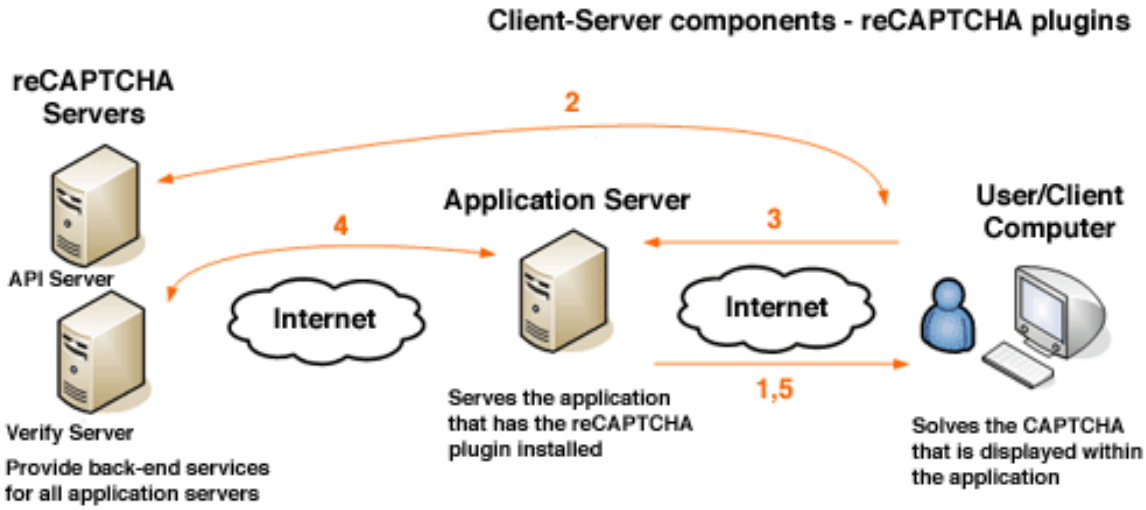

Figura 3 – Diagrama API de reCaptcha [6]

La arquitectura propuesta por google reCaptcha, busca que se implemente el API en la página web, donde a través de una validación se envían al servidor de reCaptcha usando una clave pública y una llave privada. Los servidores responden con un token en caso de ser afirmativo, el cual debemos pasar al backend del servidor nuestro y hacer una verificación del token usando ahora una llave privada contra los servidores de reCaptcha, si esto funciona, podemos continuar con la petición en nuestros servidores, de lo contrario, se debe cancelar la petición, dado que se consideraría una petición no autorizada.

5.3 Arquitectura de la página web

Para la página web, proponemos usar una arquitectura MVC (Modelo Vista Controlador), con lo cual podemos tener más control de la página web y se busca su mantenibilidad.

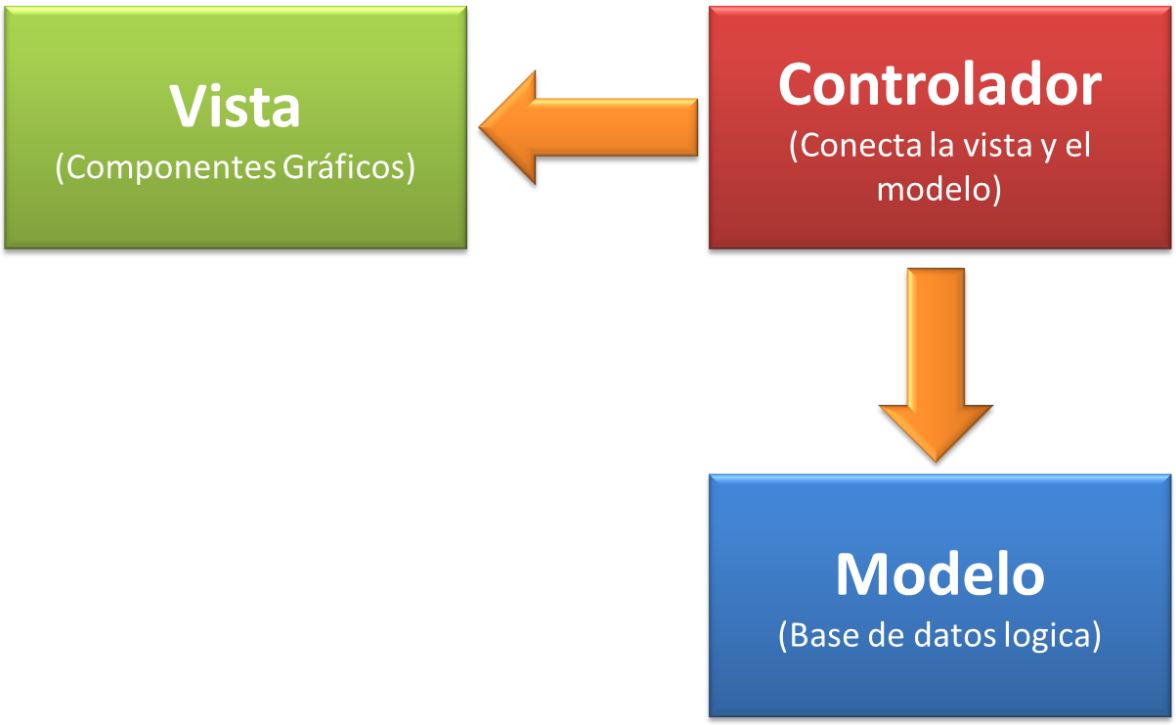

Figura 4 - Arquitectura página web

5.4. Herramientas Informáticas para el desarrollo de la página web.

Dentro de las herramientas Informáticas para el desarrollo de la página web consideramos que el uso de jHipster nos permitirá la implementación de la página web de una manera más ágil y rápida.

Tecnologías en el lado del cliente

- AngularJS v1.x or Angular v2+
- Responsive Web Design with Twitter Bootstrap
- HTML5
- Soporte de internationalization
- Soporte para CSS
- WebSocket con Spring Websocket

Tecnologías en el lado del servidor

- Spring Boot para una fácil configuración de la aplicacion
- Maven o Gradle para la configuración del build.
- Spring Security
- Spring MVC REST + Jackson
- WebSocket mediante Spring Websocket
- Spring Data JPA + Bean Validation

5.5. Prototipo.

El prototipo resultante es un modelo de la visualización de como resultaría la página web, por lo que es de esperarse que las funcionalidades sean configuradas de manera parcial, el prototipo funciona de la siguiente manera:

a) El usuario ingresa a la página web.

Figura 5 - Página web de acceso inicial

b) Por medio del menú principal, el usuario da clic en el botón “Solicitudes”. Lo cual lo lleva a la página de solicitudes, en donde puede ingresar su documento de identidad.

Figura 6 - Solicitud de autorización de acceso

c) El usuario da clic en el botón de reCaptcha, y la aplicación carga una validación que permitirá saber si quien está usando la aplicación es un humano o un robot.

Figura 7 - Resultado Recaptcha

d) La aplicación hace la validación de la respuesta, en los servidores de reCaptacha y manda el token al backend con el documento de identidad del cliente, tanto el token como el documento se deben validar internamente, y si todo es satisfactorio entonces se abre la página de solicitudes del cliente, en caso

contrario se niega el acceso, disminuyendo los riesgos asociados a los ataques spambots.

Figura 8 - Resultado de consulta

Se puede encontrar este prototipo publicado en la siguiente URL: https://invis.io/BRBWE4CTN

5.6 Plan de sensibilización

El plan de sensibilización tiene como objetivo principal crear consciencia en los usuarios de la herramienta de captcha a implementar para mejorar la seguridad de la página web de la empresa y disminuir los ataques por bots y crawlers.

Los cambios que se generan a nivel organizacional deberían ser sensibilizados para lograr la mayor aceptación posible y satisfacción al ser creados para mejorar la seguridad de los aplicativos web.

Las fechas, áreas objetivos y temas se detallan en el **Anexo 3 PLAN SENSIBILIZACIÓN CAPTCHA**.

6. CONCLUSIONES

Las organizaciones deben considerar la seguridad de la información como un valor que agrega de prestigio y confiabilidad para sus clientes y no como un costo adicional, el costo-beneficio de implementar controles debe ser adecuado de acuerdo al nivel de importancia de la información que maneje la empresa y el impacto que pudiera causar la vulnerabilidad de esta.

La globalización comercial enfrenta a las organizaciones a nuevos retos en cuanto a la seguridad informática, en donde se debe contar con todo un set de metodologías, políticas y aplicaciones que constantemente estén actualizándose para poder contrarrestar en lo posible de la medida las nuevas a amenazas que día a día emergen con el único propósito de identificar y aprovechar las vulnerabilidades informáticas con fines delictivos.

La gestión de riesgos se ha constituido en una de las principales herramientas para estar preparados contra todas las vulnerabilidades y amenazas de nuestros sistemas de información, lo cual conlleva a considerar el uso de las mejores prácticas y estándares, entre ellas la metodología OWASP se especializa en el ciclo de desarrollo del software de aplicaciones seguras. También se ha convertido en el eje primordial para controlar proactivamente los riesgos antes de comenzar el diseño del software, el monitoreo de estos desde etapas tempranas nos permite reducir los costos y pérdidas asociados a la materialización de los riesgos, por la prevención y detección antes de su aparición.

La implementación de controles como la verificación por Captcha nos permite minimizar los ataques cibernéticos que buscar tener acceso a la información expuesta en internet, el cual es uno de los mayores problemas a los que deben estar preparadas las empresas, para enfrentarlos de manera proactiva y con la misma dinámica con que aparecen.

BIBLIOGRAFIA

[1] ISO 31000. Disponible en: https://www.iso.org/standard/43170.html [Consultado 22-Abril-2017]

[2] Captcha. Disponible en https://es.wikipedia.org/wiki/Captcha [Consultado 22-Abril-2017]

[3] Usabilidad Captchas. Disponible en http://www.nosolousabilidad.com/articulos/usabilidad_captchas.htm [Consultado 22-Abril-2017]

[4] OWASP. Disponible en: https://es.wikipedia.org/wiki/Open_Web_Application_Security_Project [Consultado 22-Abril-2017]

[5] Norma Técnica Colombiana NTC-ISO 31000 Gestión del Riesgo. Principios y Directrices. Bogotá. ICONTEC. 2011

[6] "File:Recaptcha-api-diagram.gif" [En línea]. Disponible en: https://developer.salesforce.com/page/File:Recaptcha-api-diagram.gif [Consultado 7-may-2017]

[7] Javier Elío 18/08/2016 [En línea]. Disponible en: https://elandroidelibre.elespanol.com/2016/08/historia-de-los-captchas.html [Consultado 25-may-2017]

[8] Bots y botnets: Una amenaza creciente [En Línea]. Disponible en https://es.norton.com/botnet [Consultado el 28-may-2017]

[9] Ataque informático [En línea], Disponible en https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico [Consultado el 28-may-2017]

ANEXOS

ANEXO 1 MATRIZ DE ANALISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACION

ANEXO 2 IDENTIFICACIÓN DE REQUERIMIENTOS

ANEXO 3 PLAN SENSIBILIZACIÓN CAPTCHA