SÍNTESIS OWASP GESTIÓN DE RIESGOS DE LA SEGURIDAD EN APLICACIONES

Montaña, Oscar.
montana.andres@gmail.com
Universidad Piloto de Colombia

Abstract— This document provides a synthesis of the risk management on applications security according to OWASP for Heads of Information Security (CISOs) who are charged with the responsibility for applications security, focus on governance, compliance and risk.

Index Terms— Audit, Cryptographic, life cycle of the software, error control, framework, security, vulnerability.

Resumen – En este documento se realiza una síntesis de la gestión de riesgos de la seguridad en aplicaciones según OWASP para los Jefes de Seguridad de la Información (CISOs), quienes están encargados de la responsabilidad de la seguridad para las aplicaciones, enfocados al gobierno, el cumplimiento y el riesgo.

I. INTRODUCCIÓN

La gestión de riesgos es una actividad clave para garantizar y proteger los activos de información de la organización como lo son las personas, los datos sensibles, las bases de datos, la infraestructura de red y las aplicaciones; toda compañía se encuentra constantemente expuesta a una serie de vulnerabilidades y amenazas surgidas del uso de tecnologías de la información y las comunicaciones, creando la necesidad de proteger dichos activos.

Al considerar e identificar apropiadamente la exposición de amenazas emergentes y requisitos de cumplimiento ayudaría a los CISOs a gestionar los riesgos de seguridad en aplicaciones.

La gestión de riesgo permite:

- Dar visibilidad a la alta gerencia de la seguridad informática en aplicaciones por parte de los CISOs.
- Medir y administrar los riesgos de seguridad.
- Garantizar la protección de activos y seguridad de la información.
- Obtener un adecuado tratamiento del riesgo considerando diferentes aspectos.
- Tomar oportunamente decisiones sobre la protección de la información, basadas en los riesgos garantizando la confidencialidad, integridad y disponibilidad de los activos.
- Determinar los posibles impactos que pueden generarse de las vulnerabilidades y amenazas analizadas, para identificar las contramedidas necesarias.

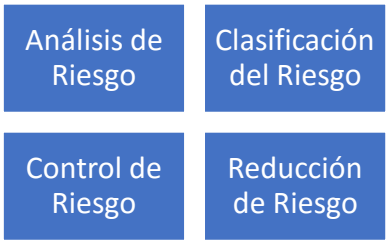

Fig. 1 Fases Gestión del Riesgo. [1].

OWASP es una organización sin fines de lucro cuya misión es “hacer visible la seguridad en aplicaciones y potenciar a las partes interesadas con información adecuada para la gestión de riesgos de seguridad en las aplicaciones”. [2].

II. GESTIÓN DE RIESGOS

Es una de las funciones básicas que debe realizar el CISO, en donde se tiene una metodología para mantener de forma organizada la seguridad de la información.

Con el aumento actual de aplicaciones web que permiten realizar diferentes tipos de transacciones con los activos, un software inseguro es un grave y frecuente problema, por esto es necesario establecer estándares que permitan asegurar la red de conexión y los datos que son enviados a través de las aplicaciones más frecuentes como redes sociales.

Para garantizar que las aplicaciones estén dentro del alcance de las evaluaciones de vulnerabilidades y requisitos de seguridad, deben realizarse validaciones de seguridad y cumplir con los requisitos que incluyen diseño, programación y operación segura. Estos requisitos son solo una de las responsabilidades de los CISOs, también es importante tener en cuenta el Gobierno, el Riesgo y el Cumplimiento.

En la gestión del riesgo, es fundamental establecer procesos claros de seguridad tanto en aplicaciones como en roles y responsabilidades, de manera que se pueda replicar esta información para generar conciencia de la seguridad del software; además se debe tener presente la importancia de la programación defensiva.

Los sistemas de información son vulnerables a una diversidad de amenazas y atentados por parte de organismos que pueden o no pertenecer a la empresa, por desastres naturales, por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de procesamiento de datos, igualmente se debe considerar riesgos de seguridad procedentes de amenazas específicas dirigidas a la obtención de brechas en los controles de seguridad en el procesamiento de datos confidenciales e información sensible.

Por tanto las partes de la organización deben procurar establecer normas de seguridad al interior de la empresa para proteger la información, implementar una planificación precisa para la seguridad informática y la gestión de los medios necesarios para la correcta administración de esta función.

La alta dirección de las organizaciones centra su atención en el cumplimiento de normas y reglamentación de seguridad, es responsabilidad de los CISOs justificar las inversiones requeridas para el acatamiento de la normatividad de la seguridad en las aplicaciones, dentro de lo que se destaca gestionar los posibles riesgos de incidentes de seguridad que contienen fraudes con tarjetas, hurto de información personal, robo de propiedad intelectual y datos confidenciales o cualquier otro incidente de filtración de datos.

Dentro de los temas relevantes en la gestión de riesgos es importante destacar que puede realizase de manera proactiva o reactiva, incluso puede hacerse centrada en los activos; y también se tienen diferentes estrategias para gestionar, entre otros.

- El análisis y el conocimiento de las nuevas amenazas.
- Responder a las expectativas del negocio después de un incidente de seguridad.
- Cuantificación del impacto al negocio por incidentes de filtración de datos.
- Analizando las medidas de seguridad como inversión.

A. Gestión de riesgos proactiva.

La gestión de riesgos proactiva consiste en enfocarse en la mitigación de riesgos de acontecimientos de amenazas antes de que éstas posiblemente puedan ocurrir y asimismo afectar negativamente a la organización.

Cuando se utiliza esta forma de gestión de riesgos se planea con anticipación proteger los activos críticos antes de que cualquier amenaza potencial pueda surgir, para las aplicaciones se centra en la información sobre amenazas, protección contra ataques, pruebas de seguridad, código fuente y corrección de posibles vulneraciones presentadas antes de que puedan ser explotadas por un ataque potencial.

Para quienes deseen optar por una gestión proactiva es necesario tener un inventario de las aplicaciones que contengan información o activos críticos y realizar sus perfiles de riesgos asociados, de esta manera se podrá priorizar y planear las actividades de mitigación necesarias; con actividades de mitigación proactivas se realizan estrategias o planes sobre eventos monitoreados, información de inteligencia de amenazas y alertas.

B. Gestión de riesgos reactiva.

La gestión de riesgos reactiva consiste en actuar a los eventos de riesgo a medida que estos se van presentando para mitigar los impactos negativos dentro de la organización.

Para las empresas que reaccionan luego de que los incidentes de seguridad han ocurrido suelen incluir investigaciones, análisis y gestión del fraude; para las aplicaciones se hace énfasis en la gestión de parches de vulnerabilidades, en la reparación de vulnerabilidades identificadas, en la evaluación de riesgos con respecto a requisitos no planeados puntuales. Dentro de la gestión de los CISOs en estas situaciones se resalta la importancia de responder a tiempo sobre eventos de gestión de riesgos no planificados, la idea principal de esto es realizar una contención de daños que permita detener estos eventos, así como también se deben remediar las vulnerabilidades presentadas en las aplicaciones; cuando se presenta este tipo de gestión reactiva se debe tener en cuenta que el costo de las remediaciones hace que sea una alternativa poco rentable después de haber sido informada o explotada por algún atacante.

Se puede realizar un enfoque de mitigación de riesgos proactivo el cual consiste en utilizar la oportunidad de una actualización de la tecnología necesaria de una aplicación para introducir nuevas funcionalidades o cuando una aplicación antigua llega al final de su vida, y tiene que migrar a un sistema/plataforma más nueva. El diseño de nuevas características para las aplicaciones representa una oportunidad para los CISOs para exigir la actualización de tecnología de seguridad a las nuevas normas y poner en práctica las medidas de seguridad más fuertes. [3].

C. La gestión de riesgos centrada en activos.

Cuando la gestión de riesgos es centrada en activos los CISOs deben considerar la implementación de un modelado de amenazas como seguridad proactiva; en estos casos para

cuando las políticas de seguridad son derivadas del cumplimiento de alguna norma de seguridad de la información debe incluirse como un dominio de seguridad a ser cubierto la gestión de activos.

Cuando un activo critico está implícito en las aplicaciones, se requiere contar con el inventario de estas para poder tener claro el enfoque, dentro de la información requerida se debe documentar el tipo de aplicaciones, tipos de datos, tipos de perfiles, perfil de riesgo, requisitos para implementar parches y sus correspondientes evaluaciones de seguridad; para este inventario se debe hacer un continuo seguimiento y así poder validar si se han realizado las correcciones necesarias en las vulnerabilidades identificadas, o si se está trabajando en alguna.

De acuerdo al perfil de riesgo identificado para cada aplicación es posible identificar la priorización que debe darse en la mitigación de vulnerabilidades existentes y planificar actividades para evaluación de la seguridad. De la misma manera también puede realizarse el modelado de amenazas para identificar las contramedidas que deben tomarse y afectar a cada activo.

D. Gestión de riesgos de negocios vs Gestión de riesgos técnicos.

Para realizar gestión de riesgos de negocios el valor del activo es el que determina el impacto en la organización, por otra parte en la gestión de riesgos técnicos representan cualquier vulnerabilidad técnica o alguna brecha de control dentro de las aplicaciones que tengan impactos técnicos negativos afectando la confidencialidad, la integridad y la disponibilidad de los activos.

Teniendo en cuenta que el riesgo se mide de acuerdo a la probabilidad de ocurrencia de un activo en peligro por el impacto causado, debe realizarse un equilibro a la hora de tomar decisiones sobre la forma de mitigar los riesgos de seguridad y se deben tener en cuenta tanto riesgos técnicos como riesgos de negocio realizando una asociación entre ambos.

La gravedad de una vulnerabilidad se puede calcular sobre la base de métodos de calificación de riesgos, como CVSS de FIRST, mientras que el tipo de vulnerabilidad puede ser clasificado en base al grupo en el que cae la vulnerabilidad tal como el uso de CWE de MITRE. Los CISOs pueden usar la puntuación de riesgos de una vulnerabilidad ALTA, por ejemplo, para darle prioridad a la mitigación antes de las vulnerabilidades que se califican con un riesgo MEDIO o BAJO. Al tomar esta decisión de gestión de riesgos técnica de vulnerabilidades, los CISOs no tendrán en cuenta el impacto económico de la vulnerabilidad para el negocio, tal como el caso del valor de los activos afectados por la vulnerabilidad los cuales son perdidos o comprometidos. [4].

La estimación de riesgos de negocio es mucho más difícil que la estimación de riesgos técnicos ya que las estimaciones de negocio requieren estimaciones de la probabilidad de determinados tipos de incidentes de seguridad (un ejemplo, la violaciones de los datos), así como las estimaciones de las pérdidas económicas (unos ejemplo, la pérdida de los ingresos, costos legales de incumplimiento, costos de reparación por la causa del incidente) que resultan de tal incidente. Normalmente estas estimaciones no son fáciles de realizar en ausencia de datos específicos y herramientas de cálculo que ayuden a factorizar la frecuencia de estos incidentes de seguridad por las violaciones de datos y el mantenimiento de registros de los costos directos e indirectos sufridos por la organización como resultado de estos incidentes. Sin embargo, los datos estadísticos, las estimaciones de los costos, así como también los cálculos de riesgos cuantitativos de incidentes de filtración de datos, nos pueden ayudar con las estimaciones de los mismos. [5].

E. Estrategias de Gestión de Riesgos.

Al identificar los riesgos de seguridad y asignar una valoración para considerarlos como alto, medio o bajo se debe establecer los siguientes pasos, en este momento el CISO determina como actuar con cada riesgo.

Para la toma de decisiones con los riesgos identificados se tienen unos procesos de gestión de riesgos en la organización que sirven de guía y contienen la estrategia de mitigación, cada proceso depende del tipo de empresa. Acorde con la estrategia de mitigación empresarial se realiza la gestión del riesgo, también se evalúa el impacto de los riesgos y la probabilidad de ocurrencia, es decir dependiendo de estos factores la organización decide qué acciones tomar, si deben mitigar, reducir, aceptar, evitar o transferir el riesgo, como se visualiza en el siguiente diagrama:

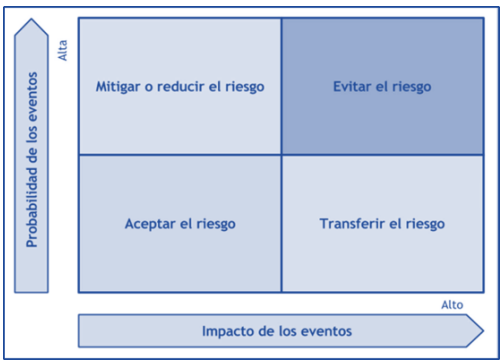

Fig. 2 Mitigación de riesgos. [6].

Los riesgos que están calificados como altos y que no se puedan evitar debido a las decisiones de negocio que se requieren para mitigarlos, y no puedan ser transferidos a terceros por medio de acuerdos contractuales y seguros, una posible estrategia de riesgos de la organización podría ser mitigar todos los riesgos que son medios y altos, y aceptar (por ejemplo, no hacer nada) sólo cuyos riesgos residuales

sean bajos (por ejemplo, el riesgo remanente después de que se apliquen medidas o controles que son aplicados o considerados). Las estrategias de mitigación de riesgos también pueden factorizar los riesgos del negocio mediante el análisis de riesgos cualitativo que factoriza riesgos, como la probabilidad y los impactos económicos. [7].

De acuerdo a la decisión tomada por la organización los CISOs tendrán un proceso para cada tipo de acción, en caso de aceptar un riesgo se debe documentar unos controles que califiquen el riesgo con un nivel bajo y debe estar aprobado por la alta dirección y el CISO; en caso de elegir un riesgo para ser mitigado lo que debe hacerse es determinar las medidas de seguridad y/o acciones correctivas aceptables y optar por la más eficaz (revisando costo/beneficio, teniendo en cuenta el costo de cada uno de los incidentes potenciales); cuando se transfiere un riesgo es importante asesorarse con el área legal de tal manera que se pueda garantizar que las clausulas de responsabilidad de riesgos estarán documentadas legalmente y firmadas por la organización con la entidad legal del proveedor de servicios.

Dentro de la estrategia de riesgos los CISOs deben decidir sobre las medidas de seguridad que funcionaran mejor utilizando una serie de controles preventivos y de detección.

F. El análisis y el conocimiento de las nuevas amenazas.

Analizar casos de negocio para realizar gastos adicionales en medidas de seguridad de la aplicación no siempre es justificable sin datos sobre los riesgos obtenidos a partir del análisis del impacto de las amenazas emergentes y el aumento del nivel de riesgo que debe ser mitigado. El análisis de datos sobre amenazas permite tomar decisiones de gestión de riesgos con conocimiento de causa. En ausencia de estos datos, la gestión se queda con consideraciones subjetivas sobre las amenazas. [8].

Estas consideraciones subjetivas son, a menudo, decisiones basadas en el miedo, incertidumbre y duda (FUD - *Fear, Uncertainty and Doubt*). Actuar según FUD para mitigar los riesgos que plantean las amenazas emergentes es tardío y poco efectivo. Algunas acciones de ejemplo basadas en FUD incluyen, pero no se limitan a:

- El temor a las violaciones de datos.
- El temor a fallar en la auditoría y cumplimiento.
- La incertidumbre con respecto a las amenazas del negocio.
- Las dudas sobre la eficacia de las medidas de seguridad existentes a la luz de los recientes incidentes de seguridad.

Crear un caso de negocio adicional para la inversión en seguridad de aplicaciones basado en un análisis de amenazas objetivo en lugar de consideraciones subjetivas. [9].

G. Responder a las expectativas del negocio después de un incidente de seguridad.

La implementación de un proceso de respuesta a incidentes de seguridad es una actividad esencial para todos los CISOs. Tal proceso requiere la identificación de un punto de contacto para las cuestiones de seguridad, la adopción de un proceso de divulgación de problemas de seguridad y la creación de un equipo/s informal de respuesta a dichos incidentes. En el caso que ocurra un incidente de seguridad, los CISOs a menudo se encargan de llevar a cabo el análisis de la causa raíz de los incidentes, recopilar métricas por incidente y recomendar acciones correctivas. [10].

Una vez que las causas raíces del incidente han sido identificadas y se han tomado medidas correctivas para contener el impacto del incidente, la cuestión principal para los CISOs es, qué debe hacerse para prevenir la ocurrencia en el futuro de incidentes de seguridad similares. Si una aplicación ha sido el objetivo de ataque y se han perdido o comprometido datos sensibles, la cuestión principal es determinar si aplicaciones y softwares similares, también pueden correr riesgo de ataques e incidentes parecidos en el futuro. La pregunta principal para el CISO es qué medidas y actividades de seguridad en aplicaciones deben ser seleccionadas para gastar en mitigar los riesgos de filtración de datos sensibles debido a *malware* y ataques de terceros, a aplicaciones y software desarrollados y gestionados por la organización. [11].

Dentro de los principales objetivos en el análisis que deben realizar los CISOs se encuentra la adecuada realización del presupuesto en las medidas de seguridad que ayuden a mitigar los riesgos relacionados a incidentes de infiltración, lo que incluye el oportuno análisis de dichos riesgos, la identificación de los posibles impactos económicos, así como también determinar la probabilidad de ocurrencia e impacto que tendría en el negocio. Se debe determinar la relación costo/beneficio de la mitigación de riesgos para tomar la decisión adecuada sobre las mejores medidas de seguridad en las cuales se debe invertir.

H. Riesgos de incidentes causados por la filtración de datos.

En la determinación de los riesgos de seguridad existen factores críticos que deben tenerse en cuenta sobre todo los efectos negativos y la probabilidad de que ocurra algún incidente; para poder estimar el impacto de los costos en el caso de tener algún incidente es fundamental tener claros los costos que se ocasionar por el incidente, generalmente se tienen los siguientes impactos en las organizaciones:

- Pérdida de ingresos por denegación de servicios.
- Incapacidad para prestar el servicio de atención a los usuarios.
- Pérdida de reputación.
- Pérdida de datos sensibles (tales como: identificación de usuarios, datos confidenciales de clientes, datos de autenticación, información de propiedad intelectual y también información comercial).
- Impacto sobre usuarios que sus datos se han expuesto.

Para lograr cuantificar los posibles impactos en el negocio luego de sufrir una filtración de datos se debe tener en cuenta, que se debe basar en los cálculos de la estimación de riesgos. Con este análisis cuantitativo se puede estimar el gasto que debe tenerse para las medidas de seguridad necesarias en una base anual por cada aplicación, donde también se debe calcular el impacto de forma anual.

Cuando se realiza un análisis de costo/beneficio, es importante utilizarlo para determinar el valor óptimo, comparando los cotos de los incidentes de seguridad contra los costos requeridos en las medidas de seguridad, para maximizar el beneficio y asimismo la seguridad de la aplicación.

Se entiende que un aumento invirtiendo en las medidas de seguridad implica un menor riesgo o un menor impacto para el negocio, es decir, los riesgos disminuyen cuando la seguridad aumenta; para que esto se tenga en una organización las inversiones deben ser dirigidas en medidas efectivas de mitigación de riesgos; la toma de decisiones acerca de qué medidas de seguridad y en que invertir es lo que puede determinar que sea o no una mitigación eficaz y esto es responsabilidad de los CISOs, puesto que deben realizar un análisis de riesgos donde se tengan las medidas más rentables (como procesos, herramientas o controles) y además seleccionar aquellas que reducen el riesgo, teniendo en cuenta el precio de implementación, despliegue y mantenimiento. Cabe destacar que no siempre un mayor gasto en medidas de seguridad, representa mayor mitigación de riesgos.

Para definir la solución óptima en medidas de seguridad, se debe notar que se minimiza el costo de los incidentes y el costo de medidas de seguridad maximizando el beneficio o seguridad.

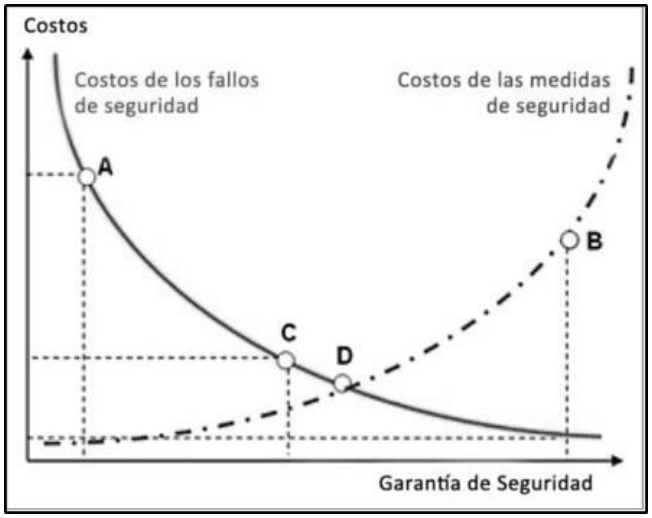

Fig. 3 Costo de los fallos vs los costos de las medidas de seguridad. [12].

III. CRITERIOS PARA GESTIONAR RIESGOS DE SEGURIDAD EN APLICACIONES

Los CISOs deben de priorizar las cuestiones de seguridad con el fin de identificar las áreas que necesitan atención primero. Con el Objetivo de tomar decisiones informadas acerca de cómo se deben de gestionar los riesgos de seguridad, los CISOs frecuentemente necesitan evaluar los costos de remediar las vulnerabilidades conocidas y de la aceptación de nuevas contramedidas, y considerar los beneficios, en cuanto a mitigación de riesgos, de llevar a cabo estas acciones. La relación costo/beneficio es crítica para decidir en cuáles medidas y controles de seguridad invertir para reducir el nivel de riesgo. Continuamente los CISOs requieren explicar a la alta gerencia los riesgos que son inherentes a las aplicaciones y manifestar los impactos potenciales para el negocio de la organización en cualquier caso de que se presente un ataque a las aplicaciones y/o una filtración de la información que es confidencial.

Los riesgos de seguridad crean riesgos para el negocio cuando siguientes características de riesgo se presentan:

- Amenaza viable.
- Vulnerabilidad que puede ser expuesta.
- Activo de valor.

Se proponen acciones de ejemplo para proveer orientación sobre la mitigación de riesgo de nuevas amenazas que pueden surgir por la implementación de nuevas tecnologías.

- Para las aplicaciones móviles.
  - Ejemplos de las preocupaciones son: dispositivos perdidos o robados, malware, exposición en la comunicación, autenticación débil.

○ Ejemplos de las acciones que debe de realizar los CISOs: deben de alcanzar los estándares de seguridad móvil, deben de realizar las auditorías de seguridad para evaluar las vulnerabilidades de las aplicaciones móviles, la seguridad del aprovisionamiento y los datos de aplicaciones en dispositivos personales.

- Web 2.0.
  - Ejemplos de las preocupaciones son: protección para los medios sociales, la gestión de los contenidos, la seguridad de las tecnologías y los servicios de los terceros.
  - ○ Ejemplos de las acciones que deben de realizar los CISOs: manejar API de seguridad, manejar CAPTCHAs, manejar tokens de seguridad únicos en los formularios y en los workflows de aprobación de las transacciones.
- Servicios de Cloud Computing.
  - Ejemplos de las preocupaciones son: las implementaciones de multi-cliente, la seguridad para las implementaciones en la nube, los riesgos de los terceros, las brechas de los datos, la denegación de servicios que es provocada por personal interno malicioso.
  - ○ Ejemplos de las acciones que deben de realizar los CISOs: las evaluaciones de la seguridad de cloud Computing, las evaluaciones de la conformidad con las auditorías por parte de los proveedores, diligencia debida, el cifrado en el tránsito y el almacenamiento, y el monitoreo.

Los agentes de amenaza hoy en día buscan el provecho financiero atacando a las aplicaciones para comprometer la información que es sensible para los usuarios y de la información que hace parte del activo de la compañía, y de esta forma poder obtener una ventaja financiera, o cometer fraude, o lograr una ventaja competitiva (por ejemplo, lo que se logra a través del ciberespionaje). Para poder mitigar los riesgos planteados por estos agentes de riesgo, es necesario determinar la exposición al riesgo y de esta forma calcular la probabilidad y el impacto de esas amenazas, así como también identificar el tipo de las vulnerabilidades de las aplicaciones ya que estas pueden ser explotadas por estos agentes de amenaza. El aprovechamiento de algunas de estas vulnerabilidades de las aplicaciones podría impactar en la organización de forma que puede ser severa y negativa, colocando en peligro el negocio.

De acuerdo al Top Ten de Riesgos de Aplicaciones Web de OWASP, la caracterización del riesgo de la vulnerabilidad es la siguiente: "Los atacantes pueden potencialmente utilizar muchos caminos diferentes a través de tu aplicación para dañar tu negocio u organización. Cada uno de estos caminos representa un riesgo que puede, o no, ser lo suficientemente serio como para justificar su debida atención". [13].

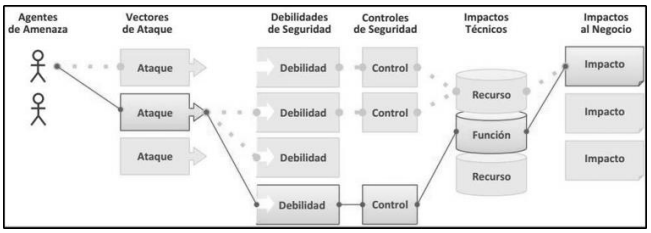

Fig. 4 Los atacantes tienen diferentes caminos para atacar una aplicación. [14].

A. Priorizar el riesgo Global.

Se debe de realizar la priorizar los riesgos a partir de las vulnerabilidades conocidas con un enfoque reactivo, pero sea tangible para una gestión clara del riesgo del negocio. Estas características de los riesgos son útiles para los CISOs en la determinación de los riesgos al negocio, en donde un agente de amenaza aprovecha las vulnerabilidades o las debilidades que existen en los controles para comprometer un activo y de esta forma causar un impacto negativo al negocio.

El riesgo de negocio por cuestiones de seguridad está inducido por:

- Probabilidad de Amenaza (PA): la probabilidad de que ocurra la amenaza.
- Exposición de la Vulnerabilidad (EV): la probabilidad de exposición de la vulnerabilidad a la amenaza.
- Valor del Activo (VA): el impacto sobre el negocio.

Fig. 5 Cálculo del riesgo. [15].

B. Comprender los factores de Riesgo: Amenazas y Contramedidas.

Para realizar una clasificación de riesgos los CISOs deben de adoptar una técnica de modelado de amenazas. Según el Modelado de Amenazas a las Aplicaciones de OWASP "el modelado de amenazas es una estrategia para analizar la seguridad de una aplicación. Se trata de una estrategia estructurada que permite identificar, cuantificar y encarar los riesgos de seguridad asociados con una aplicación" [16].

C. Agentes de amenaza.

Un agente de amenaza "se utiliza para señalar un individuo o grupo que puede manifestar una amenaza. Es fundamental identificar quien querría aprovecharse de los activos de una compañía, y como podrían usarlos contra la compañía". [17]. Un agente de amenaza puede ser definido como la función de sus capacidades, intenciones y actividades previas:

Agentes de amenaza = Capacidades + intenciones + Actividades previas

Un agente de amenaza puede ser descrito como la intersección entre los motivos del agente, los tipos específicos de ataques utilizados y las vulnerabilidades que son explotadas.

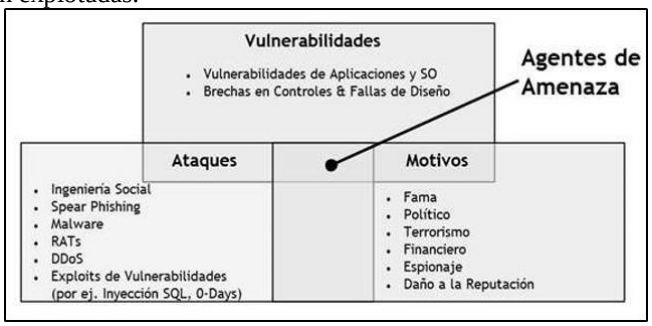

Fig. 6 Agentes de Amenazas. [18]

D. Mitigando los riesgos inherentes a las nuevas tecnologías de aplicación.

Como las tecnologías evolucionan, para el CISO es importante entender los riesgos de seguridad introducidos al adoptar las nuevas tecnologías, y que estas mismas pueden representar nuevas oportunidades de ataques tanto a las aplicaciones como a los datos. El aumento del riesgo para las aplicaciones principalmente por la adopción de nuevas tecnologías conlleva a un incremento de la superficie de exposición/ataque tales como el caso de la extensión de las aplicaciones para dispositivos móviles, la introducción de un nuevo tipo de vulnerabilidad de cliente y servidor, como es el caso de la Web 2.0 y el incremento del riesgo de pérdida de datos e integridad de transacciones debidos al uso de Cloud Computing. A fin de apuntar a la mitigación de los riesgos debidos a la adopción de dichas tecnologías, el CISO necesita tener una imagen clara de los riesgos que son introducidos y decidir invertir en un nuevo tipo de evaluación de seguridad de aplicaciones, herramientas y medidas de seguridad para mitigar los riesgos.

E. Gestión del riesgo en aplicaciones móviles.

La seguridad de las aplicaciones móviles es una preocupación particular actual para la mayoría de las organizaciones: sobre todo debido al crecimiento exponencial de la adopción de teléfonos inteligentes y tabletas, tanto para uso personal como profesional. Desde la perspectiva de la seguridad en aplicaciones, el acceso a las aplicaciones empresariales desde dispositivos móviles aumenta la posibilidad que los agentes de amenaza ataquen a las aplicaciones y los datos que se pueden almacenar en los teléfonos móviles.

F. Gestión de riesgos de tecnologías de la Web 2.0.

Como sabemos las nuevas tecnologías introducen también nuevos riesgos y para estos se deben de poner en marcha nuevas medidas en la organización para mitigar estos riesgos. Una forma de prepararse al impacto de estas nuevas tecnologías es realizar una planificación con antelación de la adopción de medidas y procesos de seguridad para reducir los riesgos al conocer que tales tecnologías se convertirán en las tecnologías dominantes y que gradualmente serán adoptadas por las organizaciones. De acuerdo con algunos analistas como Gartner, la adopción de nuevas tecnologías por el mercado sigue un ciclo también conocido como "exageración" que se compone de cinco fases que son (1) "el disparador de la tecnología", (2) "el auge de expectativas excesivas", (3) "el valle de la desilusión", (4) "la caída de la cultura", y (5) "la meseta de la productividad". En el ciclo de la exageración que Gartner publicó en 2009 abarca las tecnologías emergentes, la Web 2.0 mostró una adopción generalizada de dos años o menos. [19].

G. Medidas de seguridad para mitigar riesgos.

Para realizar el análisis de las vulnerabilidades de las aplicaciones web 2.0 lo más es crítico es determinar cuáles son las causas de raíz. Ya que través de la identificación de las causas de raíz de vulnerabilidades, se las pueden erradicar. Un ejemplo, si las vulnerabilidades se originan a partir de la falta de requisitos de seguridad para la web 2.0 que los desarrolladores de software necesita para seguir, deben ser documentados. En el caso que los problemas sean causados por errores en el diseño, estas necesidades deben evitarse asegurándose que el diseño de las aplicaciones web 2.0 es revisado por un arquitecto de seguridad que cuente con experiencia en tecnologías web 2.0. Para las vulnerabilidades de la web 2.0 introducidas por los desarrolladores de software, como errores de programación o debido a la integración con software y bibliotecas de terceros que están expuestas a vulnerabilidades de la web 2.0, es importante que los mismos estén entrenados en programación defensiva de

aplicaciones 2.0 y que los auditores de seguridad sepan cómo identificar y probar las vulnerabilidades de la web 2.0. [20].

H. Gestionar los riesgos de los servicios de computación en la nube.

El concepto de computación en la nube no es un concepto nuevo. Muchas organizaciones utilizan centros de datos de terceras partes para tener sus centros de datos, un concepto que en computación en la nube es considerado una implementación de una Infraestructura como Servicio *(IaaS - Infrastructure as a Service)*. El término computación en la nube abarca infraestructuras externas tales como el caso de Infraestructuras como Servicios, plataformas tercerizadas como es el caso de Plataformas como Servicios *(PaaS - Platform As a Service)* y a través de software externo, un término conocido como Software como Servicio *(SaaS - Software As a Service)*. [21].

Los CISOs de hoy en día enfrentan el desafío de evaluar y garantizar la seguridad de las implementaciones de computación en la nube dentro de su red (por ejemplo: en las instalaciones o en nubes privadas) o fuera de la organización (ejemplo: instalaciones propias fuera de la organización o en una nube pública). La información y la seguridad de aplicaciones es una preocupación primordial para las organizaciones que tercerizan sus componentes de infraestructura y plataformas o software y datos a proveedores de nube. Los CISOs necesitan considerar los riesgos potenciales y evaluarlos antes de decidir externalizar sus servicios a terceros. Los CISOs deberían considerar por ejemplo, el riesgo potencial que los datos de la compañía estén alojados en un proveedor de computación en la nube que puede ser comprometido debido a la ocurrencia de un incidente de seguridad. También deberían considerar por ejemplo, el riesgo que una organización podría enfrentar cuando el servicio de datos que es proporcionado a sus clientes sea tercerizado a un software de terceros y no esté disponible debido a que el proveedor de dicho servicio en la nube haya sido el objetivo de un ataque de denegación de servicios.

Por lo tanto, es importante que los CISOs consideren todo el espectro de riesgos de seguridad de la información antes que la organización decida migrar sus servicios o sus datos a un proveedor de computación en la nube. A alto nivel, estos riesgos pueden ser evaluados mediante una evaluación de seguridad de la información de terceros sobre el proveedor del servicio. Este tipo de evaluaciones buscan afirmar la postura de seguridad del proveedor contra las políticas y normas de seguridad de la información de la compañía, así como también con la auditoría de normas relevantes de TI y de seguridad de la información tales como SAS70, SOC, FISMA, PCI-DSS, ISO, FIPS-140, ISO/IEC 27001-2005, etc.; y otros como esos que son relevantes para las operaciones de negocio regulados por la organización tales como HIPPA, FFIEC, MPAA, etc.

El caso de la evaluación de computación en la nube, riesgos de seguridad y auditoría de cumplimiento son actualmente algunos de los dominios que necesariamente deben ser evaluados junto a otros tales como la arquitectura de la nube, gobierno, implicaciones legales y leyes, privacidad, continuidad de negocio y recuperación ante desastres, respuesta a incidentes, seguridad en aplicaciones, cifrado y gestión de claves e identidades, gestión de accesos y derechos, virtualización y seguridad como servicio.

Top 9 de amenazas en Computación en la Nube

1. Filtración de datos.
2. Perdida de datos.
3. Secuestro de cuentas.
4. Países inseguros.
5. Denegación de servicio.
6. Personal interno malicioso.
7. Abuso de servicios en la nube.
8. Debida diligencia insuficiente.
9. Problemas con tecnologías compartidas.

Una evaluación de seguridad ad-hoc de computación en la nube debería, como mínimo, incluir un proceso estándar que pueda ser seguido incluyendo un conjunto de herramientas, cuestionarios “sí/no” pueden ser usados para capturar y confirmar la seguridad, de cumplimento y gestión de riesgos de la seguridad del proveedor de computación en la nube antes de tomar una decisión de negocio si tercerizar servicios tales como infraestructuras, redes, plataformas y datos de software a proveedores de servicios de terceros. El objetivo principal de esta evaluación es identificar brechas de control y áreas potenciales de riesgos para la organización. [22].

IV. CONCLUSIONES

Es muy común encontrar aplicaciones con falencias de seguridad, con el crecimiento en la demanda del desarrollo de software y aplicaciones que faciliten los procesos en las organizaciones se abren cada vez más las puertas de las vulnerabilidades para ser atacadas. Esta es la razón por la cual se debe considerar la seguridad de las aplicaciones como un requerimiento más del sistema y del ciclo de vida del desarrollo de software, por eso es importante para los CISOs realizar una buena gestión del riesgo dentro de las compañías.

El proyecto OWASP brinda guías a los CISOs sobre la seguridad en sus aplicaciones y estas están abiertas al público y son alimentadas con las experiencias de un equipo a nivel mundial.

Es necesario crear software seguro, por esto es indispensable avanzar cada día para conocer, evaluar, encontrar y definir los riesgos de las aplicaciones y como mitigarlos, creando una comunidad que sea consciente de la inversión necesaria en la seguridad del software y compartiendo los resultados con el resto del mundo.

REFERENCIAS

[1] https://protejete.files.wordpress.com/2009/07/gestion-de-riesgo-en-la-seguridad-informatica.pdf.

[2] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 3.

[3] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 21.

[4] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 22.

[5] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 22-23.

[6] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 23.

[7] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 24.

[8] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 24.

[9] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 24.

[10] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 26.

[11] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 26.

[12] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 32.

[13] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 39.

[14] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 39.

[15] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 40.

[16] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 42.

[17] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 42.

[18] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 42.

[19] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 59.

[20] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 62.

[21] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 64.

[22] M. Morana, T. Gondrom, E. Keary, A. Lewis, S. Tan and C. Watso, Guía de Seguridad en Aplicaciones para CISOs, Versión 1. Traducida al español, OWASp, 2015, pp. 65 - 66.