APLICACIÓN DE LA METODOLOGÍA SCRUM PARA IMPLEMENTAR EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN ORIENTADO A SERVICIOS TECNOLÓGICOS.

Adib Manssur – Patricia Chávez
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral, ESPOL
Campus Gustavo Galindo Km 30.5 Vía Perimetral
Apartado 09-01-5863, Guayaquil, Ecuador
amanssur@gmail.com – paxichav@espol.edu.ec

Resumen-La metodología SCRUM aplicado al EGSI es sin duda uno de los proyectos que podrá hacer dar el siguiente paso a la Seguridad de la Información en el Ecuador. El desarrollo de esta nueva forma de implementar la normativa, a la cual llamamos EGSI-SCRUM, es una forma ágil, colaborativa y eficaz de realizar la implementación de lo que nos dicta el Acuerdo 166 dada por SNAP. El EGSI-SCRUM nos detalla además quienes serán los responsables de realizar las tareas o hitos específicos, esto con el afán de proponer un orden en la implementación, sin embargo no quiere decir que otros miembros del equipo puedan colaborar.

Abstract-The SCRUM methodology applied to EGSI is undoubtedly one of the projects that you can do to take the next step to Information Security in Ecuador. The development of this new way to implement the normative, which we call EGSI-SCRUM is an agile, collaborative and effective way to make the implementation of what dictates the Ordinance 166 given by SNAP. The EGSI-SCRUM we also details who will be responsible for performing specific tasks or milestones, that in an effort to propose an implementation order, however does not mean that other team members can collaborate.

I. Introducción.

La Seguridad de la Información es sin duda una preocupación del siglo XXI, las grandes empresas en la actualidad tienen mayores activos basados en su información que en toda su infraestructura, es esta la razón principal para que este sea un tema que en la actualidad sea muy discutido. Esta preocupación también la tienen las grandes instituciones públicas, aquellas que no solamente contienen información que podrían afectar al ejecutivo en el ámbito político-social, sino que existe información que podría afectar directamente a los ciudadanos.

El presente documento se enfoca en garantizar una forma ágil de implementar el Esquema de la Seguridad de la Información en las Instituciones Públicas, esquema que está basado en la Norma Internacional ISO 27001. De la misma manera se proponen técnicas para lograr aquello, basándose en una metodología ágil de implementación de proyectos de alto nivel, esta metodología es la SCRUM. Podemos referirnos entonces que es aquí donde la Seguridad de la Información va a concebirse, no solamente en la realización técnica de la misma, sino también en su gestión de desarrollo.

Se cree que el EGSI-SCRUM deberá irse desarrollando más a fondo a medida de que sea implementado en varias situaciones específicas, para denotar su efectividad y su amplitud, por supuesto que la metodología utilizada no es específica, sin embargo las situaciones podrían ser muy variables, y para ser acordes con lo que se desarrollará, la mejora continua es uno de los puntos claves.

II. Marco Conceptual.

Las metodologías ágiles, de la cual SCRUM forma parte, han alcanzado mejores rendimientos en la elaboración de proyectos, en la comparación en el CHAOS MANIFESTO del 2012 se hizo la comparación entre este tipo de metodologías versus la metodología tipo cascada, en la cual uno de los puntos

que sobresale es que la efectividad de las metodologías ágiles supera en gran proporción a las de tipo cascada. [3]

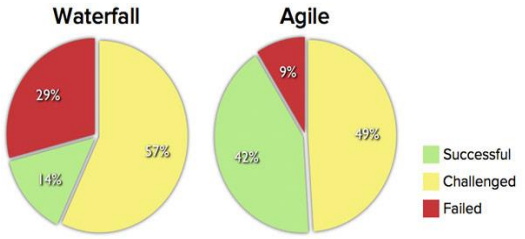

Figura 1. Comparación entre metodologías, ágil versus cascada. [3]

Para poder explicar en detalle la implementación de nuestro proyecto necesitamos definir algunas palabras que usaremos con frecuencia como:

a) Activo: Todo bien que tiene valor para la Institución.
b) Amenaza: Escenario o posible acontecimiento que puede causar daño.
c) Cloud: Término también conocido como "la nube". Se lo emplea como lugar en donde se va a almacenar información.
d) Comité de Gestión de Seguridad de la Información: Estará integrado al menos por: el Director Administrativo, el Responsable del área de Recursos Humanos, el Responsable del área de Tecnologías de la Información, el Responsable de Auditoría Interna y el Oficial de Seguridad de la Información. Este ente contará con un Coordinador (Oficial de Seguridad de la Información), quien cumplirá la función de impulsar la implementación del EGSI. [1]
e) Confidencialidad: Deberán tener acceso a la Información solo las personas autorizadas.
f) Disponibilidad: Se deberá garantizar el tener acceso a la Información en el momento en que la necesiten.
g) Impacto: La valoración de cuánto afecta la intrusión en algún activo, en función de los pilares de la Información.
h) Integridad: Se deberá garantizar que la Información sea exacta y no modificada.
i) Oficial de Seguridad de la Información: Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. El oficial de Seguridad de la Información deberá ser un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología. [1]
j) Probabilidad de Riesgo: En el presente documento no está asociado a un número del 0 al 1, sino a una escala descrita en el documento, que valora la posibilidad de que una amenaza se materialice producto de la vulnerabilidad.
k) Riesgo: El riesgo es una variable que considera que tan sensible es un activo de información y que tan posible es que este sea afectado.
l) Riesgo Residual: Riesgo que queda luego de su tratamiento.
m) SCRUM: Es una metodología utilizada para agilizar el desarrollo de proyectos, mediante el trabajo regular e incremental, y el trabajo colaborativo.
n) SCRUM Master: Es el líder que está al servicio del equipo SCRUM, es el responsable de hacer entender y de que sea aplicada la metodología.
o) Sprint: Es el núcleo de SCRUM, el cual dura un mes o menos, en este se elabora un incremento del producto terminado.
p) SQLi: Del término "SQL Injection", es una técnica de inyección SQL que consiste en hacer consultas a través de los datos de entrada en una aplicación web del cliente. Estas consultas no solo permitirán ver información confidencial, sino modificar y borrar información. [2]
q) Vulnerabilidad: Algún tipo de desacierto en la seguridad de la Institución con respecto a la Información.
r) XSS: Del término en inglés "Cross-site scripting", es un tipo de agujero de seguridad o de inseguridad informático que es típico de las aplicaciones web, son un tipo de inyección, en el que las secuencias de comandos malintencionadas se inyectan en los sitios web. [2]

III. Configuración del SCRUM para aplicabilidad en el EGSI.

Analizando detenidamente la metodología SCRUM y el EGSI nos damos cuenta de que tienen bastante en común, y al menos lo suficiente para parametrizar la metodología y hacerlo lo necesariamente aplicable a la normativa. En el caso de SCRUM podemos notar gracias a la Figura 2.1 al Equipo SCRUM, que es lo necesario para comenzar con esta metodología, en el caso del EGSI podemos recordar que es necesario conformar el CSI para proceder con la mayor parte de la implementación, la cual es dirigida por el Oficial de Seguridad de la Información, al igual que el Dueño del Producto con el Equipo de Desarrollo en SCRUM.

El EGSI define claramente que para implementar la fase inicial se debió hacerlo desde el 25 de septiembre del 2013 al 25 de marzo del 2014, y que la fase final se debió hacer desde el 25 de septiembre del 2013 al

25 de marzo del 2015, sin embargo en la mayoría de Instituciones Públicas aún no se da cumplimiento de la fase inicial hasta el 15 de Enero del 2015, en otras palabras, la mayoría de Instituciones se han demorado casi dieciséis (16) meses en lugar de los seis (6) meses estipulados, mientras que la fase final con un plazo de dieciocho (18) meses tampoco fue cumplida. En la SNAP podemos consultar el porcentaje de cumplimiento de las Instituciones hasta enero del 2015 [4].

El tiempo es uno de los aspectos más importantes en la aplicación del EGSI, por lo cual hemos elegido una metodología ágil, que nos ayude con la implementación del EGSI de una manera más rápida y eficaz. Para organizar de mejor manera la implementación lo adecuado será dividirla en dos fases: Fase 1 y Fase 2, tal y como lo recomienda la norma. En la Fase 1 se implementarán los 126 hitos base y en la Fase 2 los restantes.

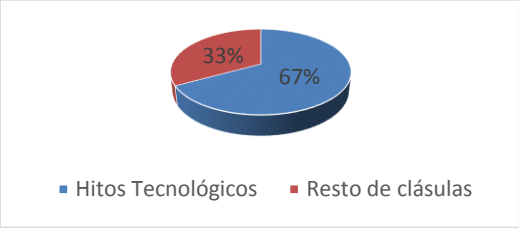

Figura 2. Porcentaje de dominios con aplicación tecnológica.

Fase 1: Conociendo esta es la fase más crítica del proyecto, es aquí donde debemos enfocar todo el esfuerzo necesario para llevar el sistema a algo cotidiano y normal dentro de la Institución. Desde que se empiece la implementación, no solo se tratará de cumplir la normativa al pie de la letra, sino de buscar que la normativa signifique algo para la Institución, que signifique una forma de trabajo, que se vea reflejado por sus buenas prácticas y que quizás en algún momento se transforme en una forma de vida. Sin embargo, retomando la Fase 1 nos damos cuenta de que son 126 hitos que deberemos cumplir en un tiempo menor a 6 meses, aproximando horas de trabajo para un individuo en seis (6) meses, serían 960 horas, asumiendo que trabaja 20 días en un mes y ocho (8) horas diarias, esto nos da como resultado que por hito un elemento debería demorar 7,6 horas, la propuesta es formar un equipo de trabajo, el cual sea avalado por la dirección, no dedicar todo el esfuerzo de trabajo al proyecto, sino tres (3) o cuatro (4) horas diarias por persona en el equipo, e incrementaremos la hora por hito cumplido, que deberá rondar entre diez (10) y veinte (20) horas. En un equipo de trabajo de entre diez y quince personas, tenemos los siguientes escenarios:

Analizando los posibles escenarios, hemos logrado descender el tiempo de implementación en un 34% en el peor escenario, y en el mejor escenario un 75%.

Fase 2: Una vez hayamos superado la Fase 1, la Fase 2 deberá realizada de la misma manera con la que realizó la Fase 2. En esta fase no nos concentraremos en el número de hitos, sino en el número de cláusulas y porcentualmente lo que estas significan.

Tabla 1. Número de cláusulas Fase 2

Dominio	Cláusulas Fase 2
Política de Seguridad de la Información	1
Organización de Seguridad de la Información	9
Gestión de los Activos	5
Seguridad de los Recursos Humanos	9
Seguridad Física y del Entorno	13
Gestión de Comunicaciones y Operaciones	29
Control de Acceso	23
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	16
Gestión de los Incidentes de la Seguridad de la Información	5
Gestión de la Continuidad del Negocio	5
Cumplimiento	10
Total	**125**

Para hacer un análisis del tiempo que será necesario en la Fase 2, retomamos las recomendaciones del EGSI con respecto al tiempo para implementar esta fase, la cual fue de dieciocho (18) meses. Aplicando linealidad nos podemos dar cuenta de que si estas 125 cláusulas necesitan 18 meses (2880 horas), entonces se debería invertir tres días de trabajo (23 horas). La propuesta será parecida a la de la Fase 1, y es por eso que la reducción porcentual deberá ser similar. Para el mejor de los casos deberemos descender 34% del tiempo necesario y en el mejor de los casos 75% del mismo. Por lo tanto, la implementación de la Fase 2 deberá durar entre 720 horas y 1900 horas, lo cual significa de cuatro (4) meses y medio hasta casi un (1) año. Finalmente, se reparten las horas para cada dominio según las cláusulas que estos tengan.

IV. Aplicación de la metodología SCRUM en la implementación del EGSI.

La Institución a la que haremos referencia existe, sin embargo por motivos de proteger su Información y todo lo que con esta viene, no revelaremos el nombre de la Institución. Además de esto los datos que se mostrarán serán válidos pero no reales, esto lo haremos

multiplicando cada valor utilizado en esta entidad por una constante.

En función de lo que tenemos, deberemos conformar lo que SCRUM nos pide en función del EGSI. Mediante la tabla 5.1 expondremos al equipo de trabajo, junto con su rol en SCRUM y en el EGSI.

Tabla 2. Equipo EGSI-SCRUM

SCRUM	EGSI	Integrantes
Dueño del Producto	Oficial de Seguridad	Oficial de Seguridad
Equipo de Desarrollo	CSI	Viceministro de Gestión Interna
		Director de Administración de Talento Humano
		Director Administrativo
		Director de Asuntos Legales de Gestión Interna
		Director de Servicios, Procesos y Calidad
		Director de la Gestión Documental y Archivo
		Coordinador General de TIC'S
		Director de Desarrollo TI
		Director de Infraestructura y Operaciones TI
		Director de Seguridad Informática TI
		Director de Servicio y Soporte al Usuario
		Coordinador General de Auditoría Interna
		Director de Comunicación Social
		Director de Documentos y Servicios
		Director de Gestión y Servicios
SCRUM Master	Especialista en Seguridad de la Información	Consultor de empresa externa

Para reducir riesgos se deberá calcular el impacto, el cual se determinará en función de los activos de información que participan dentro de cada proceso o sub proceso en evaluación. El impacto se valorará de acuerdo a la pérdida de: Disponibilidad, Integridad y Confidencialidad. El valor será la suma de estas tres variables.

Lo siguiente será realizar un Análisis y Evaluación de Riesgos, con el cual se podrá disminuir los niveles de riesgo hasta alcanzar niveles aceptables. Para hacer esto deberemos analizar las Amenazas, Vulnerabilidades y Probabilidad del Riesgo, una vez que obtenemos este valor podremos obtener el valor del Riesgo por cada Amenaza y Vulnerabilidad, el cual será la multiplicación de la Probabilidad de Riesgo y el Impacto del Activo.

La Fase 1, la cual en el EGSI está planteada para realizarla en 6 meses, según la planificación, la podremos realizar en 71 días que resulta aproximadamente en tres meses y seis días, según nuestro planteamiento. Esto lo realizaremos ejecutando siete (7) Sprints, cada uno de dos (2) semanas, y en los Sprints encontraremos las tareas a realizar, que serían la Lista de Producto, lo restante, que sería la Lista de Pendientes, la Revisión del Sprint y la Retrospectiva del mismo, los responsables de los hitos a realizar también se encuentran, estos no tienen asignadas tareas en mismo rango de fecha, salvo excepciones. Quiere decir que hemos logrado reducir el tiempo de implementación en un 50%. Cabe recalcar que se han sobredimensionado ciertos hitos, además que hay miembros en el Equipo de Desarrollo que han dado cumplimiento de sus hitos antes que otros miembros logren los suyos, esto se da particularmente por la implementación tecnológica, los miembros del Área Tecnológica tienen más tareas asignadas, lo cual era de esperarse por el sentido del EGSI.

La Fase 2, fue planificada para realizarla en 18 meses, pero con nuestra solución podría ser realizada en 191 días, que aproximadamente nos da nueve (9) meses de implementación, otro ahorro del 50% del tiempo. Además, por la gran cantidad de tareas a realizar, también aumentaron los Sprints, de tal manera que se plantearon 19 Sprints, cada uno de dos semanas de duración. Los campos del Sprint son los mismos que en la Fase 1, sin embargo las responsabilidades recaerán en los grupos de trabajo identificados por Área.

Tabla 3. Comparación de tiempos

Fase	Normativa	EGSI-SCRUM
1	6 meses	3 meses y 6 días
2	18 meses	9 meses

V. Conclusiones.

Dado que cada institución debe aceptar o rechazar los riesgos residuales, basándose en sus objetivos institucionales y su nivel de madurez en el SGSI; los riesgos residuales que hemos obtenido en el presente trabajo podrían ser rechazados en algún otro marco.

Además, el tiempo de implementación de la "Fase 1" en la institución piloto del EGSI-SCRUM propuesto en el presente trabajo fue de aproximadamente el 50%

(tres meses y seis días) de lo que plantea la SNAP. Por lo tanto, nuestro esquema tendrá un tiempo de implementación de entre noventa y ciento treinta cinco días (entre el 50% y 75%) como planteamiento inicial para así hacer más flexible la aplicación del EGSI-SCRUM.

VI. Recomendaciones.

Debido a que la Fase 2 tiene mayor cantidad de hitos que la Fase 1, la cantidad de Sprints pudo ser mayor a dos (2) semanas. Sin embargo, lo recomendable es no cambiar el sistema.

El EGSI incluye la mejora continua como uno de sus puntos de gestión clave, es por eso que mediante se vayan realizando implementaciones del EGSI-SCRUM en diferentes instituciones, este documento se deberá ir actualizando en función de las sugerencias obtenidas.

Y por último, algunas tareas necesarias del EGSI tomaron más del tiempo planificado, debido a que la Institución piloto requería de ciertos trámites específicos cuyo seguimiento en algunos casos era complejo. Debido a esto es necesario será tener un plan de contingencia, como poner aquellas tareas al principio del proyecto de manera que no afecten de manera significativa la implementación del mismo.

VII. Referencias.

[1] Castillo Peñaherrera Cristhian, Esquema Gubernamental de Seguridad de la Información, http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf, fecha de consulta abril 2015.

[2] Meucci Mateo, Guía de Pruebas OWASP, https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf, fecha de consulta abril 2015.

[3] Schwaber Ken y Sutherland Jeff, La Guía de SCRUM, http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-ES.pdf, fecha de consulta abril 2015.

[4] SNAP, RANKING DE ENTIDADES PÚBLICAS DEL CUMPLIMIENTO DE LA IMPLEMENTACIÓN DEL EGSI, fecha de consulta abril 2015.

VIII. Autores.

- Adib Manssur, estudiante de la carrera de Ingeniería en Telemática, ESPOL-Ecuador.
- Patricia Chávez, profesora de la ESPOL.