SODEP S.A.
Software Development & Products

CONSULTORÍA PARA EL SERVICIO DE IMPLEMENTACIÓN DE DEVSECOPS

E01 – Plan de trabajo

MITIC

1. ETAPAS DE LA CONSULTORÍA 3
1.2. Descripción de las etapas 3
1.3. Cronograma de los trabajos y planificación de entregables 4
1.4. Entregables de Consultoría 6
E01- Plan de Trabajo 6
E02 - Informe de relevamiento y diagnóstico 6
Evaluación del nivel de madurez 6
E03 - Informe de recomendaciones y propuestas 6
E04 - Informe de implantación 6
E05 - Informe de transferencia de conocimiento 7
E06 - Informe final de implementación 7
2. METODOLOGÍA DE TRABAJO 7
3. REUNIONES Y AGENDAMIENTOS 8
4. TRANSFERENCIA DE CONOCIMIENTO 8
5. RESULTADOS Y ENTREGABLES 8
Políticas, Procedimientos y Metodologías 9
Herramientas y guías 9

E01 - PLAN DE TRABAJO

CONSULTORÍA PARA LA IMPLEMENTACIÓN DE DEVSECOPS

1. ETAPAS DE LA CONSULTORÍA

El proceso de la consultoría se llevará a cabo en diferentes etapas que buscarán como objetivo principal la implementación de buenas prácticas de DEVSECOPS dentro del MITIC, para un grupo definido de proyectos y al mismo tiempo dejar sistematizado el proceso a implementar para replicar la experiencia en otros proyectos que no se encuentren dentro del alcance de esta consultoría.

Como primer avance, se ha realizado una reunión con varias áreas involucradas del MITIC, así como la revisión de la documentación remitida. En base a esto, se ha preparado el plan de trabajo que se expone en este documento.

1.2. Descripción de las etapas

La consultoría será implementada gradualmente en etapas:

- Relevamiento del estado actual de las tecnologías de los proyectos a ser considerados.
- Reuniones con los actores principales del MITIC a nivel transversal y con los encargados de los proyectos específicos.
- Definición, en conjunto con los actores principales, de cuáles son los objetivos a nivel de DEVSECOPS que se desean alcanzar.
- Diseño del plan de acción para alcanzar los objetivos.
- Implementación del plan de acción.
- Capacitación y traspaso de conocimientos.

1.3. Cronograma de los trabajos y planificación de entregables

N°	Entregables	Meses												Estimación en hs. aprox.
D-1	E01 - Plan de trabajo	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	231
	Reunión de presentación													
	Relevamiento de expectativas													
	Construcción del plan y calendario													
	Entrega de informe al cliente.													
D-2	E02 - Informe de relevamiento y diagnóstico	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	693
	Reuniones de relevamiento													
	Trabajo de laboratorio													
	Entrega parcial													
	Feedback del MITIC													
	Ajustes del documento													
	Entrega parcial													
	Feedback del MITIC													
	Ajustes del documento													
	Entrega informe al cliente													
D-3	E03 - informe de recomendaciones y propuestas	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	462

	Trabajo de laboratorio													
	Entrega parcial													
	Feedback del MITIC													
	Ajustes del documento													
	Entrega parcial													
	Feedback del MITIC													
	Ajustes del documento													
	Entrega informe al cliente													
D-4	E04 - informe de implantación	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	693
	Ciclo de implementación													
	Entrega parcial/DEMO													
	Ciclo de implementación													
	Entrega parcial/DEMO													
	Ciclo de implementación													
	Entrega parcial/DEMO													
	Entrega de inform al cliente													
D-5	E05 - Informe de transferencia de conocimiento	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	462
	Planificación final y ajustes del taller													
	Capacitación													

	Preparación de informe													
	Entrega de informe al cliente													
D-6	E06 - Informe final de implementación	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	set	231
	Preparación de informe													
	Entrega parcial													
	Feedback del MITIC													
	Ajustes del documento													
	Entrega de informe al cliente													

1.4. Entregables de Consultoría

E01- Plan de Trabajo

Este documento constituye el primer entregable de la consultoría como Plan de Trabajo a seguir. Este plan será revisado de manera periódica para poder ajustarlo de acuerdo a los imprevistos que puedan surgir o prioridades que puedan cambiar.

E02 - Informe de relevamiento y diagnóstico

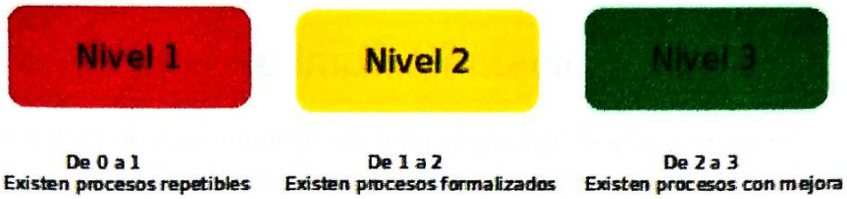
El objetivo principal es realizar un mapeo general del estado de los diferentes proyectos, cuáles son las tecnologías y sus versiones; los procesos que se llevan a cabo para: desarrollo, testing, QA, despliegue en diferentes ambientes y documentación; y la cultura dentro del equipo para incorporar estos procesos.

El diagnóstico permitirá al MITIC tomar conciencia en detalle de los diferentes desafíos a los cuales se enfrenta.

Evaluación del nivel de madurez

Se propone una validación de madurez de seguridad en el ciclo de desarrollo del software, determinando los niveles de seguridad aplicados dentro de la Institución.

Para la medición del nivel de madurez se realizará un análisis con el Modelo SAMM[1].



E03 - Informe de recomendaciones y propuestas

Teniendo en cuenta el estado actual (Etapa E02) se realizarán trabajos de laboratorio para diseñar las propuestas y realizar las recomendaciones para los diferentes puntos.

El informe irá acompañado de un plan de acción a corto, mediano y largo plazo que dará al MITIC un norte a seguir posterior a la consultoría.

Se deberá seleccionar cuales son los puntos con los que se avanzará de acuerdo a las expectativas y recursos de la consultoría.

E04 - Informe de implantación

Durante la fase de implementación se definirán ciclos de trabajos de 1 a 2 semanas con objetivos específicos. Al finalizar cada uno de los ciclos se realizarán reuniones de demostración y análisis sobre los aspectos que estuvieron bien y los que que se encuentra a mejorar.

El MITIC podrá incorporar al equipo de trabajo recursos de la propia Institución, en caso que lo desee. Esto podría tener impacto en el tiempo de implementación pero tendría una ganancia en el traspaso de conocimiento y empoderamiento por parte del equipo del MITIC, al estar involucrado en el proceso de implantación de las soluciones.

A medida que se avanza con la implementación se irá construyendo documentación técnica sobre el proceso y las configuraciones que se realicen para poder replicarlas posteriormente.

[1] SAMM: Software Assurance Maturity Model, es un marco abierto para ayudar a las organizaciones a formular e implementar una estrategia a seguir para la seguridad en el software.

E05 - Informe de transferencia de conocimiento

Se realizarán cursos a las personas definidas por el MITIC donde se realizarán tareas de capacitación sobre el proceso realizado. Estás capacitaciones tendrán ejemplos prácticos basados en los casos de uso de la consultoría realizada. Se tendrá en cuenta también las capacidades necesarias para los trabajos a mediano y largo plazo definidos en el entregable de la etapa E03.

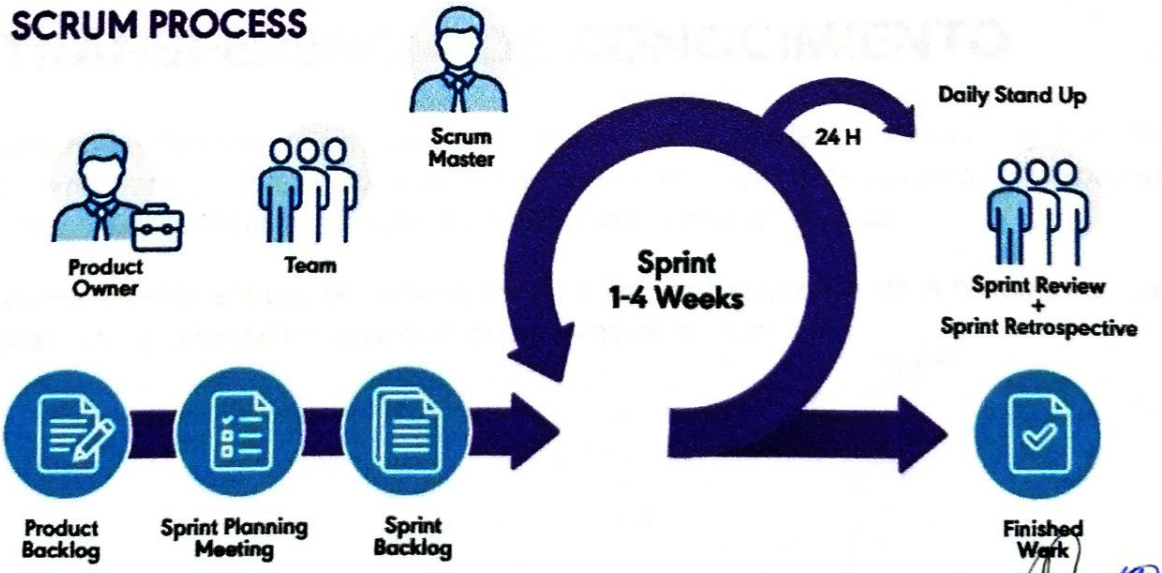
E06 - Informe final de implementación

SODEP se encargará de ir sistematizando todo el proceso desde la etapa E01 hasta la etapa E05. El informe final contendrá un resumen de las acciones realizadas, los avances en cada una de las áreas y la evidencia sobre las mejoras alcanzadas.

2. METODOLOGÍA DE TRABAJO

La implementación de metodologías ágiles nos permitirán ir avanzando por las etapas teniendo en cuenta la retroalimentación de la contraparte del MITIC en todo momento. De esta manera nos aseguraremos de que los procesos de DEVSECOPS a ser implementados no solo cumplan con las normas esperadas, sino que sean implementadas de manera adecuada atendiendo la realidad del MITIC y las prioridades que establezcan.

En este sentido, se propone utilizar la metodología Scrum. Scrum es un marco de gestión de proyectos ágil que ayuda a los equipos a construir e iterar rápidamente.



Para ellos serán planeados Sprints de trabajo, con objetivos bien definidos. De parte de SODEP se propondrá un Scrum Master que planee los Sprints, y de parte del MITIC deberá existir la figura de Product Owner, que tomará decisiones en base a ciertos criterios y prioridades, y gestionará el Backlog de tareas.

3. REUNIONES Y AGENDAMIENTOS

Nuestras principales herramientas para avanzar de acuerdo a esta metodología son:

- Reuniones periódicas con los actores claves que puedan aportar retroalimentación sobre los procesos relevados.
- Reuniones de demostración de procesos a implementar.
- Herramienta de seguimiento de tareas que permita a la contraparte del MITIC monitorear los avances según lo acordado.

Para las primeras etapas de relevamiento y diagnóstico, se propone la realización de reuniones semanales para la captura de información.

Para la etapa de implantación se propone la metodología ágil, que cuenta con las siguientes reuniones:

- Planeamiento del Sprint - Reunión para establecer los objetivos y tareas
- Standup Meeting - 2 veces por semana (aproximadamente 15 a 20 minutos) para actualización de avances
- Revisión del Sprint - Reunión al final del Sprint para revisión de objetivos logrados y demostración

La herramienta de trabajo para una comunicación fluida entre ambas partes será Slack, y las reuniones podrán ser coordinadas en base a la disponibilidad de ambos equipos.

4. TRANSFERENCIA DE CONOCIMIENTO

La transferencia de conocimiento será parte de la etapa 5, para las personas designadas por MITIC. Se realizarán cursos, ejemplos prácticos basados en los casos de uso de la consultoría así como capacitaciones para los trabajos de mediano, largo y plazos definidos.

Se realizará además entrega de documentación sobre la implantación de la herramienta, sus funcionalidades y cómo se fortalece en el ciclo de vida de los sistemas.

5. RESULTADOS Y ENTREGABLES

Los resultados y artefactos a entregar se dividirán dos grandes áreas:

A. Políticas, procedimientos generales y metodologías por un lado; y
B. Herramientas y guías para la aplicación de los puntos relacionados al punto A)

Esta división es importante debido a que así como las políticas pueden cambiar con el tiempo, así también las herramientas pueden tener su ciclo de vida único que no tiene que afectar en medida importante las políticas y procedimientos generales. Esta división también ayuda a otro propósito: pueden tener avances independientes y solo haría falta revisar los puntos en común para mantener la consistencia. En otras palabras, un grupo de personas altamente técnicas podrían seguir los manuales y guías rápidas de las herramientas, sin tener el conocimiento profundo de las políticas que están detrás y aún así estar contribuyendo a la seguridad de todo el proyecto. De la misma forma, el equipo encargado de las políticas y los delineamientos generales podrán ir avanzando sin tener que hacerlo dependiendo de las herramientas particulares. En base a esta partición de entregables, SODEP generará la siguiente serie de resultados.

Políticas, Procedimientos y Metodologías

- **Introducción sencilla y clara de DevSecOps adaptado a la realidad del MITIC**.
    - Todos los procedimientos serán localizados al entorno deseable por el MITIC considerando las restricciones de los desarrollos gestionados por el MITIC. Es decir, no se presentará un escenario ideal que no pueda ser aplicado en la producción de software a cargo del MITIC.
- **Listado detallado de los objetivos y metas al implementar DevSecOps**.
    - Esto incluye objetivos medibles, objetivos cualitativos, junto a las guías para realizar las mediciones y los criterios para las medidas cualitativas.
- **Metodología de migración a la cultura DevSecOps**.
    - Se incluirá la documentación que permitirá una adecuación armoniosa, que, partiendo de las metodologías actualmente utilizadas, permitan la migración a una cultura orientada a la seguridad. Esto asegurará que la cultura sea incorporada desde el comienzo (en forma total en nuevos proyectos) o en forma parcial (en proyectos que estén en curso). Este punto también enunciará claramente las mejores prácticas (incluyendo sugerencias de modificación de plataformas) que SODEP considere apropiadas para un desarrollo que incluya DevSecOps en la mayoría de los desarrollos. En otras palabras, se sugerirá las mejores alternativas tanto metodológicas, así como técnicas (siguiente punto) que mejor se adapten a la cultura deseada.

Herramientas y guías

Se propone abordar el proyecto de implantación de DevSecOps en tres procesos.

Procesos	Integración Contínua	Chequeo de Seguridad	Chequeo de Licencias
Proceso de Desarrollo	✓	✓	
Proceso de Operaciones		✓	✓
Proceso de Vigilancia		✓	✓

- **Herramienta para la CI/CD (Integración contínua y distribución contínua)**
  - Esta herramienta será seleccionada en base a las restricciones locales y se utilizarán los criterios brindados por el MITIC según sus necesidades y experiencia. En general se buscará tener la herramienta que cumpla con todas los objetivos. En caso que esos objetivos sean imprácticos (debido a las restricciones del entorno), se sugerirá un conjunto de herramientas complementarias que puedan subsanar los puntos débiles.
- **Herramienta para el Chequeo de Seguridad**
  - De forma similar al punto anterior, se seleccionará la herramienta más general y que cumpla con la mayor cantidad de objetivos y se adapte al conjunto de plataformas (stack tecnológico) especificadas por el MITIC. Esta herramienta estará orientada al análisis del código fuente de todo el proyecto y es justo destacar en este momento que este análisis se desdobla en dos tipos de análisis:
    - *Análisis de código fuente específico*. Esto incluye todo el código fuente desarrollado particularmente para el proyecto. Es el código escrito con miras a entregar el producto.
    - *Análisis de vulnerabilidades heredadas*. En general, el código específico (punto anterior) constituye sólo una parte del proyecto total ya que es muy frecuente el uso de bibliotecas, librerías y paquetes que no fueron desarrollados por el equipo en particular. Este código prefabricado puede presentar vulnerabilidades que también deberán ser analizadas de forma sistemática.

SODEP S.A. // Confidencial // 2010225

- **Herramientas para el chequeo de licencias**.
    - Es importante tener una visión general del estado de las licencias (tanto de las herramientas DevSecOps) así como de las licencias relacionadas al código heredado (bibliotecas, librerías, paquetes, webservices, etc.)

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

CERTIFICADO DE APROBACIÓN DE E01 PLAN DE TRABAJO

Asunción, 18 de noviembre del 2022

Señores
Guillermo Zacur
SODEP S.A., Representante Legal
Presente.

Por medio de la presente, conforme al **Contrato N° 101/2022** para la Contratación del Servicio ***"CONSULTORÍA PARA EL SERVICIO DE IMPLEMENTACIÓN DEVSECOPS EN MITIC***" del Programa de Apoyo a la Agenda Digital, Préstamo 4650/OC-PR**,** y en referencia a la Nota remitida con fecha 17 de noviembre del 2022, en la cual se realiza la entrega formal en 2 copias originales del producto denominado "**E01 – Plan de Trabajo**".

Al respecto, se certifica que la firma **SODEP S.A.**., ha presentado en tiempo y forma el informe y que el mismo corresponde a lo establecido y esperado en los términos de referencia del Contrato.

Agradecemos de antemano su atención a la presente y hacemos propicia la oportunidad para saludarlo con la seguridad de nuestra mayor consideración y estima.

Firmado digitalmente por GABRIELA MARIA RATTI BITTINGER
Fecha: 2022.11.23 12:31:23 -03'00'

Ing. Gabriela Ratti

Administrador del Contrato
Directora General de Ciberseguridad y
Protección de la Información