Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Software

Implementación de la práctica DevSecOps aplicada a microservicios para una entidad financiera

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Software

AUTOR

Manuel Omar MACHUCA PAJUELO

ASESOR

Jorge Santiago PANTOJA COLLANTES

Lima, Perú

2021

Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Machuca, M. (2021). *Implementación de la práctica DevSecOps aplicada a microservicios para una entidad financiera*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Software]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Manuel Omar Machuca Pajuelo
Tipo de documento de identidad	DNI
Número de documento de identidad	48597706
URL de ORCID	https://orcid.org/0000-0003-3952-4509
Datos de asesor	
Nombres y apellidos	Jorge Santiago Pantoja Collantes
Tipo de documento de identidad	DNI
Número de documento de identidad	06254022
URL de ORCID	https://orcid.org/0000-0002-7172-1206
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Raúl Marcelo Armas Calderón
Tipo de documento	DNI
Número de documento de identidad	07156168
Miembro del jurado 1	
Nombres y apellidos	Arturo Alejandro Bartra More
Tipo de documento	DNI
Número de documento de identidad	40233946
Miembro del jurado 2	
Nombres y apellidos	Jorge Santiago Pantoja Collantes
Tipo de documento	DNI
Número de documento de identidad	06254022
Datos de investigación	
Línea de investigación	No aplica

Grupo de investigación	No aplica
Agencia de financiamiento	Propio
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2021
URL de disciplinas OCDE	2.02.04 -- Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Software

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 21:00 horas del día 22 de diciembre del año 2021, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Ing. Armas Calderón Raúl Marcelo (Presidente), Ing. Bartra More Arturo Alejandro (Miembro) y el Lic. Pantoja Collantes Jorge Santiago (Miembro Asesor), usando la plataforma Meet (https://meet.google.com/jjy-yahj-fza), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: ***"IMPLEMENTACIÓN DE LA PRÁCTICA DEVSECOPS APLICADA A MICROSERVICIOS PARA UNA ENTIDAD FINANCIERA",*** *por el Bachiller* ***Machuca Pajuelo Manuel Omar;*** *para obtener el Título Profesional de Ingeniero de Software.*

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de ***19 DIECINUEVE.***

A continuación el Presidente de Jurados el Ing. Armas Calderón Raúl Marcelo, declara al Bachiller ***Ingeniero de Software****.*

Siendo las 21:4 horas, se levantó la sesión.

Presidente
Ing. Armas Calderón Raúl Marcelo

Miembro
Ing. Bartra More Arturo Alejandro

Miembro Asesor
Lic. Pantoja Collantes Jorge Santiago

DEDICATORIA

Dedico mi presente trabajo a mi familia. A mis abuelos Julia, Benigna, Marino y Máximo, a mis padres Gloria y Edgard por brindarme los principios y valores en mi vida.

A mis hermanos Enrique, Gisenm, Willy y Francisco a quienes amo, respeto y agradezco el ejemplo y apoyo en cada etapa de mi vida.

A mis tíos, tías, primos y amigos los cuales me brindaron su cariño, apoyo y consejos importantes en mi vida.

AGRADECIMIENTOS

- A la compañía NTT DATA por darme la oportunidad de desarrollarme profesionalmente.
- A mi Facultad de Ingeniería de Sistemas e Informática y a mi Universidad Nacional Mayor de San Marcos, por haber sido mi casa de estudios en la cual pase buenos años de mi vida acompañado mis mejores amigos.
- A mi asesor Jorge Pantoja por los consejos brindados en las asesorías.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SOFTWARE

IMPLEMENTACIÓN DE LA PRÁCTICA DEVSECOPS APLICADA A MICROSERVICIOS PARA UNA ENTIDAD FINANCIERA

Autor:	**Machuca Pajuelo, Manuel Machuca**
Asesor:	**Pantoja Collantes, Jorge Santiago**
Título:	**Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniería de Software**
Fecha:	**Noviembre 2021**

RESUMEN

El presente informe de suficiencia profesional describe mi participación en la implementación de la practica DevSecOps aplicada a microservicios en una entidad bancaria, el cual tenía como objetivo realizar la validación de madurez de seguridad en el ciclo de desarrollo de software e incorporar capacidades tecnológicas que garanticen la seguridad del software durante el ciclo de desarrollo. La implementación de la práctica DevSecOps fue enfocada utilizando el framework SAMM v2.0 de OWASP, el cual permitió integrar la seguridad en un entorno DevOps maduro y alinearse a los objetivos de la organización estratégicamente.

Palabras Clave: *DevSecOps, SAMM, OWASP, DevOps, Ciberseguridad y Microservicios.*

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SOFTWARE

IMPLEMENTACIÓN DE LA PRÁCTICA DEVSECOPS APLICADA A MICROSERVICIOS PARA UNA ENTIDAD FINANCIERA

Author:	**Machuca Pajuelo, Manuel Machuca**
Advisor:	**Pantoja Collantes, Jorge Santiago**
Title:	**Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniería de Software**
Date:	**Noviembre 2021**

ABSTRACT

This professional sufficiency report describes my participation in the implementation of the DevSecOps practice applied to microservices in a banking entity, which aimed to carry out the validation of security maturity in the development cycle and incorporate technological capabilities that guarantee the security of the software during the development cycle. The implementation of the DevSecOps practice was focused using the OWASP SAMM v2.0 framework, which allowed integrating security into a mature DevOps environment and aligning it with the organization's objectives strategically.

Keywords: *DevSecOps, SAMM, OWASP, DevOps, Cybersecurity and Microservicios.*

ÍNDICE GENERAL

DEDICATORIA iii
AGRADECIMIENTOS iv
RESUMEN v
ABSTRACT vi
ÍNDICE DE FIGURAS ix
ÍNDICE DE TABLAS x
INTRODUCCIÓN 1
CAPÍTULO I TRAYECTORIA PROFESIONAL 2
1.1. Presentación profesional 2
1.2. Formación académica 2
1.3. Cursos, Seminarios y programas 2
1.4. Experiencia profesional 3
CAPÍTULO II CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA 5
2.1. Empresa 5
2.1. Misión 5
2.2. Visión 5
2.3. Organización de la empresa 6
2.4. Área, Cargo y funciones desempeñadas 6
2.5. Experiencia profesional realizada en la compañía 7
CAPÍTULO III ACTIVIDADES DESARROLLADAS 8
3.1. Situación problemática 8
3.1.1 Definición del problema 9
3.2. Solución 9
3.2.1 Objetivos 9
3.2.2 Alcance 10
3.2.3 Etapas y metodología 12
3.2.4 Fundamentos utilizados 15
3.2.5 Implementación de las áreas de procesos y sus buena practicas 19
3.3. Evaluación 49
3.3.1 Evaluación económica 49
3.3.2 Evaluación del VAN y del TIR 50
CAPÍTULO IV REFLEXIÓN CRÍTICA DE LA EXPERIENCIA 52
CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES 53
5.1 Conclusiones 53
5.2 Recomendaciones 54

ANEXOS 55
ANEXO 1. PLANTILLA DE ACTA DE REUNIÓN 55
ANEXO 2. PLANTILLA SAMM ASSESSMENT TOLLBOX 2.0 56
ANEXO 3. NIVELES DE MADUREZ SEGUN SAMM 59
ANEXO 4. REPORTES DE ESCANEOS DE SEGURIDAD DE LOS MICROSERVICIOS 60
BIBLIOGRAFÍA 62

ÍNDICE DE FIGURAS

Figura 1: Organigrama de la empresa NTT DATA Perú 6
Figura 2: Diagrama referencial a la metodología COM de NTT DATA 12
Figura 3: Planificación de ejecución del proyecto 13
Figura 4: Pirámide DevSecOps 16
Figura 5: Estructura OWASP SAMM v2.0 18
Figura 6: Plan de trabajo 21
Figura 7: Niveles de madurez según SAMM 25
Figura 8: Plantilla para responder el SAMM Assessment Tollbox v2.0 26
Figura 9: Nivel de madurez actual resumen de la entidad bancaria 27
Figura 10: Nivel de madurez actual de la entidad bancaria 27
Figura 11: Plantilla para respuestas de nivel de madurez deseado según SAMM 29
Figura 12: Nivel de madurez objetivo deseado para la entidad bancaria 31
Figura 13: Nivel de madurez objetivo deseado detallado para la entidad bancaria 31
Figura 14: RoadMap de iniciativas por función de negocio 34
Figura 15: Referencia AS-IS de la plataforma tecnológica de los microservicios 36
Figura 16: Pipeline DevOps de desarrollo 37
Figura 17: Pipeline DevOps de calidad 37
Figura 18: Pipeline DevOps de producción 38
Figura 19: Stage SAST 41
Figura 20: Stage SAILC 42
Figura 21: Stage DAST 43
Figura 22: Referencia a la metodología para Guías de Hardening 44
Figura 23: Ejecución del pipeline DevSecOps calidad del microservicio 1 45
Figura 24: Ejecución del pipeline DevSecOps de desarrollo del microservicio 2 45
Figura 25: Proceso de gestión de vulnerabilidades 48

ÍNDICE DE TABLAS

Tabla 1: Formación académica profesional 2
Tabla 2: Certificado de terminación del curso CISSP 2
Tabla 3: NTT DATA Perú 3
Tabla 4: Accenture Perú 3
Tabla 5: Uptime Business Consulting 4
Tabla 6: Cenpro UNMSM 4
Tabla 7: Grupos de trabajo 20
Tabla 8: Entrevistas realizadas en la evaluación del S-SDLC 23
Tabla 9: Iniciativas de la Fase I 32
Tabla 10: Iniciativas de la Fase II 33
Tabla 11: Iniciativas de la Fase III 33
Tabla 12: Costo referencial de la consultoría 49
Tabla 13: Costo referencial de suscripción de herramientas 49
Tabla 14: Gasto referencial de pruebas de seguridad manual 51
Tabla 15: Flujo efectivo para el cálculo del VAN y TIR 51

INTRODUCCIÓN

En los últimos años las empresas del sector financiero se encuentran en un proceso de transformación digital, esto representa un gran reto en el que vale la pena incursionar. La entidad financiera partícipe de este proyecto tiene como objetivo implementar capacidades tecnológicas de seguridad de información que permitan garantizar mejorar la experiencia de usuario y ser un banco digital con los estándares del momento.

La entidad bancaria dentro de su plan de transformación digital ha encontrado la necesidad de implementar buenas prácticas que permitan mejorar los procesos involucrados en la tecnología y conseguir la colaboración entre la seguridad, desarrollo y operaciones, para la cual la practica DevSecOps es uno de sus objetivos a implementar, buscando que se garantice la seguridad en el ciclo de vida de desarrollo de aplicaciones.

Por lo tanto, se ha encargado a NTT DATA, la implementación de la practica DevSecOps para la plataforma de microservicios.

El presente documento está organizado en los siguientes capítulos:

- EL CAPÍTULO I, se describe mi trayectoria profesional y los conocimientos adquiridos.
- EL CAPÍTULO II, se describe la empresa en donde laboré durante el desarrollo del proyecto del presente informe y el rol desempeñado.
- EL CAPÍTULO III, se describe las actividades desarrolladas y el aporte del proyecto del presente informe.
- EL CAPÍTULO IV, se describen las reflexiones acerca del proyecto realizado en el presente informe.

EL CAPÍTULO V, se describen las conclusiones y recomendaciones del autor del proyecto realizado en el presente informe.

CAPÍTULO I
TRAYECTORIA PROFESIONAL

1.1. Presentación profesional

El autor del presente trabajo tiene el grado de bachiller en Ingeniería de Software, actualmente con el rol de Ingeniero de Ciberseguridad en compañía donde labora, con una experiencia laboral de más de 5 años de experiencia en ciberseguridad y desarrollo de software en proyectos empresariales bancarios; implementación de evaluaciones de seguridad, desarrollo de procesos automatizados de desarrollo seguro y aseguramiento para plataformas o sistemas.

1.2. Formación académica

Tabla 1: Formación académica profesional

Periodo 2012-2017	**Universidad Nacional Mayor de San Marcos** Grado de Bachiller Escuela académica profesional en la escuela de Ingeniería de Software de la Facultad de Ingeniería de Sistemas e Informática.

Nota: Elaboración propia

1.3. Cursos, Seminarios y programas

Tabla 2: Certificado de terminación del curso CISSP

Curso para la certificación CISSP	
Centro de estudio	New Horizons
Descripción	Este curso está dirigido a profesionales experimentados en seguridad de TI, auditores, consultores, investigadores o instructores, incluidos analistas e ingenieros de red o de seguridad, administradores de red, especialistas en seguridad de la información y profesionales de la gestión de riesgos, que persiguen la capacitación y certificación de CISSP para adquirir la credibilidad y la movilidad para avanzar dentro de sus carreras actuales de seguridad informática o para migrar a una carrera relacionada.

Nota: Elaboración propia

1.4. Experiencia profesional

Tabla 3: NTT DATA Perú

NTT DATA Perú S.A.C. Setiembre 2020 – Actualidad	
Cargo	Ingeniero de Ciberseguridad
Funciones	• Experiencia en DevSecOps y sus implicancias con herramientas como Veracode, Prisma Cloud y Burp Suite Enterprise Edition. • Experiencia en generación y documentación de procesos de gestión de vulnerabilidades para microservicios o aplicaciones. • Desarrollo de Guías de Hardening en servicios de la plataforma Azure. • Desarrollo de historias de seguridad para aplicaciones empresariales.

Nota: Elaboración propia

Tabla 4: Accenture Perú

Accenture Perú Febrero 2018 – Junio 2020	
Cargo	Analista
Proyecto	Ciberseguridad • Evaluación con el Framework Ciberseguridad de Accenture para el grupo corporativo Breca. • Evaluación de los procesos operativos y capacidades tecnológicas del grupo. • Presentación y creación de informes de directorio. • Aplicación de técnicas en ingeniería social. Desarrollo de software • Desarrollo y mantenimientos de aplicaciones con lenguajes de programación Java, .NET y JavaScript. • Desarrollo y mantenimientos de aplicaciones con los frameworks Spring Framework y Spring Boot. • Gestión y manteamiento de proceso con lenguajes PL/SQL en bases de datos Oracle y SQL Server. • Java 7 para mantenimiento y creación de aplicaciones Web. • Mantenimiento de servicios web SOAP.

Nota: Elaboración propia

Tabla 5: Uptime Business Consulting

Uptime Business Consulting **Junio 2017 – Octubre 2017**	
Cargo	Analista Funcional
Funciones	• Análisis, diseño y desarrollo del Sistema de Gestión de Cumplimiento Normativo versión 1. • Rol de líder de equipo de proyectos para el desarrollo en Front-End con JSF, Ajax y JavaScript. • Rol de líder de equipo de proyectos para el desarrollo Back-End Java 8, Framework Spring, integración con BD Oracle, SQL Server e Hibernate. • Ejecución de pruebas unitarias con Junit.

Nota: Elaboración propia

Tabla 6: Cenpro UNMSM

Centro de Producción de la UNMSM **Febrero 2016 – Junio 2017**	
Cargo	Analista Funcional
Funciones	• Análisis, diseño y desarrollo del Sistema de Gestión de Cumplimiento Normativo versión 1. • Rol de líder de equipo de proyectos para el desarrollo en Front-End con JSF, Ajax y JavaScript. • Rol de líder de equipo de proyectos para el desarrollo Back-End Java 8, Framework Spring, integración con BD Oracle, SQL Server e Hibernate. • Ejecución de pruebas unitarias con Junit.

Nota: Elaboración propia

CAPÍTULO II
CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA

2.1. Empresa

De acuerdo a la definición de NTT DATA (2021):

> NTT DATA tiene como su sede principal en la ciudad de Tokio, es la 6ª compañía proveedora de servicios de TI del mundo, y cuenta con 140.000 profesionales y opera en más de 50 países.
>
> La compañía NTT DATA Europe & Latam nace de la alianza entre everis (con presencia en Europa y América Latina) y NTT DATA EMEA (con presencia principalmente en Reino Unido, Italia, Alemania y Rumanía) para ayudar a las compañías en Europa y Latinoamérica a realizar su transformación digitales y proyectos de innovación.
>
> La firma busca ayudar a sus clientes en su transformación y desarrollo digital mediante su amplia gama de ofertas de servicios en consultoría y tecnologías de vanguardia. NTT DATA aprovecha su amplia experiencia y conocimientos en todos los sectores del mercado para brindar un nivel óptimo de servicios.

2.1. Misión

De acuerdo a NTT DATA (NTT DATA GLOBAL, 2021), la misión de NTT DATA es crear nuevas formas de trabajo y valores para contribuir a un mundo próspero y armonioso, a través de las tecnologías de la información.

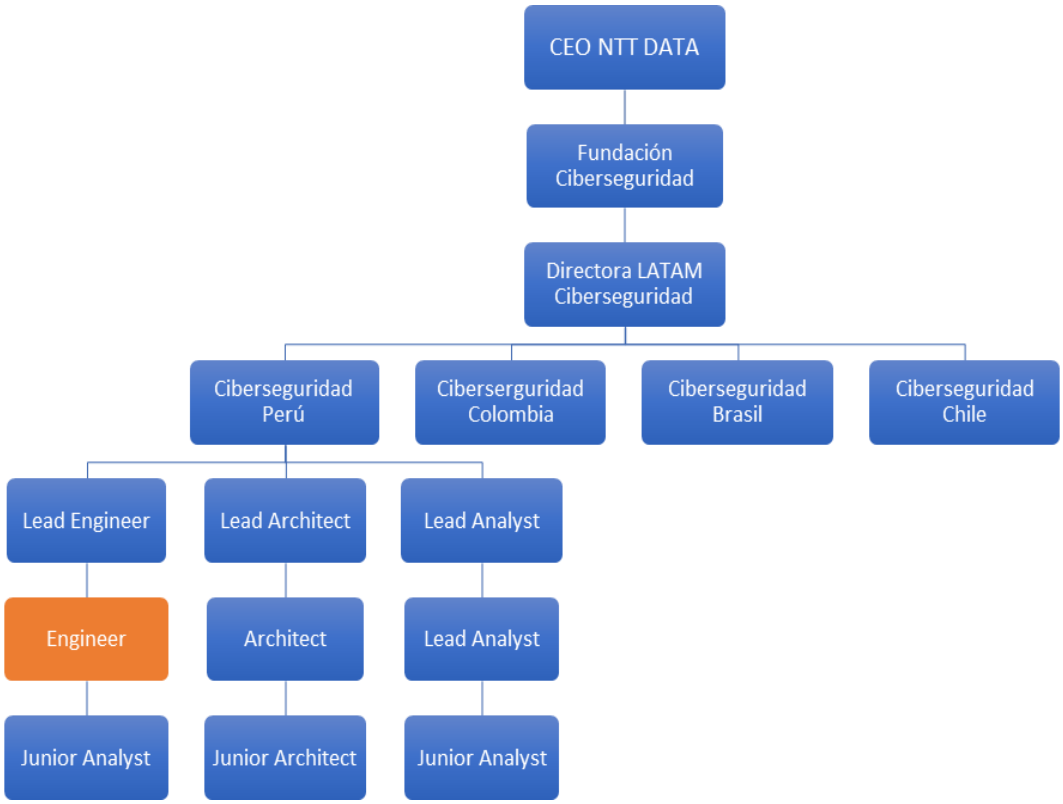
2.2. Visión

De acuerdo a NTT DATA (NTT DATA GLOBAL, 2021), la visión del grupo NTT DATA es realizar los sueños de sus clientes en todo el mundo mediante las relaciones a largo plazo y desarrollar un ambiente en conjunto en evolución mediante las tecnologías de vanguardia en el mundo.

2.3. Organización de la empresa

A continuación, en la figura 1 se presenta el organigrama de la compañía y la fundación de ciberseguridad en la región.

Figura 1: Organigrama de la empresa NTT DATA Perú



Nota: Elaboración propia

2.4. Área, Cargo y funciones desempeñadas

El autor actualmente se desempeña el rol de Ingeniero en el área de Ciberseguridad de la compañía.

Las funciones que realiza la categoría Ingeniero en los proyectos de los cuales forma parte de le equipo son las siguientes:

- Atender los requerimientos de clientes de los proyectos de implementación o consultoría.
- Definir soluciones equilibradas según demanda y viabilidad.
- Diseñar técnicamente programas, módulos o modelos.
- Construir, probar y documentar elementos estructurales de la solución.

- Transmitir y presentar los resultados parciales o finales de su trabajo, siguiendo un hilo argumental coherente.
- Consolidar, transmitir y poner en práctica el conocimiento funcional, técnico y metodológico adquirido en este u otros proyectos en los que ha participado.

2.5. Experiencia profesional realizada en la compañía

El autor como parte de la compañía ha participado en los siguientes proyectos estratégico:

- Proyecto Implementación de un modelo DevSecOps basado en las prácticas de seguridad del Framework OWASP SAMM, donde el autor automatizó las pruebas de seguridad en los pipelines DevOps para el desarrollo de microservicios del cliente.
- Proyecto Post Implementación del modelo DevSecOps del desarrollo de microservicios, donde el autor definió y automatizó procesos para la remediación de vulnerabilidades de la plataforma de microservicios.
- Proyecto de evaluación de Hardening de componentes tecnológicos de Azure, donde el autor encontró más de 30 debilidades de seguridad y recomendó más de 60 controles de seguridad.
- Proyecto de evaluación y construcción de un marco de desarrollo, donde le autor identifica las brechas de seguridad de del proceso de desarrollo del cliente y plantea un plan de remediación las brechas encontradas.

CAPÍTULO III
ACTIVIDADES DESARROLLADAS

3.1. Situación problemática

Desde el año 2020, la entidad bancaria se encuentra en un proceso de transformación digital, donde buscan incorporar buenas prácticas, estándares y seguridad en los servicios que brindan a sus clientes. A partir del presente año la entidad bancaria tenía implementado una arquitectura cloud on-premise para su plataforma de microservicios, así mismo comenzó con la construcción de su arquitectura de seguridad.

La plataforma de microservicios de la entidad bancaria da soporte al despliegue y operación de microservicios a través del enfoque DevOps, teniendo como uno de sus principales pilares la automatización y autogestión. Para implementar un DevOps se han redefinido y definido procesos, se han instalado un conjunto de herramientas libres y licenciadas que permitan conseguir la eficiencia en la integración y entrega continua de software (CI/CD), herramientas tales como Jenkins, Docker, OpenShift y Dynatrace, sin embargo, no se han implementado herramientas automatizadas para la detección de defectos de seguridad en los microservicios o sobre la pila tecnológica.

Esta plataforma de microservicios bajo el enfoque DevOps involucra equipos de desarrollo, arquitectos de aplicaciones, equipos de infraestructura y sistemas operativos, que aseguran que los microservicios sean construidos, implementados correctamente, sin embargo, se carece de un rol de seguridad que integra la seguridad tanto en el desarrollo como en las operaciones en el ciclo de vida de los microservicios.

Otro problema que enfrentan es la falta de un proceso para la gestión de los defectos de seguridad o vulnerabilidades de las aplicaciones identificadas en pruebas de penetración o verificación de controles de seguridad en la plataforma tecnológica de microservicios. Acorde a las buenas prácticas la organización debería de adoptar un cambio cultural, tecnológico y de seguridad.

3.1.1 Definición del problema

El principal problema radica en la falta de integración de la seguridad en el ciclo de vida de desarrollo de software (SDLC) en la entidad bancaria, esto significa que podemos estar expuestos ante amenazas y no tomar las acciones preventivas y adecuadas para la protección de nuestros activos y datos. A esto se debe añadir las exigencias de las regulaciones a la banca en el Perú mediante la resolución N° 504-2021 para la gestión de la seguridad de la información y ciberseguridad, en cumplimiento de la normativa, ya que podrían generar impacto de tipo financiero y reputacional.

3.2. Solución

3.2.1 Objetivos

Objetivo general

Implementar la práctica DevSecOps aplicado a microservicios para la entidad financiera, que permita identificar y remediar los defectos de seguridad.

Objetivos específicos

- Realizar una evaluación del ciclo de vida de desarrollo de microservicios actual para conocer la forma de trabajo actual.
- Identificar las necesidades de seguridad en el proceso de implementación/pipelines de los microservicios en la entidad bancaria.
- Diseñar la solución DevSecOps de integración de la seguridad en la plataforma actual de microservicios alineada a los estándares de la organización.
- Integrar las herramientas de escaneo y pruebas de seguridad en los pipelines manteniendo el principio de automatización.
- Definir el proceso de gestión de vulnerabilidades del modelo DevSecOps implementado.

3.2.2 Alcance

El proyecto comprende en la implantación de DevSecOps, para la cual se establece el siguiente alcance:

- Evaluación del nivel de madurez del S-SDLC
  - Estado actual de la entidad bancaria según el modelo de madurez SAMM de OWASP.
  - Nivel de madurez objetivo de la entidad bancaria, según capacidades de las células, capacidades tecnológicas y realidad de la operadora.
  - Plan y cobertura de brechas para la implementación.
- Implantación DevSecOps

  Se busca realizar la implementación de un modelo operativo DevSecOps. A continuación, se muestra el alcance de este servicio brindado por el área de ciberseguridad de la compañía.

  - Construir una Guía de Hardening para un conjunto de componente consensuados que intervienes en el ciclo de vida de microservicios.
  - Crear el pipeline piloto de 2 microservicios Mobile al entorno DevSecOps para la ejecución automática de pruebas de seguridad.
  - Construir los pipelines de ejecución de herramientas de seguridad
  - Realizar pruebas de la implementación DevSecOps de los microservicios piloto.
  - Construir guía operativa de herramientas SAST, SAILC y DAST.
  - Hacer transferencia de conocimiento a los responsables de la entidad bancaria.
  - Definir políticas, lineamientos de seguridad y KPI's para el modelo operativo DevSecOps.

Se proyecta a futuro evolucionar el DevSecOps implementado, utilizando los resultados generados por la evaluación de nivel de madurez actual de seguridad en el S-SDLC de la entidad bancaria. El resultado de la evaluación propone desarrollar un conjunto de prácticas de seguridad que elevan el nivel de madurez en el DevSecOps y en el desarrollo seguro en la organización.

3.2.3 Etapas y metodología

Metodología COM para la gestión de proyecto

La metodología COM (COM: Corporate Methods) que NTT DATA ha desarrollado permite gestionar los proyectos desde la concepción comercial (venta) y finaliza con la entrega del proyecto. Para cada etapa, la metodología te ayuda guiándote con las tareas que se deben realizar en cada fase, con el objetivo de obtener la venta del proyecto y con la conclusión de la entrega.

Concepción comercial

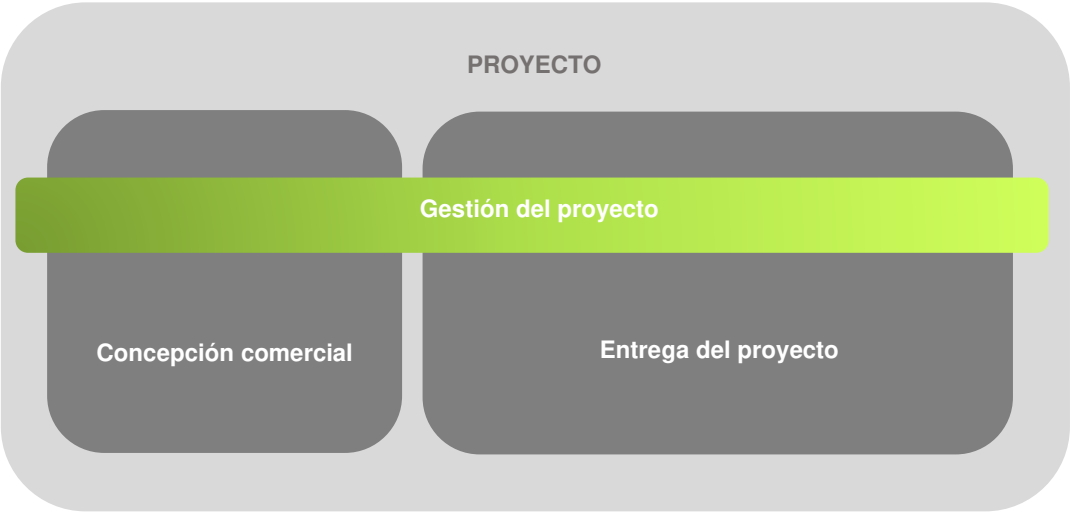
La gestión de un proyecto inicia desde la venta, donde se analizan los costes y rentabilidad, para finalmente dar la propuesta de proyecto como contratada.

Entrega del proyecto

La ejecución del proyecto se inicia alineando las expectativas del cliente, y utilizan las herramientas necesarias para cumplir con los objetivos y expectativas, para finalmente preparar el cierre y aprobación del proyecto.

En la figura 2 se muestra las etapas de concepción comercial y entrega del proyecto que son parte de gestión de proyectos, según la metodología COM.

Figura 2: Diagrama referencial a la metodología COM de NTT DATA

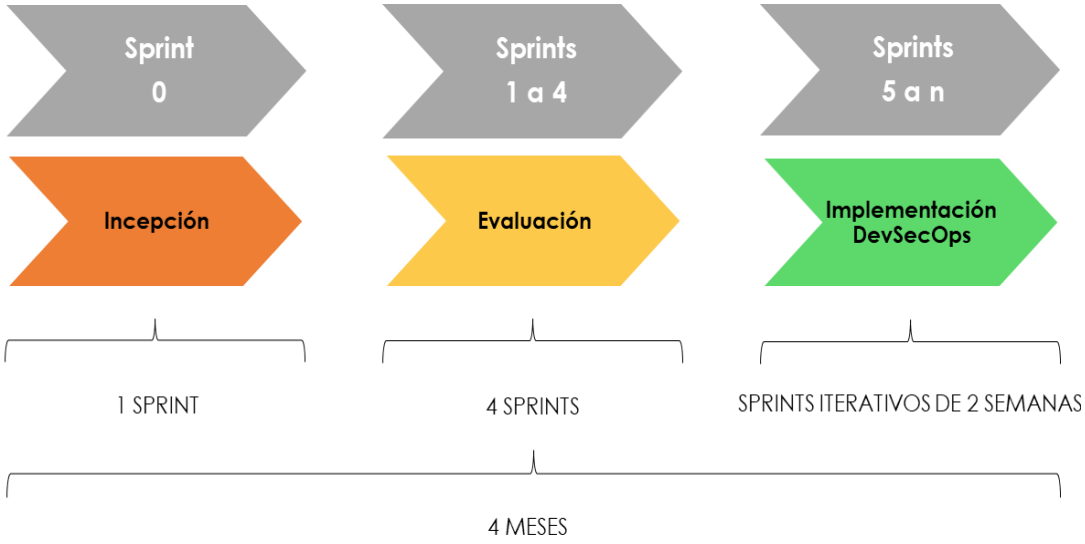


Nota: Elaboración propia

Metodología Agile para la implantación DevSecOps

Se propone abordar el proyecto de implantación de DevSecOps en tres fases bajo la modalidad agile, alineados con el marco de referencia SAFe conocido por el proveedor y cliente, como se muestra en la figura 3.

Figura 3: Planificación de ejecución del proyecto



Nota: Elaboración propia

Para llevar a cabo cada una de las siguientes fases para la ejecución del proyecto, se utilizó como marco de trabajo el modelo SAMM en su versión 2.0 propiedad de OWASP, para la definición de actividades, hitos y entregables.

- **Fase 1: Incepción**
  - Definir los grupos de trabajo a ser impactados, utilizando como input la estructura organizacional del cliente.
  - Definir los stakeholders involucrados en el proyecto.
  - Definir los releases de la implantación DevSecOps.
- **Fase 2: Evaluación**
  - Realizar la evaluación del estado actual de la entidad bancaria según el modelo de madurez SAMM.

- Definir el modelo de madurez deseado de la entidad bancaria, según capacidades de los equipos de trabajo del proyecto, capacidades tecnológicas y realidad de la organización
- Definir una hoja de ruta para la obtención del nivel de madurez deseado a trabajar en la fase de Implementación DevSecOps.

- **Fase 3: Implementación DevSecOps**

  Se busca realizar la implementación del modelo operativo DevSecOps y plantear su evolución según la identificación de brechas obtenidas en la fase evaluación mencionada en el punto anterior.

  - **Entendimiento**

    Realizar la revisión de la documentación y ejecución de sesiones para la comprensión del entorno DevOps actual en el desarrollo de microservicios.

  - **Guías**

    Generar las guías de aseguramiento de seguridad para las 7 herramientas que conforman el entorno DevSecOps.

  - **Herramientas**

    Colaborar con la adquisición de licencias, aprovisionamiento infraestructura, instalación, configuración y afinamiento de las herramientas de seguridad.

  - **Lineamientos**

    Definir los lineamientos correspondientes a los procesos del entorno DevSecOps relacionados a las tareas operativas.

  - **Piloto**

    Ejecución del piloto correspondiente de las aplicaciones en su funcionalidad del flujo DevSecOps para dos microservicios.

3.2.4 Fundamentos utilizados

Antes de desarrollar la base teórica de los fundamentos utilizados, se explicarán los conceptos básicos:

- SAST: son pruebas de seguridad estáticas, su objetivo es informar defectos de seguridad y la calidad en el código estático (Static Application Security Testing).
- DAST: son pruebas dinámicas de aplicaciones, su objetivo es informar defectos de seguridad en aplicaciones en ejecución (Dynamic Application Security Testing).
- SAILC: son pruebas de seguridad en las imágenes y contenedores (Security Along Image Lifecycle).
- IAST: son pruebas de seguridad interactivas, su objetivo es informar defectos de seguridad en aplicaciones en ejecución (Interactive Application Security Testing).
- Metodología ágil: es una metodología de trabajo flexible, con desarrollo incremental mediante interacciones, buscando la mayor inmediatez en la respuesta al proyecto con la entrega del producto.
- DevOps: Es una práctica para el desarrollo de software ágil y veloz, implica integración, entrega continua y automatización. Es la combinación de las palabras “Development” y “Operations”.
- Ciberseguridad: Área o disciplina de la tecnología con el objetivo de proteger la información digital de las organizaciones.
- SDLC: Son las siglas en ingles del ciclo de vida de desarrollo de software (Software Development Life Cycle).
- S-SDLC: Son las siglas en ingles del ciclo de vida de desarrollo de software seguro (Secure Software Development Life Cycle).

DevSecOps

De acuerdo a la definición de Myrbakken y Colomo-Palacios (2017):

> La práctica DevSecOps es considerada una evolución de DevOps, que tiene el desafío de integrar controles y procesos de seguridad modernizados en el ciclo de desarrollo de software.

De acuerdo a la definición de Tomas, Li y Huang (2019) :

> DevSecOps es una práctica que promueve la colaboración entre equipos de desarrollo, operaciones y seguridad, buscando la garantía de calidad de la seguridad, enraizados en los pilares de DevOps como: cultura, automatización, intercambio y medición.
>
> En la figura 4 podemos ver tres de los principales pilares según el autor.

Figura 4: Pirámide DevSecOps

Nota: Adaptado de Tomas, Li y Huang (2019)

OWASP SAMM v2.0

Las fases para la implementación DevSecOps se fundamentó con el marco de referencia el proyecto abierto OWASP SAMM en su versión 2.0.

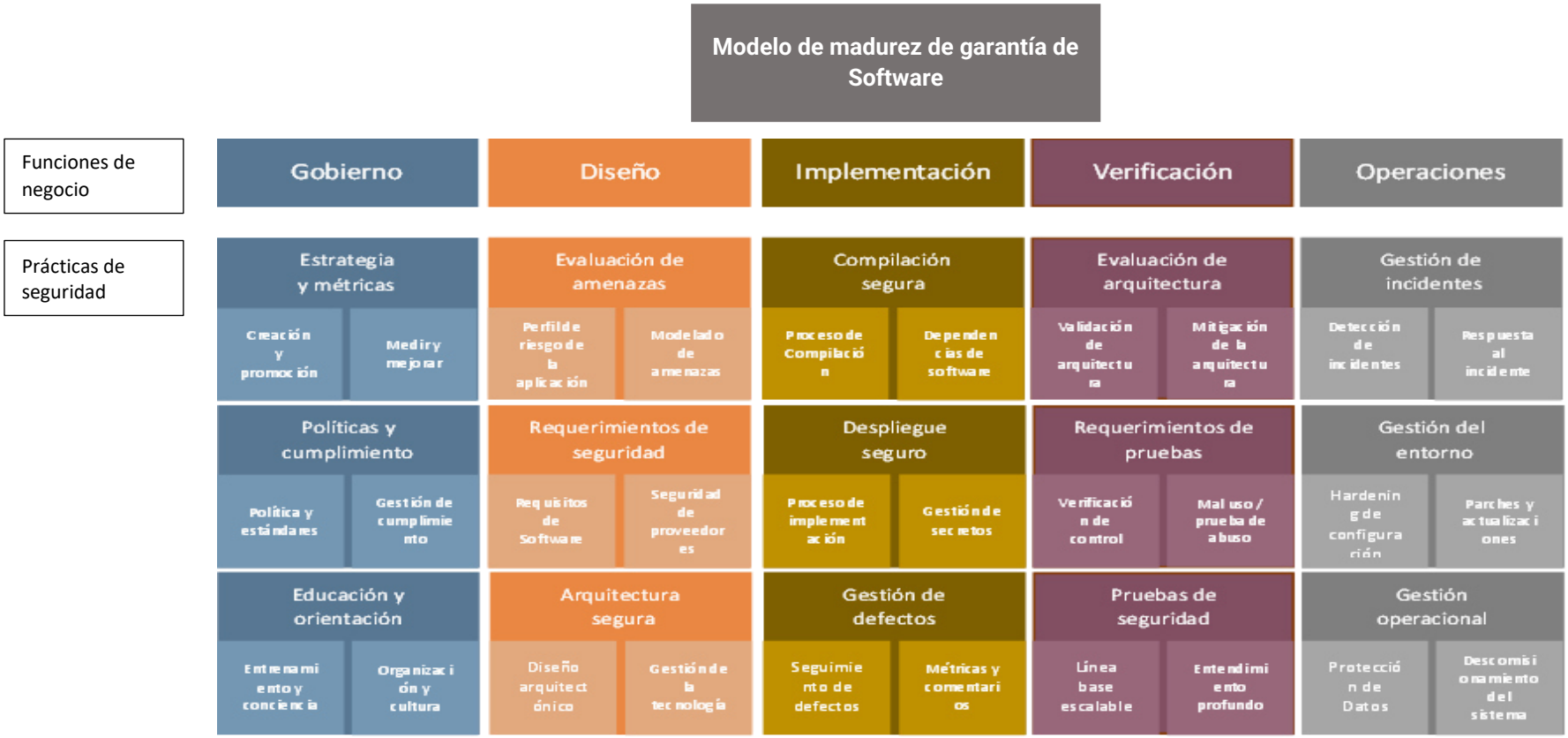
De acuerdo a la definición de OWASP (2021):

> OWASP SAMM 2.0, es un framework que permite a las organizaciones formular e implementar una estrategia de seguridad de software adaptada a los riesgos que enfrenta una organización.

De acuerdo a la definición de OWASP SAMM (2021):

> OWASP SAMM 2.0, es un marco abierto que tiene como misión proveer de una forma efectiva y medible para que las organizaciones establezcan su postura de seguridad de software.
>
> Las principales características de SAMM son:
>
> - Medible: Permite definir el nivel de madurez del estado actual en seguridad de software.
> - Procesable: Permite definir el camino para mejorar nivel de madurez de seguridad de software.
> - Versátil: Es independiente de la tecnología y tipo de organización.
>
> SAMM es un modelo prescriptivo simple de usar incluso para conocedores en TI con pocos conocimientos en seguridad de la información o ciberseguridad.
>
> Estructura OWASP SAMM
>
> - En el nivel más alto, el framework define cinco Funciones de negocio función (en inglés Business Function) críticas.
> - Para cada función comercial, el framework define tres Practicas de seguridad (en inglés Security practices), para cada práctica de seguridad se define tres niveles de madurez como objetivos.
> - Para cada práctica de seguridad, el framework define dos Flujos (en inglés Streams).
>
> En la figura 5 se muestra la estructura del framework SAMM.

Figura 5: Estructura OWASP SAMM v2.0



Nota: Elaboración propia

3.2.5 Implementación de las áreas de procesos y sus buena practicas

A continuación, se explica las actividades desarrolladas en cada una de las fases, las cuales se basan en las metodologías y marcos de trabajo para la ejecución del proyecto de Implantación DevSecOps acorde a lo indicado en el numeral 3.2.3.

Fase 1: Incepción

Con la finalidad de cumplir los objetivos del proyecto de forma eficiente y ordenada, en la presente fase se realizan las actividades iniciales de presentación del proyecto, la obtención de insumos iniciales para la gestión del proyecto y creación del plan de trabajo final.

- Inicio de proyecto

  Una vez hecha la venta del proyecto Implantación DevSecOps, se dio inicio formal al proyecto a través de la presentación del Kick Off, donde se expuse los siguientes puntos al cliente:

  - Introducción
  - Alcance
  - Metodologías
  - Equipo de trabajo
  - Plan de trabajo inicial

- Definición de los grupos de trabajo

  Según el marco SAMM, el cual nos dice que para la evaluación de la madurez de la estrategia de seguridad de aplicaciones y el desarrollo seguro, debemos analizar las cinco funciones de negocio. Por lo tanto, se definieron los siguientes seis grupos de trabajo alineados al framework SAMM considerando la estructura organizacional de la entidad bancaria, las cuales serán habilitadores de información requerida para la ejecución de las fases posteriores.

Tabla 7: Grupos de trabajo

Grupo de trabajo	Función de negocio SAMM
Seguridad de la información	Gobierno Diseño
Infraestructura y Soporte	Implementación Verificación Operaciones
Desarrollo de aplicaciones	Gobierno Diseño Implementación Verificación Operaciones
Gestión de proyectos	Gobierno
Área de calidad	Implementación Verificación
Arquitectura Empresarial	Diseño Verificación

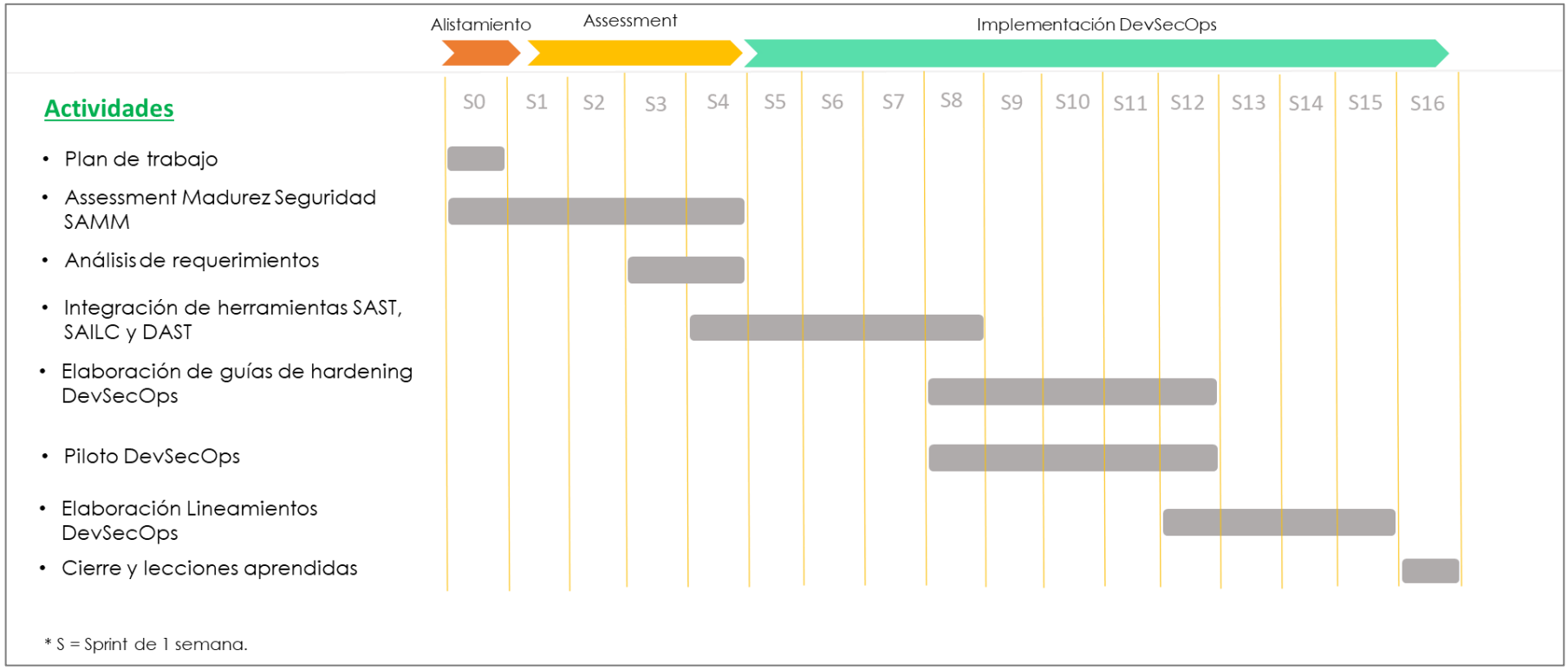
Nota: Elaboración propia

- Definición de los stakeholders del proyecto
    - Gerencia de TI
    - Gerencia de seguridad de la información
    - Oficial de seguridad de la información
- Definición del plan de trabajo

  La realización del proyecto se plantea bajo metodología ágil trabajando sobre iteraciones y así evolucionar en el tiempo, a continuación, se muestra el plan a alto nivel que, acorde a nuestra metodología.

  En la figura 6 se muestra el plan de trabajo.

Figura 6: Plan de trabajo



Nota: Elaboración propia

Fase 2: Evaluación del nivel de madurez S-SDLC

El assessment de nivel de madurez del desarrollo seguro realizado a la entidad bancaria, contiene tres secciones principales que representan el contenido del entregable de evaluación, siendo estas secciones el AS IS, TO BE y el Plan de cobertura de brechas, a continuación, se detalla lo realizado en cada sección:

- **AS IS**

  Esta sección contiene el dos puntos clave; uno conocer el nivel de madurez en la seguridad en el ciclo de vida de desarrollo de aplicaciones, y describir el estado actual por cada función de negocio en la entidad bancaria.

  Para obtener información de las prácticas de seguridad en los procesos de la organización, así mismo obtener las evidencias de que estas prácticas se vienen desarrollando, se organizaron un conjunto de entrevistas con las mesas de trabajo entre la entidad bancaria y el equipo de trabajo definidas en la fase de alistamiento, a continuación, se muestran las entrevistas realizadas:

Tabla 8: Entrevistas realizadas en la evaluación del S-SDLC

Actividad	Participantes		Función de negocio SAMM
Entrevista Seguridad 20 de julio 2020	**Entidad Bancaria** • Gerente de Seguridad de Información. • Jefe de Seguridad de Información. • Jefe Seguridad TI. • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor de Ciberseguridad. • Líder de Ciberseguridad.	Gobierno Diseño
Entrevista Calidad 30 de julio 2020	**Entidad Bancaria** • Jefe de Calidad y Mantenimiento TI. • Especialista de Calidad TI. • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad. • Líder de Ciberseguridad.	Implementación Verificación
Entrevista Desarrollo 5 de agosto 2020	**Entidad Bancaria** • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad. • Líder de Ciberseguridad.	Gobierno Diseño Implementación Verificación Operaciones
Entrevista Infraestructura y Soporte 6 de agosto 2020	**Entidad Bancaria** • Ingeniero Cloud. • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad.	Verificación Operaciones
Entrevista Proyectos 10 de agosto 2020	**Entidad Bancaria** • Líder de PMO • Analista Senior de PMO	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad. • Líder de Ciberseguridad.	Gobierno
Entrevista Arquitectura Empresarial 30 de septiembre 2020	**Entidad Bancaria** • Gerente de Arquitectura Empresarial. • Arquitecto Digital. • Arquitecto de Infraestructura. • Ingeniero de integración API. • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad. • Líder de Ciberseguridad.	Implementación Verificación
Entrevista Proyectos 01 de octubre 2020	**Entidad Bancaria** • Jefe de Proyectos Estratégicos TI • Ingeniero de Microservicios.	**NTT DATA Ciberseguridad** • Consultor Ciberseguridad. • Líder de Ciberseguridad.	Gobierno

Nota: Elaboración propia

Para cada entrevista realizada se redactó un acta de reunión, donde se evidencian: los participantes de la reunión, los puntos revisados según el marco SAMM, y los acuerdos entre los participantes, a continuación, se muestra un ejemplo de la entrevista, y adjuntado las evidencias en el **Anexo 1**.

- **Entrevista:**

  ¿Cómo se viene gestionando de parte del gobierno desde la perspectiva de seguridad con respecto a lo que es construcción y medidores de seguridad?

  Básicamente son consideraciones enfocadas en OWASP top 10 donde vemos transversalmente este estándar y pedimos que sean incluidas dentro de los proyectos, los que son publicadas en internet o tienen una exposición más alta pedimos que se realice un ethical hacking justamente para verificar las vulnerabilidades de los proyectos de desarrollo no tengan un nivel de impacto significativo para el banco.

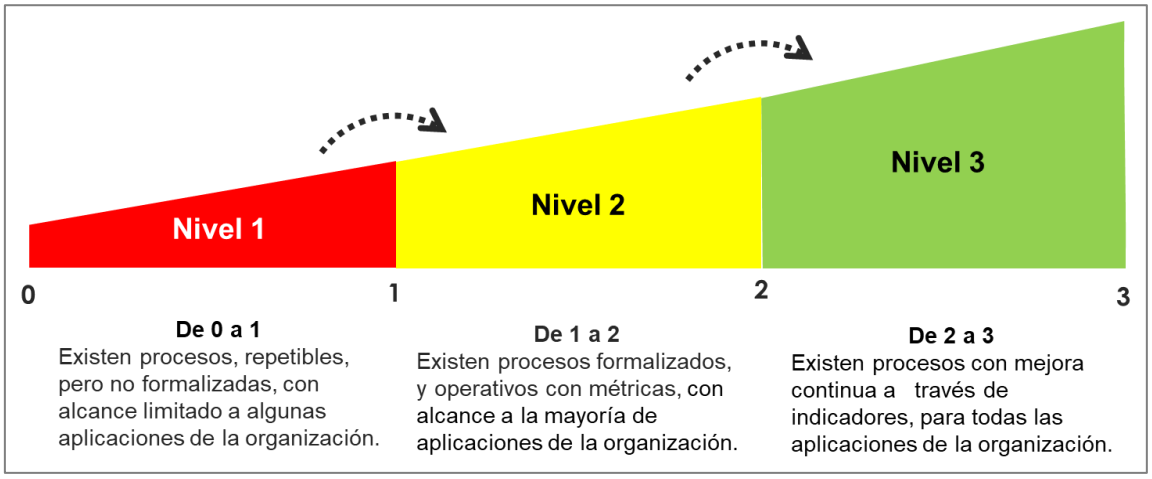
  En cuanto a indicadores puntuales de seguridad cómo por ejemplo cantidad de issues de seguridad detectados en producción ¿se tiene ese nivel de visibilidad?

  Lo que se identifica durante las pruebas o evaluaciones de seguridad se trata de que el mismo proyecto se encargue de las remediaciones y estas vulnerabilidades se superen.

Luego de obtener la información necesaria sobre los procesos y prácticas de seguridad, se procede cuadrar el nivel de madurez actual que tiene la entidad bancaria, para esto se usó una plantilla libre estructurada según el framework SAMM que provee OWASP llamada SAMM Assessment Tollbox v2.0, la cual se encuentra en el **Anexo 2**.

Para seleccionar el nivel de cada practica de seguridad, es necesario saber cuáles son los niveles de madurez, a continuación, en la figura 7 se muestra los tres niveles de madurez según el framework SAMM.

Figura 7: Niveles de madurez según SAMM



Nota: Elaboración propia

La plantilla de soporte para la evaluación nos provee dos hojas llamadas Entrevista y Scorecard las cuales tienen el objetivo de facilitarnos el trabajo para obtener el nivel de madurez actual, las cuales se encuentran en el **Anexo 2**.

La primera hoja contiene tres preguntas por cada Flujo de cada Practica de seguridad, que a su vez pertenecen a una Función de negocio, preguntas que al ser respondidas nos darán el nivel de madurez de cada Flujo. Con cada puntaje de los Flujo se calcula el promedio de cada Practica de seguridad, que a su vez calculan el nivel de madurez de cada Función de negocio, estos cálculos son realizados automáticamente por la plantilla, solo nos enfocamos en responder las preguntas considerando la información y evidencias obtenidas en las entrevistas.

Al aplicar el uso de plantilla y responder el cuestionario, mediante el juicio de experto en base a las evidencias de los procesos de la entidad bancaria, se generarán los puntajes de los Flujos, los cuales representarán el nivel de madurez actual. A continuación, en la figura 8 se muestran la plantilla de evaluación y el nivel de madurez actual obtenido de la entidad bancaria:

Figura 8: Plantilla para responder el SAMM Assessment Tollbox v2.0

SAMM Assessment Interview: For

Instructions
nterview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

Governance					
Stream	**Level**	**Strategy & Metrics**	**Answer**	**Interview Notes**	**Rating**
Create and Promote	**1**	**Do you understand the enterprise-wide risk appetite for your applications ?**			**0.00**
		You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location			
	2	**Do you have a strategic plan for application security and use it to make decisions?**			
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives You have buy-in from stakeholders, including development teams			
	3	**Do you regularly review and update the Strategic Plan for Application Security?**			
		You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, making sure they are available to all stakeholders			

Nota: Elaboración propia

En la figura 9 y 10, como resultado se observa que la entidad bancaria se encuentra en un nivel de madurez uno, esto quiere decir que aplican algunas prácticas de seguridad de manera ad-hoc, sin embargo, se requiere formalizar y dar mayor alcance a los procesos, actividades, y roles de seguridad.

Figura 9: Nivel de madurez actual resumen de la entidad bancaria

Funciones	Actual
Gobierno	0.38
Diseño	0.54
Implementación	1.00
Verificación	0.42
Operaciones	0.63
	0.59

Nota: Elaboración propia

Figura 10: Nivel de madurez actual de la entidad bancaria

			Madurez		
Funciones	Prácticas de seguridad	Actual	1	2	3
Gobierno	Estrategia y métricas	0.25	0.25	0.00	0.00
Gobierno	Política y cumplimiento	0.38	0.25	0.13	0.00
Gobierno	Educación y orientación	0.00	0.00	0.00	0.00
Diseño	Evaluación de amenazas	0.25	0.25	0.00	0.00
Diseño	Requerimientos de seguridad	0.38	0.25	0.13	0.00
Diseño	Arquitectura segura	0.38	0.25	0.13	0.00
Implementación	Compilación segura	0.50	0.50	0.00	0.00
Implementación	Despliegue seguro	1.00	0.75	0.25	0.00
Implementación	Gestión de defectos	0.13	0.13	0.00	0.00
Verificación	Evaluación de arquitectura	0.63	0.50	0.00	0.13
Verificación	Requerimientos de pruebas	2.13	1.00	1.00	0.13
Verificación	Pruebas de seguridad	0.88	0.50	0.25	0.13
Operaciones	Gestión de incidentes	2.50	0.50	1.00	1.00
Operaciones	Gestión del entorno	1.00	0.25	0.63	0.13
Operaciones	Gestión operacional	0.75	0.50	0.25	0.00

Nota: Elaboración propia

- **TO BE**

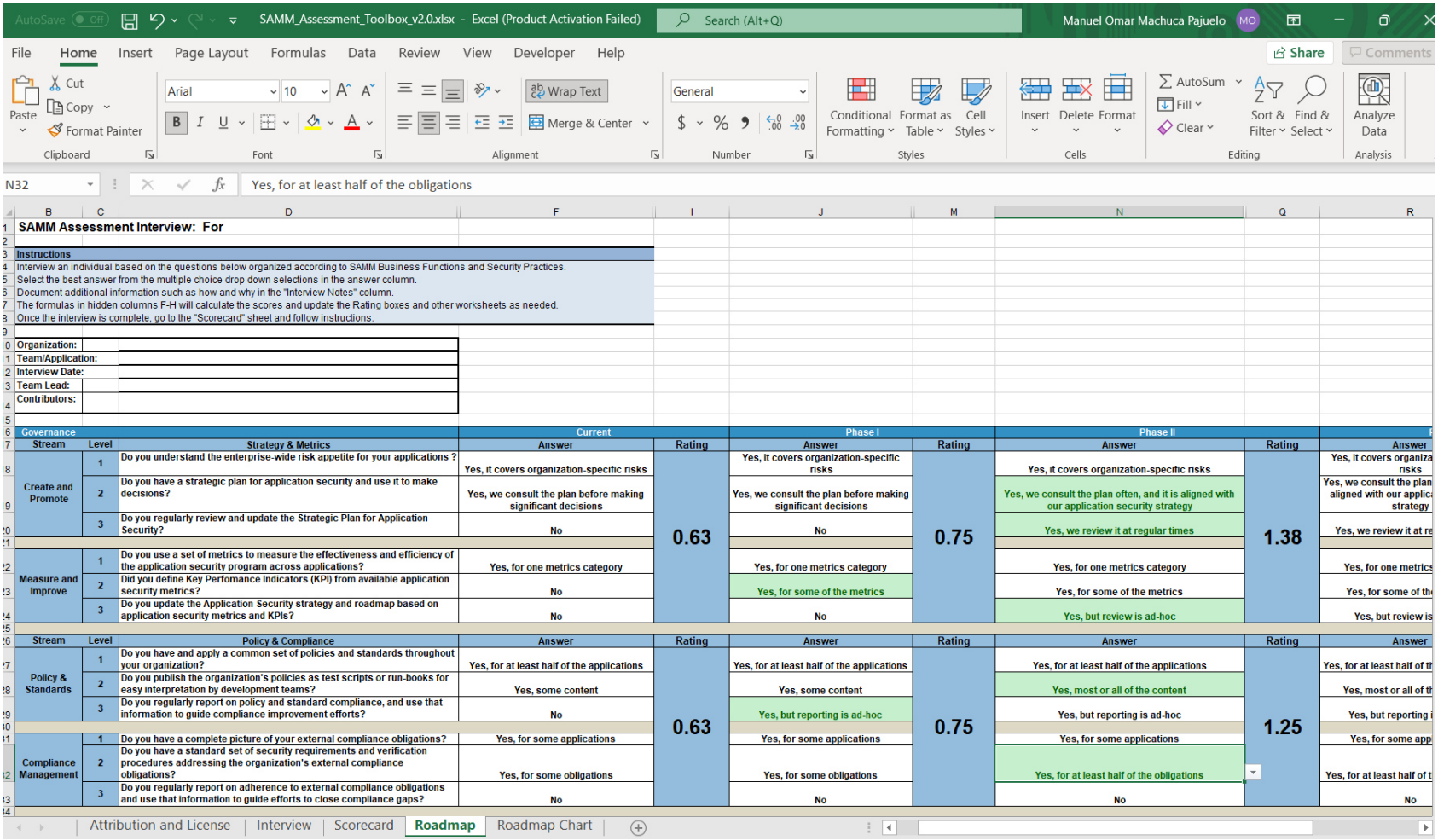
  Esta sección del entregable contiene dos puntos claves; uno plantear el nivel de madurez deseado a través de fases y definir los criterios y objetivos específicos de cada fase planteada. Es importante recalcar que definir el nivel madurez deseado, se depende principalmente de las necesidades de seguridad de los aplicativos de la organización y las capacidades actuales y futuras de la organización.

  Por parte de los consultores que brindamos el servicio, planteamos un workshop para explicar los niveles de madurez según SAMM, la cual se encuentra en el **Anexo 3** y compartir una propuesta inicial del nivel de madurez deseado para la entidad bancaria, para generar esta propuesta inicial hacemos uso de la plantilla de SAMM Assessment Tollbox v2.0, con la hoja Roadmap.

  En este ejercicio completamos las respuestas en un nivel superior para cada Flujo y cada una de las fases planteadas, de esta forma al completar las respuestas obtenemos un nivel de madurez deseado en un numero de fases definido.

  En la figura 11, se muestra la estructura de la plantilla SAMM Assessment Tollbox v2.0 que nos brinda OWASP.

Figura 11: Plantilla para respuestas de nivel de madurez deseado según SAMM



SAMM Assessment Interview: For

Instructions

Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

Governance			Current		Phase I		Phase II		
Stream	Level	Strategy & Metrics	Answer	Rating	Answer	Rating	Answer	Rating	Answer
Create and Promote	1	Do you understand the enterprise-wide risk appetite for your applications ?	Yes, it covers organization-specific risks	0.63	Yes, it covers organization-specific risks	0.75	Yes, it covers organization-specific risks	1.38	Yes, it covers organiza risks
	2	Do you have a strategic plan for application security and use it to make decisions?	Yes, we consult the plan before making significant decisions		Yes, we consult the plan before making significant decisions		Yes, we consult the plan often, and it is aligned with our application security strategy		Yes, we consult the plan aligned with our applic strategy
	3	Do you regularly review and update the Strategic Plan for Application Security?	No		No		Yes, we review it at regular times		Yes, we review it at re
Measure and Improve	1	Do you use a set of metrics to measure the effectiveness and efficiency of the application security program across applications?	Yes, for one metrics category		Yes, for one metrics category		Yes, for one metrics category		Yes, for one metrics
	2	Did you define Key Perfomance Indicators (KPI) from available application security metrics?	No		Yes, for some of the metrics		Yes, for some of the metrics		Yes, for some of th
	3	Do you update the Application Security strategy and roadmap based on application security metrics and KPIs?	No		No		Yes, but review is ad-hoc		Yes, but review is
Stream	Level	Policy & Compliance	Answer	Rating	Answer	Rating	Answer	Rating	Answer
Policy & Standards	1	Do you have and apply a common set of policies and standards throughout your organization?	Yes, for at least half of the applications	0.63	Yes, for at least half of the applications	0.75	Yes, for at least half of the applications	1.25	Yes, for at least half of th
	2	Do you publish the organization's policies as test scripts or run-books for easy interpretation by development teams?	Yes, some content		Yes, some content		Yes, most or all of the content		Yes, most or all of th
	3	Do you regularly report on policy and standard compliance, and use that information to guide compliance improvement efforts?	No		Yes, but reporting is ad-hoc		Yes, but reporting is ad-hoc		Yes, but reporting i
Compliance Management	1	Do you have a complete picture of your external compliance obligations?	Yes, for some applications		Yes, for some applications		Yes, for some applications		Yes, for some app
	2	Do you have a standard set of security requirements and verification procedures addressing the organization's external compliance obligations?	Yes, for some obligations		Yes, for some obligations		Yes, for at least half of the obligations		Yes, for at least half of t
	3	Do you regularly report on adherence to external compliance obligations and use that information to guide efforts to close compliance gaps?	No		No		No		No

Nota: Elaboración propia

Por parte de los consultores que brindamos el servicio, planteamos un workshop para compartir la propuesta inicial del nivel de madurez deseado para la entidad bancaria, para esto hacemos uso de la plantilla de SAMM Assessment Tollbox v2.0, con la hoja Roadmap. En este ejercicio completamos las respuestas en un nivel superior para cada Flujo y cada una de las fases planteadas, de esta forma al completar las respuestas obtenemos un nivel de madurez deseado en un numero de fases definido.

Como resultado del workshop de nivel de madurez deseado, se definición lo siguiente:

- Serán tres el número de fases para llegar al nivel de deseado
- Cada fase debe tener un objetivo y alcance definido
- Se debe apuntar al nivel dos y estar listo para iniciar a futuro actividades de nivel tres.

Los objetivo y alcance para cada fase son las siguientes:

- Fase I

  Se establece aumentar y homogenizar el nivel de madurez de las diferentes prácticas de seguridad. Se busca definir estrategias y ejecutar actividades prioritarias.

- Fase II

  Se establece el aumento de nivel de madurez en las prácticas de seguridad. Iniciar con la implementación de las estrategias definidas en la etapa anterior y complementar con nuevas actividades.

- Fase III

  Se relacionan las actividades correspondientes a revisión, validación, actualización de las estrategias y controles de seguridad ejecutados en las fases anteriores, buscando mejorar y extender el alcance de las prácticas de seguridad.

En la figura 12 y 13, se muestra los niveles de madurez objetivo.

Figura 12: Nivel de madurez objetivo deseado para la entidad bancaria

Funciones	Nivel Actual	Fase I	Fase II	Fase III
Gobierno	0,38	0,67	1,13	1,46
Diseño	0,54	0,92	1,38	1,75
Implementación	1,00	1,17	1,54	2,13
Verificación	0,42	1,08	1,54	2,42
Operaciones	0,63	1,00	1,46	1,63

Nota: Elaboración propia

Figura 13: Nivel de madurez objetivo deseado detallado para la entidad bancaria

Funciones	Prácticas de seguridad	Actual		Fase I		Fase II		Fase III	
Gobierno	Estrategia y métricas	0,25	0,38	0,75	0,67	1,38	1,13	1,88	1,46
Gobierno	Política y cumplimiento	0,63		0,88		1,13		1,63	
Gobierno	Educación y orientación	0,25		0,38		0,88		0,88	
Diseño	Evaluación de amenazas	0,25	0,54	0,75	0,92	1,00	1,38	2,00	1,75
Diseño	Requerimientos de seguridad	0,50		0,63		1,00		1,13	
Diseño	Arquitectura segura	0,88		1,38		2,13		2,13	
Implementación	Compilación segura	1,25	1,00	1,38	1,17	1,63	1,54	2,63	2,13
Implementación	Despliegue seguro	1,50		1,50		1,88		1,88	
Implementación	Gestión de defectos	0,25		0,63		1,13		1,88	
Verificación	Evaluación de arquitectura	0,25	0,42	1,25	1,08	1,25	1,54	2,63	2,42
Verificación	Requerimientos de pruebas	0,38		0,63		1,50		2,00	
Verificación	Pruebas de seguridad	0,63		1,38		1,88		2,63	
Operaciones	Gestión de incidentes	0,50	0,63	1,00	1,00	1,50	1,46	1,50	1,63
Operaciones	Gestión del entorno	0,63		0,63		1,38		1,38	
Operaciones	Gestión operacional	0,75		1,38		1,50		2,00	

Nota: Elaboración propia

- **RoadMap de cobertura de brechas**

Luego de definir el nivel de madurez deseado, se procede a plantear una hoja de ruta para llegar al objetivo por cada fase plantada.

Por lo tanto esta sección del entregable tiene el objetivo de brindarle un camino claro y aterrizado a la entidad bancaria por el cual pueden lograr le nivel de madurez deseado y adoptar una postura de seguridad con respecto a sus aplicaciones; entonces aparecen dos puntos claves; uno plantear un conjunto de iniciativas desarrollar las prácticas de seguridad según las buenas prácticas de SAMM, y dos plantear una hoja de ruta para las iniciativas según las fases definidas, con el objetivo de que la entidad bancaria evolucione al nivel de madurez deseado. A continuación, se muestran algunas de las iniciativas de las fases planteadas:

Tabla 9: Iniciativas de la Fase I

ID	Título de iniciativa	Función de negocio	Practica de seguridad
F01-I001	Estrategia de seguridad de las aplicaciones	**Gobierno**	Estrategia y métricas
F01-I002	Estrategia de modelado de amenazas	**Diseño**	Evaluación de amenazas
F01-I003	Controles de seguridad automatizados en la implementación	**Implementación**	Despliegue seguro
F01-I004	Pruebas de seguridad automatizadas	**Verificación**	Requerimientos de pruebas
F01-I005	Proceso de detección de incidentes	**Operación**	Gestión de incidentes

Nota: Elaboración propia

Tabla 10: Iniciativas de la Fase II

ID	Título de iniciativa	Función de negocio	Practica de seguridad
F02-I001	Identificación de indicadores clave	**Gobierno**	Estrategia y métricas
F02-I002	Principios de diseño seguro	**Diseño**	Arquitectura segura
F02-I003	Definición estrategia gestión de secretos	**Implementación**	Despliegue seguro
F02-I004	Personalización pruebas de seguridad automatizadas	**Verificación**	Requerimientos de pruebas
F02-I005	Lineamientos para protección de datos	**Operación**	Gestión operacional

Nota: Elaboración propia

Tabla 11: Iniciativas de la Fase III

ID	Título de iniciativa	Función de negocio	Practica de seguridad
F03-I001	Revisión estrategia de seguridad de las aplicaciones	**Gobierno**	Estrategia y métricas
F03-I002	Definición proceso manejo dependencias de software	**Diseño**	Construcción segura
F03-I003	Planteamiento ANS para remediación	**Implementación**	Gestión de defectos
F03-I004	Actualización arquitectura de referencia	**Verificación**	Requerimientos de pruebas
F03-I005	Actualización catálogo de datos	**Operación**	Gestión de incidentes

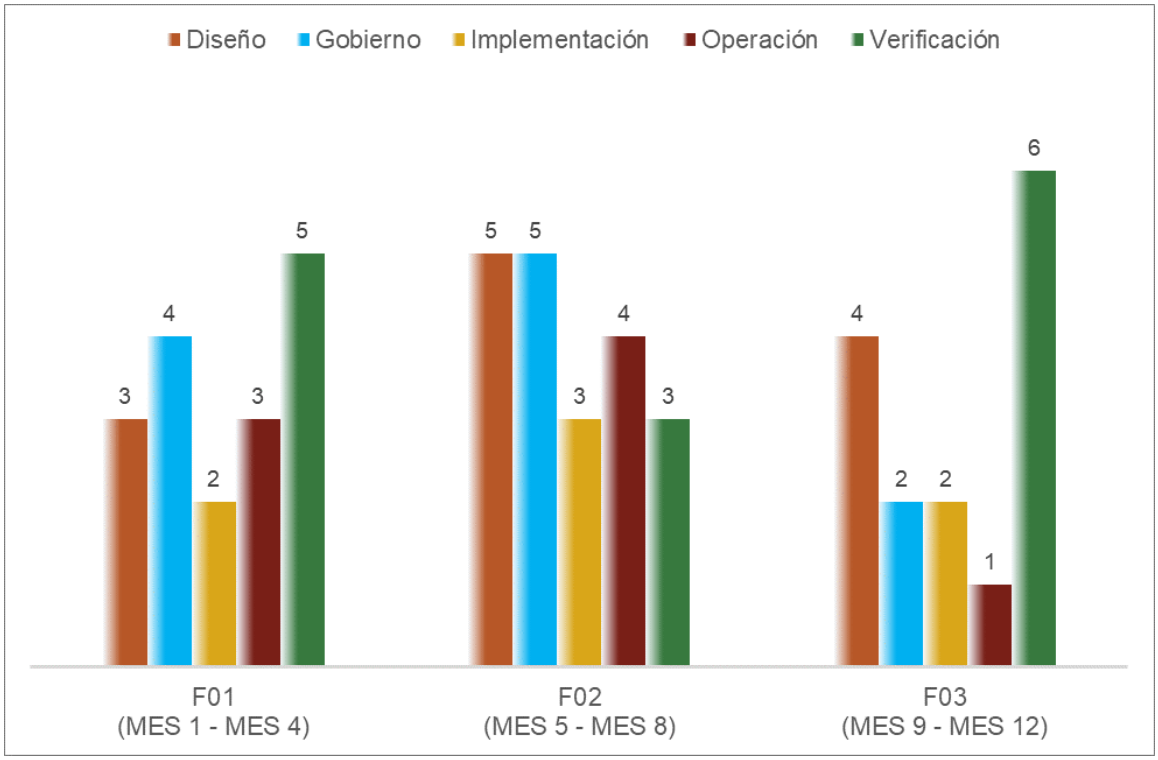
Nota: Elaboración propia

Por último, se define un RoadMap de iniciativas que pretenden generar el aumento de nivel de madurez de las prácticas de seguridad y por consiguiente el nivel de madurez de las funciones de negocio.

Cada fase se plantea con una duración de 4 meses, tiempo en el cual se desarrollarán las diferentes iniciativas dentro del ciclo de vida de desarrollo de software.

En la figura 14, se muestra el RoadMap de iniciativas, donde podemos ver un total de diecisiete iniciativas a ejecutar en la fase I, veinte iniciativas a ejecutar en la fase II y quince iniciativas en la fase III; se asocian las iniciativas a su respectiva función de negocio (Business Function).

Figura 14: RoadMap de iniciativas por función de negocio



Nota: Elaboración propia

Fase 3: Implementación DevSecOps

Esta fase tiene como objetivo implantar la practica DevSecOps en la entidad bancaria, donde se incluye las herramientas correspondientes para la automatización de las tareas de seguridad junto con los lineamientos de seguridad correspondientes para la operación de la plataforma de microservicios.

Para realizar la implantación de DevSecOps se realizaron las siguientes actividades, las cuales detallaremos a continuación:

- Análisis de requerimientos

  Esta fase inicia con el levantamiento de requisitos para la implementación DevSecOps, realizándose los siguientes análisis:

  - Análisis de la plataforma tecnológica DevOps de microservicios en la entidad bancaria.

    La plataforma tecnología de microservicios ha estado trabajando bajo una arquitectura de microservicios y practicas DevOps.

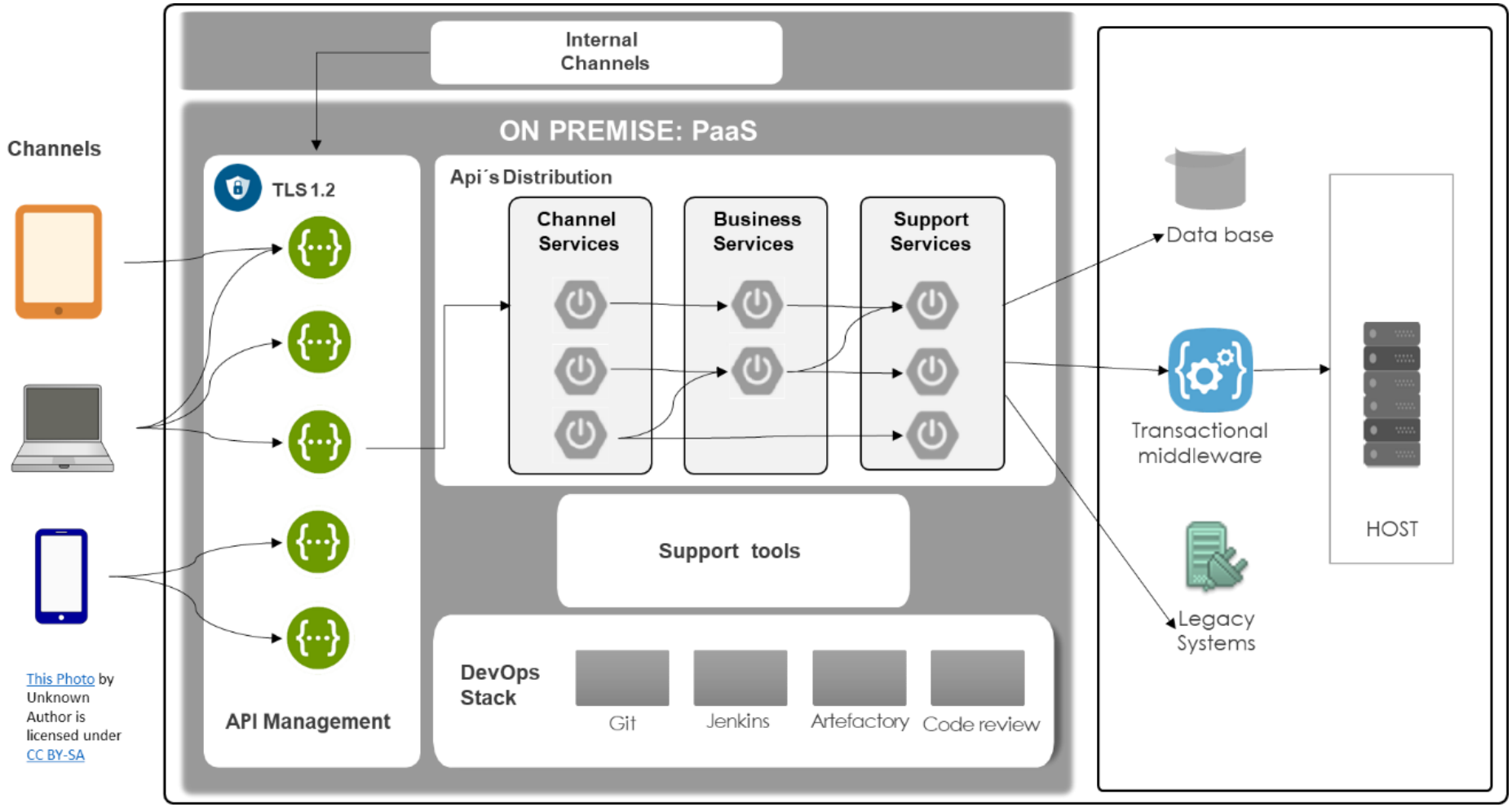
    La arquitectura de microservicios está desplegada sobre un ambiente on-premise, específicamente en una nube privada tipo PaaS.

    La arquitectura de microservicio cuenta una API Managment para el control de acceso, un ambiente de distribución de API's donde se cuenta con API's de tipo canales, negocio y de soporte, cada una con su objetivo específico y seguridad.

    Para la construcción y despliegue de microservicios se cuenta con DevOps implementado, por lo tanto, se ha implementado un stack de herramientas para la integración y entrega continua (CI/CD).

    En la figura 15 se muestra una referencia de la plataforma tecnología de los microservicios.

Figura 15: Referencia AS-IS de la plataforma tecnológica de los microservicios



Nota: Elaboración propia

- Análisis de la CI/CD de los microservicios

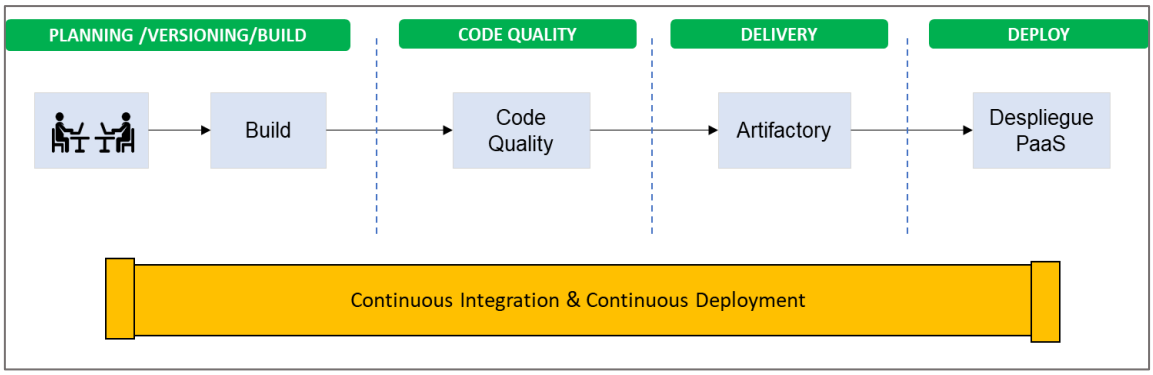
  Luego de analizar la plataforma tecnológica de los microservicios, se procede a realizar un análisis de los Pipelines DevOps, ya que, la integración de la seguridad mediante pruebas automatizadas se realizará sobre estos pipelines.

  Se implementaron los pipelines DevOps para los ambientes de desarrollo, calidad y producción, cada uno con sus particularidad y herramientas.

  Esos pipelines son ejecutados desde una herramienta de orquestación para CI/CD y han sido creados en el lenguaje Groovy.

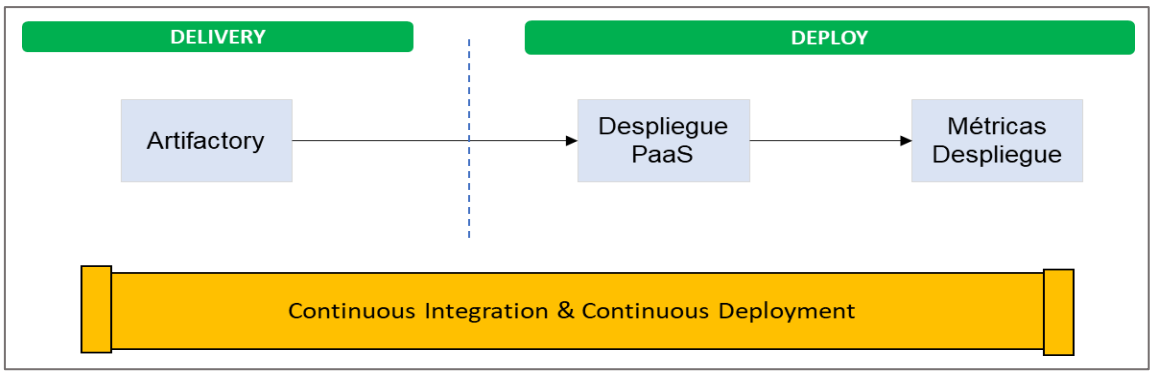
  En las figuras 16, 17 y 18 se muestra en alto nivel los pipelines de cada ambiente antes de hacer la implementación DevSecOps.

Figura 16: Pipeline DevOps de desarrollo



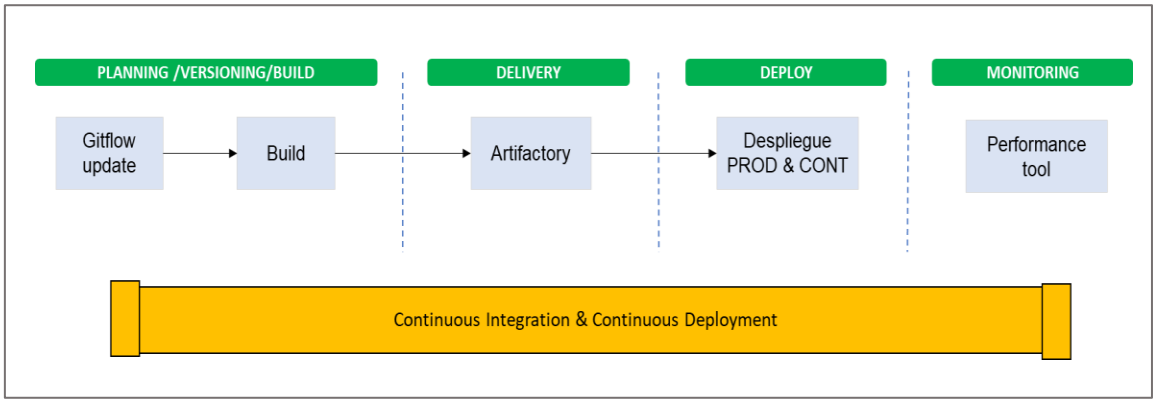
Nota: Elaboración propia

Figura 17: Pipeline DevOps de calidad



Nota: Elaboración propia

Figura 18: Pipeline DevOps de producción



Nota: Elaboración propia

- Definición de requisitos de seguridad en el DevOps implementado (operación de la plataforma de microservicios).

  A través de los resultados encontrados en la evaluación de desarrollo seguro SAMM, se identificó la falta de herramientas de seguridad y controles de seguridad en la construcción en la plataforma de microservicios, como resultado, se definieron como requisitos instalar herramientas de seguridad, mejorar la configuración de seguridad de las herramientas y definir lineamientos DevSecOps.

  A continuación, se detalla la especificación de requisitos para la implementación DevSecOps:

  Herramienta de seguridad SAST

  Se identificó la falta de escaneo de vulnerabilidades de seguridad en el código y los componentes de terceros de los microservicios en el ambiente de desarrollo (librerías externas).

  Herramienta de seguridad SAILC

  Se identificó la falta de escaneo de vulnerabilidades en las imágenes y los contenedores desplegados de los microservicios en el ambiente de desarrollo.

Herramienta de seguridad DAST

Se identificó la falta de pruebas de seguridad en el ambiente de calidad, tales como pruebas dinámicas de seguridad.

Guías de Hardening

Se identificó la falta de refuerzo en las configuraciones de seguridad en la mayoría del stack de herramientas DevOps.

Lineamientos DevSecOps

Se identifico la necesidad de definir los lineamientos de un ambiente DevSecOps, las buenas prácticas, estándares e indicadores que la operación de esta práctica requiere.

- **Instalación e integración DevSecOps**

  Esta actividad se dividió en dos tareas claramente diferenciadas, la primera consiste en realizar la gestión de adquisición de las herramientas SAST, SAILC y DAST.

  El rol principal en encargada en hacer la adquisición de herramientas fue la entidad bancaria, sin embargo, la elección y especificación de las características de las suscripciones de las herramientas fue realizada principalmente por el equipo de trabajo de NTT DATA.

  Finalmente, se adquirió la suscripción de las herramientas SAST y SAILC de tipo SaaS por un año, mientras que la herramienta DAST se implementaría en el ambiente on premise e instalándose en el stack de herramientas DevOps, contando cada herramienta con las siguientes características:

  - Herramienta SAST

    Proviene de una empresa y herramienta líder en análisis de código estático y composición de software automatizado.

  - Herramienta SAILC

    Plataforma líder en escaneo de seguridad automatizado de imágenes y monitoreo de compliance y políticas de contenedores en tiempo real.

  - Herramienta DAST

    Plataforma web para pruebas dinámicas automatizadas en APIS y microservicios.

  Se procedió a realizar la instalación e integración de las herramientas de seguridad en el DevOps, principalmente generar las keys de integración de las herramientas de seguridad y configurar las keys generadas en la herramienta orquestadora CI/CD.

  Luego de realizar la integración y según lo explicado en el análisis de requerimientos, los pipelines están desarrollados en lenguaje Groovy, por lo tanto, el arquitecto de seguridad de NTT DATA tuvo la

responsabilidad de modificar los pipelines de desarrollo y calidad según los lineamientos DevOps de la entidad bancaria, para el presente proyecto, se realizo el piloto DevSecOps para dos microservicios.

- Pipeline desarrollo DevSecOps

  Se crearon dos nuevos stages que se ejecutaran automáticamente en la orquestación CI/CD.

  En la figura 19, se muestra el stage de escaneo SAST que inicia con la obtención y validación de credenciales para validar la integración con la herramienta SAST, luego se envía el compilado del microservicio a la herramienta para que realice el escaneo, finalizando el escaneo, se muestra un reporte en el Job del pipeline del escaneo para facilidad de los desarrolladores.

Figura 19: Stage SAST

```
stage(Escaneo SAST') {
      def ap_name = getApplicationName()
      def scanName = currentGitCommit()

      withCredentials(credentials){
            veracode applicationName: "${ap_name}",
            createProfile: false,
            canFailJob: false,
            debug: true,
            fileNamePattern: '',
            replacementPattern: '',
            scanExcludesPattern: '',
            scanIncludesPattern: '',
            scanName: "${scanName}",
            teams: 'Default Team',
            timeout: 60,
            uploadExcludesPattern: '',
            uploadIncludesPattern: 'target/**.jar',
            vid: veracode_mb_username,
            vkey: veracode_mb_password,
            waitForScan: true
      }
}
```

Nota: Elaboración propia

En la figura 20, se muestra el stage de escaneo SAILC inicia con la obtención y validación de credenciales para obtener el acceso al registry de las imágenes, luego se procede a enviar dicha imagen a la herramienta para que realice el escaneo, finalizando el escaneo, se muestra visualmente el reporte en el Job del pipeline del escaneo para los arquitectos de microservicios.

Figura 20: Stage SAILC

```
stage(Escaneo SAILC') {
      credentialBinding = getCredentialMap(credentials)

      def DOCKER_SUPPORT_REGISTRY="registry-default.bco:443"
      def MASTER_URL = "https://masterdescal.bco:8443"
      def DOCKER_SUPPORT_REGISTRY_URL="${DOCKER_SUPPORT_REGISTRY}"
      def DOCKER_SERVER="tcp://host:2385"

      withCredentials(credentialBinding){
            sh(returnStdout: true, script: " login -- username ${
            EXTERNAL_REGISTRY_USERNAME} --password
            ${EXTERNAL_REGISTRY_PASSWORD} ${MASTER_URL})

            prismaCloudScanImage ca: '',
            cert: '',
            dockerAddress: "${DOCKER_SERVER}",
            image: "${project}".toLowerCase()+"++"/${pom_ap_name}:*",
            key: '',
            logLevel: 'info',
            podmanPath: '',
            project: '',
            resultsFile: 'prisma-cloud-scan-results.json',
            ignoreImageBuildTime:true
      }
}
```

Nota: Elaboración propia

La integración con la herramienta SAILC (IAST) incluye la instalación de defenders en los clústeres de desarrollo, claridad, producción y contingencia, estos componentes son los que permiten el monitoreo en tiempo real de los contenedores, los cuales fueron instalados.

- Pipeline calidad DevSecOps

En la figura 21, se muestra el pipeline de calidad donde se creó un nuevo Stage llamado Pruebas DAST que se ejecuta automáticamente en la orquestación CI/CD.

El stage de pruebas DAST inicia con la obtención y validación del token de acceso a la herramienta DAST, luego se procede a enviar los endpoints de Swagger del microservicio para que la herramienta pueda realizar las pruebas respectivas.

Figura 21: Stage DAST

```
stage('Pruebas DAST ') {
     def urlJson = "https://${utils.getApplicationName()}}/swagger/swagger2.json"
     def endpoints = urlJson.getEndpoints()

     withCredentials(credenciales) {
         def Burp_server="http://url.burp.bco:8080"
         def app_name = getApplicationName()

         sh label: 'Create scan in Burp Server',
         script: """
         curl -X POST \'${Burp_server}/api/${vToken}/v0.1/scan'\
         -H "Expect:" \
         -H "Content-Type: text/json; charset=utf-8" \
         - d \'{ "name":"${app_name}",
              "scan_configurations":[{"name":"API","type":"NamedConfiguration"}],
              "urls":${endpoints}
            }\'
        """
    }
}
```

Nota: Elaboración propia

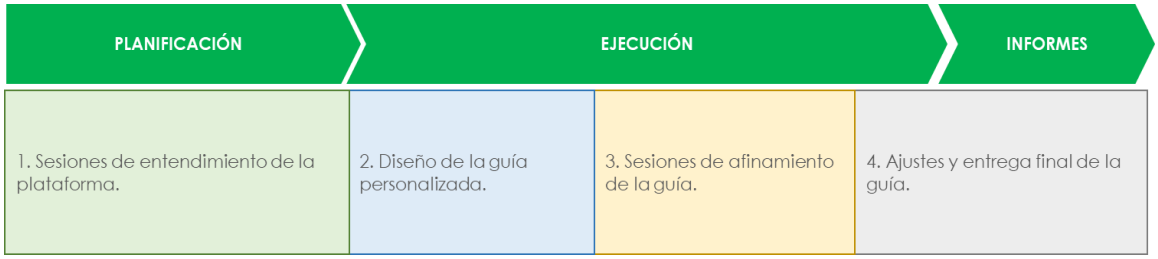
- Elaboración de Guías de Hardening

  Esta actividad se traduce a un entregable por cada herramienta que se requiere mejorar su configuración de seguridad. Se seleccionaron las siguientes herramientas para securizar su configuración:

  - Guía de Hardening CI/CD
  - Guía de Hardening GIT
  - Guía de Hardening Artefactory
  - Guía de Hardening Plataforma SaaS
  - Guía de Hardening de herramienta SAST
  - Guía de Hardening de herramienta DAST
  - Guía de Hardening de herramienta SAILC

En la figura 22, se muestra la metodología propia de NTT DATA para la generación de las Guías de Hardening, por lo tanto, solo se explicará una referencia de la metodología aplicada.

Figura 22: Referencia a la metodología para Guías de Hardening



Nota: Elaboración propia

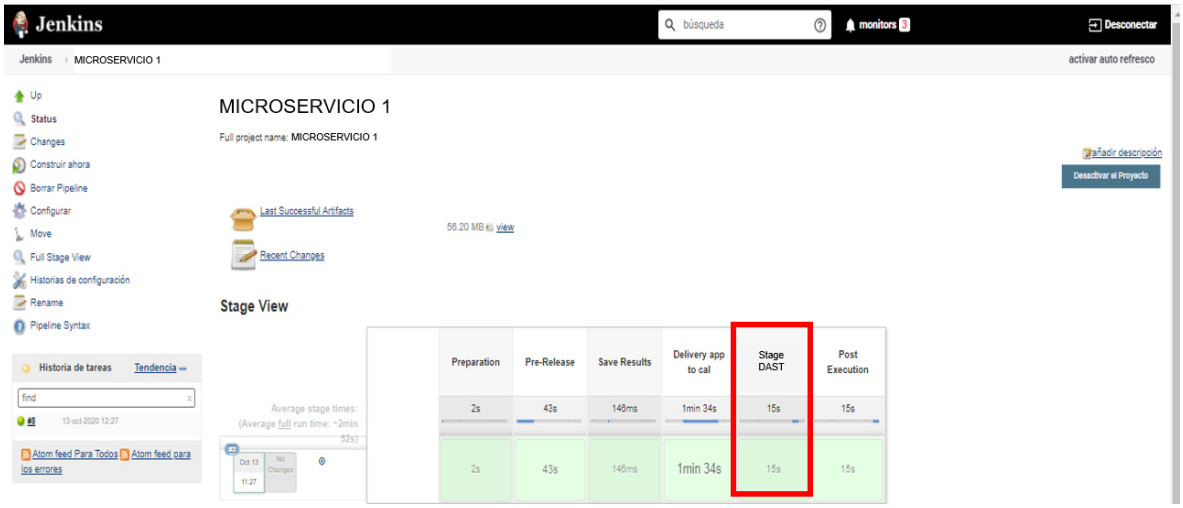
El diseño y contenido de las guías se basan en las buenas prácticas y lineamientos de configuración que nos brinda el Centro para la seguridad del internet (CIS Center for Internet Security), estándar PCI (Security Standars Council) y la documentación del fabricante de la herramienta o plataforma.

- Piloto DevSecOps

  Posterior a la instalación e integración de las herramientas de seguridad se ejecutó los pipelines construidos de dos microservicios, con el objetivo de evaluar los resultados y verificar que se cumplen con los requisitos especificados.

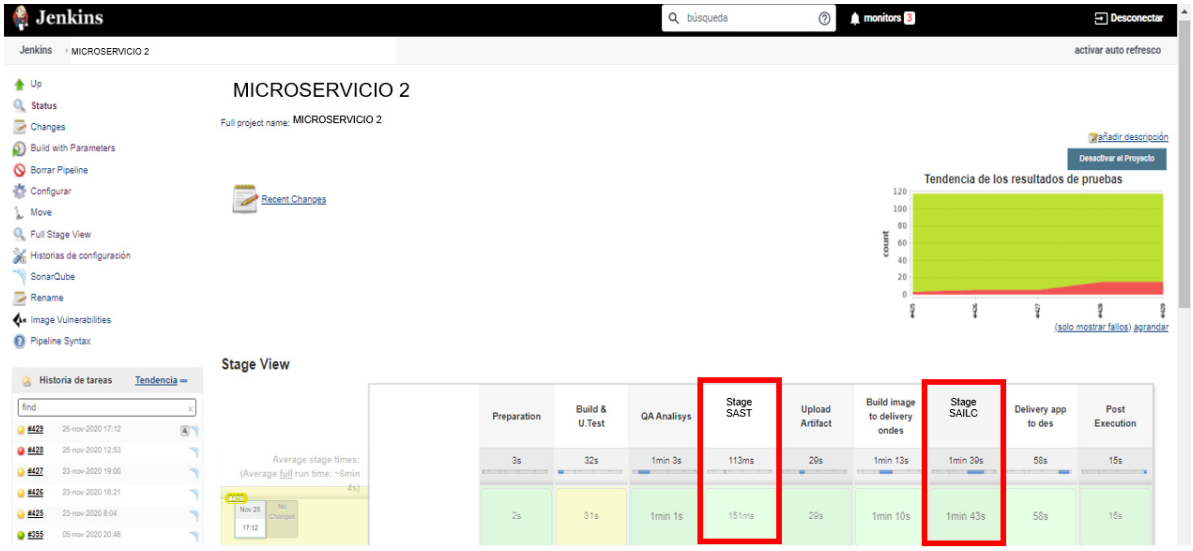
  En las figuras 23 y 24, mostraremos el resultado de la ejecución de satisfactoria de cada Stage de los pipelines DevSecOps de desarrollo y calidad en la herramienta CI/CD de los microservicios.

Figura 23: Ejecución del pipeline DevSecOps calidad del microservicio 1



Nota: Elaboración propia

Figura 24: Ejecución del pipeline DevSecOps de desarrollo del microservicio 2



Nota: Elaboración propia

Adicional a las evidencias del resultado satisfactorio de los pipelines DevSecOps, se muestra un ejemplo de los reportes de los escaneos generados por cada herramienta en el **Anexo 4.**

- Elaboración Lineamientos DevSecOps

  Posterior la implementación DevSecOps, se deben definir las bases sobre la cual se regirán esta nueva practica y el alcance de lo implementado.

  A continuación, se definirán los lineamientos con respecto a la operación del DevSecOps:

  - Entorno DevSecOps

    a. Software de automatización

      - Se debe automatizar los ´pipelines con una herramienta CI/CD.
      - Se diseña los pipelines con el estándar Groovy.

    b. Dependencias del Pipeline

      - Se deben utilizar plugin para la integración con las herramientas en los pipelines.

    c. Diseño de Pipeline

      - Las credenciales de conexión deben parametrizadas.
      - Se deben imprimir los logs por cada Stage claros.
      - Se deben manejar las excepciones por cada aplicación.

  - Pruebas de seguridad

    Se definieron los siguientes lineamientos para las pruebas de seguridad implementadas.

    a. Seguridad del Código

      - Todas las buenas prácticas y estándares de seguridad para el desarrollo del código de los microservicios serán validadas.
      - Todos los microservicios deben ser validados por las herramientas de pruebas SAST, para ser desplegados en los ambientes productivos sin excepción alguna.

b. Pruebas de seguridad en el entorno

- En la ejecución de pruebas deben validarse a nivel de red, sistema y aplicación.
- Las imágenes generadas deben ser validados por Prisma la herramienta SAILC, para ser desplegados en los ambientes productivos sin excepción alguna.

c. Pruebas de aplicación

- Se debe garantizar que se identifiquen las vulnerabilidades documentadas por OWASP.
- Todos los microservicios deben ser validados por la herramienta de pruebas DAST para ser desplegados en los ambientes productivos sin excepción alguna.

- Políticas de seguridad

Las herramientas encargadas de hacer las pruebas de seguridad deben ser configuradas de acuerdo con los siguientes lineamientos.

a. Todos los microservicios que son escaneadas deben ser registrada con un nivel de criticidad de negocio en la herramienta de seguridad.

b. Los microservicios deben ser escaneadas con los escenarios y técnicas que brinda la herramienta acorde a la arquitectura de los microservicios.

c. La herramienta debe definir reglas para verificación de estándares de seguridad y complaince.

- Tableros de control

a. Métricas

Se definen las siguientes métricas para la operación DevSecOps:

- Riesgo de microservicios

- Número de microservicios complaince
- Vulnerabilidades según severidad
- Estado de remediación de vulnerabilidades

b. Trazabilidad y Reportes

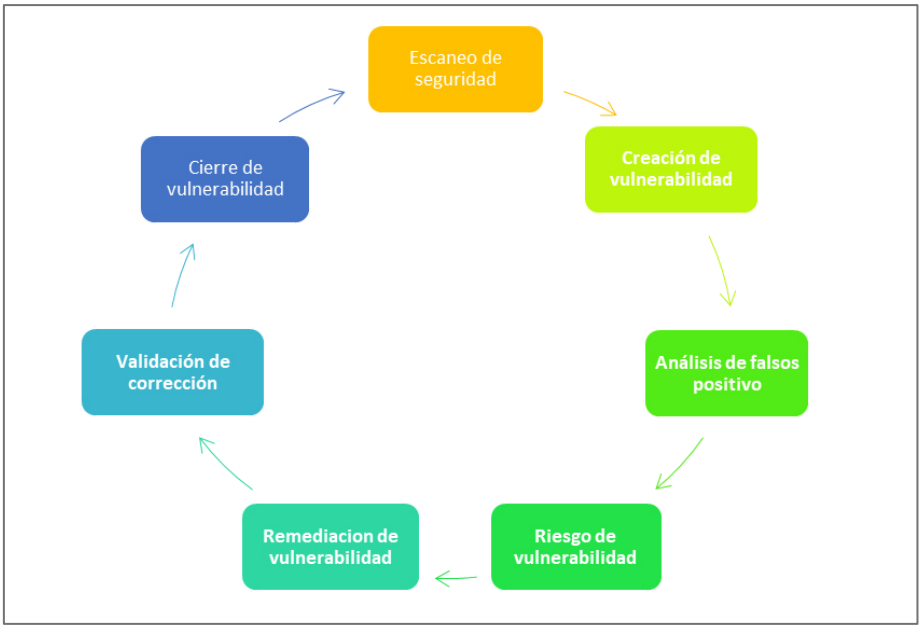
Se debe generar informes técnicos y ejecutivos con periodicidad mensual, para el seguimiento de la seguridad de ellos microservicios en DevSecOps.

- Gestión de vulnerabilidades

Con esta nueva practica DevSecOps implementada, se identificarán defectos de seguridad a las cuales llamaremos vulnerabilidades, por lo tanto, se debe definir un proceso de gestión de vulnerabilidades.

En la figura 25, se muestran las fases de este proceso cíclico.

Figura 25: Proceso de gestión de vulnerabilidades



Nota: Elaboración propia

El enfoque DevSecOps no consiste solo en instalar herramientas y lineamientos de seguridad, sino que permite evolucionar un modelo operativo al nivel de madurez del desarrollo seguro en la entidad bancaria.

3.3. Evaluación

3.3.1 Evaluación económica

El presente proyecto se divide en dos tipos de costo para el cliente, le primero es el costo de la consultoría, y el costo de las herramientas DevSecOps implementadas.

El principal costo de la consultoría está asociado a las horas hombres de los consultores e instalación de herramientas DevSecOps. El otro costo son las suscripciones anuales de las herramientas de seguridad.

En la tabla 12 se muestra el costo de la consultoría brindad por NTT DATA, es importante resaltar que los datos son referenciales, debido a la restricción a dicha información.

Tabla 12: Costo referencial de la consultoría

Servicio	N° Meses	Costo total
Consultoría	4	150,000.00
Total	4	150,000.00

Nota: Elaboración propia

En la tabla 13 se muestra el costo de la adquisición y suscripciones de las herramientas de seguridad, las suscripciones son de tipo anual, es importante resaltar que los datos son referenciales, debido a la restricción a dicha información.

Tabla 13: Costo referencial de suscripción de herramientas

Suscripción	N° Suscripciones	Costo total
Herramientas de seguridad	3	200,000.00
Total	**3**	**200,000.00**

Nota: Elaboración propia

- Costo de inversión de proyecto: S/ 350,00.00

3.3.2 Evaluación del VAN y del TIR

A continuación, se simulará el cálculo de viabilidad de inversión a través de la reducción de costos, mediante la reducción de los Ethical Hacking, pruebas manuales de seguridad solicitada a externos como servicios de seguridad (Las posibles multas por la regulación de SBS N° 504-2021 no será tomada para el siguiente ejercicio).

Se uso la fórmula del Valor Actual Neto (VAN) para la evaluación de del proyecto:

$$\mathrm{VAN} = \sum \frac{\mathrm{FC_n}}{(1 + \mathrm{TDP})^{\mathrm{n}}}$$

Donde:

- $\mathrm{FC_n}$: son los flujos de caja por cada periodo n.
- TPD: la tasa privada de descuento.
- n: número de períodos de evaluación.

Inversión total

- El costo de inversión de proyecto es S/ 350,000.00.
- El costo anual que se generará por las suscripciones de las herramientas será de S/ 160,000.00.

Egresos antes de la ejecución del presente proyecto

- Los egresos anuales antes generados por las pruebas manuales de seguridad son S/ 291,600.00. En la tabla 14, podemos ver los costos referenciales de pruebas de seguridad manual, es importante resaltar que los datos son referenciales.

Tabla 14: Gasto referencial de pruebas de seguridad manual

Servicio	Aplicaciones	Costo total
Pruebas DAST	6	97,200.00
Pruebas SAST	6	194,400.00
Total	**12**	**291,600.00**

Nota: Elaboración propia

Las variables de la ecuación de TAR y TIR son las siguientes:

- TDP: 12%
- Flujo efectivo: S/ 131,600.00 (el mismo para los 5 años), ver la tabla 14.

El valor del flujo efectivo se calculó en esta simulación como la resta de los egresos generados por pruebas manuales de seguridad antes del proyecto y los costos de la suscripción de las herramientas de seguridad del proyecto (en las fórmulas se incluye el total de la inversión del proyecto).

Tabla 15: Flujo efectivo para el cálculo del VAN y TIR

Flujo Efectivo	
Año	**Valor**
1	S/ 131,600.00
2	S/ 131,600.00
3	S/ 131,600.00
4	S/ 131,600.00
5	S/ 131,600.00

Nota: Elaboración propia

A continuación, se muestra los resultados del VAN y TIR, como se observa le TIR es positivo y mayor al 12% del TDP, por lo tanto, el proyecto será rentable.

- VAN: S/ 124,388.55
- TIR: 26%

CAPÍTULO IV
REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

El autor del presente informe ha tenido el rol de ingeniero y su participación en el proyecto de implementación de la practica DevSecOps ha logrado aportar lo siguiente:

- Implementar una práctica de seguridad en la plataforma de microservicios moderna, ágil y escalable.
- Iniciar con la incorporación de la cultura de seguridad en el desarrollo de software del cliente.
- Completar un proyecto de calidad, efectivo y alineado a las políticas del cliente.

En el presente proyecto he podido identificar la importancia de crear un plan de trabajo para cada etapa del proyecto especificada y aprobada, esto permite que el cliente este alineado a los objetivos del proyecto. Así mismo, aprendí que existen estándares, frameworks y herramientas que pueden ayudar a la mejorar los entregables y las propuestas en desarrollo seguro o DevSecOps, tales como OWASP ASVS, BSIMM y DefectDojo.

He logrado identificar que una de las principales mejoras que se puede plantear para un proyecto DevSecOps sobre un DevOps robusto, es incluir una iniciativa de gestión de vulnerabilidades bajo herramientas y procesos automatizados, esto debido a que la practicas DevSecOps incluirá nuevas actividades como: generación de informes técnicos, responsabilidades, interacción con áreas involucradas y remediaciones de defectos de seguridad de aplicaciones.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

A continuación, describiremos las conclusiones del proyecto en el desarrollo del presente informe:

- La utilización de metodologías para la gestión del proyecto permitió crear una propuesta comercial sólida y ejecutar un proyecto con la calidad esperada.
- La metodología SAMM de OWASP ha sido una base fundamental para el desarrollo del proyecto del presente informe, permitió alinear los objetivos de la entidad bancaria a los lineamientos y buenas prácticas en el aseguramiento de las aplicaciones.
- La implementación de las herramientas de seguridad automatizadas, incorporaron buenas prácticas de seguridad e iniciaron el camino hacia la automatización de controles de seguridad, lo que significa la adopción de un nivel alto de seguridad en el ciclo de desarrollo de los microservicios.
- Se evidenció que una de las principales brechas de seguridad en los equipos de desarrollo es la cultura de seguridad, principalmente se debe a la falta de procedimientos, roles y responsabilidades para la corrección de nuevos defectos de seguridad.
- Se evidenció que es importante definir un proceso de gestión de vulnerabilidades para el DevSecOps de los microservicios, ya que en las pruebas piloto se encontraron vulnerabilidades de nivel críticas.

5.2 Recomendaciones

A continuación, se detallarán las recomendaciones a cerca del proyecto desarrollado:

- Se recomienda continuar la practica DevSecOps, con una primera etapa de socialización, donde se pueda capacitar a las áreas involucradas en el ciclo de vida de desarrollo se los microservicios.
- Se recomienda que la practica desarrollada se incluye a las políticas generales de seguridad de la información.
- Se recomienda actualizar o definir roles, procesos y responsabilidades, de tal modo que la practica DevSecOps sea gobernada por un área de la entidad bancaria.
- Se recomienda tener clara las responsabilidades de administración de herramientas de seguridad incorporadas.
- Se recomienda tener un seguimiento de la practica DevSecOps mediante los KPIs y métricas definidas en los lineamientos generados por parte de NTT DATA.
- Si bien se han incluido nuevas herramientas con un costo a incluir en el presupuesto anual de la entidad bancaria, se debe plantear la inclusión de nuevas herramientas licenciadas o libre, buscando la evolución y eficiencia de la practica DevSecOps, como por ejemplo herramientas de gestión de vulnerabilidades o herramientas de gestión de secretos.

ANEXOS

ANEXO 1. PLANTILLA DE ACTA DE REUNIÓN

Resumen					
Acta reunión Entrevista Grupo Seguridad Evaluación SAMM					
Registro de modificaciones					
Versión	**Descripción**	**Autor**	**Fecha creación**	**Aprobado por**	**Fecha aprobación**
1.0	Versión inicial	Manuel Machuca	20/12/2020		

ACTA DE REUNIÓN		
Citada por: Líder de Ciberseguridad		**Fecha:** 20/12/2020
Hora inicio: 02:00 pm	**Hora Fin:** 3:00 pm	**Lugar:** Reunión Virtual Microsoft Teams
Objetivo: Realizar la entrevista al grupo de seguridad para la evaluación de nivel de madurez en prácticas de desarrollo seguro acorde al marco de trabajo SAMM		
ASISTENTES		
Entidad Bancaria • Ingeniero de microservicios		NTT DATA • Consultor S-SDLC

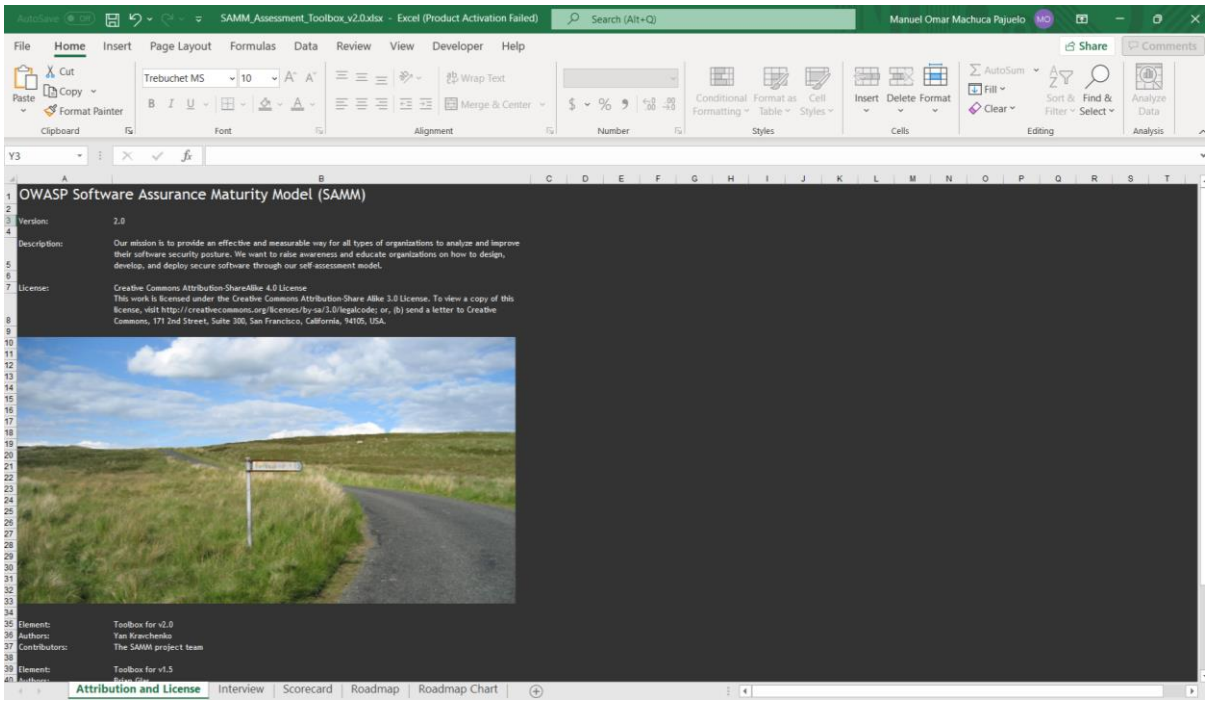
Puntos desarrollo en la entrevista

- Consultor S-SDLC: ¿Cómo se viene gestionando de parte de gobierno desde la perspectiva de seguridad con respecto a lo que es construcción y medidores de seguridad?
- Entrevistado: Respuesta

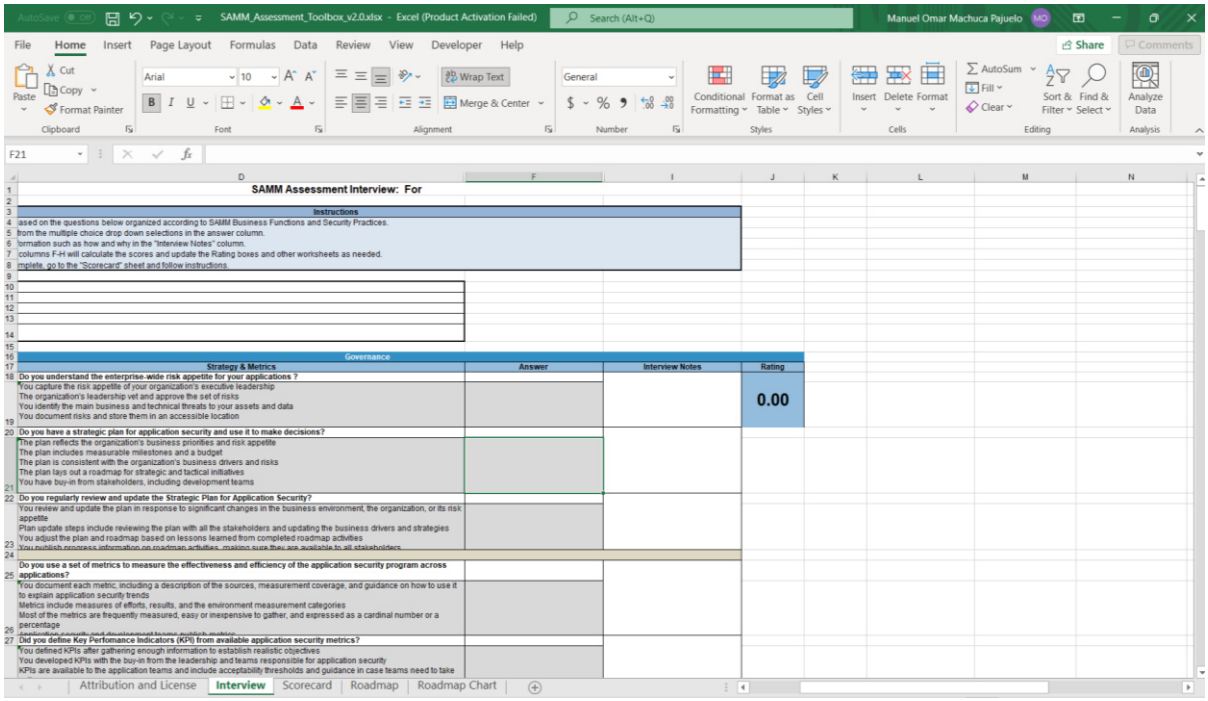
Descripción	**Responsable**	**Fecha de ejecución**	**Estado**
Lineamientos de desarrollo	Ingeniero de microservicios	05/08/2020	Pendiente

ANEXO 2. PLANTILLA SAMM ASSESSMENT TOLLBOX 2.0

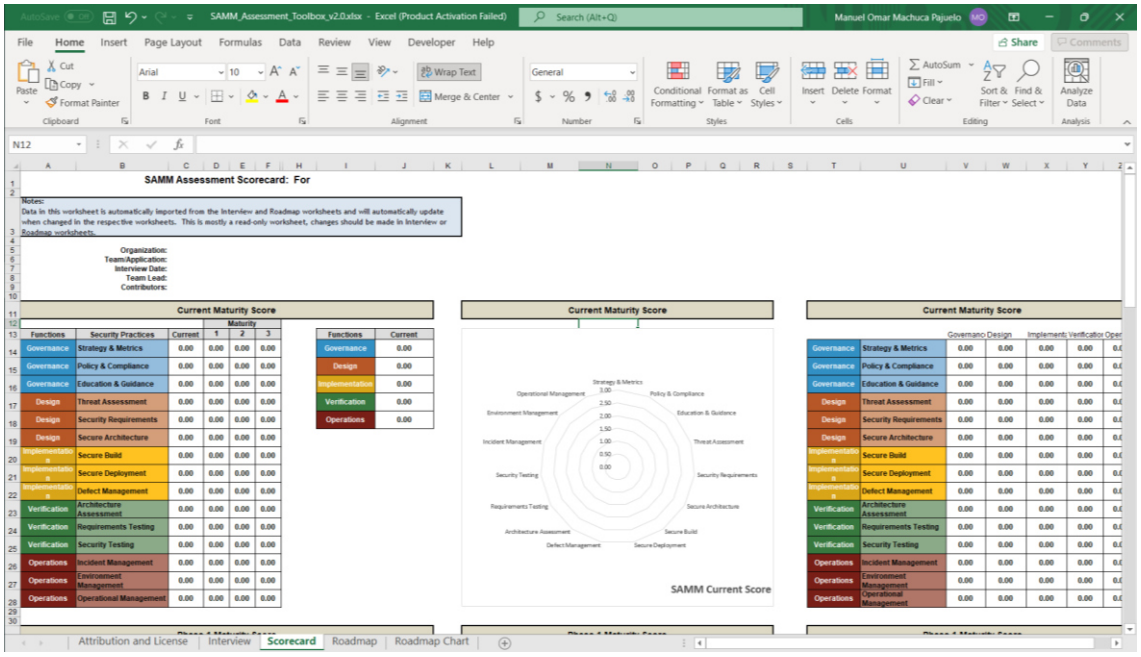
Hoja de presentación



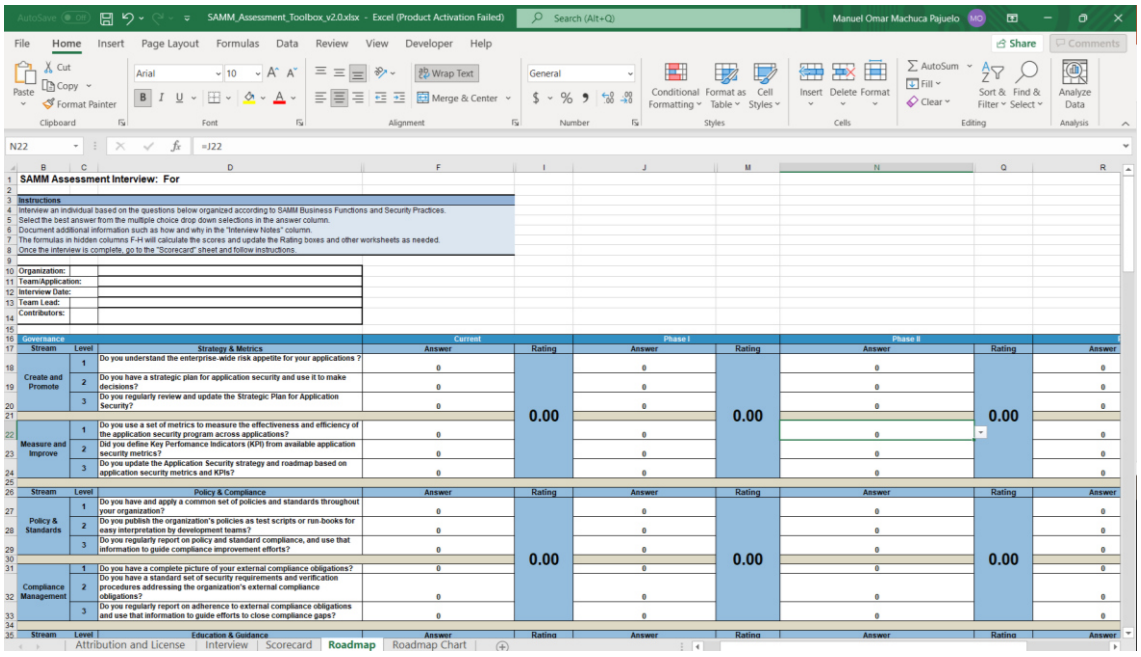
Hoja de entrevista



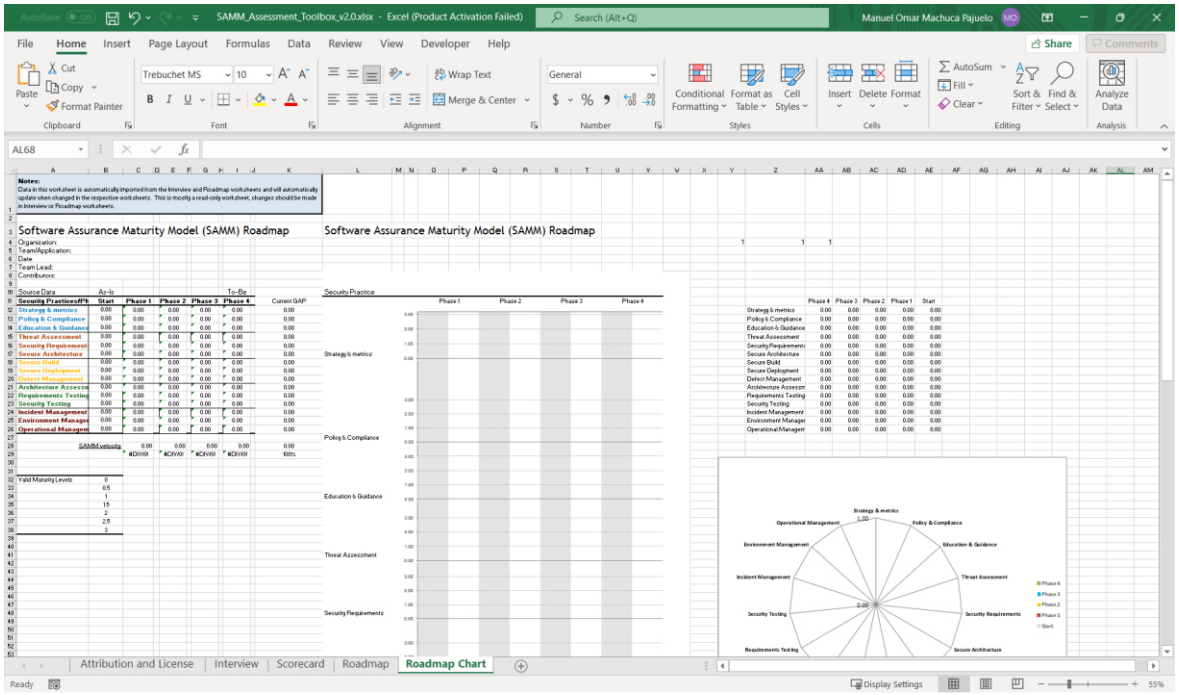
Hoja de Scorecard



Hoja de roadmap

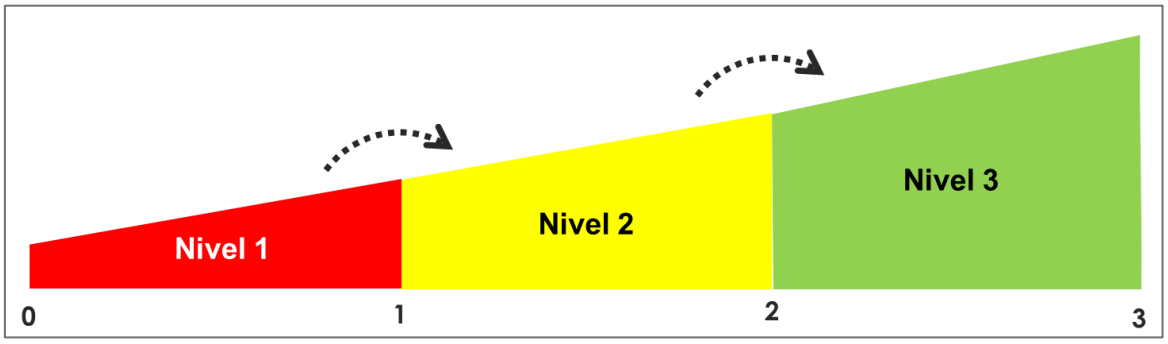


Hoja de Roadmap Chart



ANEXO 3. NIVELES DE MADUREZ SEGUN SAMM

Cada nivel tiene un objetivo sucesivamente más sofisticado con actividades específicas y métricas de éxito más estrictas.



Nivel 1: De 0 a 1

Existen procesos formalizados, y operativos con métricas, con alcance a la mayoría de las aplicaciones de la organización.

Nivel 2: De 1 a 2

Existen procesos, repetibles, pero no formalizadas, con alcance limitado a algunas aplicaciones de la organización.

Nivel 3: De 2 a 3

Existen procesos con mejora continua a través de indicadores, para todas las aplicaciones de la organización.

ANEXO 4. REPORTES DE ESCANEOS DE SEGURIDAD DE LOS MICROSERVICIOS

Reportes de los escaneos de la herramienta SAST, que adicionalmente muestra resultados SCA (librerías externas).

Resultados de escaneo SAST

	A	B	C	D	E	F	G	H	I	J	K	L	M
181	Medium	Insufficient Entropy	331		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
182	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
183	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
184	Medium	Insufficient Entropy	331		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
185	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
186	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
187	Medium	Insufficient Entropy	331		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
188	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
189	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
190	Medium	Insufficient Entropy	331		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
191	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
192	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
193	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
194	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
195	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
196	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
197	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
198	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
199	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
200	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
201	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
202	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
203	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
204	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
205	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
206	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
207	Medium	Improper Output Neutralization for Logs	117		Feb. 26, 2021	103	13	Admin User	SAST Scan	Active, Verified			
208	Medium	Use of a Broken or Risky Cryptographic Algorithm	327		May 17, 2021	23	67	Admin User	SAST Scan	Active, Verified			
209	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			
210	Medium	Improper Output Neutralization for Logs	117		May 20, 2021	20	70	Admin User	SAST Scan	Active, Verified			
211	Medium	Improper Output Neutralization for Logs	117		Feb. 16, 2021	113	23	Admin User	SAST Scan	Active, Verified			

Resultados de escaneo SCA

	A	B	C	D	E	F	G	H	I	J	K	L
396	Medium	Vulnerable Component: Netty-Codec-Http:4.1.36.Final		CVE-2019-16869	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
397	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36179	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
398	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-11620	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
399	Medium	Vulnerable Component: Spring-Cloud-Config-Client:2.1.1.RELE...		CVE-2020-5405	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
400	Medium	Vulnerable Component: Netty-Codec-Http:4.1.36.Final		CVE-2019-20444	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
401	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36180	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
402	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-14060	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
403	Medium	Vulnerable Component: Spring-Security-Crypto:5.1.5.RELEASE		CVE-2020-5408	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
404	Medium	Vulnerable Component: Netty-Codec-Http:4.1.36.Final		CVE-2019-20445	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
405	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36181	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
406	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-14061	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
407	Medium	Vulnerable Component: Snakeyaml:1.23		CVE-2017-18640	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
408	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36182	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
409	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-14062	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
410	Medium	Vulnerable Component: Netty-Codec:4.1.36.Final		CVE-2020-10707	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
411	Medium	Vulnerable Component: Netty-Codec-Http:4.1.36.Final		SRCCLR-SID-21787	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
412	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36183	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
413	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-14195	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
414	Medium	Vulnerable Component: Netty-Codec:4.1.36.Final		CVE-2020-11612	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
415	Medium	Vulnerable Component: Netty-Codec-Http:4.1.36.Final		SRCCLR-SID-3108	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
416	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36184	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
417	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-24616	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
418	Medium	Vulnerable Component: Commons-Codec:1.11		SRCCLR-SID-22742	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
419	Medium	Vulnerable Component: Reactor-Netty:0.8.8.RELEASE		CVE-2019-11284	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
420	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36185	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
421	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-24750	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
422	Medium	Vulnerable Component: Reactor-Netty:0.8.8.RELEASE		CVE-2020-5403	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
423	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36186	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
424	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-25649	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
425	Medium	Vulnerable Component: Reactor-Netty:0.8.8.RELEASE		CVE-2020-5404	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		
426	Medium	Vulnerable Component: Jackson-Databind:2.9.8		CVE-2020-36187	May 18, 2021	22	68	Admin User	SAST Y SCA Scan	Active, Verified		

Reportes de los escaneos de la herramienta SAILC y DAST.

Resultados de escaneo SAILC

Findings List

Severity	Name	CWE	CVE	Date	Age	SLA	Reporter	Found By	Status
Info	Cacheable HTTPS Response	524		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Cross-Site Scripting (Reflected)	79		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active
Info	Input Returned in Response (Reflected)	20		June 2, 2021	1		Admin User	DAST Scan	Active

Resultados de escaneo DAST

94	High	CVE-2019-11745: NSS-Util - 3.36.0-1.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
95	High	CVE-2020-1971: Openssl-Libs - 1.0.2k-16.el7_6.1	CVE-2020-1971	June 3, 2021	0	30	Admin User	SAILC Scan	Active
96	High	CVE-2019-13734: Sqlite - 3.7.17-8.el7	CVE-2019-13734	June 3, 2021	0	30	Admin User	SAILC Scan	Active
97	High	CVE-2019-11729: NSS - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
98	High	CVE-2019-11729: NSS-Softokn-Freebl - 3.36.0-5.el7_5	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
99	High	CVE-2019-11745: NSS - 3.36.0-7.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
100	High	CVE-2019-11745: NSS-Softokn-Freebl - 3.36.0-5.el7_5	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
101	High	CVE-2021-27219: Glib2 - 2.56.1-4.el7_6	CVE-2021-27219	June 3, 2021	0	30	Admin User	SAILC Scan	Active
102	High	CVE-2019-11729: NSS-Util - 3.36.0-1.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
103	High	CVE-2019-11729: NSS-Softokn - 3.36.0-5.el7_5	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
104	High	CVE-2019-11745: NSS-Util - 3.36.0-1.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
105	High	CVE-2019-11745: NSS-Softokn - 3.36.0-5.el7_5	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
106	High	CVE-2019-13734: Sqlite - 3.7.17-8.el7	CVE-2019-13734	June 3, 2021	0	30	Admin User	SAILC Scan	Active
107	High	CVE-2019-11729: NSS - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
108	High	CVE-2019-11745: NSS - 3.36.0-7.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
109	High	CVE-2020-1971: Openssl-Libs - 1.0.2k-16.el7_6.1	CVE-2020-1971	June 3, 2021	0	30	Admin User	SAILC Scan	Active
110	High	CVE-2019-11729: NSS-Tools - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
111	High	CVE-2019-11745: NSS-Tools - 3.36.0-7.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
112	High	CVE-2021-27219: Glib2 - 2.56.1-4.el7_6	CVE-2021-27219	June 3, 2021	0	30	Admin User	SAILC Scan	Active
113	High	CVE-2019-11729: NSS-Util - 3.36.0-1.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
114	High	CVE-2019-11729: NSS-Softokn - 3.36.0-5.el7_5	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
115	High	CVE-2019-11745: NSS-Util - 3.36.0-1.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
116	High	CVE-2019-11745: NSS-Softokn - 3.36.0-5.el7_5	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
117	High	CVE-2019-13734: Sqlite - 3.7.17-8.el7	CVE-2019-13734	June 3, 2021	0	30	Admin User	SAILC Scan	Active
118	High	CVE-2020-1971: Openssl-Libs - 1.0.2k-16.el7_6.1	CVE-2020-1971	June 3, 2021	0	30	Admin User	SAILC Scan	Active
119	High	CVE-2019-13734: Sqlite - 3.7.17-8.el7	CVE-2019-13734	June 3, 2021	0	30	Admin User	SAILC Scan	Active
120	High	CVE-2019-11729: NSS-Sysinit - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
121	High	CVE-2019-11745: NSS-Sysinit - 3.36.0-7.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active
122	High	CVE-2019-11729: NSS - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
123	High	CVE-2019-11729: NSS-Tools - 3.36.0-7.1.el7_6	CVE-2019-11729	June 3, 2021	0	30	Admin User	SAILC Scan	Active
124	High	CVE-2019-11745: NSS - 3.36.0-7.1.el7_6	CVE-2019-11745	June 3, 2021	0	30	Admin User	SAILC Scan	Active

BIBLIOGRAFÍA

Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A Multivocal Literature Review. International Conference on Software Process Improvement and Capability Determination.

NTT DATA GLOBAL. (2021). NTT DATA GLOBAL. Obtenido de https://www.nttdata.com/global/en/about-us/our-way.

NTT DATA PERÚ. (2021). NTT DATA PERÚ. Obtenido de https://pe.nttdata.com/about-us.

OWASP. (2021). OWASP . Obtenido de https://owasp.org/www-project-samm/.

OWASP SAMM. (2021). OWASP SAMM. Obtenido de https://owaspsamm.org/about/.

Tomas, N., Li, J., & Huang, H. (2019). An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).