Asunción 13 de diciembre de 2023

Dirección General de Ciberseguridad
y Protección de la Información - MITIC
Presente

En el marco de la "CONSULTORÍA PARA EL SERVICIO DE IMPLEMENTACIÓN DEVSECOPS EN MITIC", se remite dos copias del informe final de implementación correspondiente al sexto entregable de la mencionada consultoría.

Se pone a su consideración el informe del entregable 6 a fin de que pueda evaluar si cumple con los requerimientos.

Sin otro particular, atentamente.

Leticia Pfannl

Gerente General Sodep S.A.

SODEP S.A.
Software Development & Products

CONSULTORÍA PARA EL SERVICIO DE IMPLEMENTACIÓN DE DEVSECOPS

E06 – Informe de Implementación final

MITIC

Diciembre 2023

Nelson Canatta
SODEP S.A.

1. Introducción 3
2. Resumen general de las mejoras alcanzadas 4
3. Resumen, documentación y/o evidencia 5
3. 1 Durante el desarrollo de los productos de software nuevos acordados. 5
3. 2 Proceso de migración de stack tecnológico 6
4. Medición de las métricas al finalizar la implementación en los proyectos seleccionados 8
4.1. OWASP SAMM 8
5. Recomendaciones 10
6. Conclusión 11

Nelson Canatta
SODEP S.A.

E06 - INFORME DE IMPLEMENTACIÓN FINAL

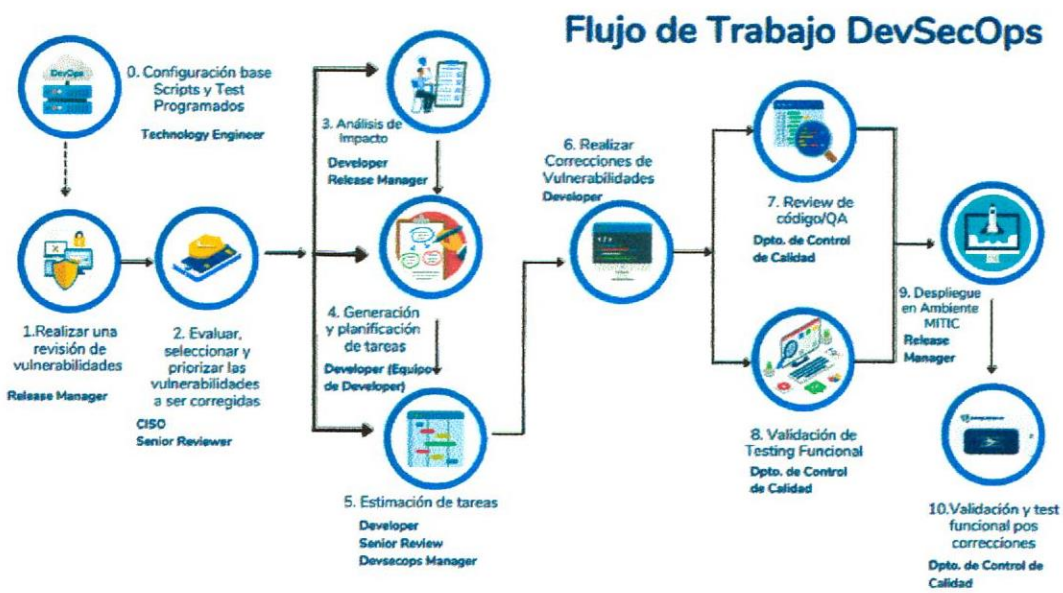
CONSULTORÍA PARA LA IMPLEMENTACIÓN DE DEVSECOPS

1. Introducción

El presente documento constituye el entregable final de la consultoría de Implementación de DevSecOps en MITIC. La consultoría se enfocó en iniciar prácticas efectivas de DevSecOps en una selección de proyectos. Los hitos clave incluyeron la presentación del plan de trabajo (Entregable 01), el diagnóstico de la adopción de DevSecOps según el Modelo SAMM (Entregable 02) y la entrega de recomendaciones para mejorar los procesos.

Durante el proceso, se identificaron roles, se propusieron cambios y se sugirieron herramientas para automatizar procesos, facilitando la implementación de DevSecOps (Entregable 03). La fase de implementación (Entregable 04) se centró en proyectos específicos como Portal PY y Portal AIP, abarcando tanto los proyectos del backend como del frontend, totalizando de esta manera 4 proyectos abarcados.

Durante el proceso de implementación se consideró el flujo de procesos definido previamente junto con herramientas específicas para garantizar medidas de seguridad y agilidad en el desarrollo. Se muestra a continuación el flujo de proceso.



El entregable 05 consistió en la transferencia de conocimientos para que los miembros designados del equipo del MITIC pudieran intervenir en los procesos de DevSecOps por sí mismos.

Este documento presenta un resumen general de las mejoras alcanzadas, evidencias de las mismas y documentación respaldatoria. Además presenta una comparativa el Modelo SAMM,

Canatta
S.A.

SODEP S.A.
Software Development & Products

luego de la implementación de DevSecOps en los proyectos mencionados, de modo a poder tener claridad en los aspectos mencionados en esta primera iteración.

Como apartado final, se mencionan algunas recomendaciones y conclusiones generales.

2. Resumen general de las mejoras alcanzadas

Una de las conclusiones del diagnóstico inicial realizado durante esta consultoría destacó la calidad técnica disponible brindada por los funcionarios del MITIC, así como también el constante exceso de tareas repetitivas a las que se tienen que enfrentar. Este escenario se consideró propicio para la inclusión de DevSecOps como paradigma principal de producción de un software más seguro. Los resultados en este proceso pueden dividirse conceptualmente en tres grandes áreas, sabiendo que, en la implementación, están solapadas y complementadas.

Cultura. La inclusión de una nueva metodología para el enfoque de desarrollo demostró ser exitosa no solamente en términos estrictamente prácticos sino que evidenció que el MITIC está preparado para incorporar los conceptos y la cultura asociadas a esta metodología. Las ventajas obtenidas por la adherencia a DevOps (y su extensión a DevSecOps) fueron recibidas positivamente.

Procesos. Los procesos contemplados ahora ya están disponibles para todos los involucrados y los ciclos de desarrollo, entrega y puesta en producción están completamente articulados y documentados suficientemente. Cada paso tiene una descripción detallada y la participación de cada uno de los actores también está explícitamente descrita, así como las entradas (inputs) y salidas (outputs) de cada etapa.

Herramientas. Existen en el mercado herramientas que soportan la mayoría de las tareas relacionadas con DevSecOps. Se analizaron las principales plataformas de desarrollo utilizadas en el MITIC y se seleccionaron las más adecuadas para facilitar el seguimiento del proceso de desarrollo, así como las más documentadas y confiables. El conjunto seleccionado se ha probado exitosamente tanto en las pruebas iniciales, así como durante la transferencia de conocimiento.

Nelson Canatta
SODEP S.A.

3. Resumen, documentación y/o evidencia

3. 1 Durante el desarrollo de los productos de software nuevos acordados.

El proceso de desarrollo, acompañado de la Metodología DevSecOps permite tener evidencias muy concretas acerca de las bondades que emergen una vez que se comienzan a utilizar las herramientas y se cierran los primeros ciclos de entrega. Estos son algunos resultados concretos que quedan como recursos disponibles para el MITIC.

- Scripts automatizados para la detección de vulnerabilidades en las tecnologías de los proyectos seleccionados
- Videos que muestran el enfoque general que facilita la interpretación y corrección del código que podría resultar en amenazas a la seguridad.
- Roles y responsabilidades bien delimitadas con funciones específicas en cada paso. Cada actor cuenta con uno o más roles que permiten identificar su contribución o aporte en los diferentes pasos.Existen roles transversales a todo el proceso. El acompañamiento de las transferencias se realizaron a los roles involucrados y las mismas se repitieron cuando la situación permitía un seguimiento más personalizado a los nuevos integrantes del equipo a medida que se fueron incorporando.
- Replicabilidad de una gran parte de la metodología para la inclusión de nuevos proyectos.
- Visión general de los ciclos de entrega que pueden ser la base para la generación de informes a nivel directivo o gerencial.

Los puntos mencionados se encuentran detallados en los entregables 4[1] y 5[2] respectivamente. El entregable número 4 contiene documentación detallada sobre las configuraciones, herramientas y scripts automatizados utilizados para la detección de vulnerabilidades, en las secciones 3 y 4 del correspondiente entregable.

En cuanto al entregable número 5, se documentan las sesiones de capacitación llevadas a cabo para los diferentes funcionarios de MITIC. Estas sesiones se ajustaron a los roles específicos involucrados en el proceso y se dispone tanto de grabaciones como de presentaciones de cada sesión.

Se ha compartido un directorio que contiene toda la información de las capacitaciones y los entregables en formato digital. Este recurso está disponible como una fuente de conocimiento para aquellos roles que serán incorporados para fortalecer los procesos institucionales.

[1] https://drive.google.com/drive/folders/1EW9qCejAPuUaPEmpJ-RoLlyFiiokILAW

[2] https://drive.google.com/drive/folders/11pbeAdqOyOPrq9CmDr_orsrq6ViO-NH7

SODEP S.A. Software Development & Products

Nelson Canatta
SODEP S.A.

3. 2 Proceso de migración de stack tecnológico

Durante el proceso de implantación de la infraestructura de MITIC, se llevaron a cabo instalaciones de herramientas clave y configuraciones detalladas en los servidores designados. El documento respaldatorio presenta un resumen detallado de esta actividad, incluyendo evidencia, especificaciones técnicas y herramientas instaladas para el proceso DevSecOps y el entorno de ejecución.

En la infraestructura de MITIC, se desplegaron tres servidores, cada uno con especificaciones distintas para atender a diferentes propósitos dentro de la consultoría.

1. MITIC-Proyectos: Un servidor destinado al despliegue de proyectos.
2. MITIC-Monitoreo: Un servidor que albergó Jenkins y Sonarqube.
3. MITIC-Repo: Servidor diseñado para el repositorio de los proyectos.

Además, se implementaron herramientas específicas tanto para DevSecOps como para el entorno de ejecución. En el ámbito de DevSecOps se instalaron herramientas como Jenkins, Sonarqube, Trivy, Postgres, Node, Npm y Gitlab siendo esta última preinstalada por el equipo de MITIC, y configurada finalmente por el equipo de SODEP. Respecto al entorno de ejecución se incluyeron herramientas como el Wildfly, Nginx, Postgres y Redis.

Los Jobs configurados para los proyectos seleccionados abarcaron los siguientes proyectos:

1. Para el proyecto Portal PY,
    a. Backend: Jobs de análisis del Sonarqube, jobs de análisis de Trivy y jobs de despliegue del proyecto.
    b. Frontend: Jobs de análisis del Sonarqube, jobs de análisis de NPM Audit y NPM-Depchek, y por último jobs de despliegue del proyecto.
2. Para el Proyecto de Portal AIP,
    a. Backend: Jobs de análisis del Sonarqube, jobs de análisis del Trivy y el jobs de despliegue del proyecto.
    b. Frontend: Jobs de análisis del Sonarqube, jobs de análisis de NPM y el jobs de despliegue del proyecto.

Para una descripción y detalles más exhaustivos de las configuraciones e implantaciones se puede consultar el entregable Nro. 4, en la sección 3 y 4 respectivamente.

Como punto importante de este apartado se puede destacar que el proceso de implantación y configuración de DevSecOps en la infraestructura de MITIC ha sido exitoso. La instalación meticulosa de herramientas clave en servidores específicos ha culminado en un entorno robusto y funcional.

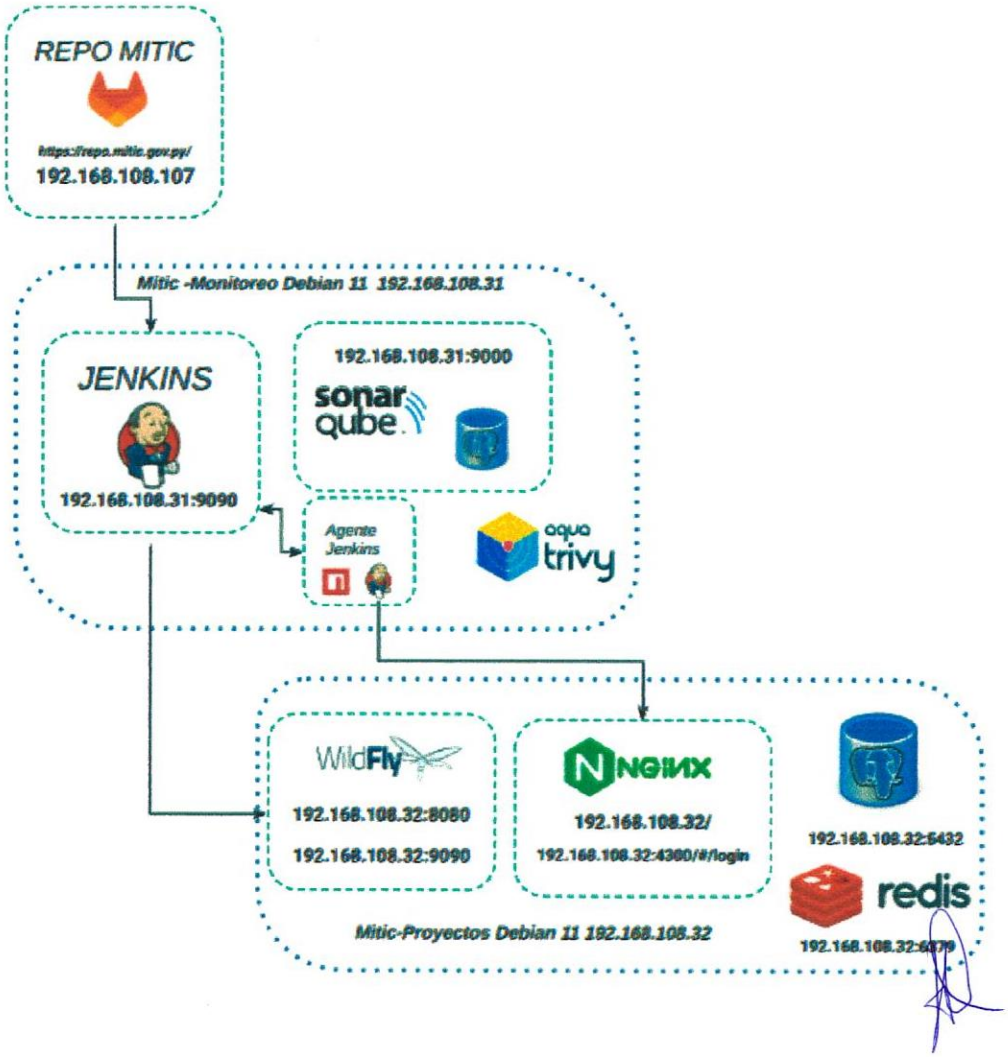
La distribución eficiente de recursos en los servidores, cada uno diseñado para un propósito específico, ha demostrado una planificación cuidadosa y una ejecución precisa.

La documentación remitida en el entregable E04 respalda este éxito, mostrando una visión completa de las configuraciones, herramientas y trabajos implementados para los diferentes proyectos enfocados y comprometidos en esta consultoría.

Nelson Canatta
SODEP S.A.

SODEP S.A.
Software Development & Products

Se muestra a continuación el mapa de los servidores, que ilustra la distribución de las herramientas instaladas en los puntos que menciona el apartado.



SODEP S.A. Software Development & Products

Nelson Canatta
SODEP S.A.

4. Medición de las métricas al finalizar la implementación en los proyectos seleccionados

Después de implementar DevSecOps y evaluar los procesos de desarrollo de software del MITIC, se destacan los siguientes puntos clave:

- La adopción de procesos ágiles alineados con DevOps es factible cuando se asignan roles claves y se prioriza adecuadamente la metodología.
- Aunque las primeras etapas no generen resultados inmediatos, representan una base fundamental. Tras la implementación, se observan mejoras notables, incluyendo procesos controlados, automatizados y monitorizados con fiabilidad.
- La implementación de procesos DevOps no implica directamente la incorporación inmediata de la seguridad (DevSecOps). Este proceso no se manifiesta de manera inmediata, sino que más bien representa una evolución gradual. Sin embargo representa el camino ideal para cumplir con los estándares establecidos dentro del proceso de mejora continua.
- La contratación de los perfiles para la implementación del proceso, evidencia el compromiso para la mejora continua dentro de la Institución.
- La Metodología DevSecOps podría convertirse en el estándar de procesos de desarrollos productivos para el MITIC, integrándose progresivamente en proyectos actuales y futuros con roles definidos y un flujo de trabajo cohesivo.

Como factor de métrica en este apartado se menciona a continuación la evaluación realizada posterior a la implantación

4.1. OWASP SAMM

En seguimiento al plan de acción establecido durante la consultoría, se utilizó el Modelo SAMM[3] (Software Assurance Maturity Model) para la evaluación del nivel de madurez de la Metodología DevSecOps en el MITIC.

El modelo de madurez implementado constituye una herramienta invaluable para evaluar la eficiencia de los procesos dentro de la organización y para identificar las áreas de mejora necesarias para potenciar el rendimiento. Es importante subrayar que no todas las organizaciones deben aspirar a alcanzar el máximo nivel de madurez. Cada institución tiene la capacidad de tomar decisiones respecto a las prácticas de mejoras que serán aplicadas dentro de la organización.

En esta sección, se presentan los resultados derivados de la implementación de la Metodología DevSecOps, los cuales se han obtenido como resultado del proceso de evaluación según el Modelo SAMM.

A continuación, se muestran los resultados obtenidos al comparar el puntaje inicial del análisis realizado durante la consultoría con la fase 1 de implementación. La columna con título "Score" muestra los resultados al inicio de la consultoría. La columna con título "Phase 1 - Score" muestra

[3] https://owasp.org/www-project-samm/

SODEP S.A. Software Development & Products

Nelson Canatta
SODEP S.A.

los resultados de aplicar la misma encuesta a la Organización, luego de la consultoría. Se puede observar una mejora considerable que se refleja de manera positiva en el siguiente recuadro.

Business Functions	Score	Phase 1 - Score
Governance	0,17	0.54
Design	0,33	0.71
Implementation	0,04	0.54
Verification	0,08	0.08
Operations	0,79	0.83
Overall	0,28	0.54

MITIC debería definir los siguientes objetivos de mejora en ciertas funciones de negocio, e ir realizando siguientes fases o iteraciones para ir alcanzando dichos objetivos. En el caso de esta consultoría se ha realizado una sola fase.

5. Recomendaciones

El informe revela progreso en la implementación de DevSecOps en MITIC, destacando mejoras en la metodología, procesos y herramientas. Para que estos avances y mejoras aseguren un crecimiento continuo y sostenible dentro de la institución se recomienda los siguientes puntos:

- Continuar con la formación y capacitación dentro de la institución. Se cuenta con las documentaciones necesarias como activo valioso para futuras incorporaciones, de manera a dar continuidad a las sesiones para los nuevos miembros y reforzar los conocimientos existentes, permitiendo así incorporar la metodología DevSecOps en futuros proyectos.
- Incorporar la metodología DevSecOps de forma progresiva. Esta metodología debería de ser integrada en todos los proyectos donde sea posible, de forma evolutiva. Esto ayudará a estandarizar procesos y garantizar una adopción uniforme, fortaleciendo la eficiencia operativa en toda la institución. Merece atención especial la consolidación de un departamento de Calidad más integrado desde el inicio de los proyectos, incluyendo pruebas automatizadas, pruebas periódicas, etc.
- Generar una base de conocimientos que permita centralizar la información referente a los futuros proyectos y sus delineamientos de seguridad y desarrollo ágil.
- Completar el equipo de perfiles sugeridos y ampliar la oferta de servicios misionales con las prácticas DevSecOps a otras entidades del estado.
- Mejora continua de herramientas y procesos. Una selección adecuada de herramientas actualizadas y un monitoreo continuo de la efectividad de las mismas, así como los procesos ajustados a la incorporación de mecanismos de seguridad conforme las necesidades cambiantes, contribuye a estar mínimamente preparados para posibles amenazas de seguridad.
- Investigación previa y cautela a la hora de seleccionar las tecnologías para desarrollar sistemas y aplicaciones que estarán expuestos a potenciales ataques de seguridad. Es recomendable verificar si existen herramientas para revisión de vulnerabilidades y análisis estático de código que soporten el lenguaje a ser utilizado. Estas son decisiones estratégicas antes del arranque de un proyecto.
- Previo al proceso de selección de herramientas para análisis de seguridad, es crucial realizar un análisis exhaustivo. Se citan a continuación los siguientes puntos a verificar en la selección de herramientas:
    - Es utilizada por la comunidad activamente.
    - Es propensa a dejar de ser utilizada en el futuro cercano (¿quién respalda su mantenimiento?, ¿es utilizada por empresas importantes?).
    - Está en fase productiva.
    - Recibe actualizaciones con frecuencia.
    - Posee varios colaboradores (para casos de herramientas open source).
    - Se integra adecuadamente a las tecnologías utilizadas.

SODEP S.A. Software Development & Products

Nelson Canatta
SODEP S.A.

6. Conclusión

Con la realización de esta consultoría se ha demostrado que la inclusión de la metodología DevSecOps es aplicable en el MITIC con una adecuada asignación de recursos según la demanda. El trabajo realizado se adaptó convenientemente tanto a los recursos humanos así como a los técnicos, proporcionando una sólida metodología que brinda la agilidad y confianza que requieren los desarrollos liderados por el Ministerio que requieran controles de seguridad más estrictos.

MITIC absorbió e incorporó los nuevos roles necesarios para poder llevar adelante esta licitación, lo que hace sostenible el proceso DevSecOps a corto y mediano plazo. Ante la falta de los roles ideales, las mismas personas han desempeñado varios roles para cubrir ciertas tareas; sin embargo la sostenibilidad de la metodología a largo plazo está sujeta en mayor medida a la contratación de forma dedicada y exclusiva de ciertos roles aún pendientes en la Institución.

Las bases están sentadas y las ventajas ya son evidentes, por lo que la continuación y el fortalecimiento del compromiso del Ministerio con los actuales paradigmas de desarrollo y producción de software, hará que la cultura se haga parte integrante de todos los procesos de producción de software y se convierta en el estándar de facto para los proyectos venideros.

SODEP S.A. Software Development & Products

Nelson Canatta
SODEP S.A.

Guillermo Zacur	Nelson Canatta	Ale Feltes
Representante Legal SODEP S.A.	Experto Clave - Personal Operativo	Experto Clave - Supervisor del Proyecto

Mauricio Kreitmayr

Experto Clave - Personal Operativo

SODEP S.A.
Software Development & Products

Nelson Canatta
SODEP S.A.