CULTURA ORGANIZACIONAL Y CAPACITACIÓN, DOS NECESIDADES DE LAS EMPRESAS PARA EL DESARROLLO DE SOFTWARE SEGURO

Carlos Alberto Maldonado Naizir
Universidad Piloto de Colombia
Bogotá D.C, Colombia
camnaizir@hotmail.com

***Resumen*—**Recientemente ha tomado fuerza un término que no era usado en años anteriores, este es el Desarrollo de Software Seguro. Con el paso de los años, las compañías venían desarrollando software basados en funcionalidad o en prisas asociadas a plazos de tiempo, pero hoy en día este paradigma ha logrado cambiarse, y el desarrollo de aplicaciones está teniendo en cuenta técnicas y estándares de seguridad. Quizás esta toma de conciencia ha sido causada por los impactos generados en ataques previos, regulaciones o requerimientos del negocio, pero independiente de la fuente asociada a esta tendencia, hay que destacar que las empresas están tratando de implementar políticas de prevención y seguridad para así poder tener un sistema lo más seguro posible y hacerle más difícil la tarea a un atacante. Este artículo constituye una propuesta de diferentes pasos, técnicas o métodos a los que una compañía puede ajustarse para sacarle provecho y que seguramente le ayudaran a implementar una estrategia de desarrollo de software seguro, pero entre estos especialmente se resaltan dos en el artículo: Cultura Organizacional y Capacitación. Ambas estrategias hacen más fácil la ejecución de cualquier marco de trabajo, política o método que persiga un objetivo de seguridad claro y contribuye a obtener como resultado, que todas los esfuerzos, proyectos y actividades dentro de una empresa estén orientados hacia un misma dirección, es decir, que todos apunten a lograr la implementación de una alternativa de desarrollo de software seguro.

***Abstract*—**Recently it has been taking force a concept that wasn't used in the precedent years, this is the Secure Software Development. In the past, the companies developed software focused on functionality and the rush of deadlines criteria, but nowadays, this paradigm has changed, and the software development is taking into account security standards and techniques. Perhaps this awareness has been caused by the impact derived from previous attacks, by regulation or business requirements, but despite of the source of this trend, the bright side is that the companies are trying to implement security and prevention strategies in order to accomplish a secure system and making harder the challenge to a hacker. This article is a proposal of different methods, steps or techniques that a company could apply to take advantage of and surely help to execute a secure software development strategy, but specially, there are two main topics that the article is based about: Enterprise Culture and Training. Both strategies make easier an implementation of any framework, policy or any other method that is going to pursuit a specific security goal, and will have as a result that all the efforts, projects and activities in the company are moving towards the same direction, in this case, everyone are aiming to achieve an implementation of a secure software development strategy.

***Palabras Claves*—**Vulnerabilidades, OWASP, OWASP Top Ten Project, Secure-SDLC, ISO27001:2013

I. INTRODUCCIÓN

Hoy en día hay un concepto que está tomando fuerza y que hace pocos años no estaba en el radar de las necesidades dentro de una compañía; este es el desarrollo de software seguro. Por cultura, falta de conciencia y de capacitación, el desarrollo y la implementación de software en las organizaciones, tanto para las que tienen en esta actividad su core de negocio como aquellas que simplemente son usuarios, estuvo por mucho tiempo enfocado a entregables limitados a temas de calidad en cuanto a funcionalidad, pero en ningún momento se tenía en cuenta dentro la manera en que se podía llegar a desarrollar un software, técnicas o metodologías que ayudaran a minimizar lo mayormente posible la exposición y debilidades que el mismo presentaría ante un ataque, por lo que rara vez se tenía conocimiento por parte de los desarrolladores que se podían introducir al software vulnerabilidades a causa de las malas prácticas aplicadas en la construcción del código fuente.

La evolución misma de las amenazas, de los ataques informáticos y el impacto de estos, han generado una conciencia en las empresas sobre la necesidad de desplegar software sin vulnerabilidades potenciales que puedan ser parte de vectores de ataque hacia la compañía misma. Junto con el despertar de las organizaciones sobre este tema, también han surgido grupos de trabajo enfocados a promover y homologar de alguna manera el trabajo que se debe desempeñar por cada uno de los desarrolladores en aras de poder entregar software con especificaciones de seguridad que dificulten la tarea de los atacantes informáticos. Dentro de estos grupos de trabajo se destaca OWASP, que consiste en un proyecto de código abierto que está enfocado a investigar las causas que hacen a un software inseguro. Así mismo también se puede encontrar dentro de normas internacionales, ampliamente aceptadas y aplicadas para la gestión del riesgo, referencias asociadas al desarrollo de software seguro, como por ejemplo la ISO27001 la cual contempla dentro de sus controles, medidas para asegurar el desarrollo de aplicaciones en todo su ciclo de vida.

Lo anterior abre las puertas a una mayor inclusión de modelos de ciclos de vida de desarrollo de software seguro, a no dejar de lado la seguridad para solo tener en cuenta la funcionalidad en las aplicaciones y a compromisos sólidos de las empresas para la incorporación de estrategias de seguridad de una manera proactiva, incentivándose así la generación de conciencia en las organizaciones de no solo reaccionar ante eventos de seguridad perjudiciales o de gran impacto para las mismas, sino que la prevención de incidentes de seguridad también es útil y que una manera proactiva de alcanzar este objetivo es comenzar a remediar brechas de seguridad desde los inicios del ciclo de vida del software.

II. DEFINICIONES ASOCIADOS A DESARROLLO DE SOFTWARE SEGURO

Antes de poder contextualizar y reseñar conceptos o estrategias asociadas al desarrollo de software seguro y a las vulnerabilidades de aplicaciones, se hace necesario entender de qué se tratan estos términos y las definiciones que están relacionadas al mismo. En primer lugar es necesario conocer el concepto base de toda esta temática; las vulnerabilidades. Se conoce como vulnerabilidad a una brecha o debilidad en una aplicación, que puede ser un defecto de diseño o error de implementación, que permite a un atacante generar daño o perjuicios sobre las partes involucradas con dicha aplicación [1]. En el caso del software se pueden identificar muchos tipos de vulnerabilidades, siendo algunas clasificaciones de estas las que se mencionan a continuación: de autenticación, de autorización, asociada a criptografía, manejo de errores, validación de entradas, manejo de sesiones, etc. Estas se distinguen unas de otras por su impacto, método de explotación, origen, entre otros ítems, dando como resultado una amplia lista, razón por la cual se torna más complejo cada día el análisis, seguimiento y remediación de las mismas, convirtiéndose también este en el motivo por el que se ha impulsado el surgimientos de grupos de trabajo que se encargan de facilitar y apoyar el mejoramiento de la seguridad en las aplicaciones. Un ejemplo de esto es el caso de OWASP (Open Web Application Security Project), que consiste en una organización conformada por una comunidad abierta dedicada a impulsar a las compañías a concebir, desarrollar, adquirir, operar y mantener aplicaciones que puedan ser confiables [2]. Dentro de las referencias más populares suministrada por este grupo de trabajo está el OWASP Top Ten Project, que corresponde a un importante documento generado por expertos de seguridad a nivel mundial donde se suministra una lista de las contempladas como vulnerabilidades más importantes a nivel de seguridad en las aplicaciones Web y que es considerado como un punto inicio dentro de la adopción de procedimientos y cultura de desarrollo de software seguro en las organizaciones [3].

Aunque la anterior terminología y referencias no surgieron precisamente en los últimos años, por mucho tiempo se tuvo la concepción errada que la seguridad solo era parte de las fases de pruebas, o bien que era responsabilidad de otras capas del servicio y de la infraestructura misma que los soportaba. Sin embargo, en los últimos años ha cambiado este paradigma y se ha tomado conciencia en el sentido que muchas de las vulnerabilidades en las aplicaciones pueden ser mitigadas desde las etapas de desarrollo aplicando metodologías y procedimientos que avalen resultados exitosos en ese sentido. Es por esto que ha cobrado cada vez más importancia un término asociado a esta temática conocido como Ciclo de Vida de Software Seguro (S-SDLC, siglas correspondientes al término en inglés Secure Software Development Life Cycle).

Por sí solo el concepto SDLC (Software Development Life Cycle) es un marco de trabajo que define los procesos usados por las organizaciones desde el primer instante del proyecto hasta su entrega [4]. En base a este marco se han propuesto diferentes modelos, cada uno adaptado a las distintas necesidades en torno al desarrollo de las aplicaciones y a las compañías, pero en todo caso no era costumbre incluir validaciones a nivel de seguridad en estos ciclos, conllevando a muchas brechas de seguridad descubiertas una vez desplegada la aplicación en ambientes productivos, o bien explotadas por distintos agentes de amenaza, pero no detectadas en etapas tempranas. Es así como tomó fuerza el concepto de S-SDLC, que consiste en incluir actividades a lo largo del Ciclo de Vida del desarrollo del Software que ayuden a descubrir y reducir las vulnerabilidades del mismo, siendo algunas de estas las que se relacionan a continuación y que se pueden observar en la Figura 1: pruebas de penetración, revisión de código, análisis de arquitectura, cumplimiento de requerimientos de seguridad en el código fuente, etc [5]. El marco de trabajo S-SDLC de esta manera se ha convertido en un ciclo que ha ganado aceptación con el paso de tiempo y que aporta en la mejora continua de los procesos de desarrollo de software en torno a la seguridad, siendo una referencia para la introducción de diferentes modelos que se basan en este, donde podemos encontrar por ejemplo: MS Security Development LifeCycle (MS SDL de Microsoft), NIST 800-64, OWAP CLASP (Comprehensive, Lightweight Application Security Process), Cigital's Security Touchpoints, etc [5].

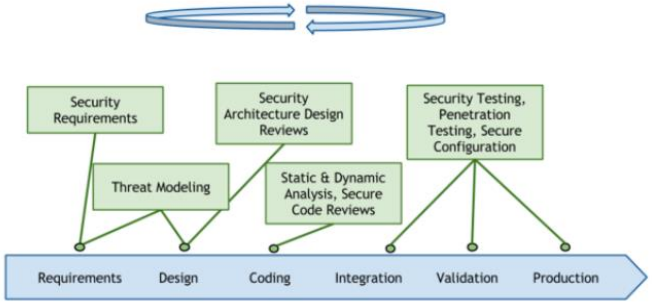

Fig. 1 Seguridad en el proceso SDLC, Fuente: OWASP

Así mismo como han surgido modelos de desarrollo de software, grupos de trabajo asociados, etc, también se ha incluido la temática en marcos y estándares de gestión de riesgo en seguridad de la información que van más allá de inducir la utilización de un esquema de desarrollo u otro y se centran en el hecho de tener en cuenta la construcción de

aplicaciones dentro de la implementación de un sistema de gestión de riesgo o en la consecución de una madurez a nivel de seguridad informática dentro de las compañías. Un ejemplo de esto es el caso de la ISO27001:2013 la cual incluye todo un objetivo de control correspondiente a la seguridad en los procesos de desarrollo y soporte (A.14.2) [6]. Dentro de dicho objetivo se pueden destacar diferentes controles tales como política de desarrollo seguro, procedimientos de control de cambios en sistemas, revisión técnica de aplicaciones después de cambios, principios de organización de sistemas seguros, ambiente de desarrollo seguro, pruebas de seguridad de sistemas, etc. Estos controles, como es evidente en el nombre de los mismos, buscan la inclusión de políticas y procedimientos claros en torno a la seguridad de los sistemas a partir de las etapas de desarrollo de software con el fin de buscar minimizar impactos adversos en las operaciones y servicios de la organización. Como se puede notar, existen diversas metodologías, técnicas y marcos de referencias aplicables dentro de una compañía en torno al aseguramiento del software que se desarrolla, incluso adaptables o enfocadas a necesidades particulares de cada entorno dentro de su sistema de gestión del riesgo, que tienen a la final todos un objetivo común de buscar mitigar o eliminar las vulnerabilidades aso ciadas a las aplicaciones desde las primeras fases de desarrollo de las mismas.

III. CONTEXTO SOBRE LAS VULNERABILIDADES DE SOFTWARE

Son diversos estudios y encuestas que se han realizado en los últimos años asociados a la seguridad de la información, que dan una idea de la actualidad y evolución que esta ha tenido tanto en las empresas como en la vida cotidiana de las personas en sus interacciones con la tecnología. Todos los resultados de dichos trabajos han permitido tener un instantánea en el momento de su realización sobre el estado de la seguridad de la información en sus diferentes ámbitos, dando a conocer tanto avances como retrocesos en la materia, así como también permite dar una idea de las prioridades, focos de trabajo y necesidad asociadas en dicha materia para cada uno de los distintos sectores de la sociedad, ya que con la dinámica que ofrece la tecnología hoy en día, estos varían constantemente con el paso del tiempo.

En el informe realizado por HP Security Research, por ejemplo, se denota la alarmante cifra de vulnerabilidades encontradas en el software evaluado [7]. En dicho estudio se realizó un enfoque sobre las aplicaciones móviles donde se evidenció que al menos el 46% de las revisadas empleaban encriptación de manera incorrecta, por lo que la información sensible estaba cifrada mediante algoritmos débiles cuyas salidas son fácilmente obtenibles. Así mismo en esta investigación se encontró que el 80% de las aplicaciones evaluadas contenían vulnerabilidades fuera de su código fuente, es decir, que no solo las brechas de seguridad están atadas a desarrollos incorrectos realizados a las empresas, sino también a librerías y fuentes externas que muchas veces se utilizan por los mismos desarrolladores de manera recurrente para sus aplicaciones, siendo en definitiva una debilidad compartida entre estas. En este estudio además se hace referencia a que en el año de realización del mismo se habían disminuido en un 6% el total de vulnerabilidades divulgadas, al igual que dentro de ese grupo, las categorizadas como graves también bajó para entonces en un 9%. Más que ser aparentemente satisfactoria esta estadística, presenta un punto de preocupación muy importante si se tiene en cuenta que la cantidad de ataques, estudios sobre las aplicaciones y malware que se desarrolla, crece día a día de manera exponencial, por lo que los valores arrojados en el estudio no parecerían ser fieles a la realidad y más bien demuestran que las organizaciones en general cada día se cuidan más de compartir o publicar información de las vulnerabilidades, haciendo más débiles a las empresas que desconocen las brechas que pueden llegar a tener en sus sistemas y que por esta razón terminan teniendo una desventaja significativa respecto a los atacantes los cuales si trabajan usualmente en un medio colaborativo. Una muestra de esto es un estudio realizado por McAfee Labs en el 2014 en base a investigaciones también desarrolladas por la NIST donde se estima un aumento respecto al número de vulnerabilidades y se prueba que también esta tendencia se venía dando desde años anteriores [8].

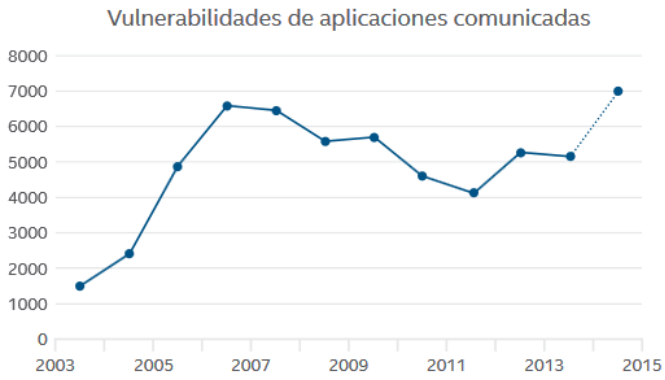

Fig. 2 National Vulnerability Database, Fuente: National Institute of Standard and Technology

En este mismo informe realizado por McAfee Labs se concluye que el número de vulnerabilidades nuevas irá incrementando con el paso del tiempo y así mismo en un porcentaje similar aumentará el volumen del malware que las aprovechará. Esta es una tendencia que se ha mantenido y cuya proyección apunta a que seguirá bajo esa línea si tomamos como base encuestas realizadas por prestigiosas firmas como PricewaterhouseCooper a través del The Global State of Information Security Survey 2016, en la que se evidencia un aumento reportado por las compañías en un 38% del total de incidentes de seguridad detectados respecto al año anterior [9]. Ahora bien, aunque no todos estos incidentes de seguridad son ocasionados por deficiencias en el código, si se puede deducir que hay un porcentaje considerable que es atribuible a este tipo de causas.

Referenciando investigaciones que se han realizado a lo largo de los últimos años podemos encontrar algunas en

particular que hacen zoom sobre problemática de desarrollo de software inseguro. Uno de estas es una encuesta sobre Riesgos de Seguridad TI Corporativa dirigida por B2B International en colaboración con Karpesky Lab donde se evidenció para el 2013 que el 39% de los incidentes de seguridad presentados en las organizaciones estuvieron asociados a deficiencias en las aplicaciones [10]. Para el año 2014, este mismo estudio contempla a las vulnerabilidades como una de las causas de con mayor relevancia e impacto para los fraudes financieros en línea tanto en las pequeñas, medianas y grandes empresas. Si se llegara a pensar que esto solo aplica a los desarrollos inhouse o de uso de un cliente en particular, sería necesario ampliar esta visión. En revisiones realizadas sobre la evolución de la seguridad desde la perspectiva del software se han encontrado interesantes hallazgos sobre aplicaciones populares de diferentes casas matrices que suponen vienen llevando a cabo la implementación de altos estándares en el desarrollo de las herramientas que sacan al público. Dentro de esta investigación se evidencia por ejemplo que las vulnerabilidades descubiertas sobre los navegadores web más populares han aumentado en un 44% en el 2015 respecto al año inmediatamente anterior y así mismo sucede también en los lectores de PDF más populares que pasaron de 45 vulnerabilidades descubiertas en el 2014 a 147 en el 2015 [11]. Dado lo anterior, si lo evidenciado para los grandes desarrolladores de software es preocupante no es difícil dilucidar qué se puede esperar para las aplicaciones que son implementadas en las diferentes compañías para uso interno o con el fin de ofrecer servicios a los clientes, y que no siguen pautas para la construcción de aplicaciones seguras.

IV. ALTERNATIVAS PARA UN DESARROLLO DE SOFTWARE SEGURO

Son muchas los métodos o sugerencias que pueden surgir para poder llegar al objetivo de desarrollar software seguro en una compañía. A continuación se enunciaran como guía algunos de estas alternativas que se pueden implementar, sin que por ello deban limitarse las organizaciones solamente a las opciones que se mostrarán a continuación:

A. Implementar Framework de Seguridad

Más allá de sugerir la implementación de un marco de trabajo, u otro, o incluso de llegar a combinar aspectos destacados de cada uno estos, lo realmente relevante en este punto es la importancia de contemplar la adopción de una metodología de análisis y gestión del riego dentro de las empresas, que incluya un sistema completo de gestión de seguridad de la información donde se implementen todos los aspectos prioritarios del mismo, como por ejemplo, definición de políticas, manual de seguridad, gestión y respuesta a incidentes de seguridad, etc.

En este punto se puede identificar como crítico la adopción y adherencia por parte de la organización del marco de trabajo sobre el cual va a trabajar la seguridad de la información y que este se ajuste al alcance, visión, misión del negocio, necesidades o expectativas de la compañía. Existen muchos marcos de trabajos sobre los cuales pueden trabajar las empresas, tales como ITIL, COBIT, ISO27000, SANS Security Policy Project, modelos de SSDLC o incluso guías tan puntuales y específicas como OWASP. Desde el punto de vista del desarrollo de software seguro, se hace relevante que para cualquier framework de seguridad implementado se contemple el desarrollo de las aplicaciones en todo su ciclo de vida, desde la especificación de requerimientos del mismo, hasta su despliegue o instalación.

Hoy en día se puede observar que las organizaciones por las necesidades y presiones que impone los negocios y la tecnología misma, están adoptando framework de seguridad. Esto puede constatarse en la encuesta realizada en el 2016 llamada The Global State of Information Security, donde fue evidenciado que el 91% de las compañías encuestadas estaban implementando un marco de trabajo de seguridad basado en análisis de riesgos, destacándose entre los más utilizados la ISO27001 y el Framework de Ciberseguridad de la NIST [9].

B. Aplicar modelos de "defensa en profundidad" para un software más seguro.

Si bien es cierto que el término de Defensa en Profundidad está enfocado principalmente a implementar la seguridad en general desde distintas capas (Firewall, IPS, IDS, etc) de la infraestructura de una compañía, no deja de ser útil y adaptable el concepto a un software resultante más seguro. Este punto hace referencia a que independiente del marco de gestión de riesgos y de seguridad de la información que esté siendo aplicado en la compañía, debe abordarse el tema de mitigar las vulnerabilidades de software desde varios frentes, es decir, que no solo la aplicación de técnicas y guías para un desarrollo de software seguro (por ejemplo OWASP o SSDLC) es suficiente para salvaguardar al mismo ante los ataques o amenazas a las que se expone. Debe por esto, abordarse desde distintas capas o fases la manera de aplicar la seguridad a las aplicaciones.

Por ejemplo, una fase que se establecería como un punto de control sería la revisión de código en sus distintas variantes, sea análisis de código estático o dinámico, permitiendo así validar la efectividad de los métodos y técnicas utilizadas para la construcción de las aplicaciones respecto a la remediación o eliminación de las vulnerabilidades más comunes dentro de su código fuente. En esta fase se podría tener un filtro que permita identificar las brechas o falencias a nivel de desarrollo que se tengan en el software entregado, generando un insumo para controlar despliegues en producción, o bien para identificar y trabajar planes de acción sobre las deficiencias detectadas en el grupo de programadores que trabaja para la compañía de manera directa o a través de terceros.

Una tercera etapa dentro de este concepto de capas de seguridad para las aplicaciones son las herramientas, plataformas o agentes de seguridad (endpoints, antimalware, IDS o IPS en cualquiera de sus variantes, etc) que realicen el monitoreo y control sobre comportamiento del software una vez desplegado y en ejecución. Este punto permitirá hacer seguimiento al funcionamiento de la aplicación con el fin de poder evidenciar la utilidad de los controles implementados en

las anteriores fases además de poder tener una visión de la aplicación en tiempo real, dando la posibilidad de detectar y reaccionar ante ataques que se pudieran estar llevando a cabo. El elemento a utilizar para aplicar seguridad en esta capa dependerá del sitio, lenguaje o instalación que se haya hecho del software que requiere ser controlado, siendo entre otras alternativas, Web Application Firewalls (WAF) para entornos web, HIDS, HIPS o Aplication Protocol Based IDS – IPS para entornos cliente servidor, o por ejemplo para aplicaciones móviles en ambientes tanto corporativos como personales podrán ser utilizados endpoints que permitan manejar perfiles o controlar las aplicaciones y la información almacenada en los dispositivos. En resumen, el concepto de defensa en profundidad para el software, está orientado a aplicar conceptos y elementos de seguridad durante todo el ciclo de vida de las aplicaciones, permitiendo alcanzar niveles aceptables de riesgo para la compañía que lo utiliza o implementa.

C. Cultura organización y capacitación

Quizás el punto más importante y sobre el cual se requiere más esfuerzo en las compañías, tanto para las que tienen como core de negocio el desarrollo de software como las que son usuarias de los mismos, son dos necesidades muy apremiantes en la actualidad: una es capacitar al personal sobre la importancia, métodos, guías y normas para el desarrollo seguro de software, y la otra es la obligación de crear una cultura organizacional en torno a este tema. La importancia de trabajar estos dos puntos radica en que si no se llegan a fortalecer, probablemente no dará resultados la implementación de un framework o fases de seguridad para el software, o cualquier otra opción que se pretenda implementar. La razón de esto es que si no se cumple con dichos requisitos posiblemente la adopción de cualquier alternativa no tendrá la suficiente aceptación dentro de la organización, y por ende, carecerá de apoyo de cada uno de las áreas y jerarquías establecidas dentro de la misma, siendo estos requisitos fundamentales para el éxito de cualquier implementación que se llegue a hacer.

Respecto a la capacitación, es necesario que esta sea trabajada desde dos frentes: uno técnico y otro como generador de conciencia. La razón por la que se contemplan dos frentes es porque ambos se requieren para poder obtener los resultados esperados y son complemento uno del otro. La parte técnica se puede suplir con capacitación o cursos en donde se eduque sobre temas de seguridad informática, vulnerabilidades, metodologías o guías existentes sobre las cuales se orientará y apoyará el trabajo de los desarrolladores y personal de seguridad de la información, por lo cual la complejidad de este punto no dependerá de la creación de técnicas, métodos o buscar crear un estándar para lograr el objetivo dado que estos ya existen y son asequibles para quien tenga la intención de utilizarlo, sino que dicha dificultad podrá estar más sujeta a elegir un marco de trabajo sobre el cual se adapten los procesos asociados al software y este deberá ser escogido de acuerdo a las necesidades propias de la organización.

Como complemento de la capacitación técnica, está la labor de concienciación a distintas áreas sobre los riesgos, impactos y requerimientos asociados a la seguridad en el desarrollo de software. Esta tarea no solo va dirigida a equipos de desarrollo o personal de seguridad informática, sino que tiene alcance en todo el equipo de trabajo que puede llegar a estar involucrado dentro del ciclo de vida o uso del software, abarcando desde los altos directos que aprueban los proyectos y su presupuesto, hasta las mismas áreas usuarias de la aplicación que se pretende desplegar. Lo anterior es fundamental teniendo en cuenta que desde la perspectiva de muchas áreas en las empresas, especialmente las que no están relacionadas a temas de seguridad, ven a esta última como un obstáculo o un agente de retraso para sus proyectos y objetivos, siendo vista solamente como un agente reactivo y no proactivo, por lo que se hace importante lograr mostrar el impacto que se puede llegar a tener para la compañía, por ejemplo, si una vulnerabilidad pudiera llegar a ser explotada, y por ende, el valor de poder implementar de manera proactiva seguridad sobre las aplicaciones y servicios que se pretenden sacar a producción. Aunque las organizaciones han venido tomando en serio las iniciativas de concienciación y capacitación observándolo desde una perspectiva general de seguridad informática, todavía existe mucho terreno por avanzar en este campo, como por ejemplo fue evidenciado en uno de los hallazgos obtenidos de la encuesta The Global State of Information Security donde se detectó que el 53% de las compañías emplean programas de entrenamiento y concienciación sobre seguridad con sus empleados, siendo este un porcentaje importante si se tiene en cuenta el terreno ganado en este tema con el paso del tiempo, pero denota el camino que queda por recorrer al respecto [9].

En lo que concierne a la cultura organizacional, se requiere un cambio de mentalidad y orientación en la manera como se maneja la puesta en marcha de productos, software y servicios en las compañías, es decir, que debe considerarse la seguridad desde la concepción misma de los proyectos y no solo contemplando funcionalidad sobre el resultado de los mismos, además que también todos en la organización tengan la misma orientación y entendimiento cuando de seguridad se trata en el sentido que cada una de las áreas entienda las necesidades, retos y objetivos de seguridad que debe perseguir la empresa, adicional al rol y tareas que cada una de las partes desempeña dentro de este objetivo común. Este punto va atado a los programas de capacitación y concienciación expuestos anteriormente que permiten poder divulgar, replicar y aterrizar esta información con los diferentes grupos de trabajo, sin embargo, la ejecución de dichos programas no son la única fuente para generar una cultura organizacional sólida en torno a la seguridad informática, y en especial, orientada al desarrollo de software bajo estándares óptimos de seguridad. Además del entrenamiento para los funcionaros de la compañía, también es necesario construir y oficializar una política de seguridad que contemple todos estos aspectos, por lo que se requiere generar convicción, apoyo y compromiso desde la misma junta directiva. Desde los mismos directivos y dueños de las empresas es necesario aprobar, generar y hacer seguimiento a los lineamientos que en materia de seguridad deben aplicarse y sobre los cuales cada uno de los funcionarios tiene que regirse en su actuar. Muchas empresas a nivel mundial en la actualidad han entendido esta necesidad y muestra de ello lo expone el estudio The Global State of

Information Security mencionado anteriormente, donde quedó registrado que la participación de las juntas directivas sobre la estrategia de seguridad en las compañías ha llegado para el 2015 a un 45%, representando esto un aumento respecto al año inmediatamente anterior y que marca una tendencia en este aspecto la cual se puede observar de manera discriminada en la siguiente figura [9].

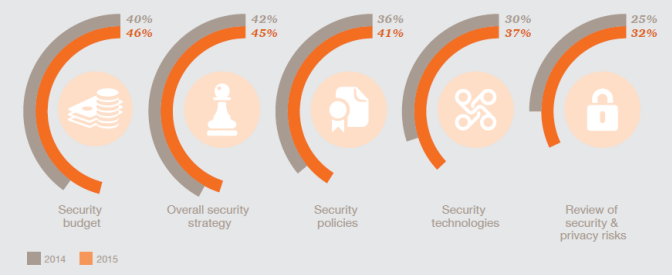

Fig. 3 Participación en seguridad informática de los directivos a nivel mundial
Fuente: Global State of Information Security Survey 2016

A pesar que los porcentajes de participación de las juntas directivas en los temas de seguridad siguen siendo bajos, es evidente a través de la figura anterior que la tendencia es el aumento en estas proporciones y una marcada necesidad en las empresas que se logre más apoyo de los altos directivos en temas de seguridad. Aunque es importante que la cultura organizacional a nivel de seguridad informática sea adoptada y aceptada en todas las áreas de la compañía, se hace indispensable esto se logre principalmente con los altos directivos. Lo anterior se basa en el hecho que desde los niveles jerárquicos más altos de una institución se realiza la aprobación de políticas, y para ser más específicos, son quienes llegan a oficializar y divulgar antes sus grupos de trabajo los lineamientos de seguridad de la organización. Así mismo, es desde los niveles directivos en los cuales se aprueban, impulsan y otorgan presupuesto para la ejecución de los diferentes proyectos, por lo que un entendimiento y compromiso con la estrategia de seguridad desde esos niveles pueden brindar oportunidades de apoyo financiero a la implementación de modelos o estrategias de seguridad, donde puede ir incluido entre otros, adopción de sistemas de gestión de riesgos de seguridad de la información, implementación de soluciones tecnológicas para el control, aseguramiento y monitoreo de las distintas plataformas, apoyo a programas de entrenamiento y concienciación a nivel de seguridad, etc, donde cada abarquen aspectos correspondientes al desarrollo seguro de software y la remediación de vulnerabilidades en las aplicaciones.

Sin embargo, hay un aspecto muy relevante dentro del apoyo que una junta directiva puede brindar a la estrategia de seguridad de la organización que sin ser menos importante, no es tan tangible como lo es aporte económico o aprobación de una política de seguridad. Este es el respeto y cumplimiento de las directrices de seguridad desde los altos niveles jerárquicos de la compañía. Lo anterior se menciona dado que no es un secreto que la presión y necesidad de sacar adelante proyectos, servicios, aplicaciones o iniciativas dentro de una organización se genera en mayores proporciones desde los directivos, siendo esto lo que marca en muchas ocasiones las pautas sobre las cuales se basa la ejecución de los procesos y que determina a la final si se sacrifica seguridad sobre los desarrollos para priorizar sobre funcionalidad o reducción en tiempos de entregas para los mismos. En definitiva, de nada sirve estructurar los mejores marcos de trabajo de seguridad, adquirir las mejores tecnologías o generar planes arduos de capacitación para las distintas áreas involucradas en los proyectos, si desde la gerencia no se muestra un compromiso y respeto sobre los lineamientos de seguridad, permitiendo que estos sean tenidos en cuenta en todos los procesos de la organización sin objeciones o excepciones, facilitando así que la seguridad pueda ser vista como un aliado del negocio y no como impedimento para el desenvolvimiento del mismo.

V. CONCLUSIONES

La gestión de riesgo en seguridad de la información, sea motivada por cumplimiento de normativas, acercamiento a una madurez de seguridad o como una estrategia corporativa, ha tenido una aceptación y acogida en las compañías convirtiéndose día a día en un concepto ampliamente implementado a nivel empresarial, no solo en el ámbito local sino mundial. Así mismo dentro de dicha gestión del riesgo, existe una estrategia que ha tomado fuerza y sobre la cual se ha adquirido mayor conciencia en los últimos años, este es el desarrollo de software seguro. Este término no era prioridad ni se tenía en cuenta en años anteriores, sin embargo han sido mucho los factores que lo han puesto en la mira de las empresas y actualmente se observa incluido en los marcos de trabajo de seguridad que tienen mayor aceptación. Tal es el caso de la norma ISO27001, la cual destina todo un objetivo de control para esta temática, recalcando así la importancia que esta tiene dentro de la gestión del riesgo de seguridad de la información.

Es evidente a través de estadísticas y estudios realizados por importantes compañías auditoras y de seguridad a nivel mundial, que el desarrollo de software seguro tiene una gran relevancia para las empresas, cualquiera que sea su área de negocio, ya que la explotación de vulnerabilidades en las aplicaciones se ha convertido en uno de los principales dolores de cabeza para las organizaciones y en uno de los eventos de seguridad asociados a mayor cantidad de incidentes y a los de más impacto sobre las mismas. La anterior es una realidad que golpea a la gran mayoría de compañías, incluso aquellas con software comercial o servicios de gran popularidad que se presumen deben tener modelos de seguridad con alta madurez. De allí la importancia de tomar conciencia que las vulnerabilidades hacen parte del resultado cuando se entrega una aplicación, sea para uso interno o como servicio de las compañías hacia sus clientes o partners, y que solo adoptando estándares y estrategias de seguridad en torno al desarrollo de software se podrá minimizar las debilidades del mismo, y por ende la probabilidad o impacto de un ataque.

Sin embargo, no es solo cuestión de adoptar una metodología o estándar para el manejo de seguridad de la información en la empresa, sino que también es necesario incluir modelos donde se contemplen distintas capas de

seguridad al software que en su momento se despliegue en ambientes productos, como por ejemplo, implementando técnicas de desarrollo de aplicaciones seguras con el fin de reducir las brechas de seguridad que puedan asociadas a las mismas en su código fuente, estableciendo análisis de software desde perspectivas no solo de calidad o funcionalidad, sino también de seguridad como seguimiento a la efectividad de los controles y métodos seguros de desarrollo utilizados sobre la aplicación, al igual que una vez desplegado el software en producción realizar análisis dinámicos de vulnerabilidades, instalar agentes o plataformas que brinden una protección y control de seguridad de la aplicación ya en funcionamiento (WAF, APIDS, etc).

Adicionalmente, y más importante aún, se requiere generar una capacitación y cambio de cultura organizacional profunda que oriente todos los esfuerzos dentro de la compañía en sus distintas áreas a obtener aplicaciones, productos y servicios seguros para usuarios tanto internos como externos. Esta capacitación no solo implica entrenamiento a equipos de desarrollo y seguridad sobre los métodos de desarrollo seguro o vulnerabilidades asociadas a las aplicaciones (sin ser esto menos prioritario), sino también establecer y ejecutar un plan de concienciación que involucre a todos las áreas impactadas en la compañía, en donde se pueda ver y adoptar a la seguridad dentro de la estrategias del negocio como un aliado que le brinda valor al mismo y que se deje de percibir como un bloqueante o entorpecedor de este. Para esto es necesario hacer visible para la organización, por ejemplo, la importancia de la seguridad, qué son las vulnerabilidades, el logro que representa minimizarlas y el impacto que pueden llegan a tener en la organización si en un momento dado pudieran llegar a explotarse. Lo anterior, con el fin de generar una mayor conciencia en los funcionarios de la empresa involucrando a toda la estructura jerárquica de la misma, incluyendo a los altos directivos, siendo esto último vital para la implementación de procesos como el desarrollo de software seguro, porque es un punto de partida para obtener apoyo a nivel gerencial de este tipo de proyectos tanto a nivel de presupuesto, capacitación o contratación de personal calificado, así como también represente un pilar para fomentar el respeto y la conciencia del valor que tendrá en la compañía el cumplimiento de dichos procesos, dado que la tendencia usualmente en las empresas, se centra en buscar funcionalidad, agilidad, eficiencia en términos de tiempo de desarrollo y pasos a producción, pero muchas veces sacrifica o hace a un lado requisitos de seguridad en el software no siendo estos en realidad menos importantes, pero evidenciando así que no hacen parte de la cultura y misión organizacional dado que no se les da la prioridad debida. Sobre este punto se ha notado avances en las empresas, que han venido adoptando políticas y estrategias de seguridad donde reconocen al desarrollo de software como un componente importante dentro de esta temática, sin embargo el camino por recorrer a nivel local, regional e incluso mundial aún es largo y requiere compromiso desde todos los niveles dentro de las organizaciones, así como también que tengan la conciencia que no solo serán suficientes implementación de tecnologías, o metodologías de seguridad, sino también requieren cambios culturales fuertes que las orienten a tener una visión y misión unificada en torno a este tema.

REFERENCIAS

[1] OWASP, About OWASP, Septiembre 2015 [En línea] Disponible: https://www.owasp.org/index.php/OWASP_Top_Ten_Project

[2] OWASP, Category: Vulnerability, Abril 2014 [En línea] Disponible: https://www.owasp.org/index.php/Category:Vulnerability

[3] OWASP, Cetegory: OWASP Top Ten Project, Abril 2014 [En línea] Disponible: https://www.owasp.org/index.php/Category:Vulnerability

[4] Pablo González, Ciclos de Vida del Software Seguro S-SLDC Parte, Enero 2016 [En línea] Disponible: http://www.flu-project.com/2014/05/ciclos-de-vida-del-software-seguros-s.html

[5] Ernest Mougoue, SSLDC 101: What is the Secure Software Development Life Cycle?,January 2016 [En línea] Disponible: https://www.cigital.com/blog/what-is-the-secure-software-development-lifecycle/

[6] ISO/IEC 27001:2013 Information Security Management

[7] HP Security Research, Informe de Ciber Riesgos, 2013 [En línea] Disponible: http://www.pcworld.com.mx/Articulos/31846.htm

[8] McAffe Labs, Informe sobre amenazas, Noviembre 2014 [En línea] Disponible: http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q3-2014.pdf

[9] Data Group Inc, Global State of Information Security Survey 2016 [En línea] Disponible: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[10] Karpesky Lab y B2B International, Global It Security Risks – Online Financial Fraud Prevention, 2014 [En línea] Disponible: https://press.kaspersky.com/files/2014/08/IT_Security_Risks_Survey_2014_Financial_Security_report.pdf

[11] Secunia Research,Vulnerability Review, 2016 [En linea] Disponible: http://learn.flexerasoftware.com/SVM-WP-Vulnerability-Review-2016