Componente de seguridad de la información en el Ciclo de Vida del Desarrollo de Software aplicado al procedimiento PR-M7-P5-033 en la Gobernación de Antioquia

Information security component in the Life Cycle of Software Development applied to procedure PR-M7-P5-033 in the Government of Antioquia

Santiago Elías Díaz Ayala. Ingeniero de Sistemas. Estudiante Especialización en Seguridad de la Información. sedahackers@gmail.com
Diego Adrian Castaño Castaño. Ingeniero de Software. Estudiante Especialización en Seguridad de la Información. diegoadrian.castano@gmail.com

Resumen

El Ciclo de Vida de Desarrollo de Software (CVDS), como una de las actividades más importantes de la ingeniería de software, representa una secuencia estructurada y bien definida para desarrollar el producto deseado. El CVDS se compone de una serie de pasos a seguir con la finalidad de diseñar y desarrollar un producto de manera eficiente en su funcionamiento (Becerra & Sanjuan, 2014). Partiendo del hecho que una de las finalidades más importantes de una aplicación es la óptima administración de la información en ella contenida y acorde a los lineamientos de familia de normas ISO 27000 y de las directrices del Ministerio de la Tecnologías y Comunicaciones de Colombia en materia de seguridad y privacidad de la información (MinTIC, 2016) para el sector público; este artículo pretende aumentar la conciencia en materia de prácticas de seguridad de información teniendo de cuenta los pasos o etapas correspondientes para tal fin en el marco de esta temática enmarcada en el procedimiento PR-M7-P5-033 de desarrollo de software en la Gobernación de Antioquia.

Palabras claves: Ciclo de Vida de Desarrollo de Software, Seguridad de la Información, Amenazas y Vulnerabilidades

Abstract

The Software Development Life Cycle (CVDS), as one of the most important activities of software engineering, represents a structured and well defined sequence to develop the desired product. The CVDS must provide a series of steps to follow in order to design and develop a product efficiently in its operation (Becerra & Sanjuan, 2014). Based on the fact that one of the most important purposes of an application is the optimal management of the information contained therein and in accordance with the guidelines of the ISO 27000 standards and the guidelines of the Ministry of Technology and Communications of Colombia on information security and privacy (MinTIC, 2016) for the public sector; this article aims to raise awareness of information security practices by taking into account the corresponding steps or stages for this purpose in the context of this topic under the PR-procedureM7-P5-033 software development in the Government of Antioquia.

Keywords: Software Development Life Cycle, Information Security, Threat, Vulnerability

1 - Introducción

La seguridad en las aplicaciones de software ha incrementado su análisis desde la aparición de la transmisión de datos basados en internet. En su libro, Principles of Information Security, los autores describen la seguridad de la información como "preservación de la confidencialidad, la integridad y la disponibilidad de la información" (Whitman & Mattord, 2012). lo cual se encuentra igualmente fundamentado en la norma ISO 27001 (Mesquida, Mas, & Amen, 2019).

Basados en la anterior afirmación, y teniendo en cuenta que día a día se vulnera la seguridad de la información a compañías por atacantes que en gran medida buscan un beneficio económico y teniendo en cuenta que algunas compañías prefieren no divulgar sus vulnerabilidades para preservar un tema de reputación corporativa (Alcalá, 2008), vale la pena realizar un análisis de las salvaguardas de la seguridad de la información tales como; controles de acceso, formación de personal y seguridad física (Bertolín, 2008), como argumento sustentable de mitigación de los impactos negativos e incontenibles de las laceraciones que dichas vulnerabilidades causan en las empresas. En congruencia con esto, se realiza este artículo de revisión enfatizando la seguridad en el CVDS.

Uno de los proyectos más notorios de OWASP (Proyecto abierto de seguridad de aplicaciones web), proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro, es el OWASP Top 10, el cual consiste en un listado de los problemas más comunes encontrados en las aplicaciones web organizados por criticidad, además es un estándar de facto en las auditorías web. (OWASP, 2017). Producto del análisis de la tabla 1, se puede observar que existen amenazas que suben o bajan su categoría de peligrosidad (OWASP, 2017). Otras se mantienen o desaparecen, así como surgen nuevas dentro de las 10 más comunes (OWASP, 2017).

Directamente relacionado con el componente de software se encuentra en la tabla 1, donde amenazas como SQL Injection (A1) y Broken Authentication (A2) continúan estando para el 2019 muy bien posicionadas en el Top 10 de las posibles amenazas a que está expuesta un proyecto software en la web. Con base a lo anterior se debe tener en cuenta dicha estadística en la fase 1 "Definición de Requisitos" del CVDS.

***Tab1a 1**. Top-10 de amenazas y vulnerabilidades de software web*

OWASP Top 10 - 2017	**Comportamiento**	**OWASP Top 10 - 2019**
A1 – Injection	Igual	A1: Injection
A2 – Broken Authentication and Session Management	Igual	A2: Broken Authentication
A3 – Cross-Site Scripting (XSS)	Baja	A3: Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	Nueva	A4: XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	Baja	A5: Broken Access Control [Merged A4+A7]
A6 – Sensitive Data Exposure	Sube	A6: Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	Nueva	A7: Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	Desaparece	A8: Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	Igual	A9: Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	Desaparece	A10: Insufficient Logging&Monitoring [NEW]

***Fuente:** (OWASP, 2017, p 4).*

Por un lado, los ataques cibernéticos cada vez más se concentran en vulnerar las aplicaciones web. Por otra parte, están los responsables de darle seguridad a las aplicaciones para impedir o reducir el riesgo de ser objeto de un ataque que ponga en riesgo la aplicación o la transmisión de la información.

El constante actuar de los atacantes, conlleva de igual forma, a una firme respuesta de los defensores para hacer los sistemas más seguros e incluso predecir el comportamiento de las agresiones e impedir la pérdida o filtración de la información. Eliminar, disminuir o mitigar los incidentes de seguridad que impliquen las aplicaciones o sus datos, conlleva una serie de políticas que las empresas deben adoptar, acoplar e implementar (Gómez Vieites, 2011).

La Gobernación de Antioquia, entidad en la norma ISO 9001, rige sus procesos y procedimientos a través del SIG (Sistema Integrado de Gestión). La Dirección de Informática y Tecnología no es ajena a esta directriz. El objeto de este artículo es proporcionar una revisión a la documentación científica respecto del tema central del que compone el procedimiento PR-M7-P5-033 de la Gobernación de Antioquia para garantizar la triada de seguridad de la información; seguridad, disponibilidad e integridad, desde el CVDS y evaluar la incorporación de un componente de seguridad antes de la salida a producción de las aplicaciones desarrolladas (CHERDANTSEVA & Hilton, 2013). En este sentido, dicho procedimiento se refiere a los pasos fundamentales del ciclo del desarrollo que serán analizados incluyendo los componentes de seguridad.

2- Metodología

Mediante una investigación cualitativa con enfoque de revisión documental, el objetivo de esta investigación es evaluar la seguridad del CVDS y contemplar la incorporación de un componente de seguridad a cada uno de sus procesos. Congruentemente, se busca dar las pautas para proponer que el procedimiento PR-M7-P5-033 de la Gobernación de Antioquia, el cual se basa en el CVDS para el desarrollo de aplicaciones, tenga un componente de seguridad que prevenga los ataques más comunes.

3 - Marco teórico

Las aplicaciones desarrolladas para operar en ambientes web, están potencialmente más expuestas a amenazas que las aplicaciones que corren en servidores en sitio. La seguridad de este tipo de aplicaciones debe estar contemplado desde el momento del levantamiento de los requisitos, y así llegar a la fase de implementación con un software robusto que esté construido para prevenir el ataque de las principales amenazas existentes en la red.

3.1 Amenazas y vulnerabilidad

La norma ISO-27001 describe las amenazas y vulnerabilidades como componentes que indisponen a un sistema de información y por ende factores de inmediata solución para determinar que un sistema de información sea seguro.

La materialización de un ataque es la consecuencia de un sistema de información que no contó con los estándares de seguridad necesarios para detectar una vulnerabilidad existente. Ataques de tipo SQLi, DoS, Broken Authentication, MitM o XSS difundidos mediante Malware, Ransonware e ingeniería social, generan gran

impacto en las compañías que deben pagar altos precios posteriores a la materialización de un ataque. (VIEITES, 2014)

WannaCry, un ataque de tipo secuestro de información, es un claro ejemplo de esto. Las compañías afectadas operaban con sistemas propensos a amenazas y con vulnerabilidades no contempladas. Una vez se materializó este ataque, las empresas afectadas hicieron grandes inversiones para reestablecer la operatividad y las que no fueron atacadas, de igual forma hicieron inversiones para fortalecer la seguridad informática. En la figura 1 se observa el comportamiento de las empresas antes, durante y después del lanzamiento de WannaCry. En marzo de 2017, Microsoft advierte la presencia de la vulnerabilidad MS17-010 (WannaCry) y se registran 400.000 ataques. Posteriormente en abril descienden a 250.000 ataques, pero una vez explotada la vulnerabilidad en mayo, se registran casi 600.000 ataques. Una vez identificada la solución, los ataques bajan casi a 0 finalizando mayo, no sin antes afectar a varias compañías en el mundo.

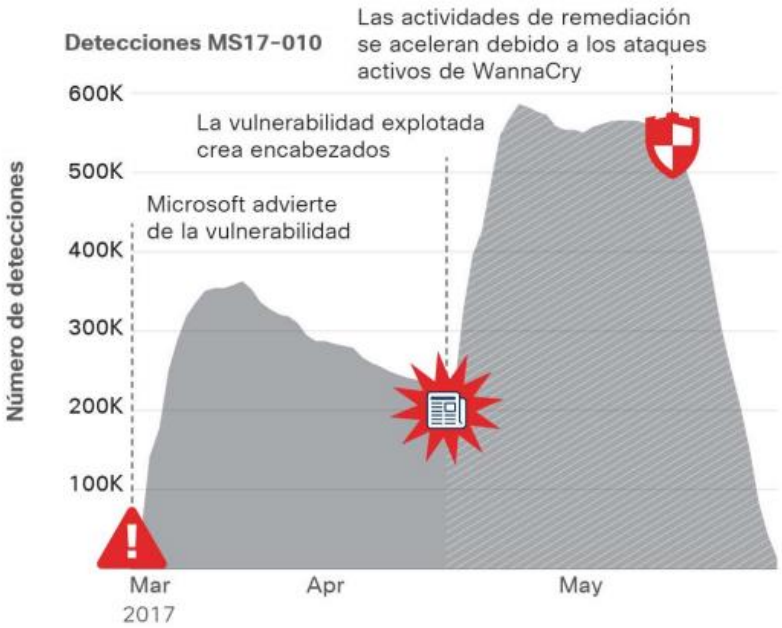

Figura 1. Comportamiento de las empresas antes y después de WannaCry .
Fuente: (Reporte anual de cyber seguridad. *Cisco 2018. p44).*

En la tabla 2 se pueden visualizar estadísticas referentes a Seguridad Informática, Costos de la Seguridad Informática, Ransomware y Phishing, para dimensionar el accionar de los ataques cibernéticos. (Prey Nation, 2018). Estas estadísticas nos muestran el estado actual de la seguridad informática y además es una base para tomar decisiones e implementar medidas correctivas en cuanto a amenazas y vulnerabilidades.

***Tab1a 2**. 24 estadísticas de Seguridad Informática que Importan en el 2019*

#	Seguridad Informática	Fuente
1	70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017.	https://www.ibm.com/downloads/cas/ZYKLN2E3
2	Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones.	https://www.scmagazine.com/home/research/video-300-billion-passwords-by-2020-report-predicts/
3	43% de los ciberataques afectan a pequeños negocios.	https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html
4	230,000 nuevos malware son producidos cada día, y se predice que este número crecerá.	https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/
5	90% de los hackers cubren sus rastros utilizando encriptación.	https://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf
6	A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad.	https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/
7	Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar.	https://www.computerworld.com/article/2475964/98--of-mobile-malware-targets-android-platform.html
8	Hubo más de 3 millones de golpes de crypto jacking entre Enero y Mayo del 2018.	https://www.deccanchronicle.com/technology/in-other-news/260618/3-million-cryptojacking-hits-detected-in-2018-so-far-research.html
9	El número de variantes de malware de crypto jacking creció de 8 en el 2017 a 25 en Mayo del 2018.	https://www.deccanchronicle.com/technology/in-other-news/260618/3-million-cryptojacking-hits-detected-in-2018-so-far-research.html
#	**Costos de la Seguridad Informática**	**Fuente**
10	El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los $124 billones.	https://www.computerweekly.com/news/252446970/Global-infosec-spending-to-top-114bn-in-2018-says-Gartner
11	El costo total de un ciberataque exitoso es de más de $5 millones de dólares, o $301 por empleado.	https://www.ponemon.org/blog/the-2017-state-of-endpoint-security-risk-report
12	El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos.	https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS%20-%20block-insights-and-innovation
13	Se proyecta que el daño relacionado a ciberataques llegará a los $6 trillones de dólares anuales para el 2021.	https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
14	La brecha de seguridad de Equifax le costó más de $4 billones a la empresa.	http://money.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/
15	Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de $2.4 millones en defensa.	https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS%20-%20block-insights-and-innovation
#	**Ransomware**	**Fuente**
16	Ocurren más de 4,000 ataques de ransomware por día.	https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
17	75% de las organizaciones infectadas con ransomware tenían protección activa.	https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx
18	Los daños globales relacionados a ataques de ransomware llegarán a $11.5 billones en el 2019.	https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/
19	Se estima que habrá un ataque de ransomware cada 14 segundos para el fin del 2019. Esto no incluye ataques a individuos, que ocurren con mayor frecuencia.	https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/
20	91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones.	https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email
#	**Phishing**	**Fuente**
21	En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática.	https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018/
22	76% de las negocios reportaron ser víctimas de ataques phishing en el último año.	https://www.wombatsecurity.com/state-of-the-phish
23	Verizon reporta que usuarios Estadounidenses abren un 30% de todos los correos maliciosos y un 12% de ellos dan clic al enlace peligroso.	https://enterprise.verizon.com/resources/reports/dbir/
24	Kaspersky's ha detectado 246,231,645 intentos de phishing en el 2017, y evidenció un crecimiento de 91 millones con respecto al 2016.	https://securelist.com/spam-and-phishing-in-2017/83833/

Fuente: (Prey Nation, 2018).

3.2 Seguridad de la información

Desarrollar sistemas seguros, no es la prioridad de las casas productoras de software, es más un plus adicional que deciden incluir en las aplicaciones diseñadas. Esto es, lamentablemente una verdad existente (ITIL, 2007). Sabiendo de antemano las amenazas a las que están expuestas las aplicaciones de tipo web, incorporar un componente de seguridad a las aplicaciones debe ser un paso más en el CVDS.

En el documento ITIL v3, se establece que el principal objetivo de la seguridad de la información es:

> La Gestión de la Seguridad será por tanto cumplir con los requisitos de seguridad de los Acuerdos de Niveles de Servicio relacionados con la legislación, las políticas externas y los contratos, de manera que el servicio disponga de un nivel de seguridad concreto, para evitar la dependencia de los aspectos externos. (ITIL, 2007, p. 36)

Haciendo una correcta planificación y ejecución de la seguridad de la información, la implementación de un CVDS que incluya el componente de seguridad al procedimiento PR-M7-P5-033 es necesario para que los desarrollos tengan los más altos estándares de calidad.

3.3 ICONTEC

El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es una entidad sin ánimo de lucro de Colombia que tiene entre sus funciones la reproducción de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. Está compuesta por un grupo multidisciplinario entre los que están sectores privados, sectores tecnológicos, gobierno y todas aquellas personas que propendan el desarrollo del país para alcanzar una economía óptima, el mejoramiento de la calidad y las relaciones empresariales nacionales e internacionales. Actúa como representante de Colombia ante diferentes organismos de normalización internacional y regional, tales como: Organización Internacional de Normalización ISO, la Comisión Electrotécnica Internacional IEC, y la Comisión Panamericana de Normas Técnicas COPANT. De igual forma, soporta al Gobierno Nacional en grupos negociadores como: Comunidad Andina, Área de Libre Comercio de las Américas ALCA y TLC con Estados Unidos. (ICONTEC, 2019)

3.4 Gobernación de Antioquia

La provincia de Antioquia, también llamada gobierno de Antioquia durante el imperio colonial español, fue una entidad administrativa y territorial de la Nueva Granada, creada en 1576. Posteriormente a la disolución de este país (1830) perteneció a la República de la Nueva Granada, de carácter centralista, hasta que finalmente se implantó el sistema federal en la Nueva Granada en 1858 y la provincia pasó a ser entonces el Estado Soberano de Antioquia. (Gobernación de Antioquia, 2019)

Así Antioquia se constituye como uno de los principales departamentos de Colombia compuesto por 9 subregiones y 125 municipios. (Gobernación de Antioquia, 2019)

La Gobernación de Antioquia con sede administrativa ubicada en la ciudad de Medellín, es un ente público del sector gobierno y según la Constitución Política, son fines esenciales del estado:

> Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. (Gobernación de Antioquia, 2019)

La Gobernación de Antioquia se comporta con toda fidelidad a este mandato, y para lograrlo y como se observa en la figura 2, desarrolla 23 procesos de los cuales "Planeación y Administración de las TIC" es al que se dirigen las recomendaciones del presente artículo.

Figura 2. Mapa organizacional de la Gobernación de Antioquia
Fuente: Sistema Integrado de Gestión. *Gobernación de Antioquia. (2018). Opción Procesos*

3.5 Sistema de Gestión de Seguridad de la Información SGSI

El SGSI es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Mesquida, Mas, & Amen, 2019).

4 – Reflexión

Desarrollar software por parte de los funcionarios de una entidad gubernamental, como la Gobernación de Antioquia, es una de las tareas asignadas al personal de Desarrollo de Software de la Dirección de Informática. Dicha actividad se encuentra documentada en el procedimiento PR-M7-P5-033 tabla 3, que en sus apartes dice; (Gobernación de Antioquia, 2018) existen dos posibilidades para que una idea o necesidad que requiera el apoyo de un software sea implementada:

1. Producto de la contratación de su implementación por parte de una empresa del área de Desarrollo de Software.
2. Que el componente software y sus respectivas bases de datos sea implementado por el recurso humano interno del área de Desarrollo de Software de la Dirección de Informática. (Gobernación de Antioquia, 2018) Cap. 2.6.

Tab1a 3. *Procedimiento PR-M7-P5-033 de acuerdo al SIG (Sistema Integrado de Gestión) para la Gobernación de Antioquia)*

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	**Identificar los procesos de la Organización**	Se elabora y aprueba el **Modelo de Negocio.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Negocio
2	**Planificar la Solución**	Se realizan estimaciones razonables de recursos, costos y planificación inicial. Se elabora y aprueba el **Modelo de Planeación.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Planeación
3	**Analizar Requerimientos**	Se realiza el análisis y afinamiento de los requerimientos Se elabora y aprueba el **Modelo de Requisitos.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Requisitos
4	**Diseñar la Solución Informática**	Se realizan los diagramas UML necesarios Se elabora, verifica y aprueba el **Modelo de Diseño.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Diseño
5	**Desarrollar la Solución Informática**	Se realiza el desarrollo de la solución informática, sea contratada o interna **Nota:** Si es contratada se procede acorde a lo descrito en el Proceso CA-M7-P3-01 de **Contratación Administrativa.**	Profesional Universitario, Técnico	Software o Aplicativo Manual del usuario, Manual del sistema y de instalación (digitales y/o impresos)
6	**Probar la solución informática**	Realizar las pruebas que apliquen Se elabora, verifica y aprueba el **Modelo de Pruebas.** conjuntamente con el organismo solicitante	Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Pruebas

7	**Implementar la Solución Informática**	Se realiza la implementación de la solución informática Se elabora el . **Modelo de Implementación.** conjuntamente con el organismo solicitante Se recibe el Certificado de licencia y/o registro de propiedad del Departamento (Derechos de Autor)	Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Implementación Certificado de licencia y/o registro de propiedad del Departamento (Derechos de Autor)

Fuente: *Gobernación de Antioquia – Normatividad interna, 2018*

Sin embargo, se observa que el componente de seguridad de información no ha sido tenido en cuenta en dicho procedimiento.

Por lo expuesto anteriormente, se genera una reflexión que busque incorporar el componente de seguridad al CVDS, que permita construir una propuesta estandarizada permitiendo que las aplicaciones en las que se desarrollan aplicaciones de software; tales como Visual Basic, PHP, Java, C#, JavaScript, etc, incorporen prácticas seguras para prevenir o mitigar vulnerabilidades conocidas.

Se busca introducir elementos de seguridad en este proceso de CVDS, de manera que sea independiente de normatividad, herramienta, estándar o metodología., encaminando la propuesta a un ciclo de desarrollo más sencillo pero usado actualmente. Las fases del CVDS según Mahalakshmi & Sundararajan (2013) son:

- Requisitos: reuniones y levantamiento de información de la necesidad a suplir con el desarrollo
- Diseño: diseño del desarrollo, reglas de negocio, diagramas, etc.
- Desarrollo: codificación en lenguajes de programación
- Pruebas de funcionamiento: verificación de funcionamiento del desarrollo
- Producción: entrega del desarrollo al cliente completamente funcional

En la figura 3 podemos ver el diagrama del CVDS que representa las mencionadas fases.

Figura 3. Ciclo de Vida de Desarrollo de Software (CVDS).
Fuente: Elaboración propia

En diferentes organizaciones o departamentos de desarrollo para no implementar seguridad en los mismos, suelen dar excusas como las siguientes, no obstante, a estas afirmaciones se tienen algunos argumentos de seguridad que sustentan la necesidad de no dejarlos pasar desapercibidos. Algunos de estos son:

- Argumento de excusa cultural: Nadie sabe cómo funciona, por ende, no la van a atacar. Argumento de seguridad: Un atacante invertirá el tiempo que necesite para saber cómo funciona.
- Argumento de excusa cultural: Si no se encontraron vulnerabilidades hasta ahora, entonces no se encontrarán. Argumento de seguridad: Un atacante encontrara una o varias vulnerabilidades con tan solo un vistazo en la misma.
- Argumento de excusa cultural: A nadie le interesaría atacar nuestra aplicación. Argumento de seguridad: Existen millones de bots o sistemas automáticos escaneando constantemente en búsqueda de deficiencias de seguridad.
- Argumento de excusa cultural: La aplicación es segura porque corre detrás de un componente hardware y/o software que controla el acceso a la red llamado firewall. Argumento de seguridad: Si tiene un elemento de hardware de seguridad es más segura, pero este hecho no implicara nunca que sea segura.
- Argumento de excusa cultural: La aplicación es segura porque usa https (protocolo de transferencia de hipertexto Seguro). Argumento de seguridad: En este caso la comunicación es segura pero el desarrollo no tiene por qué serlo.
- Argumento de excusa cultural: Si no corre como Administrador / root, no puedes hacer nada peligroso. Argumento de seguridad: Esto es una buena práctica de seguridad, pero que el usuario tenga pocos privilegios no indica que la aplicación sea segura.

Entre todas las excusas posibles para no implementar la seguridad en el CVDS la que más se suele escuchar es "No hay tiempo para incluir la seguridad", ya que la mayoría de los desarrollos van ajustados de tiempo y es más importante poner algo en producción en el plazo adecuado que incluir la seguridad en cada una de sus partes.
Más vale prevenir que curar, por lo que es mucho más productivo y menos comprometedor evitar o detectar un ataque para el desarrollo que restaurar el estado tras un ataque exitoso.

Para desarrollar de forma segura, existen varios modelos de seguridad para ser implementados. Uno de los más recomendables que se suele implantar, es el Modelo de Madurez para el Aseguramiento de Software SAMM (Chandra, 2009), el cual es un marco de trabajo abierto y flexible desarrollado por OWASP. Este modelo sirve para ayudar a las organizaciones a formular e implementar una Estrategia de Seguridad para el Desarrollo de Software que sea adecuada a las necesidades específicas de cada organización.

En la figura 4, se observa que cada fase tiene su correspondiente componente de seguridad. Por ejemplo, en el momento que se están realizando pruebas del correcto funcionamiento de la aplicación, se debería realizar una auditoría dinámica de la misma en la que se puedan ver las vulnerabilidades antes de la fase de producción.

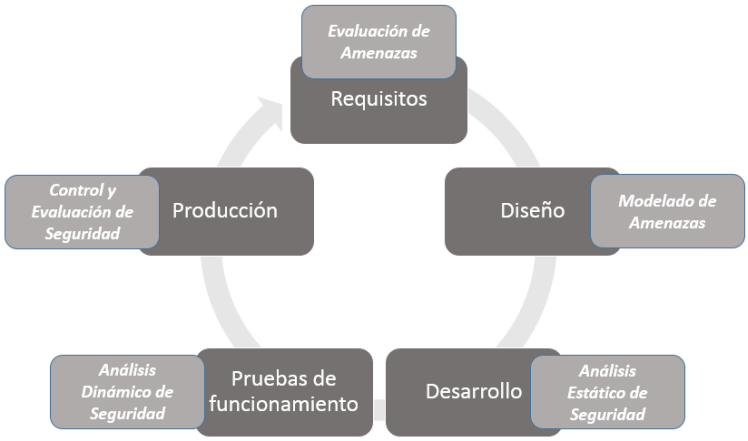

Figura 4. Ciclo de vida de desarrollo de software con componente de seguridad.
Fuente: Elaboración propia

Las fases que se contemplan según Microsoft (2019) adjuntas al CVDS como componente de seguridad son:

- Evaluación de amenazas: definir las amenazas que pueden afectar el desarrollo.
- Modelado de amenazas: incorporación de código fuente para prevenir ataques al desarrollo.
- Análisis estático de seguridad: revisar el código fuente de forma escalable para comprobar las directivas de codificación segura.
- Análisis dinámico de seguridad: comprobar la ejecución de desarrollo para verificar su funcionalidad sea acorde al diseño.
- Control y evaluación de seguridad: verificar vulnerabilidades contempladas en la evaluación.

Lo que se busca es introducir seguridad al CVDS, definiendo unas fases de seguridad paralelas a la vez que se van desarrollando aplicaciones.

La implementación de medidas de seguridad debe hacerse desde el inicio del Ciclo de Vida del Desarrollo del Software, ya que el coste de solucionar cualquier problema de seguridad es mayor cuanto más tarde se detecte. Fundamentado en la revisión del marco teórico anterior, se presenta una postura representada en la tabla 4 que describe una nueva propuesta de *Procedimiento PR-M7-P5-033* aplicable a la Gobernación de Antioquia para desarrollar aplicaciones seguras bajo los proceso de CVDS.

Tab1a 4. *Procedimiento PR-M7-P5-033 PROPUESTO al SIG (Sistema Integrado de Gestión) para la Gobernación de Antioquia)*

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	**Identificar los procesos de la Organización**	Se elabora y aprueba el **Modelo de Negocio** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Negocio

2	**Planificar la Solución**	Se realizan estimaciones razonables de recursos, costos y planificación inicial. Se elabora y aprueba el **Modelo de Planeación.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Planeación
2.1	**Visibilización hacia la S.I**	Agregar al Modelo de Planeación la importancia de la Seguridad de la Información dependiendo de la arquitectura y tecnologías a utilizar en la solución propuesta. Los equipos de proyecto no deben abordar deprisa y corriendo las características de seguridad y de privacidad	Oficial de seguridad, Analista Líder de desarrollo	Modelo de Planeación
3	**Analizar Requerimientos**	Se realiza el análisis y afinamiento de los requerimientos Se elabora y aprueba el **Modelo de Requisitos.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Requisitos
3.1	**Evaluación de Amenazas**	-definir los requisitos de fiabilidad de un proyecto de software. -evaluación de los riesgos de seguridad y privacidad - niveles mínimos aceptables de calidad en materia de seguridad y privacidad	Equipo de Desarrollo (Profesional Especializado, Profesional Universitario, Técnico del área TIC's)	Modelo de Requisitos
4	**Diseñar la Solución Informática**	Se realizan los diagramas UML necesarios Se elabora, verifica y aprueba el **Modelo de Diseño.** conjuntamente con el organismo solicitante	Profesional Especializado, Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Diseño
4.1	**Modelado de Amenazas**	Mitigar los problemas de seguridad y de privacidad -Modelar la reducción de la superficie de ataques -modelos de riesgos	Equipo de Desarrollo (Profesional Especializado, Profesional Universitario, Técnico del área TIC's)	Modelo de Diseño
5	**Desarrollar la Solución Informática**	Se realiza el desarrollo de la solución informática, sea contratada o interna **Nota:** Si es contratada se procede acorde a lo descrito en el Proceso CA-M7-P3-01 de **Contratación Administrativa.**	Profesional Universitario, Técnico	Software o Aplicativo Manual del usuario, Manual del sistema y de instalación (digitales y/o impresos)
5.1	**Análisis estático de la seguridad**	Asegurar que se observan las directivas de codificación segura y revisar el código de seguridad de forma escalable. -usar herramientas aprobadas -prohibir funciones no seguras -revisión humana, según sea necesaria.	Equipo de Desarrollo (Profesional Especializado, Profesional Universitario, Técnico del área TIC's)	Software o Aplicativo Manual del usuario, Manual del sistema y de instalación (digitales y/o impresos)
6	**Probar la solución informática**	Realizar las pruebas que apliquen Se elabora, verifica y aprueba	Profesional Universitario, Técnico	Modelo de Pruebas

		el **Modelo de Pruebas.** conjuntamente con el organismo solicitante	de las diferentes áreas u organismos	
6.1	**Análisis dinámico de la seguridad**	Comprobar los programas de software en tiempo de ejecución para asegurar que su funcionalidad sea acorde con el diseño - pruebas de exploración de vulnerabilidades mediante datos aleatorios - revisión de los modelos de riesgos y de la superficie de ataques	Equipo de Desarrollo (Profesional Especializado, Profesional Universitario, Técnico del área TIC's)	Modelo de Pruebas
7	**Implementar la Solución Informática**	Se realiza la implementación de la solución informática Se elabora el **Modelo de Implementación.** conjuntamente con el organismo solicitante Se recibe el Certificado de licencia y/o registro de propiedad del Departamento (Derechos de Autor)	Profesional Universitario, Técnico de las diferentes áreas u organismos	Modelo de Implementación Certificado de licencia y/o registro de propiedad del Departamento (Derechos de Autor)
7.1	**Control y evaluación de la seguridad**	Después de la salida en vivo o producción se debe contar con: -plan de respuesta a incidentes -plan de respuesta a incidentes -lanzamiento o archivado	Equipo de Desarrollo (Profesional Especializado, Profesional Universitario, Técnico del área TIC's) Oficial de Seguridad	Modelo de Implementación Certificar (mediante la revisión de seguridad final y otros datos) que el equipo de proyecto ha cumplido los requisitos de seguridad.

Fuente: *Elaboración propia, basado en el procedimiento PR-M7-P5-033 en la Gobernación de Antioquia*

La importancia del uso de un modelo o una metodología radica principalmente en el hecho de que es precisamente lo que permite comprender cuáles son los elementos específicos de una organización, a la vez que ayuda a formular y hablar de lo que se debe mejorar dentro de la misma y de cómo se pueden lograr dichas mejoras. Dicho esto, algunas de las ventajas del uso de un modelo son las siguientes:

- Proporciona un marco y un lenguaje común, lo que se traduce en la ruptura de las barreras de la comunicación en el interior de las organizaciones.
- Permite que los usuarios puedan enfocarse específicamente en la mejora, ya que ayudan a que no pierdan la idea global.
- Aporta años de experiencia.
- Ayudan a mejorar la satisfacción del cliente.
- Permiten producir productos y servicios de alta calidad.
- Poder aplicar prácticas de alta madurez mucho más robustas
- Cumplir de forma mucho más completa con las normas ISO-27001

La utilización de estándares como ITIL, metodologías agiles como SCRUM (Mahalakshmi & Sundararajan, 2013) permiten evidenciar que el propósito de un modelo, es hacer la evaluación de la madurez de los procesos de una organización, para así proporcionar una orientación referente a cómo se pueden llevar a cabo las mejoras de aquellos procesos que darán lugar a mejores productos.

5 – Conclusiones

El mundo actual, tal como lo conocemos, tiene una dependencia total de las TIC, y es inviable su existencia sin el soporte de las mismas, sin el adecuado funcionamiento de los sistemas soportados por las TIC, que son prácticamente todos los que tienen influencia en nuestra vida diaria.

Por ello es necesario que exista una garantía del adecuado funcionamiento de todos estos sistemas, hay que generar en los usuarios una confianza en que su funcionamiento es correcto, ello significa que hay que demostrar, y convencer de su adecuado funcionamiento.

La forma de garantizar el correcto funcionamiento de las TIC, y en este caso un software, es la aplicación de normas y estándares en todo su ciclo de vida. Incluyendo desde la fase de análisis y diseño, pasando por la fase de explotación de estos y finalizando con los procesos de retirada del servicio de los sistemas.

Si un sistema de información se desarrolla y explota cumpliendo las normas y estándares adecuados, se puede deducir que su funcionamiento es el adecuado, y proporciona la garantía suficiente para que se pueda confiar en él.

Abordar el tema de la seguridad de la información tanto a nivel nacional como trasnacional tempranamente desde la primera fase del CVDS es apuntar a la calidad del software, lo cual redundara inevitablemente en el cumplimiento de la norma ISO 27001 y por ende a las directrices del MinTic. Por otra parte, la OCDE, organismo al cual Colombia recientemente logro ser aceptada en su más recientemente conferencia ministerial estipulo:

> Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en 1998 en Ottawa, los ministros reafirmaron "su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales." Declararon concretamente que "trabajarían para vincular los diferentes enfoques adoptados por los países miembros con vistas a asegurar la protección de la privacidad en las redes globales basándose en las directrices de privacidad de la OCDE. (OECD, 2002), p.3).

El propósito general de las referencias y modelos presentados es establecer una aproximación a la categoría de capacidades y prácticas susceptibles de sostener un pensamiento de seguridad de la información desde la etapa más temprana en la construcción de un producto de software.

Se trata de comprender y medir de qué manera madurar un componente de seguridad de la información en cada etapa del CVDS que impacte en la confidencialidad, integridad y disponibilidad de los datos. Además, si es capaz de generar o fomentar nuevas rutinas metodológicas que impacten en general la seguridad del negocio o empresa.

Se clara que en la Gobernación de Antioquia se observa un déficit relevante sobre la seguridad de la información a la hora de implementar un nuevo desarrollo software y en materia de seguridad. Es por ello que la propuesta presentada en una versión 2 del procedimiento PR-M7-P5-033 pretende coadyuvar en el cierre de brechas en este aspecto. En este sentido se sugiere un ajuste del mencionado procedimiento, así como la implementación de medidas de seguridad en el Ciclo de Vida del Desarrollo del Software, desarrollado al interior de la organización.

Referencias

Alaimo, M. (2013). *Proyectos Ágiles con #Scrum.* Buenos Aires: Kleer.

Alcalá, M. Á. (10 de Abril de 2008). *Reputación.* Obtenido de http://www.mindvalue.com/reputacion.pdf

Becerra, P., & Sanjuan, M. (2014). Revisión de estado del arte del ciclo de vida de desarrollo de software seguro con la metodología SCRUM. *I+D en TIC*, 3.

Bertolín, J. A. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid: Editorial Paraninfo.

Certificación, I. C. (22 de Marzo de 2006). *Norma NTC-ISO-IEC 27001.* Obtenido de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Chandra, P. (01 de Enero de 2009). *OpenSAMM.* Obtenido de http://www.cs.unh.edu/~it666/reading_list/SDLC/opensamm_1.0.pdf

CHERDANTSEVA, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *Research Gate*, 7.

Cisco. (2018). *Reporte Anual de Ciberseguridad de Cisco.* San Diego: Cisco.

Gobernación de Antioquia. (01 de Febrero de 2018). *Gobernación de Antioquia - SIG*. Obtenido de http://isolucion.antioquia.gov.co/IdentificaUsuario.asp?Pagina1=FrameSetGeneral.asp&

Gobernación de Antioquia. (01 de Enero de 2019). *Gobernación de Antioquia - Datos*. Obtenido de http://www.antioquia.gov.co/index.php/gobernacion/mision-vision

Gobernación de Antioquia. (01 de Enero de 2019). *Gobernación de Antioquia - Regiones*. Obtenido de https://www.antioquia.gov.co/index.php/antioquia/regiones

Gómez Vieites, Á. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición.* Vigo: RA-MA.

ICONTEC. (17 de Junio de 2019). *Instituto Colombiano de Normas Técnicas y Certificación*. Obtenido de https://www.icontec.org/NC/QS/Paginas/Qui.aspx

ITIL. (2007). *Information Technology Infrastructure Library.* Nueva York.

Mahalakshmi, M., & Sundararajan, M. (2013). Traditional SDLC Vs Scrum Methodology – A Comparative. *International Journal of Emerging Technology and Advanced Engineering*, 1-2.

Mesquida, A. L., Mas, A., & Amen, E. (2019). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *Revista Española de Innovación*, 2.

Microsoft. (21 de Marzo de 2019). *Microsoft Security Development Lifecycle*. Obtenido de https://www.microsoft.com/en-us/securityengineering/sdl/

MinTIC. (25 de Abril de 2016). *Procedimientos De Seguridad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

OECD. (23 de Septiembre de 2002). *Organisation for Economic Co-operation and Development.* Obtenido de http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

OWASP. (3 de Marzo de 2007). *Open Web Application Security Project.* Obtenido de https://www.owasp.org/images/1/18/Owasp-training-samm-greece.pdf

OWASP. (12 de Diciembre de 2017). *Open Web Application Security Project.* Obtenido de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Prey Nation. (3 de Diciembre de 2018). *24 Estadísticas de Seguridad Informática que Importan en el 2019*. Obtenido de https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

VIEITES, Á. G. (2014). *AUDITORÍA DE SEGURIDAD INFORMÁTICA.* Madrid: RA-SA.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security Cherdantseva.* Boston: Course Technology.