risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 21/11/2017
Aceitação/Acceptance: 12/02/2018

Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana

Oswaldo Díaz [1], Mirna Muñoz[2]

oswaldo.diaz@inegi.org.mx, mirna.munoz@cimat.mx

[1] Grupo de Ingeniería de Sistemas, Instituto Nacional de Estadística y Geografía (INEGI) Av. Héroe de Nacozari no 2301, Aguascalientes, México.

[2] Centro de Investigación en Matemáticas – Unidad Zacatecas, 98068, Zacatecas, Zacatecas, México

DOI: 10.17013/risti.26.43–53

Resumen: En México la importancia de los Centros de Datos ha incrementado el interés en enfoques DevOps (Developer Operations). Implementar un enfoque DevOps en Centros de Datos permite establecer estrategias para la gestión de operaciones automatizadas, ingeniería de software y aseguramiento de la calidad. Este artículo presenta la implementación de un enfoque evolucionado de DevOps nombrado como DevSecOps+ Risk Management, que además de lo antes mencionado permite establecer estrategias para gestionar la seguridad informática y gestión de riesgos. El artículo incluye tanto la descripción del enfoque, cómo su implementación para el desarrollo de proyectos en un centro de datos de una empresa gubernamental mexicana. Los resultados han demostrado que este enfoque apoya en la finalización exitosa de proyectos críticos de la organización.

Palabras-clave: DevOps, Ingeniería de Software, Control de Calidad, Infraestructura Tecnológica, Centro de Datos, Seguridad informatica, Gestión de Riesgos.

Implementation of a DevSecOps + Risk Management in a Data Center of a Mexican Organization

Abstract: In Mexico the importance of Data Centers has increased the interest on DevOps (Developer Operations) approaches. The implementation of a DevOps approach in a Data Center allows establishing strategies for managing automatize operations, software engineering and quality assurance. This paper presents the implementation of an evolve approach of DevOps named as DevSecOps + Risk Management, which in addition to the above mentioned allows establishing strategies for managing information security and Risk Management. The paper includes both, the description of the approach as well as its implementation for developing projects in a Data Center in a large government organization of Mexico. The results have demonstrated that this approach support the successful closure of critical projects within the organization.

Keywords*:* DevOps, DevSecOps, Software engineering, quality control, Technology infrastructure, Data Centers, Informatics security, Risk Management.

1. Introducción

En los últimos años los Centros de datos han evolucionado significativamente en todo el mundo y México no es la excepción, ya de acuerdo a (Judge, 2016) es un país que cuenta con alrededor del 20% de los Centro de Datos existentes en América Latina. Estos Centros de Datos tienen necesidades específicas al ser los que albergan los proyectos considerados "de misión crítica" para las organizaciones.

En este contexto, surge lo que se conoce como "DevOps", que es una mezcla de dos palabras, desarrolladores y Operaciones que surge de la necesidad de construir sistemas de software reduciendo el tiempo de entrega del mercado, y presentando una solución al problema de optimización del ciclo de vida de entrega (Virmani, 2015). La importancia de DevOps incrementa cada vez más, ya que se enfoca en reforzar la cooperación entre el profesional de TI y los desarrolladores de software para reducir el tiempo de entrega del proyecto, permitiendo establecer estrategias para la gestión de flujos de trabajo, control de versiones y entrega de productos de software.

Una de las empresas que cuentan con un Centro de Datos en México es Instituto Nacional de Estadística y Geografía (INEGI), que es el instituto encargado de las siguientes actividades: (1) regular y coordinar el sistema de información estadística y geográfica; (2) llevar a cabo censos nacionales; (3) integrar el sistema de cuentas nacionales y elaborar los índices nacionales de precios al productor y (4) ser la agencia cartográfica nacional de México.

El Centro de Datos de INEGI, por lo tanto desarrolla sistemas de información en múltiples tecnologías como son para internet, dispositivos móviles y servicios en la nube, entre otras; con la finalidad de diseminar información estadística y geográfica que permitan al gobierno mexicano la toma de decisiones. Para lograr el desarrollo de estos proyectos con éxito, INEGI decide implementar DevOps como una medida para el logro de los objetivos del centro de datos (Muñoz & Díaz, 2016). Sin embargo, después de su implementación y análisis de sus resultados, decidieron reforzar este enfoque con seguridad informática y gestión de riesgos surgiendo DevSecOps+Risk Management (Díaz & Muñoz, 2017).

El objetivo de este artículo es presentar cómo fue reforzado el enfoque DevOps con seguridad informática y gestión de riesgos, así como el análisis de los resultados de su implementación para el desarrollo de proyectos de misión crítica Centro de Datos de INEGI.

El artículo está organizado de la siguiente forma: en la sección 2 se describen conceptos clave. La Sección 3 presenta una visión global del enfoque. La Sección 4 describe cómo se refuerza el enfoque con seguridad informática y gestión de riesgos. En la sección 5 se presenta el análisis de los resultados de su implementación y, finalmente, la sección 6 presenta las conclusiones y trabajo fututo.

2. Conceptos clave

En esta sección se definen los conceptos considerados clave para comprender el contexto de este artículo.

- *Centro de Datos*: es una instalación dentro de una organización encargada de centralizar las operaciones el equipo de TI enfocando en el almacenamiento,

administración y despliegue de la información de la organización. (Robertazzi M., 2012).

- *DevOps*: término compuesto de dos palabras *desarrollo* y *operaciones*, y surge de la necesidad de construir sistemas de software optimizando el ciclo de desarrollo del producto hasta su entrega (Virmani, 2015).
- *Seguridad de información:* se refiere al uso de estándares, procedimientos, métodos y técnicas enfocadas en lograr sistemas de información seguros y confiables, teniendo en cuenta la integridad, confidencialidad y disponibilidad de la información (Betancourt & Valverde, 2015).
- *Gestión de Riesgos:* comprende la identificación de problemas potenciales antes de que éstos ocurran, tal que se pueden planificar actividades para gestionar los riesgos, las cuales pueden ser invocadas a través de todo el ciclo de desarrollo de un producto o proyecto, tal que puedan ser mitigados los impactos adversos que impidan el logro de los objetivos (CMMI Product Team, 2010).

3. Enfoque DevSecOps + Risk Management

3.1. Antecedentes

El enfoque DevSecOps+ Risk Management surge como una evolución del enfoque DevOps para cubrir las necesidades de proyectos de misión crítica alojados en el centro de datos.

INEGI toma la decisión de evolucionar el enfoque DevOps (Muñoz & Díaz, 2016) implementado para cubrir dos principales necesidades:

1. Reducir las vulnerabilidades que ponen a la información estadística y geográfica en riesgo de robo o secuestro
2. Gestionar los riesgos a través de todo el ciclo de desarrollo del proyecto / producto para reducir eventualidades lógicas o físicas.

Este nuevo enfoque, por lo tanto, se fortalece con seguridad informática y gestión de riesgos como a continuación se describe (Díaz & Muñoz, 2017):

1. *Seguridad Informática*: se ocupa de diseñar normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable, tomando en cuenta la integridad, confidencialidad y disponibilidad de la información alojada en un centro de datos de la organización o empresa.
2. *Gestión de Riesgos*: consiste en aumentar la probabilidad y el impacto de los eventos positivos (ejemplo: más usuarios concurrentes), y disminuir la probabilidad y el impacto de los eventos negativos (ejemplo: eventualidades las cuales el usuario experimente interrupción en el servicio) del proyecto orientado a tecnologías de información implementado en la organización o empresa.

3.2. Fases del enfoque

El enfoque DevSecOps+ Risk Management se compone de 4 fases, todas llevadas cabo dentro de un marco de gestión de riesgos, las cuales se muestran en la Figura 1 y se describen a continuación.

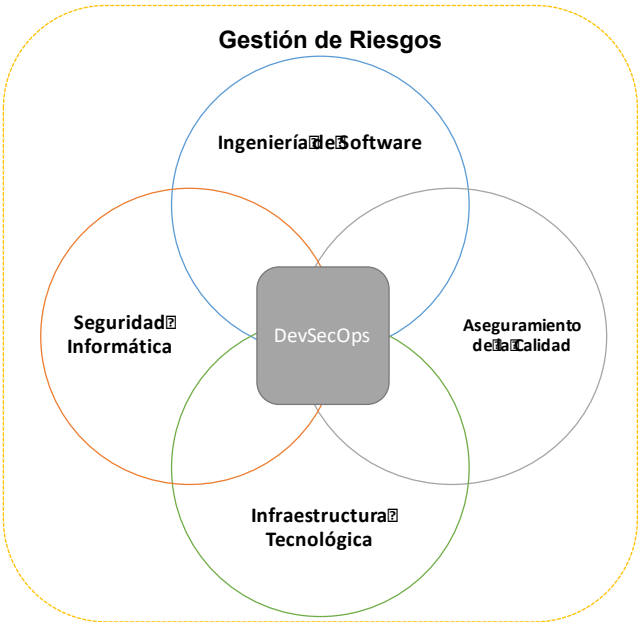

Figura 1 – Enfoque DevSecOps + Risk Management fases

1. Ingeniería de Software*:* esta fase se enfoca en el desarrollo de software. Para lograr el desarrollo de software se usa la metodología Scrum (Gloger, 2014). como una solución para eliminar liberaciones lentas.

   El flujo de trabajo de Scrum definido en el enfoque contiene 6 fases y 4 equipos como se muestran en las Tablas 1 y 2.

Fase	Descripción	Equipo Responsable
Diseño	En esta fase se definen las reglas de cumplimiento y un cronograma con fechas de compromisos, de acuerdo con los requisitos del proceso a ser automatizado para publicarlos en un ambiente controlado por TI.	Equipo de desarrollo
Desarrollo	En esta fase se construye el proceso automatizado basado en prácticas de ingeniería de software y teniendo en cuenta el hardware definido como parte del "Diseño", de manera que un avance significativo llamado "Beta" se entrega para interactuar con el proceso de prueba.	Equipo de desarrollo
Pruebas	En esta fase se realiza un plan estratégico y de pruebas específicas con base en los requisitos del proyecto y teniendo en cuenta la versión "Beta" y la retroalimentación de todas las eventualidades detectadas.	Equipo de control de calidad
Despliegue	En esta fase se publica y controla la versión del proyecto denominada "Release" en un entorno de TI controlado.	Equipo de gestión de implementación

Fase	Descripción	Equipo Responsable
Retrospectiva	En esta fase se realiza una evaluación del análisis de riesgos basado en las eventualidades detectadas en la fase de pruebas y toma las decisiones para mitigar o enfrentar los riesgos	Equipo de desarrollo
Recolección de requisitos y retroalimentación	En esta fase se realiza una reunión interactiva cara a cara, para determinar el desempeño del proyecto, tanto de progreso como de demora, con el fin de acelerar los procesos y procedimientos para que el calendario de entrega se pueda cumplir	Equipo de revisión y control

Tabla 1 – Fases Scrum definidas

Fase	Descripción	Roles involucrados
Equipo de desarrollo	Equipo responsable del desarrollo de la arquitectura de la estrategia y de la arquitectura de la base de datos.	Ingenieros de software y Arquitectos para el modelado de los daos con base al requerimiento del proceso del negocio.
Equipo de revisión y control del sistema	Equipo responsable de la integración continua, la gestión de versiones y el control de repositorio de versiones tomando en cuenta la estrategia de proceso y calendario de actividades.	Revisores de la integridad en la informacion con base a normas y cumplimientos de la organización o empresa
Equipo de control de calidad	Equipo responsable de llevar a cabo las pruebas de integración, seguimiento de soluciones a problemas en eventualidades de seguridad y percepción de servicio orientado al usuario final y la conformación de base de datos de conocimiento en base a incidencias.	Arquitectos en tecnologias de informacion revisores del control de calidad con base a niveles de servicios en la operación.
Equipo de gestión en la implementación	Equipo responsable de administrar y mantener el funcionamiento de la infraestructura de los sistemas operativos; sistemas de almacenamiento, sistemas de procesamiento, sistemas de respaldos y sistemas de comunicaciones; que habilitan la publicación de los proyectos en el ambiente de producción.	Ingenieros de procesos con base en los roles [Webmaster, SysAdmin, DBA entre otros]

Tabla 2 – Equipos definidos

Cabe mencionar que puede formarse un solo equipo de trabajo que mediante roles desempeñe las funciones descritas en los diferentes equipos.

2. *Fase de Control de Calidad:* esta fase cubre temas relacionados con la gobernanza, construcción, verificación e implementación. La fase contiene 4 proceso definidos con base en OWASP Software Assurance Maturity Model (Owasp SAMM) (Curphey & Groves 2015). El objetivo de cada proceso se describe a continuación.

- *Proceso de gobernanza*, permite que se definan indicadores cuantitativos y cualitativos basados en las políticas y controles de cumplimiento, de manera que se generen tableros de control para la toma de decisiones.

- Proceso de construcción, permite que establezcan los niveles de seguridad teniendo en cuenta las políticas internas y externas basadas en los estándares organizativos, así como las tendencias tecnológicas en hardware y software en los que la organización tenga madurez, de modo que la adopción de estos no implica un retraso en la ejecución de los proyectos de la organización
- Proceso de verificación, permite que se establezca un plan de pruebas en conjunto con el líder del equipo y tener en cuenta los aspectos del proyecto con respecto a las mejores prácticas del motor de código y el perfil de rendimiento enfocado en el cumplimiento de las líneas base establecidas por la organización Modelo-Vista-controlador (MVC).
- Proceso de Implementación, permite que se establezcan entornos tolerantes a fallos para la publicación de los proyectos, las vulnerabilidades gestión y excepciones basadas en las métricas de seguridad informática, la realización de endurecimiento 3 capas de nivel para los componentes que intervienen en el proyecto, tener un seguimiento de los procesos, recursos y del personal involucrado en la organización.

3. *Fase de Infraestructura Tecnológica para la Operación:* esta fase se enfoca en el cuidado de la infraestructura para el procesamiento de visualización, almacenamiento de la información, los requisitos específicos y estratégicos de transferencia de información. Su objetivo es difundir los productos o servicios generados de una manera segura y oportuna.

   Para lograr una administración y control de riesgos en la infraestructura del proyecto se establecen: (1) entornos controlados para escenarios de desarrollo, preproducción y producción que tienen como objetivo separar las aplicaciones y las bases de datos con el fin de reducir el riesgo y; (2) niveles de servicios mediante la implementación de prácticas ITIL (ITIL/OGC, 2010), que permite establecer indicadores cualitativos y cuantitativos para generar información permitiendo la toma de decisiones basada en las mejores prácticas de tal forma para la gestión de la infraestructura de TI.

   Las fases de Seguridad Informática y gestión de riesgos se describen en la siguiente sección.

4. Seguridad informática y Gestión de Riesgos

4.1. Seguridad Informática

La seguridad informática se refiere al uso de modelos, marcos de trabajo, estándares, metodologías, normas, técnicas, herramientas y estructuras organizacionales encaminadas a proteger la información en sus diferentes formas y estados (Muñoz & Rivas, 2015); (Mejia & Ramírez, 2016). En enfoque DevSecOps+Risk Management esta fase se enfoca en el robustecimiento del enfoque para proteger la información

Para lograr lo antes menciona, se define un decálogo que se basa en la adaptación del ISO/IEC 27005 (UNAM CERT, 2016) de acuerdo la experiencia y flujo de trabajo Instituto Nacional de Estadística y Geografía. Por lo que, tomando en cuenta la lógica del

negocio y con base en la misión y visión, gestiona la información que involucra la captura, integración, procesamiento, validación y difusión de la información. El decálogo se lista a continuación:

1. Establecer un programa de gestión de riesgos de la información formal que contenga políticas, procesos y soluciones, en áreas donde no se está realizando, permitiendo automatizar la recolección centralizada de riesgos y presentación de información.
2. Establecer una estrategia para realizar una analítica de datos de las bitácoras correlacionadas con eventos – reportes – de eventualidades reportadas.
3. Establecer procesos y procedimientos para evaluar periódicamente el conocimiento de los usuarios frente a vectores de ataques.
4. Implementar y administrar, un proceso formal de gestión de administración - reparación a eventualidades reportadas, inventario y manejo de software para servidores donde estén alojados los proyectos de información estratégica.
5. Implementar y administrar, políticas y procedimientos integrales para la gestión de vulnerabilidades, de preferencia en un laboratorio para pruebas de penetración externas con herramientas especializadas.
6. Establecer procesos de administración y gestión para la protección contra códigos maliciosos en la transferencia de información.
7. Establecer e Implementar una política, estándares y procesos para el hardening1 de servidores físicos y virtuales.
8. Definición de un programa que incluya procesos, documentación y preparación del personal para evitar la fuga de datos, además de la implementación de un programa corporativo para la prevención de fuga de la información que incluya políticas, procesos, flujos de trabajo, soluciones y personal capacitado.
9. Implementar herramientas para automatizar políticas de seguridad actualizadas, con base a reportes en líneas de cumplimiento.
10. Implementar un plan de respuesta a incidentes, incluyendo la estructura del equipo, sus roles y responsabilidades, definir responsables y empezar a documentar procesos con base a la estrategia para la continuidad de operaciones y Plan de recuperación en caso de desastres.

4.2. Gestión de Riesgos

Esta fase cubre se establece con base en el estándar ISO/ IEC 27005 (UNAM CERT, 2016) y la Metodología de análisis de riesgos OCTAVE ALLEGRO (UNAM CERT, 2016) como a continuación se describe:

Marco de trabajo con 8 actividades con base ISO/IEC 27005:

- Establecimiento del contexto de los servicios.
- Identificación del riesgo en los servicios.
- Estimación del riesgo con indicadores cuantitativos y cualitativos.
- Valoración del riesgo base a métricas de control.
- Tratamiento del riesgo en colaboración con las áreas involucradas.
- Aceptación del riesgo de forma conjunta con las áreas involucradas.
- Comunicación del riesgo – afectación y recuperación.

- Monitoreo y revisión del riesgo, así como también, su registro en una base de conocimientos para aprender de las eventualidades.

Metodología de análisis de riesgos de 4 fases con base en OCTAVE Allegro:

- *Establecimiento de controles*: establecer criterios de las métricas de riesgo para cada servicio–proceso del proyecto.
- *Perfil de activos*: desarrollar el perfil de los activos de información e identificar los contenedores de los activos de información para su resguardo e integridad.
- *Identificación de amenazas*: identificar amenazar en las áreas de preocupación, tomando en cuenta escenarios de amenaza internas y externas.
- *Identificación y mitigación de riesgos*: análizar eventualidades reportadas en el servicio con base a la selección de metodologías para la mitigación.

5. Análisis de los resultados de su implementación

Esta sección muestra la implementación del enfoque DevSecOps + Risk Management para un Centro de Datos de una organización Mexicana.

Un centro de datos es una instalación clave en una organizaciones porque aloja los sistemas más críticos de la organización, por lo que es de vital importancia para la continuidad de la operación cotidiana (Kant & Mohapatra, 2004), razón por la cual tienen una alta prioridad tanto la fiabilidad como la seguridad (Callou et al., 2014).

De acuerdo a (Callou et al., 2014), aunque los diseños de centros de datos son únicos, pueden clasificarse de acuerdo con su dominio de aplicación en dos tipos: orientados a internet y empresariales o internos.

El centro de datos de esta empresa gubernamental Mexicana es de tipo empresarial o interno, que son aquellos que dan soporte a más aplicaciones que van desde aplicaciones estándares hasta aplicaciones personalizadas, y, tienen pocos usuarios bien conocidos (Callou et al., 2014).

La empresa gubernamental Mecicana es el Instituto Nacional de Estadística y Geografía (INEGI). Como parte de las actividades realizadas en el instituto, fue necesario implementar una estrategia para controlar la operación de los proyectos: Índice Nacional de Precios, México en Cifras, Sistema Nacional de Información Estadística y Geográfica, Banco de Información Económica, Mapa Digital de México, entre otros, considerados de misión crítica, porque tiene la característica de requerir disponibilidad de acceso por internet las 24 horas, los 365 días de año y con tolerancia a fallas, permitiendo que el usuario no experimente interrupciones en el servicio.

El enfoque DevSecOps + Risk Management permitió establecer un entorno de colaboración basado en las normas de ingeniería de software; las mejores prácticas de las TIC's y la infraestructura, implementando un ambiente controlado en la operación, obteniendo beneficios para administrar la operación en centros de datos en puntos geográficos diferentes, con esquemas de seguridad y administración de riesgos.

La estrategia de la infraestrctura mediante la implementación del enfoque DevSecOps + Risk Management se muestra en la Figura 2 y se describe a continuación.

ROL \ Actividades	**Fase de ingeniería de software**	**Fase de control de calidad,**	**Fase Infraestructura tecnológica**	**Fases de Seguridad informática y de Gestión de Riesgos**
Roles	*Líderes de proyecto y desarrolladores.* *Administradores de servidores de aplicaciones.* *Administradores de sistema operativo.* *Arquitectos DBA modeladores de base de datos.*	*Establecer un equipo con el rol de Beta Tester, estas personas son responsables de aplicar las mejores prácticas en seguridad, escalabilidad, percepción y experiencia de usuario, tomando en cuenta entregar el informe de control de calidad.*	*Establecer la siguiente infraestructura para el desarrollo e implementación de proyecto:* *servidores de aplicaciones* *servidor – Clúster Base de datos (nodos) proceso* *en paralelo y tolerante a fallas.* *servidor de almacenamiento y copia de seguridad [con tecnología SAN y NAS]*	*Verificación de los 10 puntos mencionados en el apartado (fase de seguridad informática) tomando en cuenta el mapa de servicios de proyecto con base a procesos, personas y tecnología.* *Elaboración de matriz de riesgo personalizada del proyecto con puntos de control y actividades para remediar eventualidades.*
Puntos de revisión de riesgos	*Estrategias para cubrir los roles y no detener productividad.* *Adaptabilidad y tolerancia a fallas en la operación.* *Retroalimentación del equipo de trabajo involucrado en esta fase.*	*Seguimiento y control en base de datos de conocimientos referentes a las eventualidades (excepciones) reportadas en el flujo del proyecto, tomando en cuenta todos los módulos.* *Retroalimentación del equipo de trabajo involucrado en esta fase.*	*Seguimiento y control en las bases de datos de conocimientos tomando en cuenta las bitácoras del hardware y software involucrado en la operación, con la finalidad de tener elementos cuantitativos y cualitativos para la toma de decisiones en controles de cambios, incidencias y problemas en el centro de datos.* *Retroalimentación del equipo de trabajo involucrado en esta fase.*	*Documentación de la continuidad operativa del proyecto con base al proceso.* *Retroalimentación del equipo de trabajo involucrado en esta fase.*

Tabla 3 – Estrategia y Equipos de trabajo definidos implementando el enfoque DevSecOps + Risk Management

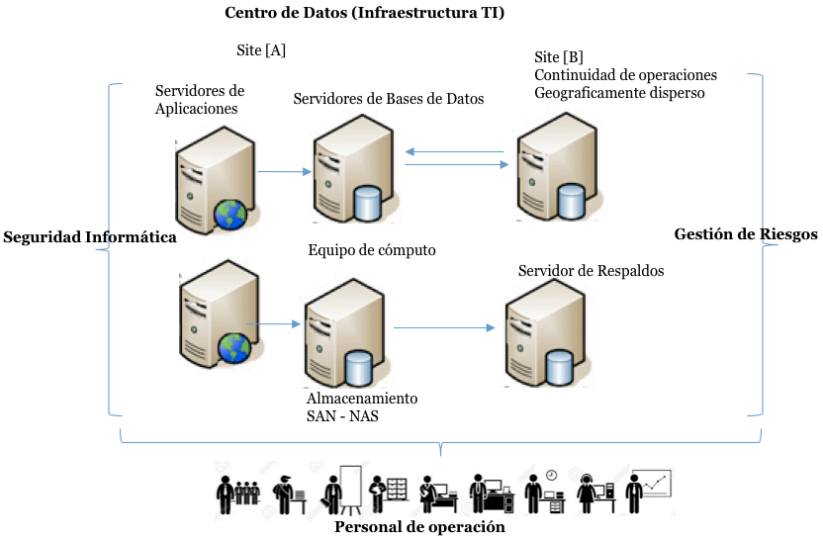

Figura 2 – Ejemplo Infraestructura de un Centro de Datos

Dentro de las fases descritas para la estrategia DevSecOps + Risk Management el equipo de trabajo colaborativo para mantener la operación se muestra en la Tabla 3.

6. Conclusiones y trabajo futuro

Hoy en día la importancia de los Centros de Datos en diferentes organizaciones se está haciendo más evidente, debido a que albergan los sistemas de misión crítica, por lo tanto, contar con estrategias que permitan lograr flujos de implementación y entrega efectivos es una creciente necesidad. Además, es necesario asegurar una alta disponibilidad y continuidad de la operación en estos centros.

En este contexto, el enfoque DevSecOps + Risk Management se presenta como una solución efectiva, permitiendo el control de la operación de las áreas involucradas en el desarrollo de un proyecto. Este enfoque ha permitido en INEGI generar valor agregado en los procesos de los proyectos de misión crítica, contemplando el ciclo de vida con niveles de servicios adecuados, manteniendo la continuidad operativa y permitiendo que el riesgo sea analizado cuantitativa y cualitativamente.

Referencias

Betancourt, D., & Valverde, D. (2015). Implementación del SGSI (ISO/IEC 27001:2013). In *Talleres y líneas de especialización del Congreso de Seguridad en Cómputo 2015*. Mexico: UNAM.

Callou, G., Ferreira, J., Maciel, P. Tutsch, D., & Souza, R. (2014). An Integrated Modeling Approach to Evaluate and Optimize Data Center Sustainability, Dependability and Cost. *Energies open access*, 2014 (7), 238–277.

CMMI Product Team. (2010). *CMMI for development v1.3 Software Engineering Institute Technical Report CMU/SEI-2010-TR-033*.

Curphey, M., & Groves, D. (2015). *OWASP-SAMM (Open Web Application Security Project - Software Assurance Maturity Model) a Guide to building security into software development Version 1.0*.

Diaz, O., & Muñoz, M. (2017). Reinforcing DevOps approach with security and Risk Management: an experience of implementing it in a Data Center of a Mexican Organization. In Proceedings of the *6th International Conference in Software Process Improvement*. Zacatecas, Mexico: IEEE.

Gloger, B. (2014). Scrum checklist. All meetings.

ITIL/OGC. (2010). *Scope and Development Plan Copyright TSO 2010*. Retrived from: www.ogc.gov.uk

Judge, P., (2016). Datacenter Dynamics: Market Focus Latin America. *datacenterdynamics.com*, 2016(14).

Kant, K., & Mohapatra, P. (2004). Internet Data Centers. Computer. *IEEE Computer Society*, 37(11) , 35–37.

Mejia, J., & Ramírez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (17), 1–15.

Muñoz, M., & Díaz, O. (2017). DevOps: Foundations and Its Utilization in Data Center. In: Marx Gómez J., Mora M., Raisinghani M., Nebel W., O'Connor R. (eds). *Engineering and Management of Data Centers. Service Science: Research and Innovations in the Service Economy*. Berlin: Springer, Cham.

Muñoz, M. & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E3) 1–15.

Robertazzi, M.T. (2012). Data Centers. *In Basics of Computer Networking*. In: *SpringerBriefs in Electrical and Computer Engineering* (pp 69-72). Berlin: Springer.

UNAM CERT. (2016). *SGSI base ISO/IEC 27001:2013, Serie 27000 ,Anexo SL and ISO/IEC 27005, Manual de referencia*.

Virmani, M. (2015). Understanding DevOps & Bridging the gap form continuous integration to continuous delivery. In Proceedings of *Fifth international conference on Innovative Computing Technology* (pp. 78–82). Galicia, España: IEEE.