**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

*Resolución: RPC-SO-02-No.053-2021*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER**

| |
|---|
| **Título del proyecto:** |
| Métricas de seguridad para evaluar los procesos en el Sistema integrado de gestión estratégica de la Universidad Israel aplicando los principios de DevSecOps. |
| **Línea de Investigación:** |
| Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable |
| **Campo amplio de conocimiento:** |
| " Tecnologías de la Información y Comunicación" |
| **Autor:** |
| Santacruz Egas Jonathan Patricio |
| **Tutores:** |
| Mg Toasa Renato<br>PhD. Urdaneta Maryori |

**Quito – Ecuador**

**2024**

**APROBACIÓN DEL TUTOR**

Yo, Toasa Guachi Renato Mauricio con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps.

Elaborado por: Jonathan Patricio Santacruz Egas, de C.I: 1003856539, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

**Firma**

**“APROBACIÓN DEL TUTOR”**

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps.

Elaborado por: Jonathan Patricio Santacruz Egas, de C.I: 1003856539, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 25 septiembre 2024

**Firma**

**DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE**

Yo, Jonathan Patricio Santacruz Egas con C.I: 1003856539, autor/a del proyecto de titulación denominado: Desarrollo de métricas de seguridad para evaluar los procesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando DevSecOps prácticas de seguridad que influyen en la calidad del software.

Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

1. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
2. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024

**Firma**

**Tabla de contenidos**

**Índice de tablas**

**Índice de figuras**

## INFORMACIÓN GENERAL

### Contextualización del tema

El término DevOps empezó a moverse a raíz de la conferencia Agile de 2008, y los "DevOpsDays" que comenzaron en Bélgica, esto fue en el 2015 como el año en el que se empezó a hablar de la integración de la seguridad en los procesos DevOps, dando lugar al término DevSecOps (o también llamado como SecDevOps).

Según Microsoft et al. (2024) DevSecOps significa desarrollo, seguridad y operaciones, es un marco que integra la seguridad en todas las fases del ciclo de vida de desarrollo de software. Las organizaciones adoptan este enfoque para reducir el riesgo de publicar código con vulnerabilidades de seguridad. A través de la colaboración, la automatización y los procesos claros, los equipos comparten la responsabilidad de la seguridad, en lugar de dejarla al final cuando los problemas pueden ser mucho más difíciles y costosos de abordar. DevSecOps es un componente fundamental de una estrategia de seguridad multinube.

DevSecOps busca unir a los equipos de desarrollo, seguridad y operaciones, promoviendo una colaboración estrecha y la integración de sus procesos. Esta colaboración mejora la comunicación entre todos los involucrados, lo que permite implementar prácticas de seguridad eficaces en cada fase del desarrollo de tecnología (Plain concepts, 2023).

El enfoque DevOps surgió como respuesta a la necesidad de acelerar el desarrollo de software y satisfacer las crecientes expectativas de los usuarios y clientes. Antes de DevOps, los métodos tradicionales separaban claramente el desarrollo de las operaciones, lo que llevaba a procesos más lentos, falta de colaboración y software que a menudo tenía errores y problemas de confiabilidad (Ferreres, 2021).

La Universidad Israel tiene un sistema conocido como SIGE, que es una plataforma que centraliza y coordina los procesos de planificación, ejecución, monitoreo y evaluación dentro de una organización. Su principal objetivo es alinear las actividades operativas diarias con los objetivos estratégicos de la Institución, facilitando una gestión eficiente y coherente. A través

del SIGE, las Universidad puede integrar diversas funciones como la planificación estratégica, la gestión académica, el control financiero, y la administración de recursos humanos, permitiendo una visión global y unificada de la organización.

Los procesos que realiza el SIGE primordialmente son: planificación estratégica, donde se definen los objetivos y metas a largo plazo; la gestión de recursos, que asegura la correcta asignación y utilización de los recursos financieros, humanos y materiales, así como el monitoreo y evaluación, que básicamente permite realizar un seguimiento constante de los indicadores de desempeño y la evaluación de resultados así como la generación de reportes y análisis, que apoya la toma de decisiones informadas. Por lo cual determinar métricas de seguridad para evaluar los procesos (SIGE) de la Universidad Israel, aplicando DevSecOps, representa de manera sustancial una mejora en la ciberseguridad y la calidad del software en entornos académicos.

El SIGE, como plataforma integral para la gestión administrativa y académica, requiere no solo eficiencia operativa, sino también robustez frente a posibles vulnerabilidades cibernéticas. La implementación de DevSecOps implica integrar prácticas de seguridad desde las fases iniciales del ciclo de vida del desarrollo de software, asegurando que los controles de seguridad sean automatizados y continuos.

Este enfoque proactivo no solo previene problemas de seguridad en etapas avanzadas del desarrollo, sino que también promueve la mejora continua mediante la identificación temprana y la mitigación de riesgos. La definición de métricas específicas, como la frecuencia de pruebas de seguridad, la tasa de corrección de vulnerabilidades y el tiempo de respuesta ante incidentes, facilita la evaluación objetiva de la efectividad de estas prácticas. Además, contribuye a la garantía de la calidad del software al asegurar que no solo cumple con los requisitos funcionales y de rendimiento, sino que también está protegido contra amenazas emergentes. La investigación se centrará en desarrollar un conjunto robusto de métricas adaptadas al contexto universitario del SIGE, con el objetivo de proporcionar recomendaciones concretas para optimizar la seguridad y la calidad del software en esta plataforma crítica.

Este estudio no solo buscará fortalecer la infraestructura digital de la universidad, sino también establecer un marco replicable que pueda beneficiar a otras instituciones educativas en su camino hacia la resiliencia cibernética y la excelencia en la gestión de datos sensibles.

**Problema de investigación**

La Universidad Tecnológica Israel gestiona datos cruciales sobre estudiantes, profesores y personal administrativo mediante el Sistema Integrado de Gestión Estratégica (SIGE). Este sistema es un proyecto de investigación de la carrera de Sistemas de Información que se inició en 2017 y se fundamenta en procesos tanto estratégicos como operativos. (Baldeón, 2022)

Al ser una herramienta muy utilizada en la actualidad por la comunidad de la UISRAEL, requiere una serie de controles que deben implementarse, para evitar posibles ataques o robo de información al acceder a la plataforma con el uso de credenciales poco seguras.

La falta de métricas específicas y cuantificables para evaluar la seguridad en el contexto de DevSecOps dificulta la medición del impacto de las prácticas de seguridad en la calidad del software y la reducción de riesgos. Además, la naturaleza dinámica y automatizada de los entornos DevSecOps requiere métricas que puedan adaptarse y proporcionar una visión continua del estado de la seguridad.

**Objetivo general**

Proponer métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps.

**Objetivos específicos**

- Contextualizar los fundamentos teóricos sobre DevSecOps para comprender su contexto y fundamentos.
- Diagnosticar las potenciales vulnerabilidades que podrían afectar la eficiencia, seguridad y estabilidad del SIGE de la Universidad Israel.

- Desarrollar métricas de seguridad específicas que permitan evaluar la efectividad de las prácticas de DevSecOps en el SIGE.
- Evaluar la efectividad de la estrategia de seguridad implementada en el SIGE, mediante criterios aportados por especialistas en la materia.

**Vinculación con la sociedad y beneficiarios directos:**

Esta investigación tiene un impacto significativo tanto en la institución como en la sociedad en general. La Universidad Israel será la primera en beneficiarse directamente de la investigación, ya que permitirá identificar y mitigar vulnerabilidades en su SIGE.

Esto contribuirá a la protección de datos sensibles y a la mejora de la calidad del software utilizado en la gestión académica y administrativa, lo cual es esencial para el funcionamiento eficiente y seguro de la Universidad.

Los estudiantes y el personal académico también se beneficiarán de un sistema más seguro y confiable, garantizando la integridad y confidencialidad de sus datos personales y académicos. Un entorno digital seguro permitirá a la comunidad educativa enfocarse en sus actividades académicas y de investigación sin preocuparse por posibles brechas de seguridad, lo que a su vez mejorará la productividad y la satisfacción general.

La identificación y mitigación de vulnerabilidades en el SIGE no solo protege datos sensibles, sino que también fomenta un entorno de innovación al garantizar que la Universidad pueda operar con confianza y seguridad.

Esta investigación tiene una alineación destacada con varios Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas, particularmente con el ODS 9 (Industria, Innovación e Infraestructura) además, la investigación pretende ajustarse con con el ODS 16, que busca promover sociedades pacíficas y con acceso a justicia mediante la construcción de instituciones responsables y eficaces.

La industria de la tecnología también puede beneficiarse de esta investigación, ya que la aplicación de las prácticas de DevSecOps y las métricas de seguridad puede ser extrapolada a

otros sectores más allá del educativo, promoviendo la adopción de estándares de seguridad en diversas industrias.

Al garantizar la seguridad de los sistemas de gestión académica, se protege la información de los usuarios y se fomenta la confianza en el uso de tecnologías digitales, lo cual es esencial en un mundo cada vez más interconectado.

De esta manera esta Investigación se ha desarrollado con referencia al Objetivo de Desarrollo Sostenible “Educación de Calidad” la educación debe convertirse en una prioridad nacional. Además, son esenciales medidas como la gratuidad y obligatoriedad de la enseñanza, la mejora continua en las Instituciones de nivel Superior y transformación digital.

También establece un precedente valioso para otras instituciones y sectores, promoviendo una cultura de seguridad y protección de la información en la sociedad en general. La vinculación con la sociedad y los beneficiarios directos de esta investigación son amplios y variados, abarcando desde la mejora de los sistemas internos de la universidad hasta el establecimiento de nuevos estándares de seguridad en la industria tecnológica, beneficiando así a la comunidad en general.

# CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

## 1.1. Contextualización general del estado del arte

DevSecOps busca integrar la seguridad en cada etapa del desarrollo y despliegue de software, desde el diseño hasta la implementación y operación. Como señala Kandula et al. (2020), esto permite identificar y mitigar vulnerabilidades de manera proactiva durante todo el proceso

Según Mehta et al. (2019), la automatización de pruebas de seguridad en pipelines de integración y entrega continua es crucial para mantener la seguridad de las aplicaciones en entornos DevSecOps.

La implementación exitosa de DevSecOps depende también de la cultura. Como discuten Chowdhury et al. (2021), esto promueve una mentalidad compartida de responsabilidad hacia la seguridad.

Existen diversas herramientas y tecnologías que facilitan la implementación de DevSecOps, como sistemas de detección de vulnerabilidades en código, análisis estático y dinámico de seguridad, gestión de identidades y accesos, entre otros (Mehta et al., 2019).

En la era digital actual, la integración de sistemas tecnológicos avanzados en organizaciones y entidades educativas como la Universidad Israel ha revolucionado la gestión estratégica mediante el uso del Sistema Integrado de Gestión Estratégica (SIGE). Este sistema permite centralizar y optimizar procesos críticos, mejorando la eficiencia operativa y la toma de decisiones informadas. Sin embargo, esta dependencia creciente de la tecnología también conlleva desafíos significativos en términos de seguridad cibernética.

La ciberseguridad se ha convertido en una prioridad esencial para asegurar la protección de datos sensibles y la continuidad de las operaciones en entornos digitales. En este contexto, las prácticas de DevSecOps han surgido como una metodología avanzada que integra la seguridad desde las fases iniciales del ciclo de vida del desarrollo de software. DevSecOps promueve una cultura de colaboración entre equipos de desarrollo, operaciones y seguridad, enfocándose en la automatización, la monitorización continua y la respuesta rápida a posibles vulnerabilidades.

La implementación efectiva de DevSecOps en entornos como el SIGE de la Universidad Israel no solo busca fortalecer la seguridad informática, sino también mejorar la calidad del software y la confiabilidad de los sistemas críticos. Esta evolución hacia prácticas más seguras y ágiles no solo beneficia a la universidad en términos de protección de datos y optimización de procesos, sino que también establece un estándar importante para otras instituciones educativas y organizaciones que buscan mejorar su postura de seguridad cibernética y adoptar tecnologías avanzadas de manera segura y eficiente.

La investigación actual en el estado del arte se centra en desarrollar métricas de seguridad específicas que puedan evaluar la efectividad de las prácticas de DevSecOps en entornos académicos como el de la Universidad Israel. Estas métricas no solo permitirán medir y mejorar la seguridad del SIGE, sino que también servirán como referencia para futuras investigaciones y desarrollos en el campo de la ciberseguridad y la gestión estratégica digital.

Es importante señalar que no solo las instituciones financieras, públicas o de salud están expuestas a riesgos de ciberataques; las instituciones educativas también pueden ser objetivo de delincuentes cibernéticos. Durante la pandemia, los intercambios de información se realizaron de manera desorganizada, con accesos masivos a sistemas y sin los controles necesarios ni la capacitación adecuada. Esto ha dejado la información de estas instituciones vulnerable. Para protegerse, es crucial establecer controles apropiados, como marcos de trabajo y estándares internacionales. (Guerra, 2021)

Según Sánchez (2021), Un marco de trabajo de seguridad se define como un conjunto de estándares, normas y buenas prácticas diseñados para gestionar y mitigar los riesgos asociados con las tecnologías digitales. Este marco establece una serie de objetivos específicos de seguridad que facilitan el control del acceso no autorizado y aseguran el uso apropiado de usuarios y contraseñas. En esencia, proporciona una estructura para proteger la información y los sistemas mediante la implementación de medidas de seguridad eficaces.

DevSecOps, una evolución de DevOps, incorpora la seguridad en todas las fases del ciclo de vida del desarrollo de software, desde la planificación hasta la operación. Este enfoque busca garantizar que la seguridad sea una responsabilidad compartida entre los equipos de desarrollo, operaciones y seguridad, permitiendo la entrega continua de software seguro y de alta calidad, esto se detalla en las tablas 1, 2, 3, 4, 5.

**Tabla 1**
*Métricas de desempeño de seguridad*

| **Métricas en DevSecOps** | **Descripción** | **Importancia** |
|---|---|---|
| Número de Vulnerabilidades Detectadas | Monitorea vulnerabilidades encontradas en desarrollo y producción. | Evaluar el estado de seguridad y la efectividad de las medidas preventivas. |
| Tiempo de Corrección de Vulnerabilidades | Mide el tiempo desde la detección hasta la corrección de vulnerabilidades. | Identificar y mitigar riesgos de seguridad de manera rápida y eficiente. |
| Disponibilidad del Sistema | Mide la disponibilidad del sistema, asegurando que los controles de seguridad no afecten la operatividad. | Mantener la accesibilidad y funcionalidad del sistema mientras se asegura la seguridad. |

**Nota:** Esta tabla muestra métricas, descripción e importancia en la gestión de la seguridad y operatividad del sistema.

**Tabla 2**
*Métricas de automatización*

| **Métricas en DevSecOps** | **Descripción** | **Importancia** |
|---|---|---|
| Cobertura de Pruebas Automatizadas | Proporción de pruebas de seguridad automatizadas vs. manuales. | Asegurar la consistencia y exhaustividad de las pruebas de seguridad. |
| Frecuencia de Despliegues | Mide la frecuencia de despliegues de código en producción. | Facilitar la entrega continua, asegurando que los controles de seguridad no retrasen el proceso. |

**Nota:** Esta tabla muestra la relación entre la automatización de pruebas y la frecuencia de despliegues en DevSecOps.

**Tabla 3**
*Métricas de Cumplimiento*

| Métricas en DevSecOps | Descripción | Importancia |
|---|---|---|
| Conformidad con Políticas de Seguridad | Verifica el cumplimiento | Garantizar que se cumplan los estándares y regulaciones establecidos. |
| Auditorías de Seguridad Exitosas | Número de auditorías completadas con éxito sin problemas significativos. | Demostrar la robustez de las prácticas de seguridad ante auditorías internas y externas. |

**Nota:** Esta tabla evidencia la importancia del cumplimiento normativo y auditorías exitosas en DevSecOps.

**Tabla 4**
*Métricas de Cultura y Colaboración*

| Métricas en DevSecOps | Descripción | Importancia |
|---|---|---|
| Participación en Formación en Seguridad | Porcentaje de personal que completa programas de capacitación en seguridad. | Promover la conciencia y el conocimiento en seguridad en toda la organización. |
| Número de Incidentes de Seguridad Reportados | Frecuencia de reportes de incidentes por parte de los equipos. | Fomentar una cultura de seguridad proactiva y colaborativa. |

**Nota:** Esta tabla muestra la relación entre la automatización de pruebas y la frecuencia de despliegues en DevSecOps.

**Tabla 5**
*Métricas de Rendimiento Operacional*

| Métricas en DevSecOps | Descripción | Importancia |
|---|---|---|
| Tiempo de Inactividad Relacionado con Seguridad | Cantidad de tiempo que el sistema está inactivo por problemas de seguridad. | Minimizar interrupciones operativas debido a incidentes de seguridad. |
| Disponibilidad del Sistema | Mide la disponibilidad del sistema, asegurando que los controles de seguridad no afecten la operatividad. | Mantener la accesibilidad y funcionalidad del sistema mientras se asegura la seguridad. |

**Nota:** Esta tabla muestra métricas operacionales que influyen en la disponibilidad y seguridad del sistema en DevSecOps.

**Tabla 6**

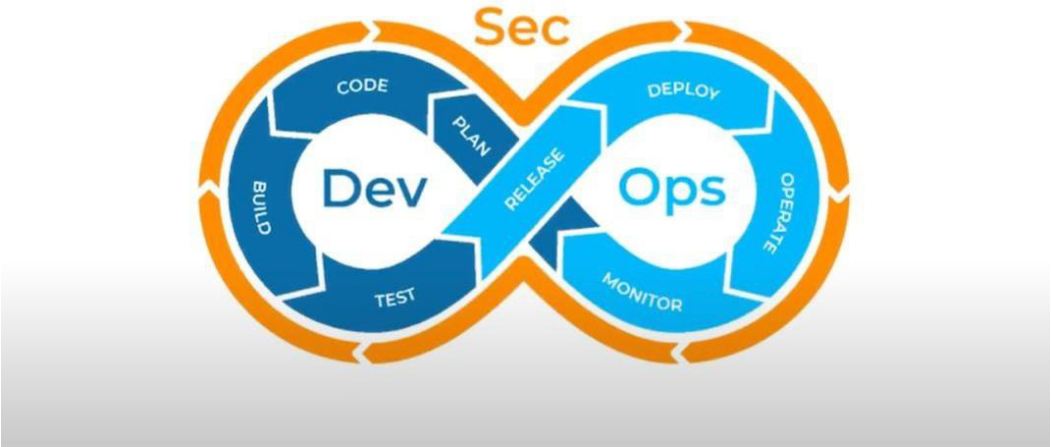
*Métricas de rendimiento operacional*

| Métricas en DevSecOps | Descripción | Importancia |
|---|---|---|
| Definir Objetivos Claros | Establecer metas alineadas con los objetivos organizacionales. | Orientar el esfuerzo hacia mejoras concretas y medibles en seguridad. |
| Automatizar la Recolección de Datos | Utilizar herramientas para recolectar y analizar datos en tiempo real. | Facilitar la monitorización continua y la respuesta rápida ante incidentes. |
| Fomentar una Cultura de Transparencia | Compartir métricas y resultados para fomentar la colaboración y la mejora continua. | Promover la responsabilidad colectiva y la participación activa en la seguridad. |
| Revisar y Ajustar Regularmente | Evaluar y ajustar métricas periódicamente para mantener su relevancia y efectividad. | Adaptar las estrategias de seguridad a medida que evolucionan las amenazas y tecnologías. |

**Nota:** Esta tabla muestra la integración de objetivos claros y la automatización para mejorar el rendimiento operacional en DevSecOps.

DevSecOps combina desarrollo, seguridad y operaciones, es un enfoque que integra la seguridad de forma automatizada en cada etapa del ciclo de vida del software, desde el diseño hasta la implementación. A continuación, se presenta una figura que ilustra esta estructura en detalle.

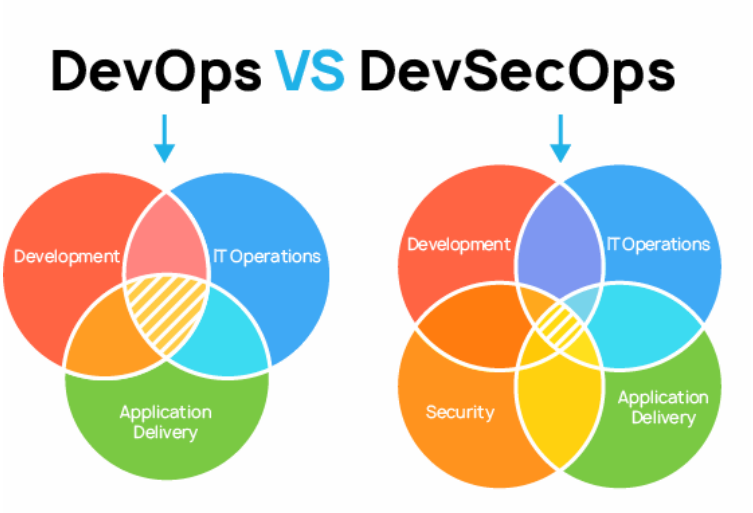
**Figura 1**
*Estructura de DevSecOps*




**Nota:** Este gráfico hace referencia a la integración de la seguridad en DevOps a través de la colaboración continua entre los equipos de desarrollo, operaciones y seguridad.

DevOps es una metodología que promueve la colaboración entre desarrolladores y equipos de operaciones para crear un proceso de implementación más ágil y eficiente. DevSecOps amplía este enfoque al automatizar las tareas de seguridad, integrando controles y procesos de seguridad dentro del flujo de trabajo de DevOps (Humphrey, 2021). A continuación, se presenta una figura que ilustra esta comparación:

**Figura 2**
*Diferencia entre DevOps y DevSecOps*




**Nota:** Tomado de (Bartolik, 2022)

### 1.2. Proceso investigativo metodológico

Sierra (1994: 28) describe a la investigación como "una actividad humana orientada a descubrir algo desconocido". En resumen, la naturaleza humana, impulsada por la curiosidad innata, impulsa a las personas a investigar para comprender cómo y por qué es el mundo que les rodea, satisfaciendo así muchas de sus preguntas y necesidades.

La investigación adopta un enfoque cualitativo para obtener una comprensión profunda de los fenómenos en estudio mediante la recolección de datos descriptivos. Según Creswell y Poth (2019), el enfoque cualitativo busca comprender las experiencias y perspectivas de los participantes en su contexto natural, proporcionando una visión rica y detallada del fenómeno de interés (Creswell y Poth, 2019).

Por lo cual, para recopilar información, se empleará una entrevista dirigida al equipo de programadores del SIGE con el objetivo de recopilar datos cualitativos que proporcionen una comprensión profunda de las vulnerabilidades del sistema y de las medidas de seguridad implementadas (Esto se detalla en el anexo 1). La información obtenida permitirá una comprensión profunda de las vulnerabilidades del SIGE y de las medidas de seguridad implementadas:

La muestra se elige de manera no probabilística, seleccionando intencionalmente al director y al programador del SIGE. Este tipo de muestra es adecuada para investigaciones cualitativas donde el objetivo es obtener información detallada de individuos clave que tienen un conocimiento especializado y relevante sobre el tema (Etikan et al., 2019).

La investigación también incluirá la comparación con estudios previos relacionados. Esto sugiere un interés en establecer un marco de referencia sólido y en identificar brechas de conocimiento que puedan ser abordadas en el estudio actual. Este aspecto es característico de investigaciones descriptivas que buscan analizar y explicar situaciones específicas.

### 1.3. Análisis de resultados

A continuación, se presenta un análisis cualitativo basado en las respuestas obtenidas en una entrevista realizada con el director y el programador del Sistema Integrado de Gestión Estratégica (SIGE). Las respuestas se analizan para identificar patrones y conclusiones clave relacionadas con la implementación y evaluación de métricas de seguridad.

**Tabla 7**
*Análisis de resultados*

| Pregunta | Respuesta del director | Respuesta del programador | Análisis de Resultados |
|---|---|---|---|
| Indicadores Críticos | Número de vulnerabilidades no corregidas. | Tiempo de corrección de vulnerabilidades. | Existe necesidad de priorizar indicadores relacionados con la rapidez y efectividad en la mitigación de riesgos. |

| | | | |
|---|---|---|---|
| Detección temprana | Moderadamente efectiva; sugiere medir el porcentaje de cobertura de pruebas de seguridad. | Efectiva; sugiere reducir falsos positivos como métrica clave. | La detección es vista como adecuada, pero existe consenso en mejorarla mediante nuevas métricas. |
| Tiempo de Respuesta | Adecuado, pero debería monitorearse el tiempo promedio de respuesta. | Aceptable; sugiere frecuencia de revisión de incidentes. | Mejorar el seguimiento y aprendizaje post-incidente. |
| Evaluación de Pruebas Automatizadas | No se utilizan métricas formalizadas; sugiere tasa de éxito de pruebas automatizadas. | Podría mejorarse mediante el monitoreo del tiempo de ejecución de las pruebas. | Falta de formalización en la evaluación actual; acuerdo en que métricas específicas pueden optimizar los procesos. |
| Integración de Métricas | Resistencia del equipo; sugiere medir la aceptación. | Oportunidad con desafíos en la complejidad añadida. | Inconvenientes en la adopción e integración de nuevas métricas, con foco en la gestión del cambio. |

**Nota**: En esta tabla se muestran las diferentes respuestas recopiladas acerca de métricas que se pretende adoptar y su aceptación por los administradores del SIGE.

# CAPÍTULO II: PROPUESTA

## 2.1. Fundamentos teóricos aplicados

DevSecOps es un enfoque que surge de la necesidad de incluir la seguridad como un componente integral y continuo a lo largo del ciclo de vida del desarrollo de software. A diferencia de los enfoques tradicionales, donde la seguridad se añadía al final del ciclo de desarrollo, DevSecOps busca incorporar la seguridad desde el inicio, en cada fase del desarrollo, asegurando que las prácticas de seguridad se integren de manera continua (Mohan & Othmane, 2016).

DevOps se ha convertido en una cultura clave para muchas empresas, enfocándose en mejorar la comunicación entre los equipos de desarrollo y operaciones. Su objetivo es asegurar que estas interacciones sean continuas y automatizadas, lo que facilita un flujo de trabajo ágil. Esta metodología promueve prácticas como la calidad del software y el Desarrollo Guiado por Pruebas (TDD), permitiendo identificar y corregir errores desde etapas tempranas del desarrollo y realizando despliegues frecuentes en producción. Además, garantiza que el código cumpla con los estándares de calidad necesarios (RedHat, 2023).

La seguridad de la información consiste en proteger la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos contra amenazas como accesos no autorizados, uso malintencionado, divulgación, interrupción o destrucción.

Al integrar la seguridad de manera continua y automatizada, DevSecOps no solo mejora la seguridad del software, sino que también optimiza el proceso de desarrollo, reduciendo el tiempo de respuesta ante amenazas y minimizando la posibilidad de fallos de seguridad en producción (Rahman et al., 2016).

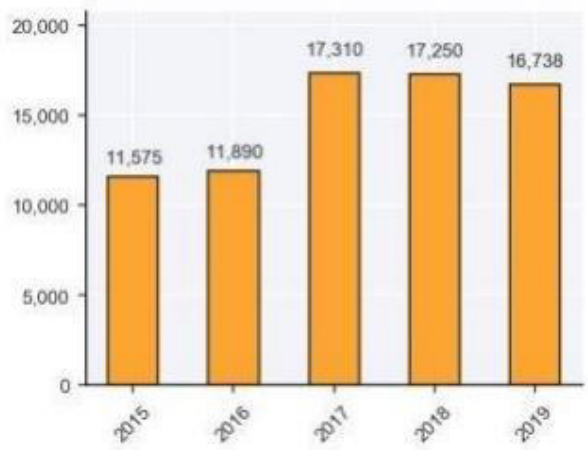
DevSecOps enfatiza la automatización como una herramienta clave para integrar UN despliegue de parches de seguridad, lo que permite detectar y corregir vulnerabilidades de manera más eficiente y rápida (Leite et al., 2019).

Tello Medina (2020) afirma que "a pesar de los notables avances en las metodologías de desarrollo y la adopción de DevSecOps, la seguridad continúa siendo una asignatura pendiente, práctica no solo prolonga significativamente los tiempos de entrega, sino que también incrementa los costos asociados a la corrección de vulnerabilidades descubiertas en sistemas en producción. La complejidad de abordar y solucionar estas vulnerabilidades en un entorno de producción se agrava, ya que pueden ser aprovechadas por actores malintencionados, resultando en pérdidas de tiempo, recursos financieros y esfuerzos considerables" (p. 7).

El gráfico refleja claramente la tendencia de que a medida que los servicios en línea se han multiplicado, también lo han hecho los problemas de seguridad y los errores en el software.

**Figura 3**

*Vulnerabilidades detectadas en los años 2015-2019*




Nota: Número de vulnerabilidades descubiertas Extraído de: VulnDB (2020)

Según Neely, Gregory, y Platts et al. (2005) “las métricas son herramientas cuantitativas utilizadas para medir el rendimiento y la eficacia de procesos organizacionales. Estas herramientas permiten a las organizaciones evaluar su éxito en la consecución de objetivos y tomar decisiones informadas para la mejora continua”.

Según Fenton y Pfleeger (2014) “las métricas en ingeniería de software son medidas cuantitativas de características específicas de un software, como su calidad, eficiencia y fiabilidad. Estas métricas proporcionan una base para evaluar el estado del software y guiar el proceso de desarrollo y mantenimiento”.

Según Sharda, Delen, y Turban (2014) “las métricas en ciencia de datos son indicadores utilizados para evaluar el desempeño de modelos analíticos y de predicción. Estas métricas ayudan a determinar la precisión, la capacidad de generalización y la efectividad de los modelos en la toma de decisiones.”

Con la creciente necesidad de integrar la seguridad en DevOps, ha surgido en los últimos años un enfoque conocido como DevSecOps, o a veces SecDevOps, que se centra en incorporar la seguridad en cada etapa del ciclo de DevOps. Este enfoque busca solucionar los problemas anteriores al promover una colaboración efectiva entre seguridad y DevOps. Según RedHat, DevSecOps implica que la seguridad sea una responsabilidad compartida y una parte integral de todo el proceso de DevOps. Por eso, se pone especial énfasis en la necesidad de incorporar medidas de seguridad en todas las fases del ciclo de DevOps (RedHat, 2023).

Según Medina (2020), la plataforma DevSecOps se basa en cuatro tipos principales de análisis y pruebas de seguridad: el análisis de código estático (SAST), el análisis de código dinámico (DAST), el análisis de código interactivo (IAST) y el análisis de código en tiempo real (RASP). Sin embargo, debido a las limitaciones de tiempo y recursos —con solo seis meses disponibles y una sola persona encargada— el enfoque actual se centrará únicamente en una parte del análisis SAST, que se dedica a desarrollar una herramienta para el análisis estático del código.

Cada uno de estos métodos tiene su propio propósito proporcionar una cobertura amplia contra diferentes tipos de vulnerabilidades. Dado el tiempo y recursos limitados para el desarrollo, el proyecto opta por concentrarse en una parte del análisis SAST. Este análisis estático es fundamental porque permite identificar problemas de seguridad en el código antes

de que se ejecute, aunque es solo una parte del panorama más amplio de la seguridad del software.

### 2.2. Descripción de la propuesta

La propuesta se centra en el desarrollo de métricas de seguridad específicas para evaluar los procesos Utilizando el enfoque de DevSecOps, se busca integrar prácticas de seguridad desde las fases iniciales del ciclo de vida del desarrollo de software. Esto no solo pretende optimizar la protección de datos sensibles y la eficiencia operativa del SIGE, sino también mejorar la calidad general del software utilizado en la gestión administrativa y académica de la universidad. El objetivo es establecer un marco metodológico que permita identificar, mitigar y prevenir vulnerabilidades de manera continua, asegurando así un entorno digital seguro y confiable para todos los usuarios de la institución entre las cuales:

**Tiempo medio de detección (MTTD)**

Cuanto más tiempo pase sin ser detectado un intruso, más tiempo podrá operar dentro de la red, obteniendo acceso a datos cada vez más confidenciales u otros activos empresariales o iniciando un ataque de escalada de privilegios. El tiempo medio de detección es el tiempo promedio entre el momento en que se produce un incidente de seguridad y el momento en que se lo detecta. Esta métrica ayuda a los equipos de detección y respuesta a evaluar la eficacia de los procesos de gestión de incidentes de la organización.

**Tiempo medio de respuesta (MTTR)**

El tiempo medio de respuesta mide el tiempo necesario para resolver una amenaza y devolver el sistema a su estado operativo completo. Medir el tiempo necesario para eliminar una amenaza y recuperar el control del sistema comprometido ayuda a los equipos de detección y respuesta a evaluar la solidez de los procesos utilizados para solucionar problemas una vez que se han identificado.

**Intentos de acceso no autorizado**

La detección y respuesta a intrusiones son parte integral del marco de ciberseguridad general de cualquier empresa. Las métricas de seguridad rastreables incluyen la cantidad de intentos de acceso no autorizado detectados y bloqueados, dónde se originaron esos intentos y con qué rapidez se abordaron. Estas métricas pueden ayudar a los equipos de seguridad a afinar sus procesos de investigación y respuesta, prevención de falsos positivos y cómo se correlacionan y analizan los datos de seguridad.

**Número de incidentes de seguridad**

El seguimiento de la cantidad de incidentes de seguridad detectados y resueltos en un período de tiempo determinado permite obtener datos de tendencias a lo largo del tiempo. Si se analiza en profundidad la cantidad de cada tipo de incidente, su efecto en la empresa y cómo se gestionaron las respuestas, como la recuperación de datos, se revelan detalles que pueden ayudar a los equipos de seguridad a mejorar los procesos de detección y respuesta.

**Niveles de preparación de seguridad del proveedor**

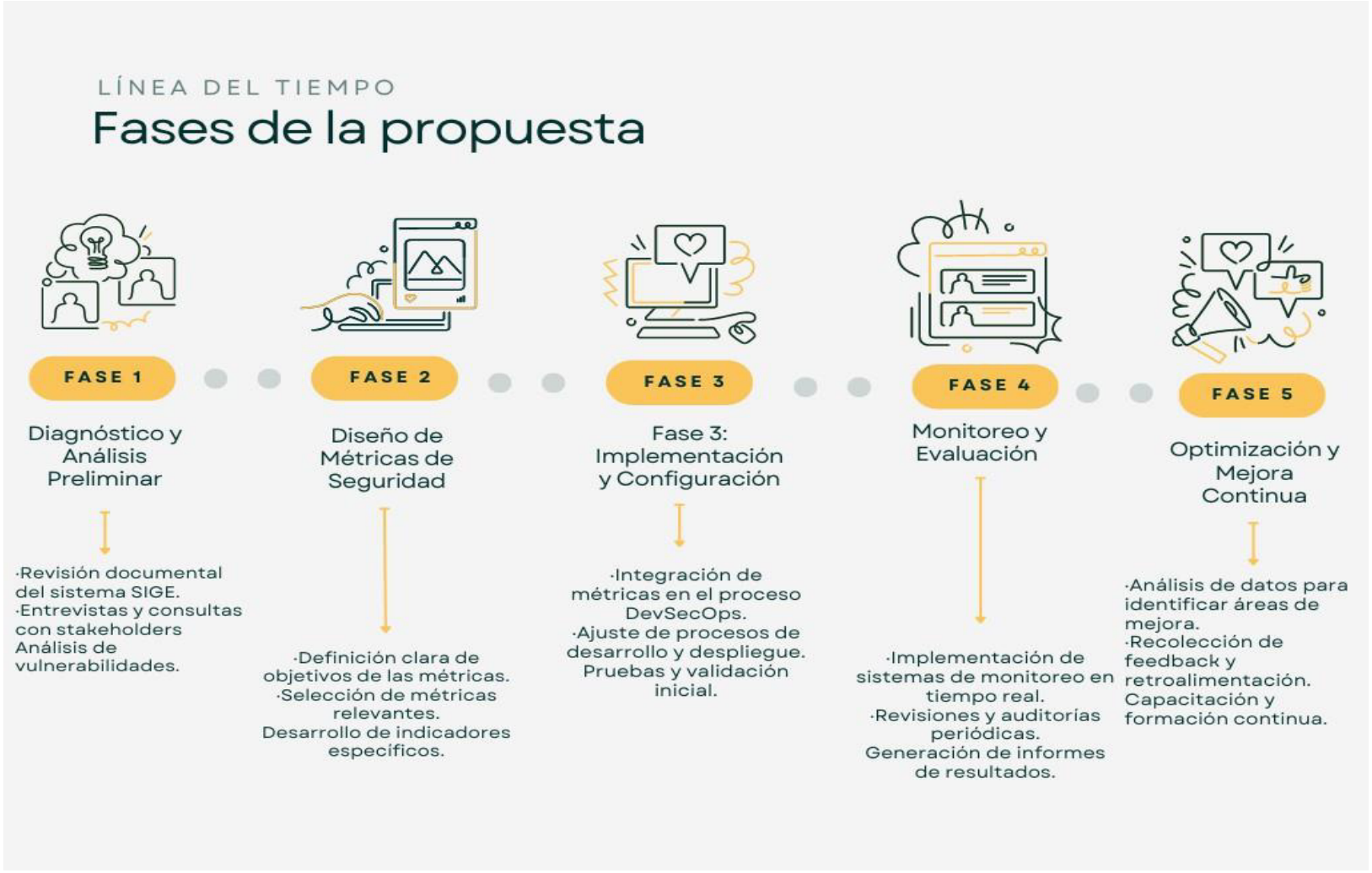
Los proveedores con controles de seguridad insuficientes pueden dar a los intrusos un punto de acceso a sistemas críticos. Un incidente de seguridad con un proveedor puede propagarse rápidamente, por lo que es esencial monitorear activamente su nivel de exposición a los riesgos relacionados con el proveedor. El seguimiento de métricas de seguridad, como las calificaciones de seguridad del proveedor, los informes del Centro de operaciones de seguridad (SOC) y otra documentación de seguridad, puede ayudar a los equipos a comprender y cuantificar mejor el nivel de riesgo que presenta cada proveedor.

### 2.2.1. Estructura general

Cada una de las fases para la implementación de métricas de seguridad en el Sistema Integrado de Gestión Estratégica (SIGE) de la Universidad Israel, aplicando DevSecOps:

**Figura 4**

*Fases para la implementación de métricas de seguridad en SIGE*



**Fase 1:** Diagnóstico y Análisis Preliminar

En esta fase inicial, se realizará un diagnóstico exhaustivo del sistema SIGE para identificar las necesidades específicas para el desarrollo de métricas. Las actividades principales son:

**Figura 5**
*Diagnóstico y análisis preliminar*


**Fase 2:** Diseño de Métricas de Seguridad

En esta fase se diseñarán las métricas de seguridad que servirán para evaluar y monitorear los procesos del SIGE desde una perspectiva DevSecOps. Los pasos principales son:

Definición de Objetivos de las Métricas:

Establecimiento claro de los objetivos que se pretenden alcanzar con la implementación de métricas de seguridad. Por ejemplo, mejorar la detección temprana de vulnerabilidades, reducir el tiempo de respuesta ante incidentes, etc.

Selección de Métricas Relevantes:

Identificación y selección de métricas que sean pertinentes y útiles para medir aspectos críticos de la seguridad en el ciclo de vida del desarrollo de software del SIGE. Ejemplos incluyen el número de vulnerabilidades detectadas, tiempo de corrección de vulnerabilidades, y cobertura de pruebas automatizadas de seguridad.

Desarrollo de Indicadores Específicos:

Especificación detallada de cómo se medirán y calcularán las métricas seleccionadas. Esto implica definir los criterios de medición, los métodos de recolección de datos y los sistemas o herramientas necesarios para recopilar la información requerida.

**Fase 3:** Implementación y Configuración

En esta etapa se llevará a cabo la implementación práctica de las métricas de seguridad dentro del proceso DevSecOps del SIGE. Las actividades clave son:

Integración de Métricas en el Proceso DevSecOps:

Incorporación de las métricas diseñadas en las diferentes etapas del ciclo de vida del desarrollo de software, desde la planificación y diseño hasta la implementación y operación.

Ajuste de Procesos de Desarrollo y Despliegue:

Modificación de los flujos de trabajo existentes para asegurar que las métricas de seguridad se integren de manera efectiva y no afecten negativamente la velocidad y eficiencia del desarrollo.

Pruebas y Validación Inicial:

Realización de pruebas piloto para validar la efectividad y precisión de las métricas implementadas. Esto incluye verificar la recolección de datos, la generación de informes y la interpretación de resultados.

**Fase 4:** Monitoreo y Evaluación Continua

Durante esta fase se establecerán los mecanismos necesarios para monitorear y evaluar de manera continua el desempeño de las métricas de seguridad implementadas. Las acciones principales son:

Implementación de Sistemas de Monitoreo en Tiempo Real:

Configuración de herramientas y sistemas automatizados para monitorear las métricas de seguridad en tiempo real. Esto permite detectar y responder rápidamente ante desviaciones o incidentes de seguridad.

Revisiones y Auditorías Periódicas:

Programación de revisiones regulares y auditorías de las métricas de seguridad para asegurar su precisión, relevancia y alineación con los objetivos organizacionales y las mejores prácticas del sector.

Generación de Informes de Resultados:

Elaboración y distribución de informes periódicos que presenten los resultados obtenidos a partir del monitoreo y evaluación de las métricas de seguridad. Estos informes son fundamentales para la toma de decisiones informadas y la mejora continua.

### 2.2.2. Explicación del Aporte

a estructura propuesta para la gestión de la seguridad en el SIGE, ofrece una diversidad de aportes clave que fortalecen la protección del sistema desde una perspectiva integral. En primer lugar, el diagnóstico y análisis preliminar proporcionan una base importante para identificar las necesidades y vulnerabilidades específicas del sistema, lo cual permite enfocar las medidas de seguridad en las áreas más críticas. Esto garantiza que las acciones posteriores sean factibles, basadas en datos concretos del entorno del SIGE.

Por lo que el diseño de métricas de seguridad es crucial ya que, al establecer métricas, facilita la evaluación y monitoreo de la seguridad del SIGE. Al definir objetivos claros y desarrollar

indicadores específicos, se asegura que las métricas seleccionadas sean relevantes y útiles para medir aspectos críticos del ciclo de vida del desarrollo del software.

### 2.2.3. Estrategias y/o Técnicas

A continuación, se presentan estrategias y técnicas que abarcan dos herramientas seleccionadas para abordar la problemática de seguridad en el Sistema Integrado de Gestión Estratégica (SIGE) de la Universidad Israel.

**SonarQube**

Es una plataforma de código abierto para la inspección continua de la calidad del código. Ofrece análisis de código estático que detecta vulnerabilidades y defectos en el código fuente. Su principal función es identificar y reportar problemas de calidad y seguridad en el código, proporcionando un análisis detallado para mejorar la seguridad y la mantenibilidad del software (SonarSource, 2023).

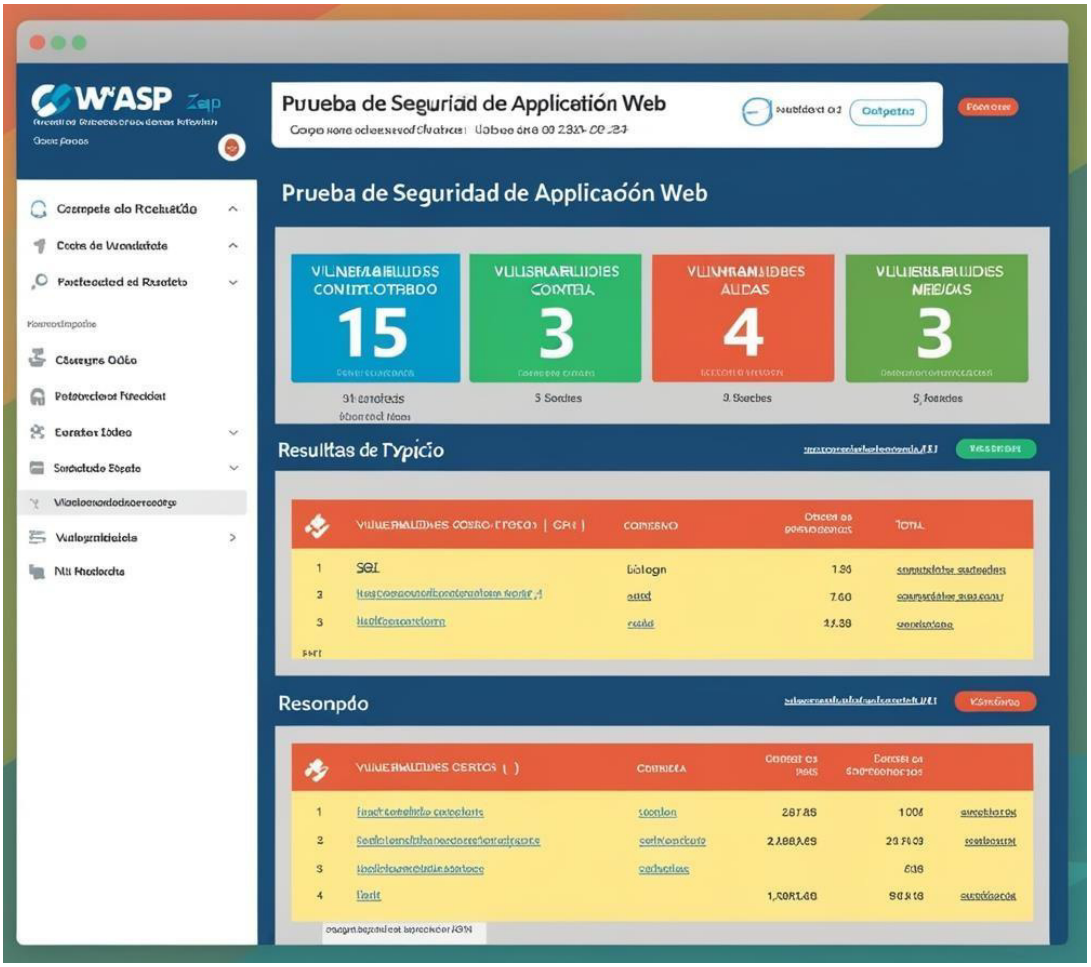
**Figura 6**
*Herramienta SonarQube*


**Nota:** Esta figura indica cómo se realizaría el análisis de código estático que detecta vulnerabilidades y defectos en el código fuente.

**OWASP ZAP (Zed Attack Proxy)**

Es una herramienta de código abierto que se utiliza para realizar pruebas de seguridad en aplicaciones web. Es muy eficaz para detectar vulnerabilidades en las aplicaciones web mediante el análisis dinámico del código y la simulación de ataques. Su función principal es identificar vulnerabilidades de seguridad en aplicaciones web en tiempo real, facilitando la detección de problemas que pueden ser explotados por actores malintencionados (OWASP Foundation, 2023).

**Figura 7**
*Herramienta OWASP ZAP*




**Nota:** Esta figura muestra que la herramienta de código abierto que se utiliza para realizar pruebas de seguridad en aplicaciones web.

**Estrategia de Diagnóstico**

SonarQube se integrará en el flujo de trabajo de integración continua para realizar análisis de código estático cada vez que se realicen cambios en el código fuente. Si se detectan vulnerabilidades o defectos, el sistema generará un informe y notificará al equipo de desarrollo.

OWASP ZAP se empleará para realizar pruebas de seguridad en aplicaciones web durante las fases de prueba y pre-producción. Las vulnerabilidades identificadas serán reportadas y notificadas al equipo de desarrollo para su corrección.

**Estrategia de Diseño de Métricas de Seguridad**

En primer lugar, establecer objetivos claros, como la reducción del número de vulnerabilidades críticas detectadas y el tiempo de corrección.

Posteriormente realizar la selección de métricas relevantes:

- SonarQube: Métricas como la densidad de defectos, el número de vulnerabilidades detectadas, y la cobertura de código.
- OWASP ZAP: Métricas como el número de vulnerabilidades encontradas, el riesgo asociado a cada vulnerabilidad, y el tiempo de respuesta ante incidentes.
- Desarrollar indicadores específicos:
- SonarQube: Criterios de medición basados en el análisis de código estático, con indicadores como la gravedad de las vulnerabilidades y la cantidad de código revisado.
- OWASP ZAP: Indicadores basados en pruebas de seguridad dinámica, con criterios como el tipo de vulnerabilidad y la exposición potencial en el entorno real.

**Estrategia de Implementación**

- Implementar SonarQube en el flujo de integración continua y OWASP ZAP en las fases de prueba de seguridad.
- Adaptar los procesos de desarrollo y despliegue para incorporar el análisis de seguridad sin afectar la eficiencia del desarrollo.

- Realizar pruebas piloto con SonarQube y OWASP ZAP para validar su efectividad en la detección y corrección de vulnerabilidades.

**Estrategia de Monitoreo y Evaluación Continua**

- Monitoreo en Tiempo Real: Configurar SonarQube y OWASP ZAP para generar informes y notificaciones en tiempo real sobre vulnerabilidades y problemas de seguridad.
- Revisiones Periódicas: Programar auditorías y revisiones regulares para evaluar la efectividad de las métricas de seguridad y hacer ajustes necesarios.
- Generación de Informes: Crear informes periódicos que presenten los resultados del análisis de seguridad y las acciones correctivas tomadas.

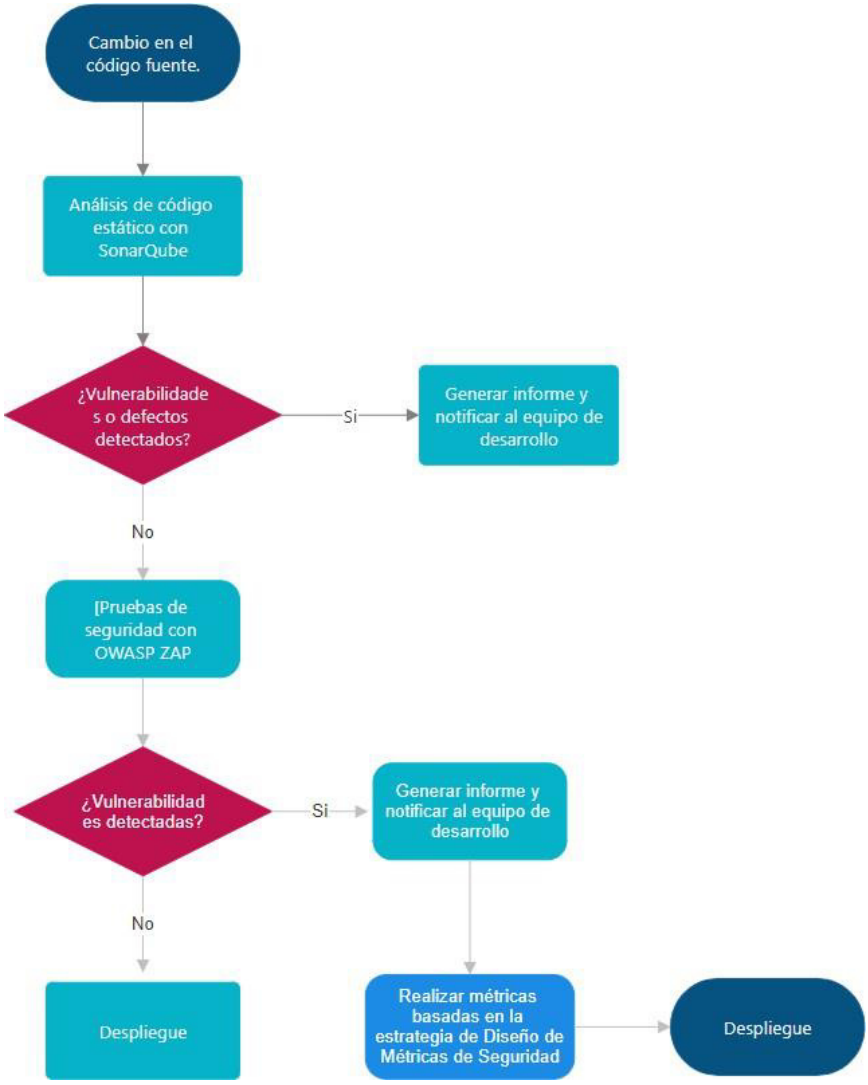
**Estrategia de Optimización y Mejora Continua**

- Análisis de Datos: Revisar los datos recolectados para identificar áreas de mejora en las métricas de seguridad.
- Recolección de Feedback: Obtener retroalimentación de los equipos de desarrollo y seguridad para ajustar las métricas y procesos.
- Capacitación Continua: Proporcionar formación sobre el uso de SonarQube y OWASP ZAP, y sobre prácticas de seguridad en desarrollo y despliegue.

En el siguiente gráfico detalla cómo SonarQube y OWASP ZAP se integran en el flujo de trabajo de desarrollo y despliegue del SIGE.

**Figura 8**

*Integración de Análisis de Código y Pruebas de Seguridad*




## 2.3. Validación de la propuesta

La validación de la propuesta a través de especialistas en seguridad y desarrollo se llevó a cabo con resultados positivos. Los especialistas revisaron la funcionalidad y adecuación de SonarQube y OWASP ZAP para el entorno del SIGE. Se evaluaron sus capacidades para detectar vulnerabilidades y su integración en el proceso de desarrollo.

**Tabla 8**
*Perfil descriptivo de especialistas validadores*

| Apellidos y Nombres | Años de experiencia | Titulación Académica | Cargo |
|---|---|---|---|
| **Mg. Esteban Silva** | 11 años | Magíster en Cyberseguridad informática | Jefe de programación |
| **Mg. Jorge Gavidia** | 25 años | Magíster en Cyberseguridad informática | Programador |

**Tabla 9**
Criterios evaluativos

| Criterio | Descripción |
|---|---|
| **Impacto** | El alcance que tendrá la propuesta y su representatividad en la generación de valor |
| **Aplicabilidad** | La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables |
| **Conceptualización** | La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada |
| **Actualidad** | Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta |
| **Calidad Técnica** | Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios |
| **Factibilidad** | El nivel de utilización de la propuesta por parte de la organización acode a los recursos disponibles |
| **Pertinencia** | La contundencia y conveniencia de la propuesta para solucionar el problema planteado. |

De acuerdo con los criterios evaluativos presentados en la Tabla 11, se utiliza la siguiente escala ponderativa para medir el grado de aceptación de cada componente evaluativo propuesto. A continuación, se detallan los condicionantes cualitativos y su correspondiente ponderación, que ha sido aprobada por cada experto en función de la importancia y relevancia de los criterios establecidos.

**Tabla 10**
*Resultados de la validación*

| CRITERIOS | EXPERTO 1 (Esteban Silva) | EXPERTO 2 (Jorge Gavidia) | TOTAL | Porcentaje |
|---|---|---|---|---|
| **Impacto** | 4 | 4 | 8 | 80% |
| **Aplicabilidad** | 5 | 5 | 10 | 100% |
| **Conceptualización** | 5 | 5 | 10 | 100% |
| **Actualidad** | 5 | 5 | 10 | 100% |
| **Calidad Técnica** | 4 | 4 | 8 | 80% |
| **Factibilidad** | 5 | 4 | 10 | 100% |
| **Pertenencia** | 4 | 5 | 8 | 80% |
| **Total** | **32** | **32** | **64** | **91.42%** |

Nota: estos son los resultados acordes al instrumento de validación (Anexo 2)

Los especialistas confirmaron que las herramientas propuestas son efectivas y adecuadas para abordar los desafíos de seguridad del SIGE. Se recomendó la implementación de una combinación de herramientas para mejorar la cobertura de seguridad, así como la consideración de futuras mejoras en el enfoque actual.

Las recomendaciones incluyeron la utilización de una variedad de herramientas para detectar una gama más amplia de vulnerabilidades y la integración de prácticas de seguridad continuas para mantener una postura de seguridad robusta y adaptable.

## 2.4. Matriz de articulación de la propuesta

**Tabla 11**
*Matriz de articulación*

| EJES O PARTES PRINCIPALES | SUSTENTO TEÓRICO | SUSTENTO METODOLÓGICO | ESTRATEGIAS / TÉCNICAS | DESCRIPCIÓN DE RESULTADOS | INSTRUMENTOS APLICADOS |
|---|---|---|---|---|---|
| **Diagnóstico y análisis preliminar** | Basado en la teoría de la gestión de riesgos y seguridad de sistemas, se enfoca en identificar y analizar vulnerabilidades iniciales (Hubbard & Seiersen, 2016). | investigación cualitativa a través de entrevistas y análisis de vulnerabilidades en el entorno específico del SIGE. | Entrevistas con administradores del sistema; análisis estático y dinámico del código; escaneos de seguridad automatizados. | Identificación de necesidades de seguridad específicas y mapeo de vulnerabilidades críticas en el SIGE. | Encuestas, seguridad |
| **Diseño de métricas de seguridad** | Teoría de la evaluación de procesos y métricas de seguridad en entornos DevSecOps (Morrison, 2015). | Diseño de métricas basadas en objetivos claros, alineadas con las mejores prácticas de seguridad en el ciclo de vida. | Definición de objetivos claros; selección y desarrollo de métricas relevantes e indicadores específicos para monitorear la seguridad. | Establecimiento de métricas que permitan medir la efectividad y mejorar la seguridad del SIGE. | Herramientas de desarrollo de métricas; documentos de planificación de seguridad. |
| **Implementación y configuración** | Teoría de la implementación y configuración de procesos seguros en el desarrollo de software (Kim, Behr, & Spafford, 2013). | Aplicación práctica de las métricas diseñadas en el proceso DevSecOps del SIGE, validación y ajustes según resultados. | Integración de métricas de procesos; pruebas piloto para validar la precisión de las métricas. | Implementación exitosa de métricas en los procesos DevSecOps del SIGE, con validación inicial de su efectividad | Plan de integración de métricas; pruebas piloto; informes de resultados preliminares. |
| **Monitoreo y evaluación** | Teoría de la retroalimentación continua y mejora en la seguridad de sistemas (Scholtes, 1998). | Establecimiento de un sistema de monitoreo en tiempo real, con revisiones y auditorías periódicas de las métricas. | Implementación de sistemas automatizados de monitoreo; revisiones y auditorías regulares; generación de informes de resultados para la toma de decisiones. | Mantenimiento continuo de la seguridad del SIGE, con capacidad para ajustes y mejoras basadas en datos reales. | Sistemas de monitoreo en tiempo real; herramientas de auditoría; software de generación de informes. |

| | | | | | |
|---|---|---|---|---|---|
| **Optimización y mejora continua** | Teoría de la mejora continua (Kaizen) y optimización de procesos de seguridad en entornos dinámicos (Imai, 1986). | Refinamiento de métricas y procesos en base a datos obtenidos y cambios en el entorno de seguridad. | Análisis de tendencias a largo plazo; implementación de nuevas herramientas o técnicas; ajustes estratégicos basados en auditorías y revisiones periódicas. | Mejora constante en la eficiencia y efectividad de las métricas de seguridad, asegurando la evolución del SIGE ante nuevas amenazas y desafíos. | Evaluaciones periódicas; informes de optimización; nuevas implementaciones de herramientas de seguridad. |

## CONCLUSIONES

El análisis de los fundamentos teóricos ha permitido entender que DevSecOps es más que una metodología es un enfoque integral. Al fomentar la colaboración entre los equipos de desarrollo, operaciones y seguridad, DevSecOps facilita la automatización de procesos clave de seguridad, lo cual es un aspecto sustancial para un sistema académico desarrollado por la Universidad Israel.

La realizar el diagnóstico del SIGE, mediante herramientas como SonarQube se detectaron vulnerabilidades que podrían afectar negativamente su eficiencia, seguridad y estabilidad. Lo cual significa de suma importancia que se adopte un enfoque proactivo en el mejoramiento o mejor gestión de la seguridad, implementando prácticas que permitan una respuesta rápida y efectiva frente a las amenazas emergentes.

El desarrollo de métricas de seguridad específicas para el sistema en mención, ha permitido la creación de indicadores precisos, que facilitan la medición de la efectividad de las prácticas DevSecOps. Estas métricas no solo son valiosas para un monitoreo constante, sino que también mejoran las respuestas a incidentes usuales en materia de seguridad, permitiendo así la toma de decisiones más acertada y basada en datos estadísticos.

La evaluación de la propuesta para implementar en el SIGE, utilizando criterios validados por expertos en la materia, ha demostrado que, si bien se han logrado avances importantes, es importante mantener el monitoreo constante, así como también realizar mejoras en la seguridad, para asegurar que el sistema siga siendo resistente frente a nuevas amenazas.

## RECOMENDACIONES

Se recomienda profundizar en la adaptación de DevSecOps específicamente en entornos académicos como el SIGE de la Universidad Israel. Así como sería de gran utilidad explorar ¿cómo otras Universidades están implementando estas prácticas y evaluar el impacto de la cultura DevSecOps en la mejora continua de la seguridad?

Como resultado de los nuevos problemas de seguridad diagnosticados en el SIGE, se recomienda que futuras investigaciones se enfoquen en la implementación de técnicas avanzadas de detección de vulnerabilidades. Estas herramientas pueden mejorar la capacidad para predecir y prevenir posibles brechas de seguridad.

Dado que las amenazas de seguridad evolucionan constantemente, se recomienda que futuras investigaciones busquen desarrollar métricas de seguridad adaptativas, que se ajusten automáticamente a las nuevas amenazas. Además, sería beneficioso investigar cómo éstas métricas pueden ser implementadas en otros sistemas universitarios para crear un marco de seguridad más robusto en el sector educativo.

Se recomienda que los resultados e impactos obtenidos en este proyecto de titulación sean divulgados ampliamente dentro de la comunidad académica y tecnológica. Es crucial socializar los hallazgos para así contribuir con el desarrollo de mejores prácticas en seguridad en DevSecOps tanto en el ámbito educativo como en otros sectores.

**BIBLIOGRAFÍA**


Baldeón, P. F. (2022). Sistema Integrado de Gestión Estratégica (SIGE) – UISRAEL. 13.

Bartolik, P. (2022). DevSecOps ayuda a anular los riesgos antes de que puedan ingresar más tarde en el flujo de compilación. *DevSecOps y SDLC: ¿Dónde estamos y dónde deberíamos estar?*

Bird, J. (2019). *DevSecOps: A leader's guide to producing secure software without compromising flow, feedback, and continual improvement.* O'Reilly Media.

Castro, Figueroa, Vera, Álava, Parrales, Murillo, Castillo (2018), INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

Fenton, N. E., & Pfleeger, S. L. (2014). *Software metrics: A rigorous and practical approach* (2nd ed.). CRC Press.

Ferreres, A. (2021). Using of SecDevOps in web applications. En B. thesis. Universitat Politècnica de Catalunya.

Guerra Byron (2021), Instituciones educativas en riesgo informático https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/

Humphrey, P. (2021). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. IT Revolution Press.

Leite, L., Rocha, C., Kon, F., Milojicic, D., & Meirelles, P. (2019). A survey of DevOps concepts and challenges. *ACM Computing Surveys (CSUR)*, 52(6), 1-35. https://doi.org/10.1145/3359981

Matos, Y., & Pasek, E. (2008). LA OBSERVACIÓN, DISCUSIÓN Y DEMOSTRACIÓN: TÉCNICAS DE INVESTIGACIÓN EN EL AULA. Laurus, 14(27), 33-52.

Medina, J. D. (2020). *PLATAFORMA FT DEVSECOPS.* Universidad de Antioquia, Medellín, Colombia.

Microsoft. (2024). *Introducción a DevSecOps*. Obtenido de Integración de seguridad en el ciclo de vida del desarrollo de software.: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/secure/innovation-security

Mohan, N., & Othmane, L. B. (2016). SecDevOps: Is it a marketing buzzword? In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 542-547). IEEE. https://doi.org/10.1109/ARES.2016.17

Neely, A., Gregory, M., & Platts, K. (2005). *Performance measurement system design: A literature review and research agenda*. International Journal of Operations & Production Management, 25(12), 1228-1263. https://doi.org/10.1108/01409170510633648

Plain concepts. (17 de octubre de 2023). *Impulsando la seguridad en tu negocio con DevSecOps*. Obtenido de https://www.plainconcepts.com/es/devsecops/

Rahman, M. A., Riyat, I., & DeFlitch, C. (2016). DevOps: Introducing infrastructure as code. In *Proceedings of the 2016 IEEE 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 9-14). IEEE. https://doi.org/10.1109/SKIMA.2016.7916203

Sánchez (2021), Frameworks de ciberseguridad y estándares que debes conocer. https://protegermipc.net/2021/08/19/frameworks-de-ciberseguridad-y-estandares-que-debes-conocer/

Sharda, R., Delen, D., & Turban, E. (2014). *Business intelligence and analytics: Systems for decision support* (10th ed.). Pearson.

## ANEXOS

### ANEXO 1

**FORMATO DE ENTREVISTA**

| |
|---|
| **Proyecto de titulación:** Desarrollo de métricas de seguridad para evaluar los procesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando DevSecOps que influyen en la calidad del software. |
| 1) ¿Cuáles son los principales indicadores de seguridad que considera más críticos para el funcionamiento seguro del SIGE, y por qué?<br>2) ¿Qué tan efectiva considera que es la detección temprana de vulnerabilidades en el SIGE utilizando las herramientas actuales? ¿Qué métricas podrían mejorar este proceso?<br>3) En términos de tiempo de respuesta ante incidentes de seguridad, ¿cómo valora el desempeño actual del SIGE? ¿Qué métricas serían útiles para monitorear y mejorar este aspecto?<br>4) ¿Qué procedimientos y métricas se están utilizando actualmente para evaluar la efectividad de las pruebas automatizadas de seguridad? ¿Hay áreas en las que estos procesos podrían mejorarse?<br>5) ¿Cómo percibe la integración de las métricas de seguridad dentro del ciclo de vida del desarrollo del SIGE? |

**ANEXO 2**

**VALIDACIÓN DE LA PROPUESTA**

Universidad Israel
ESPOG | Escuela de Posgrados

## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS "ESPOG"

### MAESTRÍA EN SEGURIDAD INFORMÁTICA

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps.

". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Mg. Esteban Leonardo Silva Llaguno** |
| **Título obtenido: Magister en Seguridad Informática** |
| **C.I.:0202330387** |
| **E-mail: stevan_386@hotmail.com** |
| **Institución de Trabajo: Universidad Israel** |
| **Cargo: Jefe de Programadores** |
| **Años de experiencia en el área: 7 años** |

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** "Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps"

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| Pertinencia | | x | | | |
| Aplicabilidad | x | | | | |
| Factibilidad | x | | | | |
| Novedad | x | | | | |
| Fundamentación pedagógica | | x | | | |
| Fundamentación tecnológica | x | | | | |
| Indicaciones para su uso | | x | | | |
| TOTAL | 20 | 12 | | | |

**Observaciones:**.....

.....

.....

**Recomendaciones:**.....

.....

.....

**Lugar, fecha de validación: Quito, 26 de agosto del 2024**

**AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

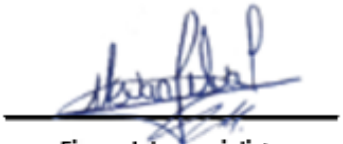
En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



**Firma del especialista**
**Mg. Esteban Silva**

**ANEXO 3**

# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFORMÁTICA

**INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps.

". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

**Datos informativos**

| |
|---|
| **Validado por: Mg. JORGUE Vinicio Gavidia Córdova** |
| **Título obtenido: Magister en Seguridad Informática** |
| **C.I.:1714852108** |
| **E-mail: jgavidia@uisrael.edu.ec** |
| **Institución de Trabajo: Universidad Israel** |
| **Cargo: Desarrollador** |
| **Años de experiencia en el área:5 años** |

**Instructivo:**

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** "Métricas de seguridad para evaluar los procesos en el Sistema Integrado de Gestión Estratégica de la Universidad Israel aplicando los principios de DevSecOps"

| Indicadores | Muy adecuado | Bastante Adecuado | Adecuado | Poco adecuado | Inadecuado |
|---|---|---|---|---|---|
| Pertinencia | | x | | | |
| Aplicabilidad | x | | | | |
| Factibilidad | x | | | | |
| Novedad | x | | | | |
| Fundamentación pedagógica | | x | | | |
| Fundamentación tecnológica | x | | | | |
| Indicaciones para su uso | | x | | | |
| TOTAL | 20 | 12 | | | |

**Observaciones:**.....

.....

.....

**Recomendaciones:**.....

.....

.....

**Lugar, fecha de validación: Quito, 26 de agosto del 2024**

**AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

**Firma del especialista**
**Mg. Jorge Gavidia**