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 MAGÍSTER

Título del proyecto:
Propuesta de plan de seguridad para mitigar vulnerabilidades en el ciclo de integración continua y despliegue de aplicaciones web en DevOps
Línea de Investigación:
Ciencias de la ingeniería aplicada a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la información y comunicación (TIC)
Autor:
Junior Jamil Párraga Párraga
Tutores:
Mg. Toasa Guachi Renato Mauricio PhD Urdaneta Herrera Maryory

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: PROPUESTA DE PLAN DE SEGURIDAD PARA MITIGAR VULNERABILIDADES EN EL CICLO DE INTEGRACIÓN CONTINUA Y DESPLIEGUE DE APLICACIONES WEB EN DEVOPS.

Elaborado por: **Parraga Parraga Junior Jamil**, de C.I: **1314002401**, 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., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO TOASA GUACHI

Mg. Toasa Guachi Renato Mauricio

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, **Maryory Urdaneta Herrera** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE PLAN DE SEGURIDAD PARA MITIGAR VULNERABILIDADES EN EL CICLO DE INTEGRACIÓN CONTINUA Y DESPLIEGUE DE APLICACIONES WEB EN DEVOPS.

Elaborado por: **Parraga Parraga Junior Jamil**, de C.I: **1314002401**, 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., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

PhD. Urdaneta Herrera Maryory

ORCID: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Junior Jamil Párraga Párraga con C.I: 1314002401, autor/a del proyecto de titulación denominado: PROPUESTA DE PLAN DE SEGURIDAD PARA MITIGAR VULNERABILIDADES EN EL CICLO DE INTEGRACIÓN CONTINUA Y DESPLIEGUE DE APLICACIONES WEB EN DEVOPS. Previo a la obtención del título de Magister en Seguridad informática.

1. 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.
2. 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.
3. 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., marzo de 2024

Firma

ORCID: 0009-0008-6326-0244

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

La seguridad informática es un tema de vital importancia en la actualidad, dado el creciente papel de la tecnología y los sistemas informáticos en nuestras vidas personales y profesionales.

Contextualización del tema

DevOps, una fusión de "Desarrollo" (Development) y "Operaciones" (Operations), representa un enfoque que apunta a la estrecha integración entre los equipos de desarrollo de software y los equipos de operaciones de tecnología de la información (TI). Surgió como una solución para superar las divisiones entre estos dos grupos y mejorar la rapidez, calidad y fiabilidad en la entrega de software (Corwell, 2020).

La necesidad de DevOps se hizo evidente con la evolución del desarrollo de software y las demandas de los usuarios y clientes por productos y servicios más rápidos y de alta calidad. Los métodos tradicionales de desarrollo de software, que implicaban una separación marcada entre el desarrollo y las operaciones, resultaban en procesos lentos, falta de colaboración, y lanzamientos de software menos confiables y más propensos a errores (Ferreres, 2021).

DevOps enfrenta estas restricciones al promover la cooperación, la interacción, la automatización y la integración ininterrumpida entre los equipos de desarrollo y operaciones. Esto se alcanza mediante actividades como la automatización de pruebas, la ejecución continua de despliegues, la supervisión de la infraestructura y aplicaciones en tiempo real, y la adopción de una cultura de mejora constante (Ferreres, 2021).

A medida que DevOps se convirtió en un enfoque ampliamente adoptado en la industria del software, surgió la necesidad de integrar la seguridad de manera más efectiva en todo el ciclo de vida del desarrollo y la entrega de software. Esto llevó al surgimiento de SecDevOps, también conocido como DevSecOps (Canyelles, 2022).

SecDevOps expande el concepto de DevOps al incorporar la seguridad desde los primeros pasos del ciclo de vida del software. Reconoce la importancia de no dejar la seguridad como un tema secundario y propone integrarla de manera anticipada en todos los aspectos del desarrollo y operaciones de software (Canyelles, 2022).

Algunas de las prácticas clave de SecDevOps incluyen la automatización de pruebas de seguridad, la implementación de controles de seguridad en todas las etapas del ciclo de vida del software, la gestión de vulnerabilidades y parches de manera proactiva, y la colaboración estrecha entre equipos de desarrollo, operaciones y seguridad (Ferreres, 2021).

Mientras que DevOps se enfoca en unir desarrollo y operaciones para mejorar la velocidad y calidad en la entrega de software, SecDevOps expande este concepto para asegurar que la seguridad esté presente en todas las fases del ciclo de vida del software. Esto facilita el desarrollo y la entrega continua de software seguro y confiable (Canyelles, 2022).

Problema de investigación

La reducción de vulnerabilidades en el ciclo de integración continua y despliegue de aplicaciones web es esencial dentro del marco de DevOps por múltiples razones fundamentales. En DevOps, el propósito principal es agilizar la entrega de software. No obstante, esta rapidez no debe comprometer la seguridad. La acción de mitigar vulnerabilidades en el ciclo de integración y despliegue asegura que el software entregado sea tanto veloz como seguro (Benedictis, 2022).

Las vulnerabilidades no corregidas pueden ser aprovechadas por ciberdelincuentes para comprometer la aplicación y los datos. Mitigar estas vulnerabilidades en etapas tempranas minimiza el riesgo de ataques y fugas de datos, protegiendo la información sensible.

¿Cuáles son las mejores prácticas recomendadas para implementar una estrategia de seguridad efectiva que mitigue las vulnerabilidades en el ciclo de integración continua y despliegue de aplicaciones web en un entorno DevOps?

Objetivo general

Proponer un plan de seguridad que detecte vulnerabilidades en el ciclo de integración y despliegue continúo en el desarrollo de aplicaciones de la empresa Aval Buró bajo la metodología DevOps.

Objetivos específicos

- Contextualizar los fundamentos teóricos, conceptos y principios fundamentales sobre SecDevOps.
- Identificar las posibles vulnerabilidades que podrían comprometer la eficiencia, seguridad y estabilidad de los sistemas de integración continua de la empresa Aval Buró.
- Diseñar el plan que permita manejar las vulnerabilidades identificadas a través de herramientas open source en aplicaciones de integración y entrega continua dentro de la metodología DevOps.
- Valorar la propuesta a través de criterios de especialistas de la aplicación de la estrategia de seguridad en un aplicativo de integración y entrega continua.

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos son los ciudadanos ecuatorianos, ya que sus datos están expuestos en la empresa Aval Buró. En caso de que estos datos no sean tratados correctamente, existe el riesgo de que sean expuestos.

La seguridad informática no se limita solo a expertos en tecnología. Al involucrar a la sociedad en general, se promueve la conciencia sobre las amenazas cibernéticas y las mejores prácticas de seguridad. Esto ayuda a que las personas adopten medidas más seguras en su uso diario de la tecnología.

Con el aumento de la recopilación de datos personales en línea, es esencial que los usuarios comprendan cómo proteger su información. La educación sobre seguridad informática permite que los individuos tomen decisiones informadas sobre la privacidad en línea (Benedictis, 2022).

Las infraestructuras esenciales, como las redes eléctricas y los sistemas de transporte, están cada vez más interconectadas con la tecnología. Al concienciar a la sociedad sobre la relevancia de la ciberseguridad en estos sistemas, se reduce la probabilidad de interrupciones y se previenen posibles impactos negativos para la sociedad en general (Benedictis, 2022).

Cuando las personas comprenden los riesgos y saben cómo protegerse, están mejor preparadas para enfrentar situaciones de crisis cibernéticas. Esto puede minimizar los daños causados por ataques y acelerar la recuperación.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

"Securing DevOps: Security in the Cloud" es una guía escrita por Julia Vehent (2018) que se centra en la integración de prácticas de seguridad dentro de los procesos de DevOps. Esta es una de las principales referencias en las que se basa el presente proyecto ya que el autor destaca los desafíos y oportunidades para implementar medidas de seguridad sólidas.

La necesidad de un enfoque de seguridad, donde las consideraciones de seguridad se integren tempranamente en el ciclo de vida del desarrollo es fundamental en el proceso de integración continua. Estos conceptos aportan significativamente al desarrollo e implementación de SecDevOps en la empresa Aval Buró. (Vehent, 2018)

Según Hernández (2022) en su documento de maestría manifiesta que la automatización de procesos desempeña un papel crucial en un ambiente de desarrollo e integración continua, permitiendo la entrega rápida y frecuente de cambios de código a entornos de producción, así como la detección temprana y la corrección de errores. Además, nos habla sobre la cultura DevOps, la cual fomenta la colaboración estrecha entre los equipos, la transparencia en la comunicación y la responsabilidad compartida por el éxito del proyecto.

El autor durante el desarrollo del documento se centra en explorar y analizar el proceso de adopción e implementación de la cultura DevOps dentro de una organización empresarial. Menciona además que DevOps es una metodología que busca integrar los equipos de desarrollo (Dev) y operaciones (Ops) para mejorar la colaboración, la entrega de software y la eficiencia operativa. (Hernandez, 2022)

Entender la evolución de las prácticas de seguridad, desarrollo y operaciones en el ámbito de la tecnología y el software es lo que menciona Lopez (2020) en su escrito “SecDevOps: Análisis de contenedores Docker e integración de herramientas SAST y DAST”, SecDevOps como concepto, surge como una respuesta a la necesidad de integrar la seguridad de manera proactiva y continua en el ciclo de vida del desarrollo de software. Este enfoque busca superar las brechas tradicionales entre los equipos de seguridad, desarrollo y operaciones, fomentando la colaboración y la integración desde el inicio del proceso de desarrollo hasta la entrega y el mantenimiento de las aplicaciones.

Benedictis (2022) observa una evolución marcada por la adopción de metodologías ágiles y DevOps, que han transformado radicalmente la forma en que se concibe y se implementa el desarrollo de software. La seguridad ya no es considerada como una fase posterior al desarrollo,

sino que se integra como un componente esencial en cada etapa del ciclo de vida del software. Esto implica la automatización de pruebas de seguridad, la implementación de controles continuos y la adopción de prácticas de gestión de identidad y acceso para asegurar la confidencialidad, integridad y disponibilidad de las aplicaciones.

También abarca la evolución de herramientas, tecnologías y marcos de trabajo que respaldan este enfoque, incluyendo soluciones de automatización, plataformas de orquestación, y servicios en la nube que facilitan la implementación y gestión de entornos seguros. Así mismo, se exploran las tendencias emergentes, los desafíos y las mejores prácticas que están moldeando el futuro de la seguridad en el desarrollo de software en un entorno cada vez más digital y dinámico (Benedictis, 2022).

A medida que las organizaciones adoptan DevOps y aumenta la velocidad de entrega de software, también se intensifica la preocupación por la seguridad. La seguridad no puede ser una ocurrencia tardía o una barrera para la velocidad de entrega. Es aquí donde surge SecDevOps, o DevSecOps (Benedictis, 2022).

SecDevOps es la progresión lógica de DevOps, que incluye la seguridad desde las etapas iniciales del ciclo de vida del desarrollo de software. Se origina como una solución a la demanda de integrar la seguridad de forma anticipada en todos los ámbitos del desarrollo y operaciones de software. Esto implica la automatización de pruebas de seguridad, la incorporación de controles de seguridad en los flujos de entrega continua, y una colaboración estrecha entre los equipos de desarrollo, operaciones y seguridad (Corwell, 2020).

La aparición de SecDevOps refleja el creciente valor de la seguridad en el contexto digital actual, donde las amenazas cibernéticas están en constante evolución y se encuentran en todas partes. Incorporar la seguridad en DevOps no solo contribuye a reducir los riesgos y salvaguardar los recursos de la empresa, sino que también fortalece la confianza del cliente y la imagen de la marca (Sarango, 2023).

DevOps y SecDevOps son enfoques progresivos en la manera en que las organizaciones desarrollan, entregan y administran el software. Mientras DevOps se enfoca en la integración y la entrega eficiente de software, SecDevOps expande esta perspectiva para asegurar que la seguridad esté presente en todas las etapas del ciclo de vida del desarrollo de software, garantizando de esta manera la seguridad y la excelencia del producto final (Corwell, 2020).

1.2. Proceso investigativo metodológico

La observación directa es una técnica de recopilación de datos utilizada en diversos campos, como la investigación científica, la psicología, la sociología, la educación y la etnografía, entre otros. Consiste en observar y registrar directamente el comportamiento, las acciones y los eventos tal como ocurren en su entorno natural, sin intervención ni manipulación por parte del observador (Mendoza, 2020).

En la observación directa, el investigador o el observador se sumerge en el contexto o la situación que está estudiando para obtener una comprensión detallada y objetiva de los fenómenos observados. Esto implica observar cuidadosamente lo que sucede, tomar notas detalladas, registrar eventos relevantes y recopilar datos de manera sistemática y no intrusiva (Mendoza, 2020).

La metodología de investigación basada en la observación directa puede ser una valiosa herramienta para examinar y entender una diversidad de fenómenos en distintos entornos.

1.2.1. Alcance de la observación

Examinar minuciosamente las vulnerabilidades presentes y potenciales en los procedimientos vigentes y en desarrollo de Aval Buró se torna esencial para identificar y abordar de manera proactiva cualquier debilidad que pueda comprometer la seguridad y el funcionamiento eficiente de la empresa. Este análisis exhaustivo permite detectar y anticiparse a posibles riesgos, asegurando así la integridad de los procesos y la protección de los activos de la organización.

1.2.2. Seleccionar el contexto y los participantes

Durante los despliegues a producción o la implementación de sistemas automatizados, se llevará a cabo una revisión exhaustiva de los procesos para identificar posibles fallas o problemas potenciales. Este proceso de revisión se realizará en colaboración con el equipo de infraestructura, cuya función será coordinar y gestionar los accesos necesarios para llevar a cabo estas actividades de manera segura y eficiente.

1.2.3. Diseñar un plan de observación

El propósito de esta observación es analizar el proceso de integración continua en el entorno de desarrollo de software para identificar eficiencias, áreas de mejora y posibles problemas que puedan surgir durante el ciclo de desarrollo.

Se llevará a cabo la observación en el entorno de desarrollo de software donde se implementa la integración continua.

Los participantes incluirán miembros del equipo de desarrollo, ingenieros de calidad, y aquellos responsables de la configuración y mantenimiento de las herramientas de integración continua.

1.2.4. Obtener permisos y consentimientos necesarios

Se presento formalmente las solicitudes de acceso al equipo de infraestructura, especificando claramente los permisos necesarios y el propósito de la solicitud.

Se entregó toda la documentación o información adicional necesaria para respaldar la solicitud de acceso.

Después de coordinar con el equipo de infraestructura, se ha obtenido un acceso temporal que permitirá llevar a cabo la observación de manera efectiva y sin contratiempos. Este acceso temporal otorga al equipo de observación la capacidad de ingresar al entorno relevante y realizar las actividades planificadas según el protocolo establecido.

1.2.5. Realizar la observación

Después de haber obtenido acceso temporal para llevar a cabo la observación, se procedió con el análisis detallado de los registros y fragmentos de código pertinentes en el entorno específico. Durante este proceso de observación meticulosa, se identificaron múltiples vulnerabilidades tanto en el código como en los registros (logs) del sistema. Es importante destacar que algunas de estas vulnerabilidades incluyen la exposición de credenciales en texto plano, lo cual representa un riesgo significativo para la seguridad de la información.

En cuanto a los registros, se observó que ciertos registros contenían información sensible, como nombres de usuario, contraseñas u otros datos confidenciales, almacenados de manera no encriptada y fácilmente accesible. Este hallazgo es especialmente preocupante, ya que la exposición de credenciales en texto plano aumenta el riesgo de comprometer la seguridad de los sistemas y la integridad de los datos.

Además, durante el análisis de los fragmentos de código, se identificaron vulnerabilidades potenciales que podrían ser explotadas por actores malintencionados para comprometer la seguridad del sistema. Estas vulnerabilidades pueden incluir problemas de inyección de código, falta de validación de datos de entrada, o prácticas de codificación inseguras que podrían conducir a brechas de seguridad y ataques exitosos.

1.3. Análisis de resultados

De las observaciones y pruebas realizadas a los procesos existentes se pudo observar algunas novedades. Por ejemplo en la Figura 1 se aprecia que durante la consulta de Jenkins se despliegan las credenciales del usuario responsable de llevar a cabo la integración continua de un proceso automatizado. Este proceso se enfoca en facilitar los pases a producción de forma rápida y precisa, minimizando posibles errores humanos. A pesar de estas ventajas, se vislumbra una preocupante brecha de seguridad que aún no ha sido corregida.

Figura 1.
Proceso pase a producción

En la **Figura 2** se puede constatar las credenciales de un colaborador de la entidad Aval Buró. Este individuo utiliza un procedimiento que compara productos, objetos, querys, entre otros del ambiente de pruebas con el ambiente de producción, lo cual conlleva riesgos significativos al exponer sus credenciales de acceso.

Figura 2.
Automatización: Comparación de productos

```
jenkins@avalburo.com
[Pipeline] echo
****
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] wrap
[Pipeline] {
[Pipeline] }
[Pipeline] // wrap
[Pipeline] echo
USER_NAME_EXECUTE_JOB-->Ivette Castrillon
[Pipeline] echo
EMAIL_PASS_EXECUTE_JOB-->ivetteAval2023
EMAIL_USER_EXECUTE_JOB-->ivette.castrillon@avalburo.com
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
```

Así mismo en la **Figura 3** se puede observar las credenciales expuestas, es un proceso en Pentaho que ejecuta una carga automática diaria en el ambiente de producción, precisamente a la medianoche. Aunque este proceso resulta de gran utilidad, es evidente que conlleva un riesgo significativo, dado que expone las credenciales del usuario responsable de la acción.

Figura 3.
Automatización carga automática

```
2024/02/29 15:40:12 - LOG 2 CONEX.0 - tagCentralizada = PBA_AVALBURO
2024/02/29 15:40:12 - LOG 2 CONEX.0 - cadenaConexion = PBA_HOST:172.18.2.51;PBA_PORT:8080;PBA_USER:portal;PBA_PASS:portal$123
2024/02/29 15:40:12 - LOG 2 CONEX.0 - esVariable = 1
2024/02/29 15:40:12 - LOG 2 CONEX.0 - tomarVariableCompleta = 0
2024/02/29 15:40:12 - LOG 2 CONEX.0 - IMAP_HOST = outlook.office365.com
2024/02/29 15:40:12 - LOG 2 CONEX.0 - IMAP_PASS = Nuk12293
2024/02/29 15:40:12 - LOG 2 CONEX.0 - IMAP_PORT = 993
2024/02/29 15:40:12 - LOG 2 CONEX.0 - IMAP_USER = testnotificaciones@avalburo.com
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SMTP_HOST = smtp.office365.com
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SMTP_PASS = Nuk12293
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SMTP_PORT = 587
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SMTP_USER = testnotificaciones@avalburo.com
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SE_USER = score_app
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SE_PASS = J4rScore
2024/02/29 15:40:12 - LOG 2 CONEX.0 - SE_URL = http://10.10.2.240:8101/jarscore/
2024/02/29 15:40:12 - LOG 2 CONEX.0 - PBA_HOST = 172.18.2.51
2024/02/29 15:40:12 - LOG 2 CONEX.0 - PBA_USER = portal
2024/02/29 15:40:12 - LOG 2 CONEX.0 - PBA_PASS = portal$123
2024/02/29 15:40:12 - LOG 2 CONEX.0 - PBA_PORT = 8080
```

CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

DevOps se basa en los principios ágiles del desarrollo de software, que enfatizan la entrega veloz, la flexibilidad y la colaboración entre equipos. Los valores ágiles, como la colaboración, la comunicación continua y la capacidad de respuesta ágil al cambio, son esenciales para la mentalidad de DevOps (Sarango, 2023).

SecDevOps es una metodología que incorpora la seguridad en todas las etapas del ciclo de vida del desarrollo y operaciones de software. Asimismo, fomenta una cultura de colaboración entre los equipos de desarrollo, operaciones y seguridad. Su enfoque se centra en eliminar los compartimentos organizativos y fomentar la comunicación y cooperación entre los equipos para integrar la seguridad de manera eficiente en todo el proceso de desarrollo y despliegue (Sarango, 2023).

Automatización de seguridad

La automatización es un principio clave tanto en DevOps como en SecDevOps. La automatización de pruebas de seguridad, análisis de código estático y dinámico, escaneos de vulnerabilidades y otras medidas de seguridad contribuyen a detectar y solucionar problemas de seguridad de forma más ágil y efectiva (Sarango, 2023).

Entrega continua y despliegue continuo (CI/CD)

SecDevOps fomenta la integración de la seguridad en los flujos de trabajo de CI/CD. Esto implica realizar pruebas de seguridad automáticamente como parte del proceso de construcción y despliegue, lo que permite identificar y solucionar problemas de seguridad de manera temprana en el ciclo de vida del desarrollo (Sarango, 2023).

Gestión de riesgos

SecDevOps se enfoca en la gestión anticipada de riesgos de seguridad, lo cual implica la evaluación y clasificación de riesgos de seguridad, la implantación de controles de seguridad apropiados, y la vigilancia constante de amenazas y vulnerabilidades en los entornos de desarrollo y producción (Sarango, 2023).

Monitoreo y respuesta ante incidentes

La detección temprana y la respuesta rápida ante incidentes de seguridad son componentes clave de SecDevOps. Se enfoca en implementar sistemas de monitoreo y detección de

intrusiones, así como en establecer procesos eficientes de respuesta ante incidentes para mitigar el impacto de posibles brechas de seguridad (Gavidia, 2022).

Educación y concienciación

La formación y sensibilización en seguridad son elementos cruciales en SecDevOps. Se centra en instruir a los equipos de desarrollo y operaciones acerca de las prácticas óptimas de seguridad, detectar y solucionar vulnerabilidades, y promover una cultura de seguridad en toda la empresa (Gavidia, 2022).

SecDevOps es una metodología que aspira a incorporar la seguridad a lo largo de todo el ciclo de vida del desarrollo y operaciones de software, promoviendo la colaboración, la automatización, la gestión de riesgos y la respuesta ágil a incidentes con el fin de asegurar la protección de las aplicaciones y sistemas implementados (Gavidia, 2022).

Para aplicar la metodología vamos a utilizar la herramienta Splunk que sirve para el análisis de vulnerabilidades ya que utiliza una arquitectura de indexación para indexar y almacenar datos de diferentes fuentes, lo que permite una búsqueda rápida y eficiente de datos y vulnerabilidades (Mohan, 2020).

Eventos y datos estructurados

Splunk trata los datos como eventos, donde cada evento representa una entrada de datos individual. Los eventos pueden ser estructurados, como registros de servidor o registros de aplicaciones, o no estructurados, como datos de texto sin procesar. Splunk puede analizar y extraer información de eventos estructurados y no estructurados para proporcionar una visión completa (Mohan, 2020).

Análisis en tiempo real

Splunk tiene la capacidad de examinar información en tiempo real, lo que habilita a los usuarios para identificar pautas, evoluciones y irregularidades en los datos conforme suceden. Este aspecto resulta particularmente valioso para supervisar el desempeño del sistema, la seguridad de la red y otros aspectos fundamentales de la infraestructura en tiempo real (Gavidia, 2022).

Visualización y reporting

Splunk proporciona funcionalidades de visualización y generación de informes que posibilitan a los usuarios desarrollar paneles de control interactivos, gráficos y tablas para representar datos y obtener percepciones relevantes. Estas representaciones visuales pueden facilitar la

identificación de tendencias, patrones y problemas en los datos de forma intuitiva y eficaz (Mohan, 2020).

Seguridad y acceso controlado

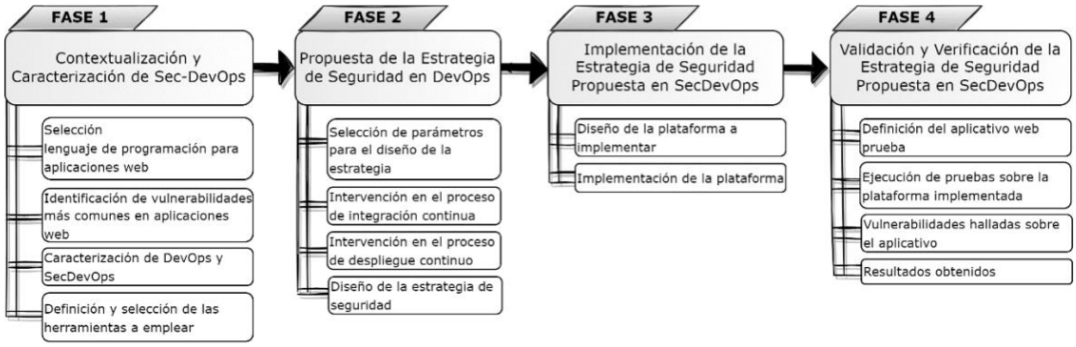
Splunk ofrece características de seguridad sólidas que posibilitan la gestión del acceso a los datos y la protección de la privacidad y la integridad de la información. Estas funcionalidades comprenden autenticación, autorización y auditoría, asegurando que únicamente los usuarios autorizados accedan a los datos y que se registren todas las actividades realizadas en la plataforma (Mohan, 2020).

1.2. Descripción de la propuesta

La estrategia de seguridad propuesta tiene como objetivo cubrir tanto aspectos técnicos como culturales, además de ser adaptable al nivel de madurez de la empresa donde se planea implementar. Siguiendo este enfoque, se describen los controles de seguridad en la metodología SecDevOps, detallados para una mejor comprensión durante el proceso de Integración Continua (CI) y Despliegue Continuo (CD).

El proyecto se estructura en cuatro (4) fases, como se indica en la **Figura 4**.

Figura 4.
Fases de la propuesta



Nota: Obtenida de Fernandez (2023).

Fase 1

En esta fase de investigación sobre la metodología SecDevOps y las herramientas para implementar el plan de seguridad en los procesos automatizados de la empresa Aval Buró, se ha tomado la decisión de proponer la herramienta Splunk. Esta elección se fundamenta en el análisis detallado de las características y capacidades de varias herramientas disponibles en el mercado, así como en la evaluación de las necesidades específicas de la empresa.

Entre las diversas opciones consideradas, Splunk se destacó como la solución más adecuada debido a su sólido soporte para el lenguaje de programación Java, el cual es ampliamente utilizado en los sistemas y aplicaciones de Aval Buró. Al ser compatible con Java, Splunk puede integrarse de manera más fluida y eficiente con el entorno tecnológico existente en la empresa, lo que facilita su implementación y adopción por parte de los equipos de desarrollo y operaciones.

Además, Splunk ofrece una amplia gama de funcionalidades avanzadas para la monitorización, análisis y gestión de datos de máquina, lo que permitirá a Aval Buró mejorar significativamente su capacidad para detectar y responder a amenazas de seguridad en tiempo real. Su capacidad para procesar grandes volúmenes de datos y generar informes detallados y visualizaciones intuitivas también será invaluable para mejorar la visibilidad y comprensión de los procesos automatizados en la empresa.

Fase 2

Se propone agregar un paso adicional al proceso actual de despliegue continuo, fundamentado en la realización de una validación previa con las herramientas seleccionadas para la propuesta. Esta medida surge como respuesta a la necesidad de elevar el nivel de seguridad y calidad en el ciclo de entrega de software.

El nuevo paso de validación se concibe como un punto de control esencial antes de llevar a cabo el despliegue definitivo. Aquí, las herramientas elegidas, KBDoctor y Splunk, desempeñarán un papel crucial al realizar un análisis exhaustivo de las aplicaciones y sistemas que están a punto de ser implementados en el entorno de producción.

Este enfoque garantizará que cualquier posible problema o vulnerabilidad sea detectado y abordado antes de que el software se ponga en producción. Además, al integrar la validación con las herramientas propuestas directamente en el proceso de despliegue continuo, se fomenta una cultura de seguridad y calidad desde las etapas iniciales del desarrollo.

La introducción de este nuevo paso refleja un compromiso con la mejora continua y la mitigación proactiva de riesgos en el ciclo de vida del software. Al agregar una capa adicional de seguridad y validación, la organización podrá reducir la probabilidad de incidentes de seguridad y mejorar la estabilidad y confiabilidad de sus sistemas en producción.

Fase 3

En esta fase, se lleva a cabo el diseño detallado de cómo operaría el proceso con la propuesta de seguridad. Para lograr esto, se ha decidido utilizar las herramientas KBDoctor y Splunk debido a su facilidad de integración y su relativa sencillez de implementación, lo que reduce la carga de conocimiento necesaria para su configuración y uso efectivo.

El diseño del proceso implica definir cómo se van a utilizar estas herramientas en conjunto para abordar los desafíos específicos de seguridad de la organización. Se establecerán los flujos de trabajo, los roles y responsabilidades de los usuarios, y los criterios de medición y evaluación del éxito del proceso.

La elección de KBDoctor y Splunk se basa en su capacidad para proporcionar una visión integral de la seguridad de la organización, desde la identificación de vulnerabilidades hasta la detección y respuesta ante amenazas en tiempo real. Además, su facilidad de integración permite aprovechar al máximo las inversiones existentes en infraestructura y herramientas de seguridad.

Es importante destacar que la selección de estas herramientas no solo se basa en su funcionalidad técnica, sino también en su capacidad para adaptarse a las necesidades y requisitos específicos de la organización. Se espera que la combinación de KBDoctor y Splunk brinde una solución robusta y escalable que contribuya significativamente a fortalecer la postura de seguridad de la empresa y proteger sus activos críticos de manera proactiva y eficiente.

Fase 4

Para esta etapa, es fundamental llevar a cabo un análisis exhaustivo con los profesionales actualmente involucrados en el área de seguridad dentro de la empresa. Este análisis implica revisar detalladamente el alcance y la idoneidad de las herramientas propuestas para su implementación en el entorno empresarial. Es crucial asegurarse de que las herramientas seleccionadas sean compatibles con las necesidades y los requisitos específicos de seguridad de la organización.

Durante este proceso de evaluación, se examinarán diversos aspectos, como la funcionalidad, la escalabilidad, la integración con los sistemas existentes, la facilidad de uso y mantenimiento, y la capacidad para abordar los desafíos de seguridad actuales y futuros de la empresa.

Además, se buscará la retroalimentación y la participación activa de los profesionales de seguridad para garantizar que se aborden adecuadamente sus preocupaciones y necesidades. Es importante aprovechar la experiencia y el conocimiento de estos expertos para tomar decisiones informadas y fundamentadas sobre la selección e implementación de las herramientas de seguridad.

En última instancia, este análisis colaborativo con los profesionales de seguridad ayudará a garantizar que las herramientas propuestas sean adecuadas y efectivas para fortalecer la postura de seguridad de la empresa y proteger sus activos críticos de manera proactiva y eficiente.

a. Estructura general

A continuación, se expone la composición de la propuesta, que engloba dos herramientas que se consideran apropiadas para resolver la problemática planteada.

Splunk es una plataforma de análisis de datos que puede ser configurada para buscar y detectar patrones de credenciales en los logs, líder en la industria para la gestión y análisis de datos de registros, así como de otros tipos de datos generados por sistemas informáticos. Su principal función es permitir a las organizaciones buscar, visualizar, analizar y actuar sobre grandes volúmenes de datos en tiempo real (Stearley, 2020).

Splunk es una plataforma versátil y potente que permite a las organizaciones gestionar y aprovechar el valor de sus datos de registros y otros tipos de datos para la toma de decisiones, la seguridad, el monitoreo, la resolución de problemas y mucho más (Stearley, 2020).

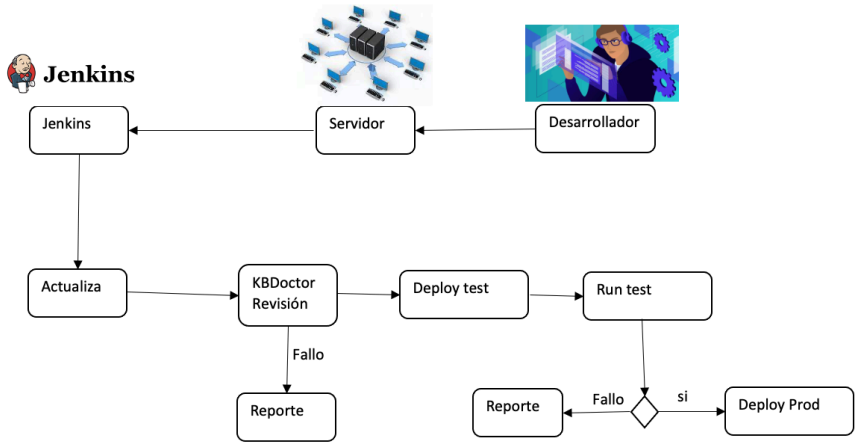
KBDoctor es una herramienta de código abierto que ha destacado en el GXchallenge en 2007. Esta herramienta es altamente beneficiosa para integrarse con plataformas como Splunk, Jenkins, entre otras, con el propósito de detectar posibles vulnerabilidades, limpiar código y generar informes, entre otras funcionalidades relevantes (Bouali, 2021).

En el gráfico se puede observar que el servidor de Jenkins está a la escucha de algún cambio realizado en el servidor, en caso de encontrarlo se realiza una actualización ya sea de micro servicios, objetos de pentaho, objetos de base de datos, etc. Luego se realiza una compilación del código con los cambios requeridos para luego someterse a un análisis por parte de las herramientas antes explicadas. Si todo el proceso fue satisfactorio y no se detectó ninguna vulnerabilidad la Herramienta KBDoctor se encarga de enviar una notificación por vía email indicando que no existieron novedades, así mismo si existen novedades se notifica con el detalle de dichas novedades.

Si el proceso de análisis es satisfactorio se procede hacer el deploy al servidor de destino de los cambios previamente analizados por las herramientas propuestas.

A continuación, en la **Figura 5** se puede apreciar el proceso automatizado propuesto.

Figura 5.
Estructura del proceso automatizado



b. Explicación del aporte

El diagrama presentado anteriormente se lo realizó con el escenario típico de una empresa en el cual vamos a implementar el plan propuesto.

Teniendo en cuenta que existe un desarrollador que subió sus cambios a un servidor de aplicaciones y luego está un servidor de Jenkins preguntando si existe algo nuevo en el servidor de aplicaciones y en el caso de encontrar algún cambio va a ejecutar todas las tareas que se encuentran dentro del rectángulo que se visualizan en la Figura 5.

En las tareas primero está una actualización de lo nuevo que encontró el JOB de Jenkins para luego subir esos cambios. Sin embargo, con la nueva propuesta antes de subir los cambios pasa por la herramienta KBDoctor que está integrada con Splunk y analizan todo tipo de posibles vulnerabilidades como por ejemplo el problema detectado que es las credenciales visibles, de ser el caso se envía una notificación indicando el problema, caso contrario realiza el Deploy y de igual manera se envía una notificación de éxito.

c. Estrategias y/o técnicas

SecDevOps es una metodología que fusiona los conceptos de seguridad (Sec), desarrollo de software (Dev) y operaciones (Ops) en un enfoque conjunto y colaborativo. Su propósito es

incorporar la seguridad en todas las etapas del ciclo de vida del desarrollo de software, desde la fase de planificación y diseño hasta el despliegue y la operación continua (Pérez, 2023).

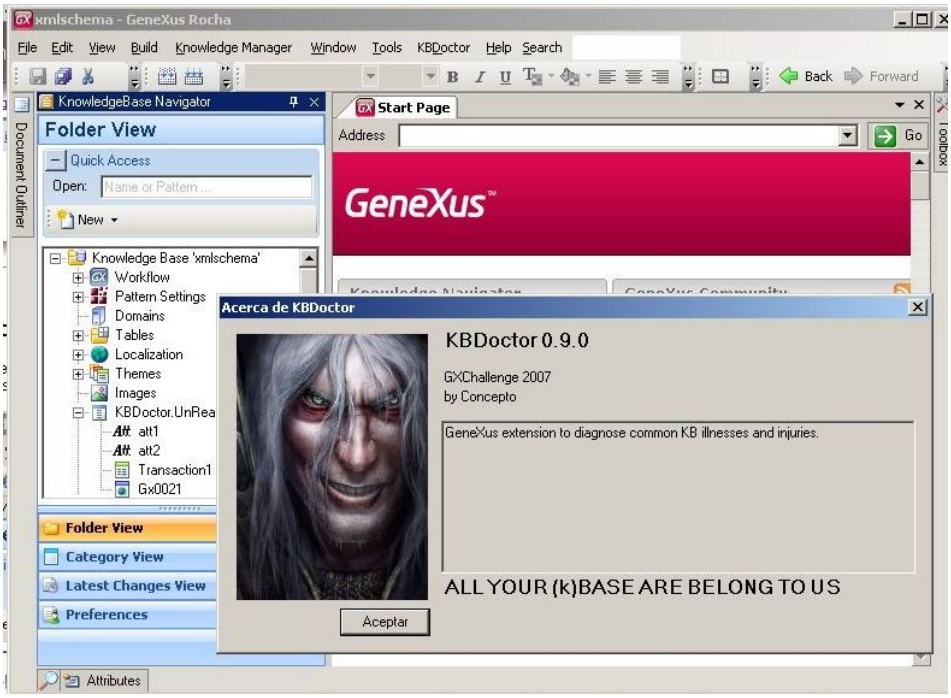
Dentro del marco de SecDevOps, se entiende que la seguridad es una responsabilidad compartida por todos los equipos que participan en el desarrollo y operación de software. En lugar de ser abordada como una preocupación secundaria, la seguridad se integra desde el inicio del proceso de desarrollo y se mantiene a lo largo de todo el ciclo de vida del software (Pérez, 2023).

Por lo tanto se recomienda utilizar las herramientas KBDoctor que es una herramienta muy fácil de usar y se integra con otras herramientas como lo es Splunk la cual sirve para analizar logs, código, etc.

Para desarrollar el plan se realizo mediante la observación directa del problema que existe en la empresa Aval buró, luego se analizo e investigo las posibles herramientas que pueden servir para mitigar el problema existente.

Se eligieron estas dos herramientas ya que son las mas fáciles de usar y gratuitas. A continuación se presenta la herramienta KBDoctor en la **Figura 6** y la herramienta Splunk en la **Figura 7**.

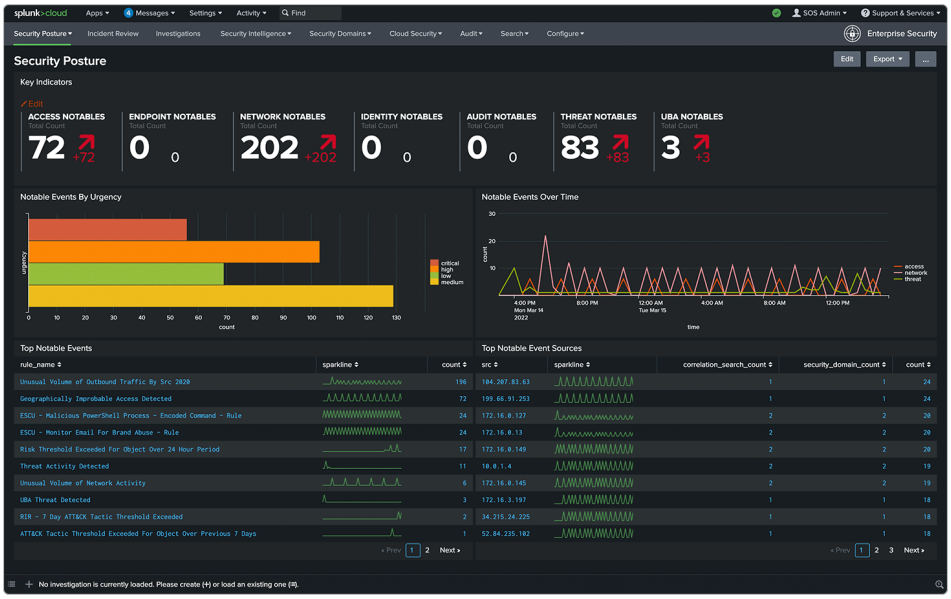
Figura 6.
Herramienta KBDoctor



Nota: Tomado de García (2020)

Figura 7.

Herramienta Splunk



Nota: Tomado de García (2020)

1.3. Validación de la propuesta

La validación realizada por parte de los especialistas resultó altamente satisfactoria, ya que no solo respaldaron el uso de las herramientas propuestas, sino que también llevaron a cabo un análisis exhaustivo de su funcionalidad y alcance potencial. Durante este proceso de evaluación, se evaluaron minuciosamente las capacidades y características de las herramientas, así como su idoneidad para abordar los desafíos específicos del contexto en cuestión.

Los especialistas no solo consideraron la utilidad inmediata de las herramientas propuestas, sino que también evaluaron su capacidad para generar valor a largo plazo. Esta evaluación se centró en la capacidad de las herramientas para satisfacer las necesidades actuales y futuras de la organización, así como en su flexibilidad y escalabilidad para adaptarse a los cambios en el entorno tecnológico y empresarial.

Al concluir la validación, los especialistas expresaron su confianza en que las herramientas propuestas son adecuadas y efectivas para abordar los desafíos de seguridad y operativos de la organización. Su respaldo respalda la viabilidad y el potencial impacto positivo de la implementación de estas herramientas en el contexto empresarial.

Con base en la revisión de los especialistas, se han identificado áreas de oportunidad para fortalecer el plan propuesto y mejorar la postura de seguridad de la organización. Se ha

evidenciado la necesidad de implementar algunas mejoras en el futuro, así como la consideración de otras herramientas que podrían complementar y enriquecer el enfoque actual.

Es importante destacar que ninguna herramienta puede identificar todas las vulnerabilidades potenciales por sí sola. Por lo tanto, los especialistas recomiendan utilizar una combinación de herramientas y enfoques para abordar de manera más completa las brechas de seguridad existentes. Esta estrategia permite aumentar la cobertura de detección y reducir las posibilidades de pasar por alto amenazas significativas para la organización.

Al adoptar una variedad de herramientas, la organización puede beneficiarse de diferentes enfoques y capacidades, lo que contribuye a una evaluación más exhaustiva de la seguridad. Además, la combinación de soluciones puede proporcionar una visión más amplia y detallada de los riesgos potenciales, permitiendo una respuesta más efectiva y proactiva ante posibles amenazas.

Finalmente pienso que la recomendación de los especialistas de utilizar una combinación de herramientas refleja un enfoque integral y adaptativo para abordar los desafíos de seguridad. Esta estrategia ayuda a fortalecer la postura de seguridad de la organización y a mitigar los riesgos de manera más efectiva en un entorno cada vez más complejo y dinámico.

La información y los criterios proporcionados por los especialistas están detallados en el Anexo 1 y Anexo 2.

1.4. Matriz de articulación de la propuesta

En la **zTabla 1** se presenta una síntesis de la correlación entre la propuesta elaborada y sus respectivos fundamentos.

zTabla 1.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Contextualización y caracterización de SecDevOps	**Título:** Despliegue preventivo de servicios web en contenedores docker basado en SecDevOps **Autores:** Azuaga Orrego, Hurson Daniel **Año:** 2021	Investigación bibliográfica.	Revisión de literatura. Explorar documentos técnicos y guías de buenas prácticas.	Se ha identificado una solución altamente compatible y funcional que se adapta a las necesidades específicas de la organización.	Motor de búsqueda en línea. Revisiones sistemáticas y meta análisis.
Propuesta de la estrategia de seguridad en DevOps	**Título:** SecDevOps: Is It a Marketing Buzzword? - Mapping Research	Investigación Descriptiva.	Fuentes bibliográficas. Revisión de casos de estudio y proyectos prácticos.	La mejora significativa en la seguridad y calidad del ciclo de entrega de software de la empresa.	Observación. Análisis de contenido. Tests y escalas de medición.

	on Security in DevOps. **Autores:** Vaishnavi Mohan, Lotfi Ben Othmane **Año:** 2016				
Implementación de la estrategia de seguridad	**Título:** OpenSource tools for a secdevops pipeline. **Autores:** Pegueroles Valles, Josep Rafael **Año:** 2022	Investigación bibliográfica.	Interacción con profesionales y expertos. Revisión de casos de estudio y proyectos prácticos.	El diseño detallado del proceso de seguridad propuesto, el cual se llevará a cabo con la ayuda de las herramientas KBDoctor y Splunk. La selección de estas herramientas se fundamenta en su capacidad para integrarse fácilmente y su relativa simplicidad de implementación.	Motor de búsqueda en línea.
Validación y verificación de	Sustentado por especialistas de la empresa Aval Buró	Observación directa.	Interacción con profesionales y expertos.	Se revisó minuciosamente el alcance y la idoneidad de las herramientas	Fotografías o imágenes. Checklists o listas de verificación.

la estrategia de seguridad				propuestas para su implementación en el entorno empresarial, asegurando su compatibilidad con las necesidades y requisitos específicos de seguridad de la organización.	

Fuente: Elaboración propia (2024)

CONCLUSIONES

SecDevOps se basa en varios conceptos y principios fundamentales que guían su implementación y práctica efectiva como por ejemplo: Integración de seguridad desde el inicio, Automatización, Colaboración y responsabilidad compartida, Transparencia y visibilidad, entre otros. Estos conceptos y principios fundamentales proporcionan una base sólida para la implementación exitosa de SecDevOps y la mejora continua de la seguridad y la calidad del software en las organizaciones.

El hecho de que se haya identificado falencias de seguridad en los procesos de integración continua dentro de la organización Aval Buró indica la existencia de riesgos significativos para la seguridad de los sistemas y datos de la empresa. Estas vulnerabilidades pueden exponer a la organización a una serie de amenazas, como brechas de seguridad, pérdida de datos confidenciales, interrupción del servicio y daño a la reputación. Diseñar un plan estratégico para mitigar estas vulnerabilidades es fundamental para proteger los activos de la organización y garantizar la continuidad del negocio.

La implementación de una estrategia de seguridad es fundamental para proteger los activos y la integridad de una organización contra amenazas cibernéticas y riesgos de seguridad. El hecho de haber diseñado una estrategia de seguridad con el apoyo de dos herramientas de código abierto altamente rígidas es una medida proactiva y significativa que puede proporcionar una sólida defensa contra posibles vulnerabilidades y amenazas.

Tras llevar a cabo un proceso de validación por parte de expertos, se identificaron posibles mejoras que podrían ser implementadas en la propuesta inicial. No obstante, es importante destacar que la propuesta recibió la aprobación de ambos profesionales del área, lo cual representa un aspecto favorable para el proyecto en cuestión.

RECOMENDACIONES

Para lograr una implementación efectiva de SecDevOps y promover la mejora continua de la seguridad y la calidad del software en las organizaciones, es fundamental que los equipos adopten y apliquen de manera proactiva los conceptos y principios fundamentales que guían este enfoque.

Es importante fomenta una cultura de seguridad en toda la organización, donde los equipos de desarrollo, operaciones y seguridad trabajen juntos hacia objetivos comunes. La colaboración y la comunicación abierta son clave para el éxito de SecDevOps.

Automatizar procesos de seguridad es importante ya que en todas las áreas de SecDevOps, incluyendo pruebas de seguridad, análisis estático y dinámico de código, verificación de configuraciones, y despliegue de parches de seguridad. La automatización ayuda a mejorar la eficiencia y la consistencia, y reduce el riesgo de errores humanos.

La implementación de una estrategia de seguridad es esencial para salvaguardar los activos y la integridad de una organización frente a las crecientes amenazas cibernéticas y riesgos de seguridad. El diseño de una estrategia respaldada por dos herramientas de código abierto altamente robustas representa una medida proactiva y significativa. Esta elección puede brindar una defensa sólida contra posibles vulnerabilidades y amenazas. Es crucial que la organización continúe evaluando y actualizando regularmente su estrategia de seguridad para adaptarse a los cambios en el panorama de amenazas y garantizar una protección efectiva a largo plazo.

A raíz del proceso de validación llevado a cabo por expertos, se han identificado áreas de mejora que podrían fortalecer la propuesta inicial. No obstante, es fundamental resaltar que la aprobación de la propuesta por parte de ambos profesionales del área subraya su viabilidad y relevancia para el proyecto. Esto indica un respaldo significativo que consolida la solidez y la credibilidad de la propuesta en cuestión. Es crucial considerar las sugerencias de mejora identificadas durante la validación de expertos para enriquecer aún más el proyecto y garantizar su éxito a largo plazo.

BIBLIOGRAFÍA

Abril Ferreres, R. (2021). Using of SecDevOps in web applications (Bachelor's thesis, Universitat Politècnica de Catalunya).

Canyelles Toledano, M. (2022). OpenSource tools for a secdevops pipeline (Master's thesis, Universitat Politècnica de Catalunya).

Casola, V., De Benedictis, A., Rak, M., & Salzillo, G. (2020). A cloud SecDevOps methodology: from design to testing. In Quality of Information and Communications Technology: 13th International Conference, QUATIC 2020, Faro, Portugal, September 9–11, 2020, Proceedings 13 (pp. 317-331). Springer International Publishing.

CUEVA QUINTANA, J. B. (2022). PROPUESTA DE UN MODELO DE SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD EDUCATIVA FRAY JODOCO RICKE BAJO LA NORMA ISO 27001 (Master's thesis, Quito: UISRAEL).

Diakun, J., Johnson, P. R., & Mock, D. (2016). Splunk Operational Intelligence Cookbook. Packt Publishing Ltd.

Gavidia Córdova, J. V. (2022). Modelo de seguridad informática en el control de accesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NIST (Master's thesis, Quito: UISRAEL).

Haber, M. J., & Haber, M. J. (2020). Secured DevOps (SecDevOps). Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations, 251-255.

Hernández-Alonso, J. J. (2022). Implementación de la cultura DevOps en la empresa (Master's thesis).

Izurieta, C., & Prouty, M. (2019, May). Leveraging secdevops to tackle the technical debt associated with cybersecurity attack tactics. In 2019 IEEE/ACM International Conference on Technical Debt (TechDebt) (pp. 33-37). IEEE.

Liu, M., Wang, Y., Sun, J., & Ji, Z. (2022). Adaptive low-rank kernel block diagonal representation subspace clustering. Applied Intelligence, 52(2), 2301-2316.

López Rodríguez, M. (2020). SecDevOps: Análisis de contenedores Docker e integración de herramientas SAST y DAST.

Mohan, V., & Othmane, L. B. (2020, August). Secdevops: Is it a marketing buzzword?-mapping research on security in devops. In 2016 11th international conference on availability, reliability and security (ARES) (pp. 542-547). IEEE.

Orrego, A., & Daniel, H. (2021). Despliegue preventivo de servicios web en contenedores docker basado en SecDevOps.

Ortega Rendón, S. P. (2022). ANÁLISIS DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON HERRAMIENTAS OPEN SOURCE (Master's thesis, Quito: UISRAEL).

Pérez Vega, F. J. (2023). INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN PYMES (Master's thesis, Quito, Ecuador: Editorial UISRAEL).

Sarango Narváez, D. F. (2023). PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL (Master's thesis, Quito, Ecuador: Editorial UISRAEL).

Sigman, B. P., & Delgado, E. (2016). Splunk Essentials. Packt Publishing Ltd.

Silva Llaguno, E. L. (2022). Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS (Master's thesis, Quito: UISRAEL).

Stearley, J., Corwell, S., & Lord, K. (2010). Bridging the gaps: Joining information sources with splunk. In Workshop on Managing Systems via Log Analysis and Machine Learning Techniques (SLAML 10).

Subramanian, K., & Subramanian, K. (2020). Introducing the Splunk Platform. Practical Splunk Search Processing Language: A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome, 1-38.

Vehent, J. (2018). Securing DevOps: security in the cloud. Simon and Schuster.

ANEXOS

A continuación se presentan los anexos recopilados.

ANEXO 1

VALIDACION DE EXPERTO OSVALDO GONZALES

Validado por: Osvaldo Gonzalez

Título obtenido
Ing. Sistemas/Mst Telemáticas
Cédula de Identidad
1750671669
E- mail
osvaldo.gonzalez@avalburo.com
Institución de Trabajo
Aval Buró
Cargo
Jefe de infraestructura
Años de experiencia en el área
24

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	El alcance que tendrá la propuesta y su representatividad en la generación de valor		X			
Aplicabilidad	La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables	X				
Conceptualización	La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada		X			
Actualidad	Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta	X				
Calidad Técnica	Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios		X			
Factibilidad	El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles		X			
Pertinencia	La contundencia y conveniencia de la propuesta para solucionar el problema planteado.		X			
Total		2	5	0	0	0

Observaciones: Me parece una buena idea aplicar la herramienta Splunk ya que es muy poderosa y versátil que proporciona capacidades avanzadas de búsqueda, monitoreo y análisis, lo que la convierte en una opción para la empresa.

Recomendaciones

Como recomendación puedo decir que sería bueno aplicar esta herramienta para todos los procesos que se tienen actualmente y no solo para aquellos procesos de automatización ya que se tienen vulnerabilidades de otros tipos lo cual con el conocimiento que tengo de la herramienta considero que si podría detectar.

Lugar, fecha de validación: Quito, 8 de marzo de 2024

ANEXO 2

VALIDACION DE EXPERTO HEYDI CRUZ

Validado por: Heydi Karelis Cruz Pantoja

Título obtenido
MsC. Ciberseguridad
Cédula de Identidad
1718658873
E- mail
headykarelis@hotmail.com
Institución de Trabajo
Aval Buró
Cargo
Analista de Seguridad Informática
Años de experiencia en el área
Tres años de experiencia

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	El alcance que tendrá la propuesta y su representatividad en la generación de valor		X			
Aplicabilidad	La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables	X				
Conceptualización	La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada		X			
Actualidad	Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta	X				
Calidad Técnica	Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios		X			
Factibilidad	El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles	X				
Pertinencia	La contundencia y conveniencia de la propuesta para solucionar el problema planteado.	X				
Total		*4*	*3*	*0*	*0*	*0*

Observaciones:

Aunque Splunk es una potente herramienta y ampliamente utilizada, también tiene algunas limitaciones y desafíos potenciales que vale la pena considerar.

Por ejemplo Splunk puede ser costoso a medida que se escalan las implementaciones y se agregan más funciones y capacidades. El modelo de licenciamiento basado en datos puede resultar prohibitivo para algunas organizaciones, especialmente para aquellas con grandes volúmenes de datos. Además, la curva de aprendizaje de Splunk puede ser empinada para usuarios nuevos ya que requiere tiempo y esfuerzo para comprender completamente todas las funcionalidades y capacidades de la plataforma. También es importante mencionar que para aprovechar al máximo Splunk, es posible que se requieran recursos significativos como servidores potentes y almacenamiento de datos escalable. Esto puede aumentar los costos operativos y la complejidad de la infraestructura.

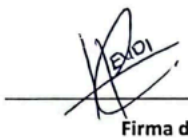
A pesar de estas observaciones, Splunk sigue siendo una herramienta muy valiosa, pero es importante considerar estos aspectos al evaluar su idoneidad para un entorno particular y lo que se requiere implementar.

Recomendaciones

En lo personal recomendaría la herramienta SonarQube ya que proporciona análisis estático de código, incluye complementos y reglas específicas para detectar vulnerabilidades en el código. Puede identificar problemas de seguridad, como vulnerabilidades de inyección de SQL, XSS (Cross-Site Scripting), y otras vulnerabilidades comunes.

Esta herramienta puede ser utilizada de manera complementaria para obtener una evaluación completa de la seguridad de una aplicación y ayudar a identificar y mitigar posibles riesgos de seguridad. Es importante recordar que ninguna herramienta puede identificar todas las vulnerabilidades potenciales, por lo que es recomendable utilizar una combinación de herramientas y realizar pruebas de seguridad periódicas durante el ciclo de vida del desarrollo del software.

Lugar, fecha de validación: Quito, 8/3/2024



Firma del especialista

ANEXO 3

Plan de seguridad

Tabla 2.

Plan de seguridad

FASE	ACTIVIDADES	RESPONSABLE	KPI	POLÍTICAS	ESTIMACIÓN
Evaluación de Riesgos y Amenazas	Realizar análisis de amenazas, modelado de ataques y evaluación de riesgos.	Equipo de seguridad, equipo de desarrollo.	Número de vulnerabilidades identificadas, nivel de riesgo evaluado.	Implementar un proceso formal de evaluación de riesgos.	Dos semanas
Implementación de Controles de Acceso	Configurar y administrar controles de acceso adecuados para limitar el acceso a recursos críticos.	Equipo de seguridad, administradores de sistemas.	Cumplimiento de políticas de control de acceso, tiempo de respuesta a solicitudes de acceso.	Establecer políticas de control de acceso basadas en el principio de privilegios mínimos necesarios.	Una semana
Pruebas de Seguridad Automatizadas	Implementar herramientas de escaneo de vulnerabilidades y análisis estático de código en pipelines de integración continua.	Equipo de seguridad, equipo de desarrollo.	Cobertura de pruebas de seguridad, número de vulnerabilidades detectadas y corregidas.	Integrar pruebas de seguridad automatizadas en pipelines de CI/CD.	Tres semanas
Gestión de Vulnerabilidades	Realizar análisis de vulnerabilidades, asignar y seguir el estado de las tareas de remediación.	Equipo de seguridad, equipo de desarrollo.	Tiempo de respuesta a las vulnerabilidades, tasa de remediación de vulnerabilidades.	Implementar un proceso de gestión de vulnerabilidades para identificar, priorizar y remediar las vulnerabilidades.	Una semana
Seguridad del Código	Realizar revisiones de código, implementar buenas prácticas de codificación segura.	Equipo de seguridad, equipo de desarrollo.	Número de problemas de seguridad resueltos en el código fuente.	Realizar análisis estático y dinámico del código para identificar y corregir vulnerabilidades.	Una semana

Monitorización Continua de Seguridad	Implementar sistemas de detección de intrusiones, monitorear registros de actividad y eventos de seguridad.	Equipo de seguridad, administradores de sistemas.	Tiempo de detección y tiempo de respuesta a incidentes de seguridad.	Configurar sistemas de monitorización continua de seguridad.	Siempre
Educación y Concientización en Seguridad	Realizar sesiones de formación en seguridad, distribuir materiales educativos sobre buenas prácticas de seguridad.	Equipo de seguridad, líderes de equipo.	Nivel de conocimiento y comprensión de los empleados sobre las políticas de seguridad.	Proporcionar capacitación y concientización en seguridad.	Una semana
Revisión y Mejora Continua	Realizar auditorías de seguridad, identificar áreas de mejora y adaptarse a cambios en las amenazas y tecnologías emergentes.	Equipo de seguridad, equipo de desarrollo.	Número de mejoras implementadas, efectividad del plan de seguridad.	Realizar revisiones periódicas del plan de seguridad en SecDevOps.	Siempre